

SIEVE METHODS LECTURE NOTES, SPRING 2020

KEVIN FORD

1. BASIC SIEVE METHODS AND APPLICATIONS

A *sieve* is a technique for bounding the size of a set after the elements with “undesirable properties” (usually of a number theoretic nature) have been removed. The undesirable properties could be divisibility by a prime from a given set, other multiplicative constraints (divisibility by a perfect square for example) or inclusion in a set of residue classes. Inclusion-exclusion yields an exact formula, however for k properties this produces 2^k summands which is usually too much to effectively deal with. A *sieve* is a procedure to estimate the number of “desirable” elements of the set using $k^{O(1)}$ summands. While inexact, oftentimes the sieve is capable of estimating the size very accurately.

The original sieve is, of course, the *Sieve of Eratosthenes*, the familiar process of creating a table of prime numbers by systematically removing those integers divisible by small primes (but keeping the primes themselves). The modern sieve was created by Viggo Brun in the period 1915-1922 as a way of attacking famous unsolved problems such as Golbach’s Conjecture and the Twin Prime problem (both, so far, unsuccessfully). Sieve methods have since found enormous application in number theory, often used as tools in many other types of problems, e.g. in studying Diophantine equations.

1.1. Notational conventions. $\tau(n)$ is the number of positive divisors of n

$\omega(n)$ is the number of distinct prime factors of n

$\Omega(n)$ is the number of prime factors of n counted with multiplicity

$\mu(n)$ is the Möbius’s function; $\mu(n) = (-1)^{\omega(n)}$ if n is squarefree and $\mu(n) = 0$ otherwise.

$P^+(n)$ is the largest prime factor of n ; $P^+(1) = 0$ by convention

$P^-(n)$ is the smallest prime factor of n ; $P^-(1) = \infty$ by convention

$\mathcal{P}(z)$ is the set of positive squarefree integers composed only of primes $\leq z$

$\Lambda(n)$ denotes the von Mangoldt function

$\mathbb{1}_X$ is the indicator function of the statement X or of the set X

the symbol p , with or without subscripts, always denotes a prime

$\pi(x; q, a)$ is the number of primes $p \leq x$ in the progression $a \pmod q$.

\mathbb{P} denotes probability and \mathbb{E} expectation

$\log_k x$ is the k -th iterate of the logarithm of x

1.2. General sieve setup. A *sieve problem* \mathcal{A} is a probability space $(\Omega, \mathcal{F}, \mathbb{P})$, together with a “total mass” quantity M and events \mathcal{A}_p , one for each prime p . The “sifting function” is

$$S(\mathcal{A}, z) = M \cdot \mathbb{P}(\text{not } \mathcal{A}_p, \forall p \leq z).$$

Oftentimes Ω will be a finite set of integers, with $\mathbb{P}(n \in \Omega) = 1/|\Omega|$ for each $n \in \Omega$ (the uniform probability measure), $M = |\Omega|$ and \mathcal{A}_p is the event that $p|n$, that is, $\mathcal{A}_p = \{n \in \Omega : p|n\}$. This is the standard “small

sieve” problem, where $S(\mathcal{A}, z)$ is the number of $n \in \Omega$ with $p \nmid n$ for all $p \leq z$; these are called the “unsifted numbers”. In the above definitions, M can be anything, but in practice it has some arithmetical meaning.

Some specific examples:

- **Eratosthenes sieve for primes.** $\Omega = [1, x] \cap \mathbb{N}$, uniform probabilities on Ω , $M = |\Omega| = [x]$, and $\mathcal{A}_p = \{n \in \Omega : p \nmid n\}$. Then $S(\mathcal{A}, \sqrt{x}) = \pi(x) - \pi(\sqrt{x}) + 1$, as the unsifted elements are the primes in $(\sqrt{x}, x]$ together with the number 1.
- **Twin primes.** $\Omega = [1, x] \cap \mathbb{N}$, $\mathcal{A}_p = \{n \in \Omega : p \nmid n(n+2)\}$. The unsifted numbers are numbers n such that $n(n+2)$ has no prime factor $\leq z$. In particular, $S(\mathcal{A}, \sqrt{x+2})$ counts $k \in (\sqrt{x+2}, x]$ for which *both* k and $k+2$ are prime.

Equivalently, \mathcal{A}_p is the set of n that avoid the residue classes $0 \pmod p$ and $-2 \pmod p$.

- **Twin primes, weighted version.** $\Omega = [2, x] \cap \mathbb{N}$, and

$$\mathbb{P}(n \in \Omega) = \frac{\Lambda(n+2)}{M}, \quad M = \sum_{2 \leq n \leq x} \Lambda(n+2),$$

$\mathcal{A}_p = \{n \in \Omega : p \nmid n\}$. Here $M = \sum_{2 \leq n \leq x} \Lambda(n+2) \sim x$ by the Prime Number Theorem, and

$$\begin{aligned} S(\mathcal{A}, \sqrt{x}) &= \sum_{\substack{2 \leq n \leq x \\ P^-(n) > \sqrt{x}}} \Lambda(n+2) = \sum_{\sqrt{x} < p \leq x} \Lambda(p+2) \\ &= \sum_{\substack{\sqrt{x} < p \leq x \\ p+2 \text{ prime}}} \log(p+2) + O(x^{1/2}), \end{aligned}$$

the error term coming from terms $p+2 = q^b$ where q is prime and $b \geq 2$.

- **Prime tuples.** Let $a_1, \dots, a_k \in \mathbb{N}$ and $b_1, \dots, b_k \in \mathbb{Z}$. Put $\Omega = [1, x] \cap \mathbb{N}$, and¹

$$\mathcal{A}_p = \{n \in \Omega : p \nmid (a_1 n + b_1) \cdots (a_k n + b_k)\}.$$

For an appropriate $c > 0$, which depends on $a_1, a_2, \dots, a_k, b_k$, $S(\mathcal{A}, c\sqrt{x})$ counts those $n \leq x$ for which $a_1 n + b_1, \dots, a_k n + b_k$ are simultaneously prime.

- **Prime values of a polynomial.** Let $f : \mathbb{Z} \rightarrow \mathbb{Z}$ be an irreducible polynomial of degree $h \geq 1$, put $\Omega = [1, x] \cap \mathbb{Z}$, $\mathcal{A}_p = \{n \in \Omega : p \nmid f(n)\}$. Let C be large enough so that $|h(n)| \leq Cn^h$ for all $n \geq 1$. Then, as before, $S(\mathcal{A}, \sqrt{Cx^h})$ captures values of n for which $f(n)$ is prime.
- **Goldbach’s problem.** Let N be an even, positive integer, put $\Omega = \{1, 2, \dots, N-1\}$, $M = |\Omega| = N-1$, and $\mathcal{A}_p = \{k \in \Omega : p \nmid k(N-k)\}$. Then $S(\mathcal{A}, \sqrt{N})$ counts numbers $k \in (\sqrt{N}, N]$ for which both k and $N-k$ are prime. In particular, $S(\mathcal{A}, \sqrt{N}) > 0$ implies that N is the sum of two primes. If one shows this for all $N \geq 4$, one deduces Goldbach’s Conjecture.
- **Primes in an arithmetic progression.** Fix coprime positive integers a and q , let

$$\Omega = \{1 \leq n \leq x : n \equiv a \pmod q\},$$

$\mathcal{A}_p = \{n \in \Omega : p \nmid n\}$. Then $S(\mathcal{A}, \sqrt{x})$ captures primes in $(\sqrt{x}, x]$ that are in the arithmetic progression $a \pmod q$.

¹Unless otherwise specified, from now on whenever Ω is a finite set, the probability measure on Ω will be the uniform measure, and M will be the number of elements of Ω .

- **Sums of two squares.** $\Omega = [1, x] \cap \mathbb{Z}$,

$$\mathcal{A}_p = \begin{cases} \{n \in \Omega : p^e \parallel n \text{ for some odd } e\} & p \equiv 3 \pmod{4} \\ \emptyset & \text{otherwise.} \end{cases}$$

Then $S(\mathcal{A}, x)$ counts integers $n \leq x$, for which we don't have $p^e \parallel n$ for any prime $p \equiv 3 \pmod{4}$ and odd exponent e . That is, $S(\mathcal{A}, x)$ is the number of integers $n \leq x$ which are the sum of two squares.

- **Sieve by multiple residue classes.** Let M, N be two integers, $\Omega = \{N + 1, M + 2, \dots, N + M\}$ and for each prime p let \mathcal{I}_p be some subset (possibly empty) of the residue classes modulo p . Put

$$\mathcal{A}_p = \{n \in \Omega : n \pmod{p} \notin \mathcal{I}_p\}.$$

Here $S(\mathcal{A}, z)$ counts the integers in $(N, M + N]$ avoiding all the residue classes \mathcal{I}_p for primes $p \leq z$. If $|\mathcal{I}_p|$ is bounded or bounded on average, then this is a very general sieving problem of "small sieve" type, whereas if $|\mathcal{I}_p|$ is unbounded on average, the problem falls under the umbrella of the "large sieve". The case of prime values of a polynomial, see above, is a special case with

$$\mathcal{I}_p = \{n \in \mathbb{Z}/p\mathbb{Z} : f(n) \equiv 0 \pmod{p}\}.$$

- **Multivariate polynomial sieve.** Let $F(\mathbf{x}) : \mathbb{Z}^k \rightarrow \mathbb{Z}^k$ be a multivariate polynomial of $\mathbf{x} = (x_1, \dots, x_k)$, take any finite $\Omega \in \mathbb{Z}^k$, and $\mathcal{A}_p = \{\mathbf{x} \in \Omega : p \mid F(\mathbf{x})\}$. Then $S(\mathcal{A}, z)$ counts $\mathbf{x} \in \Omega$ for which $F(\mathbf{x})$ has no prime factor $p \leq z$.
- **The square-free sieve.** Let Ω be a finite set of integers and for each prime p let $\mathcal{A}_p = \{n \in \Omega : p^2 \nmid n\}$. Then $S(\mathcal{A}, z)$, with an appropriately large z , will count the elements of Ω which are squarefree. A famous application is for squarefree values of a polynomial, e.g. $\Omega = \{f(n) : 1 \leq n \leq x\}$, where f is an irreducible polynomial.

One can similarly set up a k -free sieve problem.

- **Elliptic curve sieve.** Fix an elliptic curve E over \mathbb{Q} . Let Ω be the set of primes $q \leq x$. Let $\mathcal{A}_p = \{q \in \Omega : p \nmid \#E/\mathbb{F}_q\}$, where E/\mathbb{F}_q is the reduction of E modulo q . It is known that $\#E/\mathbb{F}_q \leq q + 1 + 2\sqrt{q}$, and thus $S(\mathcal{A}, 2\sqrt{x})$ counts those q for which $\#E/\mathbb{F}_q$ is prime.

If d is a square-free integer composed only of primes in \mathcal{P} , define

$$(1.1) \quad \mathcal{A}_d = \bigcap_{p|d} \mathcal{A}_p, \quad A_d = M \cdot \mathbb{P}(\mathcal{A}_d).$$

In particular, $A_1 = M$. In the case where Ω is a finite set of integers with uniform measure, $M = |\Omega|$, and $\mathcal{A}_p = \{n \in \Omega : p \nmid n\}$, A_d counts the number of $n \in \Omega$ divisible by d .

In this notation, inclusion-exclusion gives

$$(1.2) \quad S(\mathcal{A}, z) = \sum_{P^+(d) \leq z} \mu(d) A_d.$$

1.3. Legendre's sieve for primes (Legendre, 1808). Let $\Omega = [1, x] \cap \mathbb{Z}$, $\mathcal{A}_p = \{n \in \Omega : p \nmid n\}$. Then $S(\mathcal{A}, z)$ counts the positive integers $n \leq x$ with no prime factor $\leq z$; in particular, this includes all of the primes between z and x . Also, for each squarefree d , $\mathcal{A}_d = \{n \in \Omega : d \nmid n\}$ and thus

$$A_d = |\mathcal{A}_d| = \lfloor x/d \rfloor = x/d + O(1).$$

By (1.2),

$$\begin{aligned} \pi(x) - \pi(z) &\leq S(\mathcal{A}, z) = \sum_{P^+(d) \leq z} \mu(d) \left(\frac{x}{d} + O(1) \right) \\ &= x \sum_{P^+(d) \leq z} \frac{\mu(d)}{d} + O(\tau(P)) \\ &= x \prod_{p \leq z} \left(1 - \frac{1}{p} \right) + O\left(2^{\pi(z)}\right). \end{aligned}$$

Taking $z = \log x$, and using the crude bound $\pi(z) \leq z$ together with Mertens' bound, we conclude that

$$\pi(x) \leq z + \frac{x}{\log z} (e^{-\gamma} + o(1)) + O(2^{\log x}) = O\left(\frac{x}{\log_2 x}\right).$$

Remark: We can do better by observing that in fact $A_d = 0$ for $d > x$ (cf. Hooley [86]), and thus restricting the sums to such d .

1.4. The role of independence. If the events \mathcal{A}_p are independent, then the sieving problem is trivial, for then

$$(1.3) \quad S(\mathcal{A}, z) = M \prod_{p \leq z} (1 - \mathbb{P}\mathcal{A}_p).$$

In practice, the events are not independent, but are close to being so, especially for small primes. For example, in Legendre's sieve for primes, $A_d = \lfloor x/d \rfloor$ is very close to x/d . Even with this strong approximation, however, the accumulation of error terms (coming from k -correlations) becomes unwieldy when z is much larger than $\log x$.

1.5. Main goals. We will see that the right side of (1.3) is a good approximation to $S(\mathcal{A}, z)$ under very general conditions. We will accomplish this by a judicious pruning of the summands in (1.2).

To set things up, we adopt some additional notation. Take X to be an approximation of M (this can be anything, but in practice it is very close to M). We assume that there is a function g satisfying

$$(g) \quad 0 \leq g(p) < 1 \quad (\text{all primes } p),$$

which, when extended to a multiplicative function by $g(d) = \prod_{p|d} g(p)$, gives $A_d \approx Xg(d)$ for squarefree d ; that is, we require that the “remainders”

$$(r) \quad r_d := A_d - Xg(d)$$

to be “small on average”. In the case where the events \mathcal{A}_p are independent, taking $g(p) = \mathbb{P}\mathcal{A}_p$ yields $r_d = 0$ for all d and we recover (1.3). In practice, however, we will not take $g(p) = \mathbb{P}\mathcal{A}_p$ but something very close which is convenient for calculations. We also adopt the short-hand

$$(V) \quad V(z) = \prod_{p \leq z} (1 - g(p)).$$

In this notation, the right side of (1.3) is about $XV(z)$.

Broadly speaking, if r_d is not more than $1/X$ on average over “small” d , we will be able to prove the following:

$$(1.4) \quad \begin{aligned} & \text{(asymptotic)} && S(\mathcal{A}, z) \sim XV(z) && (z = X^{o(1)}); \\ & \text{(upper bound)} && S(\mathcal{A}, z) \ll XV(z) && (z \leq X); \\ & \text{(lower bound)} && S(\mathcal{A}, z) \gg XV(z) && (z \leq X^c), \end{aligned}$$

where the constant c depends on the nature of the sieve problem \mathcal{A} .

In plain language, we can prove the expected asymptotic formula for small z , an upper bound of the expected order for all z , and a lower bound of the expected order if z is at most a small power of X . The upper bound in (1.4) is amazing in its generality, and it has enormous utility as an auxiliary counting device in many problems.

1.6. Sifting density / dimension, and level of distribution. For most sieving problems, we have $g(p) \approx \kappa/p$ on average over p (we’ll make this precise below). In this case κ is referred to as the *sifting density* or *sifting dimension*. In the literature, the *linear sieve* refers to dimension 1. Various sieving procedures have been optimized for sieves of a particular density, e.g. the Rosser-Iwaniec theory of the linear sieve, and Iwaniec’s theory of the half-dimensional sieve.

Roughly speaking, the *level of distribution* of a sieve problem \mathcal{A} is the largest D for which

$$\sum_{d \leq D, P^+(d) \leq z} \mu^2(d) |r_d| \leq \varepsilon XV(z),$$

where $\varepsilon > 0$, X and z are given, and ε is small. The larger the level of distribution, the better quality of the bounds we can prove in (1.4).

1.7. More examples. There are limitations of the sieve, which are illustrated by the following examples.

1.7.1. Eratosthenes sieve. The asymptotic in (1.4) cannot be expected to hold for z being a fixed power of X . Take $\Omega = [1, x] \cap \mathbb{Z}$, $X = x$, and set $\mathcal{A}_p = \{n \in \Omega : p|n\}$. As before,

$$A_d = \#\{n \leq x : d|n\} = \lfloor x/d \rfloor = x/d + O(1)$$

Thus, taking $g(d) = 1/d$, we see that the error terms $r_d = O(1)$. Also,

$$S(\mathcal{A}, \sqrt{x}) = \pi(x) - \pi(\sqrt{x}) + 1 \sim \frac{x}{\log x}$$

by the Prime Number Theorem. However, Mertens’ theorem gives

$$XV(z) = x \prod_{p \leq \sqrt{x}} \left(1 - \frac{1}{p}\right) \sim \frac{2e^{-\gamma}x}{\log x},$$

with $2e^{-\gamma} = 1.122\dots$. The discrepancy between $S(\mathcal{A}, \sqrt{x})$ and $XV(z)$ comes from the large amount of dependence among the events \mathcal{A}_p for large primes p ; e.g. $\mathcal{A}_p \cap \mathcal{A}_{p'} \cap \mathcal{A}_{p''} = \emptyset$ if $p > p' > p'' > x^{1/3}$. In fact, for fixed $c > 0$, one has $S(\mathcal{A}, x^c) \sim w(c)XV(z)$, where $w(c) \neq 1$ for almost all $c \in (0, 1]$. Thus, in general the condition $z = X^{o(1)}$ is necessary in order to conclude the asymptotic in (1.4).

1.7.2. *Twin primes.* . Take $\Omega = [1, x] \cap \mathbb{Z}$, $X = x$, $\mathcal{A}_p = \{n \in \Omega : p|n(n+2)\}$. Here $S(\mathcal{A}, \sqrt{x+2})$ counts the number of twin prime pairs between $\sqrt{x+2}$ and x . Hardy and Littlewood [72, Conjecture B] conjectured that the count of such pairs is $\sim Cx/\log^2 x$ where

$$C = 2 \prod_{p>2} \left(1 - \frac{1}{(p-1)^2}\right) \approx 1.32.$$

For a heuristic explanation of this formula, see Section 1.10 below. By breaking up $[1, x]$ into subintervals of length d , we easily derive

$$A_d = \#\{n \leq x : d|n(n+2)\} = x \frac{\rho(d)}{d} + O(\rho(d)),$$

where

$$\rho(d) = \#\{0 \leq k \leq d-1 : k(k+2) \equiv 0 \pmod{d}\}.$$

By the Chinese remainder theorem, ρ is multiplicative, $\rho(2) = 1$ and $\rho(p) = 2$ for $p > 2$. Thus, this is a sieve problem of dimension 2 (or sifting density 2). Putting $g(d) = \rho(d)/d$ and applying Mertens, we get that

$$(1.5) \quad XV(z) = \frac{x}{2} \prod_{3 \leq p \leq z} \left(1 - \frac{2}{p}\right) \sim \frac{(4e^{-2\gamma})Cx}{\log^2 x}.$$

As in Example (a) above, $XV(z)$ differs by a constant multiplicative factor from what is expected to be true.

Sieve methods deliver an upper bound of the expected order (take $z = \sqrt{x}$)

$$\#\{n \leq x : n \text{ and } n+2 \text{ are both prime}\} \ll xV(z) \asymp \frac{x}{\log^2 x}.$$

Sieve methods only, however, deliver a lower bound for somewhat smaller z . For example, it is known that

$$S(\mathcal{A}, x^{1/5}) \gg XV(z) \asymp \frac{x}{\log^2 x}.$$

From the last estimate, we conclude that there are $\gg x/\log^2 x$ values of $k \leq x$ for which each of k and $k+2$ has at most 4 prime factors. We will prove a somewhat weaker version of this below (with 4 replaced by 10). This is a typical conclusion from a lower bound sieve. This is proved using the ‘‘linear variant’’ of the twin prime sieving problem. Here take $\Omega = \{p+2 : p \leq x\}$ a set of shifted primes, $\mathcal{A}_p = \{n \in \Omega : p|n\}$. In this set-up,

$$A_d = \pi(x; d, -2) \sim \frac{\text{li}(x)}{\phi(d)} \quad (2 \nmid d)$$

by the prime number theorem in arithmetic progressions. For the application to the sieve, we need a *uniform* estimate on $\pi(x; d, -2)$, at least on average over d . Here we take $X = \text{li}(x)$, and $g(p) = \frac{1}{p-1}$ for odd p . Since $g(p) \approx 1/p$, this is a sieve problem of dimension 1. Oftentimes, this process of ‘‘dimension lowering’’ yields stronger results, as the sieve procedures for smaller dimension are at present stronger.

1.7.3. *Prime k -tuples.* . Let $a_1, \dots, a_k \in \mathbb{N}$ and $b_1, \dots, b_k \in \mathbb{Z}$. Put $\Omega = [1, x] \cap \mathbb{N}$, and

$$\mathcal{A}_p = \{n \in \Omega : p|(a_1n + b_1) \cdots (a_kn + b_k)\}.$$

An easy counting yields

$$A_d = x \frac{\rho(d)}{d} + O(\rho(d)),$$

Admissible	Non-admissible
$(n, n + 2k); k \in \mathbb{N}$	$(n, n + 1)$
$(n, 2n + 1)$	$(n, 3n + 1)$
$(n, n + 2, n + 6)$	$(n, n + 2, n + 4)$

where

$$\rho(d) = \#\{0 \leq n < d : (a_1n + b_1) \cdots (a_kn + b_k) \equiv 0 \pmod{d}\}.$$

By the Chinese Remainder Theorem, $\rho(d)$ is multiplicative. We say that the collection of linear forms $a_1n + b_1, \dots, a_kn + b_k$ is *admissible* if $\rho(p) < p$ for all primes p . In the contrary case, for all n , one of the forms $a_jn + b_j$ is divisible by p and hence there are only finitely many n making all of the $a_jn + b_j$ simultaneously prime. Some examples:

We set $g(p) = \rho(p)/p$. Note that if

$$p \nmid \prod_{i=1}^k a_i \prod_{1 \leq i < j \leq k} (a_i b_j - a_j b_i),$$

then $\rho(p) = k$ (see Theorem 2.5 below). In particular, $\rho(p) = k$ for all sufficiently large p , and hence this is a sieve problem of density k (or dimension k). At present, sieve methods can deliver bounds of the form

$$\#\{n \leq x : a_jn + b_j \text{ are prime for all } j\} \leq C \frac{x}{(\log x)^k},$$

where C is an explicit function of $a_1, b_1, \dots, a_k, b_k$. If $k \geq 2$ we still do not know how to show that the left side goes to ∞ as $x \rightarrow \infty$.

1.7.4. *Selberg's examples.* [123]. The values of c for which sieve method deliver lower bounds (1.4) are invariably smaller than we would like. There is a fundamental barrier at work which explains this, known as the “parity barrier”. Roughly speaking, the small sieve works with inputs X , the function g and estimates for the remainders r_d . However, even if the level of distribution is very large, say $x^{1-o(1)}$, the sieve fundamentally cannot distinguish between numbers with an odd number of prime factors from those with an even number of prime factors. Consider two sequences defined as follows. Recall the Liouville function $\lambda(n) = (-1)^{\Omega(n)}$ (the completely multiplicative function which is -1 at all primes). Let $\mathcal{A}^+, \mathcal{A}^-$ be probability spaces on the sets

$$\Omega^+ = \{1 \leq n \leq x : \lambda(n) = 1\}, \quad \Omega^- = \{1 \leq n \leq x : \lambda(n) = -1\},$$

respectively, and $\mathcal{A}_p = \{n \in \Omega : p|n\}$ for each p .

The prime number theorem (with classical error term) implies

$$\sum_{n \leq x} \lambda(n) = O(xe^{-c'\sqrt{\log x}}), \text{ some } c' > 0.$$

Therefore,

$$\begin{aligned} \#\{n \in \Omega^\pm : d|n\} &= \sum_{m \leq x/d} \frac{1 \pm \lambda(dm)}{2} = \frac{1}{2} \left\lfloor \frac{x}{d} \right\rfloor \pm \frac{\lambda(d)}{2} \sum_{m \leq x/d} \lambda(m) \\ &= \frac{x}{2d} + O\left(\frac{x}{d} e^{-c\sqrt{\log(x/d)}}\right). \end{aligned}$$

In particular, taking $d = 1$, we see that $|\Omega^\pm| \sim \frac{x}{2}$. Take $X = \frac{x}{2}$ and $g(d) = \frac{1}{d}$ for all d . For both sequences, the level of distribution is $x^{1-o(1)}$ (pretty much the best range that one can hope for), and for both sieve problems we have

$$V(z) \sim \frac{2e^{-\gamma}}{\log x}.$$

However, numbers $n \leq x$ that have no prime factor $\leq \sqrt{x}$ are prime or 1, thus

$$S(\mathcal{A}^+, \sqrt{x}) = 1, \quad \text{while} \quad S(\mathcal{A}^-, \sqrt{x}) \sim \frac{x}{\log x} = \frac{2X}{\log x}.$$

Thus, although the sieve inputs (quantity X and bounds on A_d) are identical in both problems, the truth is very different. In order to distinguish primes from integers with 2 prime factors, say, further inputs into the sieve are required. Sieve procedures which include as hypotheses bilinear sum bounds for Ω have proven to be very successful in detecting primes, e.g. Friedlander-Iwaniec [56] and Harman [76].

1.8. The small sieve. Viggo Brun's fundamental idea was to replace the huge sum on the right side of (1.2) with a sum over a much smaller range of d , at the expense of replacing the equality in (1.2) with an inequality. In general, a *sieve* (or *small sieve*) is a sequence $\lambda = (\lambda_d)$ supported on squarefree integers d which replaces $\mu(d)$ in (1.2). We will suppose that either $\lambda = \lambda^+ = (\lambda_d^+)$ satisfies

$$(\lambda^+) \quad \lambda_1^+ = 1, \quad \sum_{d|m} \lambda_d^+ \geq 0 \quad (m > 1)$$

or that $\lambda = \lambda^- = (\lambda_d^-)$ satisfies

$$(\lambda^-) \quad \lambda_1^- = 1, \quad \sum_{d|m} \lambda_d^- \leq 0 \quad (m > 1).$$

We call λ^+ an *upper bound sieve* and λ^- a *lower bound sieve*, which comes from the following easy result:

Lemma 1.1. *For $z \geq 2$ let $\mathcal{P}(z)$ denote the set of squarefree positive integers, divisible only by primes $p \leq z$. Assume (λ^+) and (λ^-) . Then, for any sieve problem and $z \geq 2$,*

$$(1.6) \quad \sum_{d \in \mathcal{P}(z)} \lambda_d^- A_d \leq S(\mathcal{A}, z) \leq \sum_{d \in \mathcal{P}(z)} \lambda_d^+ A_d.$$

Further, for any multiplicative function g such that $0 \leq g(p) < 1$ for each $p \leq z$, we have

$$(1.7) \quad \sum_{d \in \mathcal{P}(z)} \lambda_d^- g(d) \leq \prod_{p \leq z} (1 - g(p)) \leq \sum_{d \in \mathcal{P}(z)} \lambda_d^+ g(d).$$

Proof. For any $\omega \in \Omega$, let

$$m_\omega = \prod_{\substack{p \leq z \\ \omega \in \mathcal{A}_p}} p.$$

Then, by (λ^+) ,

$$\begin{aligned} S(\mathcal{A}, z) &= MP(m_\omega = 1) = M \cdot \mathbb{E} \mathbb{1}_{m_\omega = 1} \\ &\leq M \cdot \mathbb{E} \sum_{d|m_\omega} \lambda_d^+ = \sum_{d \in \mathcal{P}(z)} \lambda_d^+ A_d, \end{aligned}$$

and similarly by (λ^-) ,

$$S(\mathcal{A}, z) \geq M \cdot \mathbb{E} \sum_{d|m_\omega} \lambda_d^- = \sum_{d \in \mathcal{P}(z)} \lambda_d^- A_d.$$

The claim (1.7) is a special case, where our probability space has independent events \mathcal{A}_p such that $\mathbb{P}\mathcal{A}_p = g(p)$, so that $S(\mathcal{A}, z) = M \prod_{p \leq z} (1 - g(p))$ and $A_d = Mg(d)$. \square

The major goal of sieve methods is to construct good sieve parameters λ^\pm , with *small support* and with the sums in (1.6) mimicking $S(\mathcal{A}, z)$ as closely as possible. With this notation and (r), we have

$$(1.8) \quad \sum_{d \in \mathcal{P}(z)} \lambda_d A_d = X \sum_{d \in \mathcal{P}(z)} g(d) \lambda_d + \sum_{d \in \mathcal{P}(z)} \lambda_d r_d.$$

As λ_d is a replacement for $\mu(d)$, it is reasonable to suppose (if we have constructed our sieve well) that

$$\sum_{d \in \mathcal{P}(z)} g(d) \lambda_d \approx \sum_{d \in \mathcal{P}(z)} g(d) \mu(d) = \prod_{p \leq z} (1 - g(p)) = V(z).$$

1.9. Legendre's sieve, general version.

Theorem 1.2. *Let \mathcal{A} be a sieve problem, assume (g), (r) and adopt notation (V). Then²*

$$(1.9) \quad S(\mathcal{A}, z) = XV(z) + O\left(\sum_{d \in \mathcal{P}(z)} |r_d|\right).$$

Proof. Trivially, the weights $\lambda_d^\pm = \mu(d)$ satisfy (λ^+) and (λ^-) with equality. By (1.6),

$$S(\mathcal{A}, z) = X \sum_{d \in \mathcal{P}(z)} \mu(d)g(d) + \sum_{d \in \mathcal{P}(z)} \mu(d)r_d = XV(z) + O\left(\sum_{d \in \mathcal{P}(z)} |r_d|\right). \quad \square$$

Although this sieve suffers from the large number, $2^{\pi(z)}$, of remainder summands, it is useful in situations where the “densities” $g(p)$ are rather small on average, and so the product on the right hand side of (1.9) captures the true behavior of set of interest for relatively small z . A prominent example of the use of Legendre's sieve was given by C. Hooley [82], who deduced Artin's primitive root conjecture from the Generalized Riemann Hypothesis for Dedekind zeta functions of certain number fields. Details will be given later in Section 2.2.6.

1.10. The prime k -tuples conjecture. Much of sieve theory has been driven by attempts to prove special cases of the general *Prime k -tuples Conjecture*. The setup is a finite collection f_1, \dots, f_k of nonconstant irreducible (over \mathbb{Q}) polynomials in m variables, with integer coefficients. For each prime p , let

$$\rho(p) = \#\{\mathbf{x} = (x_1, \dots, x_m) \pmod{p} : f_1(\mathbf{x}) \cdots f_k(\mathbf{x}) \equiv 0 \pmod{p}\}.$$

Definition 1. *The set (f_1, \dots, f_k) is admissible if the f_i are distinct and $\rho(p) < p^m$ for all p .*

Conjecture 1.3 (General Prime k -tuples Conjecture). *Let f_1, \dots, f_k be an admissible collection of polynomials from \mathbb{Z}^m to \mathbb{Z} . Then*

$$(1.10) \quad \#\{0 \leq x_i < x \ (1 \leq i \leq m) : f_1(\mathbf{x}), \dots, f_k(\mathbf{x}) \text{ are all prime}\} \sim \frac{\mathfrak{S}}{\prod_{i=1}^k \deg(f_i)} \frac{x^m}{(\log x)^k},$$

²Recall that r_d is supported on squarefree integers d . Thus, for any sum involving r_d , the sums is restricted to squarefree integers.

where $\deg(f_i)$ is the total degree of f_i , and

$$\mathfrak{S} = \mathfrak{S}(f_1, \dots, f_k) = \prod_p \left(1 - \frac{\rho(p)}{p^m}\right) \left(1 - \frac{1}{p}\right)^{-k}$$

is the so-called singular series associated with f_1, \dots, f_k .

One can show that $\rho(p)/p^{m-1}$ is k on average and this implies that the infinite product converges (details below in the case of univariate polynomials).

This conjecture subsumes a large number of conjectures that have been made over time, in various degrees of generality. We mention here the conjectures of Bunyakowsky [15], Dickson [27], Hardy-Littlewood [72], Schinzel [119], and Bateman-Horn [10].

Some special cases.

- **Primes in an arithmetic progression.** $m = 1, k = 1, f_1(n) = qn + a$, where $(a, q) = 1$. Dirichlet proved [28] in 1837 that there are infinitely many n with $f_1(n)$ prime; the Prime Number Theorem for arithmetic progressions (de la Valeé Poissin, 1896) gives the full asymptotic (1.10).
- **Twin primes.** $m = 1, k = 2, f_1(n) = n, f_2(n) = n + 2$. Here $\mathfrak{S} = C := 2 \prod_{p>2} (1 - \frac{1}{(p-1)^2}) = 1.32\dots$ is the “twin prime constant”.
- **“Sexy” primes.** $m = 1, k = 2, f_1(n) = n, f_2(n) = n + 6$. Here $\mathfrak{S} = 2C$ since $\rho(2) = \rho(3) = 1$ and $\rho(p) = 2$ for $p > 3$. That is, there are twice as many “sexy primes” as twin primes.
- **Sophie Germain primes.** $m = 1, k = 2, f_1(n) = n, f_2(n) = 2n + 1$.
- **Primes of form $n^2 + 1$.** $m = 1, k = 1, f_1(n) = n^2 + 1$.
- **k -term arithmetic progressions of primes.** $m = 2$, forms $n_1, n_1 + n_2, n_1 + 2n_2, \dots, n_1 + (k-1)n_2$. When $k = 3$, the asymptotic in Conjecture 1.3 was essentially proved by Vinogradov in 1937. Balog [5] extended this to include many other collections of forms with $m \geq 2$. Green and Tao [65] showed that there are infinitely many k -term arithmetic progressions of primes for any $k \geq 4$, and this was extended by Green and Tao and by Green, Tao and Ziegler [66, 67, 68, 69] in 2010–12 to prove the full asymptotic in (1.10). Their theory extends to many other collections of linear forms when $m \geq 2$.
- **Primes of the form $x^2 + y^2$.** $m = 2, k = 1, f_1(x, y) = x^2 + y^2$. Fermat showed that every prime $p \equiv 1 \pmod{4}$ is the sum of two squares.
- **Primes of the form $x^2 + y^4$.** $m = 2, k = 1, f_1(x, y) = x^2 + y^4$. The infinitude of such primes, and in fact the full asymptotic (1.10), is a celebrated theorem of Friedlander and Iwaniec [55] in 1998.

The only case of (1.10) which is known when $m = 1$ is the single linear f_1 case. In fact, other than the case $k = 1$ and f_1 linear, it is not known a single specific example of a set of forms for which there are infinitely many $n \in \mathbb{Z}$ making all of $f_i(n)$ simultaneously prime.

There is a relatively easy heuristic for (1.10). According to the Prime Number Theorem, a randomly chosen integer near x has a likelihood of about $\frac{1}{\log x}$ of being prime. Assuming that the $f_i(\mathbf{x})$ behave randomly, the likelihood of $f_i(\mathbf{x})$ being prime should be about $\frac{1}{\log f_i(\mathbf{x})} \sim \frac{1}{\deg(f_i) \log x}$ if each $x_i \in [1, x]$. This leads to the prediction that

$$\#\{0 \leq x_i < x \ (1 \leq i \leq m) : f_1(\mathbf{x}), \dots, f_k(\mathbf{x}) \text{ are all prime}\} \sim \frac{1}{\prod_{i=1}^k \deg(f_i)} \frac{x^m}{(\log x)^k}.$$

This matches (1.10) except for the singular series factor. Implicit in the “randomness” hypothesis is the assumption that for any prime p , the likelihood that each of $f_i(\mathbf{x})$ is coprime to p is about $(1 - 1/p)^k$. This

is not correct, however, and if \mathbf{x} is chosen randomly modulo p , then the likelihood that each of the $f_i(\mathbf{x})$ is coprime to p is exactly $1 - \rho(p)/p^m$. Thus, in our heuristic we should insert a correction factor

$$\left(1 - \frac{\rho(p)}{p^m}\right) \left(1 - \frac{1}{p}\right)^{-k}.$$

Doing this for all p produces a correction factor equal to $\mathfrak{S}(f_1, \dots, f_k)$, and leads to the more precise prediction (1.10).

1.11. Brun's pure sieve. Brun's sieve is based on a simple truncated version of inclusion-exclusion, due to Brun (1915).

Lemma 1.4 (Inclusion-exclusion). *Let u be a non-negative integer. Then, for any $k \in \mathbb{N}$,*

$$\mathbb{1}_{u=0} = \sum_{r=0}^{\infty} (-1)^r \binom{u}{r} = \sum_{r=0}^k (-1)^r \binom{u}{r} + (-1)^{k+1} \binom{u-1}{k},$$

where we set $\binom{-1}{j} = 0$ for all j .

Proof. We may assume that $u \geq 1$, as the statement is trivial when $u = 0$. The first equality is trivial from the binomial theorem. For the second, when $u \geq 1$ we have

$$\sum_{r=k+1}^{\infty} (-1)^r \binom{u}{r} = \sum_{r=k+1}^{\infty} (-1)^r \left[\binom{u-1}{r-1} + \binom{u-1}{r} \right] = (-1)^{k+1} \binom{u-1}{k}. \quad \square$$

Theorem 1.5 (Brun's pure sieve). *Let k be a nonnegative integer and define*

$$\lambda_d = \begin{cases} \mu(d) & \text{if } \omega(d) \leq k \\ 0 & \text{otherwise;} \end{cases}.$$

Then λ satisfies (λ^+) if k is even and (λ^-) if k is odd. Thus, if k_e is even and k_o is odd, then for any sieve problem \mathcal{A} and any $z \geq 2$ we have

$$(1.11) \quad \sum_{\substack{d \in \mathcal{P}(z) \\ \omega(d) \leq k_o}} \mu(d) A_d \leq S(\mathcal{A}, z) \leq \sum_{\substack{d \in \mathcal{P}(z) \\ \omega(d) \leq k_e}} \mu(d) A_d.$$

Proof. Let $k \geq 0$. Then, by Lemma 1.4,

$$\begin{aligned} \mathbb{1}_{m=1} = \mathbb{1}_{\omega(m)=0} &= \sum_{r=0}^k (-1)^r \binom{\omega(m)}{r} + (-1)^{k+1} W, & W &= \binom{\omega(m)-1}{k} \geq 0, \\ &= \sum_{r=0}^k (-1)^r \sum_{\substack{d|m \\ \omega(d)=r}} 1 + (-1)^{k+1} W \\ &= \sum_{\omega(d) \leq k} \mu(d) + (-1)^{k+1} W \\ &= \sum_d \lambda_d + (-1)^{k+1} W, \end{aligned}$$

from which follows (λ^+) if k is even and (λ^-) if k is odd. The final claim (1.11) follows from (1.6). \square

In probability theory, the inequalities in Theorem 1.5 were later rediscovered by Bonferroni, and are often referred to as the ‘‘Bonferroni inequalities’’.

Lemma 1.6. *Let $z \geq 2$ and $0 \leq f(p) \leq 1$ for each prime $p \leq z$. Let k be a non-negative integer. Extend f multiplicatively by defining $f(d) = \prod_{p|d} f(p)$ for any squarefree d with $d \in \mathcal{P}(z)$. Then*

$$\sum_{\substack{d \in \mathcal{P}(z) \\ \omega(d) \leq k}} \mu(d) f(d) = \prod_{p \leq z} (1 - f(p)) + (-1)^k W,$$

where

$$0 \leq W \leq \sum_{\substack{d \in \mathcal{P}(z) \\ \omega(d) = k+1}} f(d) \leq \frac{1}{(k+1)!} \left(\sum_{p \leq z} f(p) \right)^{k+1}.$$

Proof. By Theorem 1.5 and (1.7),

$$\prod_{p \leq z} (1 - f(p)) = \sum_{\omega(d) \leq k} \mu(d) f(d) + (-1)^{k+1} W, \quad 0 \leq W \leq \sum_{\omega(d) = k+1} f(d).$$

The final inequality for W comes from expanding the $(k+1)$ -fold sum (this is an old Erdős trick). \square

Theorem 1.7. *Let \mathcal{A} be a sieve problem, assume (g) and (r) . Then*

$$S(\mathcal{A}, z) = XV(z) + O(XV(z)^{3/2}) + O\left(\sum_{d \leq z^{4 \log(1/V(z))+1}} |r_d| \right).$$

where $V(z)$ is given by (V) .

Proof. Assume $V(z) > 0$ otherwise there is nothing to prove. Now apply Theorem 1.5 with $k = \left\lfloor 4 \log \frac{1}{V(z)} \right\rfloor$, followed by an application of Lemma 1.6. This gives

$$\begin{aligned} S(\mathcal{A}, z) &= \sum_{\substack{d \in \mathcal{P}(z) \\ \omega(d) \leq k}} \mu(d) A_d + O\left(\sum_{\substack{d \in \mathcal{P}(z) \\ \omega(d) = k+1}} A_d \right) \\ &= X \sum_{\substack{d \in \mathcal{P}(z) \\ \omega(d) \leq k}} \mu(d) g(d) + O\left(X \sum_{\substack{d \in \mathcal{P}(z) \\ \omega(d) = k+1}} g(d) \right) + R \\ &= XV(z) + O\left(X \frac{1}{(k+1)!} \left(\sum_{p \leq z} g(p) \right)^{k+1} \right) + R, \end{aligned}$$

where

$$|R| \leq \sum_{\substack{d \in \mathcal{P}(z) \\ \omega(d) \leq k+1}} |r_d|.$$

Lastly, by our definition of k ,

$$\begin{aligned}
 \frac{1}{(k+1)!} \left(\sum_{p \leq z} g(p) \right)^{k+1} &\leq \frac{1}{(k+1)!} \left(\sum_{p \leq z} -\log(1-g(p)) \right)^{k+1} \\
 &= \frac{1}{(k+1)!} \left(\log \frac{1}{V(z)} \right)^{k+1} \\
 &\leq \left(\frac{e \log \frac{1}{V(z)}}{k+1} \right)^{k+1} \\
 &\leq (e/4)^{k+1} \ll V(z)^{4 \log 4 - 4} \leq V(z)^{3/2}.
 \end{aligned}
 \tag{1.12}$$

This completes the proof. \square

Remarks. We have imposed virtually no hypotheses on the sieve problem \mathcal{A} in this theorem. In applications, one has typically $V(z) \asymp (\log X)^{-\kappa}$ for some fixed κ , and thus we have applied (1.11) with $k \approx 4\kappa \log_2 X$. Typically in the sum in identity (1.2) and the sums in Brun's inequalities (1.11), the summands corresponding to $d > X$ are negligible (or identically zero). Hardy and Ramanujan [74] in 1917 showed that most integers $d \leq X$ have about $\log_2 X$ prime factors, and thus it is natural to choose k somewhat larger than $\log_2 X$ in order to capture the bulk of the sum.

1.11.1. *Example: twin primes.* As before, let $\Omega = [1, x] \cap \mathbb{Z}$, $\mathcal{A}_p = \{k \in \Omega : p \mid k(k+2)\}$. Take

$$g(p) = \frac{\rho(p)}{p}, \quad \rho(2) = 1, \quad \rho(p) = 2 \quad (p > 2)$$

and then, for squarefree d we have

$$|r_d| \leq \rho(d) \leq \tau(d).$$

By Mertens' estimate (cf., (1.5)), $V(z) \sim c(\log z)^{-2}$ for some constant c . Take

$$z = x^{\frac{1}{16 \log_2 x}},$$

so that in the summation of the error terms r_d we have

$$z^{4 \log(1/V(z))+1} = z^{8 \log_2 z + O(1)} \ll x^{1/2+o(1)}.$$

Thus,

$$\sum_{\substack{d \in \mathcal{P}(z) \\ \omega(d) \leq 4 \log(1/V(z))+1}} |r_d| \leq \sum_{d \leq z^{4 \log(1/V(z))+1}} \tau(d) \ll x^{1/2+o(1)}.$$

By Theorem 1.5,

$$S(\mathcal{A}, z) \sim XV(z) \sim \frac{cx}{\log^2 z} \sim 256cx \left(\frac{\log_2 x}{\log x} \right)^2.$$

As $S(\mathcal{A}, z) \geq \#\{z < k \leq x : k, k+2 \text{ both prime}\}$, we see that

$$\#\{k \leq x : k, k+2 \text{ both prime}\} \ll x \left(\frac{\log_2 x}{\log x} \right)^2,$$

which misses the conjectured order by a factor $(\log_2 x)^2$. Applying partial summation gives an immediate corollary.

Corollary 1.8 (Brun [18], 1919). *We have*

$$\sum_{\substack{p:p,p+2 \\ \text{prime}}} \frac{1}{p} < \infty.$$

Remarks. Applying Theorem 1.5 to the sieve of Eratosthenes yields $\pi(x) \ll x \frac{\log_2 x}{\log x}$, missing the true order of $\pi(x)$ by a factor $\log_2 x$.

Brun later [19] gave a much more complicated version of his sieve, where the simple truncation (1.11) is replaced by sieves where one considers the summation over integers d with restricted prime factors of various sizes. A greatly simplified version of this idea was found by Hooley, and which will be the subject of the following section.

2. THE BRUN-HOOLEY SIEVE

In this section and the next, we present a variation of Brun's pure sieve due to C. Hooley [87], which is very simple, from a combinatorial viewpoint, and yet powerful enough to deliver quickly each of the desired sieve bounds in (1.4). Some general estimates using this method were given by Ford and Halberstam [51].

2.1. Upper bounds. The fundamental idea of the upper bound sieve is to partition the primes into sets $\mathcal{P}_1, \dots, \mathcal{P}_t$ and apply the Brun sieve bounds on each set \mathcal{P}_i separately. The partition may be finite or infinite, that is, we allow $t = \infty$.

Lemma 2.1. *Partition the primes as $\mathcal{P}_1 \cup \dots \cup \mathcal{P}_t$. For each i , let $\lambda^{(i)} = (\lambda_d^{(i)})_d$ be an upper bound sieve. For any squarefree d , let*

$$\lambda_d^+ = \prod_{i=1}^t \lambda_{d_i}^{(i)},$$

where d_1, \dots, d_t are defined uniquely by

$$(2.1) \quad d = d_1 \cdots d_t, \quad (\forall i, p|d_i \Rightarrow p \in \mathcal{P}_i).$$

Then λ^+ is an upper bound sieve, i.e., satisfies (λ^+) .

Proof. Clearly $\lambda^+ = 1$. Also, for any $m > 1$, m has a unique decomposition as $m = m_1 \cdots m_t$, where for each i , all of the prime factors of m_i are in \mathcal{P}_i . Then, by (λ^+) ,

$$\sum_{d|m} \lambda^+ = \prod_{i=1}^t \left(\sum_{d_i|m_i} \lambda_{d_i}^{(i)} \right) \geq 0,$$

as required. □

Taking each $\lambda_d^{(i)}$ to be an upper bound Brun sieve (from Theorem 1.5) with $k = k_i$ even, we arrive at

Lemma 2.2 (The Brun-Hooley upper bound sieve). *Let $\mathcal{P}_1 \cup \dots \cup \mathcal{P}_t$ be any partition of the primes, and let k_1, \dots, k_t be arbitrary non-negative even integers. Then the sequence λ given by*

$$(2.2) \quad \lambda_d^+ = \begin{cases} \mu(d) & \text{if } \omega(d_j) \leq k_j \quad (1 \leq j \leq t) \\ 0 & \text{otherwise} \end{cases}$$

is an upper bound sieve satisfying (λ^+) . Here d uniquely decomposes as in (2.1).

The number theoretic motivation for this comes from looking at the statistical distribution of prime factors of integers $\leq X$. Not only does a typical integer have about $\log_2 X$ prime factors, but the prime factors themselves are typically uniformly distributed on a \log_2 -scale; that is, there are about $\log_2 t$ prime factors $\leq t$, uniformly for $t \leq X$. With Lemma 2.2, we can restrict the number of large prime factors of the summands d while still retaining almost all significant summands.

Suppose that we have a sieve problem \mathcal{A} , $z \geq 2$ and assume (g) and (r) . Define

$$P_i = \prod_{\substack{p \in \mathcal{P}_i \\ p \leq z}} p \quad (1 \leq i \leq t)$$

From Lemma 2.2 and (1.6) we immediately get

$$\begin{aligned} S(\mathcal{A}, z) &\leq \sum_{\substack{d_1|P_1 \\ \omega(d_1)\leq k_1}} \cdots \sum_{\substack{d_t|P_t \\ \omega(d_t)\leq k_t}} \mu(d_1) \cdots \mu(d_t) A_{d_1 \cdots d_t} \\ &= XU_1 \cdots U_t + R, \end{aligned}$$

where

$$(2.3) \quad U_j = \sum_{\substack{d_j|P_j \\ \omega(d_j)\leq k_j}} \mu(d_j)g(d_j), \quad R = \sum_{\substack{d_1|P_1 \\ \omega(d_1)\leq k_1}} \cdots \sum_{\substack{d_t|P_t \\ \omega(d_t)\leq k_t}} \mu(d_1 \cdots d_t)r_{d_1 \cdots d_t}.$$

Define

$$(2.4) \quad V_j = \prod_{\substack{p \in \mathcal{P}_j \\ p \leq z}} (1 - g(p)), \quad L_j = \log \frac{1}{V_j}.$$

Notice that $V_1 \cdots V_t = V(z)$. Lemma 1.6 plus $g(p) \leq -\log(1 - g(p))$ implies

$$V_j \leq U_j \leq V_j + \frac{L_j^{k_j+1}}{(k_j+1)!} = V_j \left(1 + e^{L_j} \frac{L_j^{k_j+1}}{(k_j+1)!} \right) \leq V_j \exp \left\{ e^{L_j} \frac{L_j^{k_j+1}}{(k_j+1)!} \right\}.$$

The last inequality appears wasteful, but in practice the quantity in the exponential is small. When $k_j = 0$ we can omit the factor e^{L_j} since

$$U_j = 1 = V_j V_j^{-1} = V_j e^{L_j}.$$

This leads to small improvements in numerical constants. Multiplying these inequalities together for all j , we have

$$(2.5) \quad V(z) \leq U_1 \cdots U_t \leq e^E V(z),$$

where

$$(2.6) \quad E := \sum_{j=1}^t e^{L_j} \mathbb{1}_{k_j > 0} \frac{L_j^{k_j+1}}{(k_j+1)!}.$$

We conclude from (1.6) and (1.8) the following.

Theorem 2.3. *Let \mathcal{A} be a sieve problem and assume (g) , (r) and (V) . Partition the set of primes in $[1, z]$ into $\mathcal{P}_1 \cup \cdots \cup \mathcal{P}_t$, let $P_i = \prod_{p \in \mathcal{P}_i} p$ and let k_1, \dots, k_t be non-negative even integers. Then*

$$S(\mathcal{A}, z) \leq XV(z)e^E + R',$$

where E is given by (2.6) and

$$(2.7) \quad R' := \sum_{\substack{\omega((d, P_j)) \leq k_j \ (1 \leq j \leq t) \\ P^+(d) \leq z}} |r_d|.$$

In particular, defining λ_d^+ as in Lemma 2.2, we have

$$(2.8) \quad \sum_d \lambda_d^+ g(d) \leq e^E V(z).$$

To make further progress and produce an upper bound of general utility, we make a very mild assumption on the function g , which is satisfied in a large number of cases. It is sometimes called the Iwaniec condition. We assume that for some $\kappa \geq 0$ and $B > 0$ that

$$(\Omega) \quad \prod_{y \leq p \leq w} (1 - g(p))^{-1} \leq \left(\frac{\log w}{\log y} \right)^\kappa \exp \left(\frac{B}{\log y} \right) \quad (2 \leq y \leq w \leq z)$$

Roughly speaking, this states that $g(p) \lesssim \kappa/p$ on average over p . Although B, κ are not uniquely defined by (Ω) , the smallest admissible value of κ (with B remaining bounded) is sometimes referred to as the “dimension” or “sifting density”. It is easy to show (cf., Exercise 2.1 below), that condition (Ω) is implied by the condition

$$(\Omega_0) \quad g(p) \leq \min(\kappa/p, 1 - \delta),$$

with the same value of κ and $\delta > 0$ depending on κ and B . Although (Ω_0) is easy to verify, for many problems we have (Ω) holding with a smaller value of κ than the global bound (Ω_0) , and this produces quantitatively better sieve bounds.

We can now obtain a general purpose upper bound of type in (1.4). In sums of remainders r_d we recall that r_d is supported only on squarefree d .

Theorem 2.4. *Let \mathcal{A} be a sieve problem, let $z \geq 2$ and assume (g) , (r) and (V) . Let $\kappa_0 > 0$ and $B_0 \geq 0$. Assume (Ω) with $0 \leq \kappa \leq \kappa_0$ and $0 \leq B \leq B_0$. Then for any $z \geq 2$ we have*

$$S(\mathcal{A}, z) \leq O_{\kappa_0, B_0}(XV(z)) + \sum_{d \leq z} |r_d|,$$

the implied constant depending only on κ_0, B_0 .

Proof. Before invoking (Ω) , we will work out a general procedure for producing upper bounds from Theorem 2.3. We suppose that

$$(2.9) \quad \begin{aligned} z_{t+1} &= 2 < z_t < z_{t-1} < \cdots < z_1 = z \\ \mathcal{P}_j &= \{p \text{ prime} : z_{j+1} < p \leq z_j\} \quad (1 \leq j \leq t-1), \\ \mathcal{P}_t &= \{p \text{ prime} : z_{t+1} \leq p \leq z_t\}. \end{aligned}$$

This way, $\mathcal{P}_1, \dots, \mathcal{P}_t$ partition the primes in $[2, z]$. The primes $> z$ play no role in $S(\mathcal{A}, z)$ and may be ignored (or assigned arbitrarily to \mathcal{P}_1 , for example). In the sum (2.7) defining R' , we have

$$d_1 \cdots d_t \leq z_1^{k_1} \cdots z_t^{k_t}.$$

A convenient choice is

$$z_j = z^{1/4^{j-1}} \quad (1 \leq j \leq t),$$

where t is chosen maximally so that (2.9) holds. We also take

$$k_1 = 0, \quad k_j = 2^{j-1} \quad (j \geq 2).$$

In (2.7), we have

$$(2.10) \quad d \leq z_1^{k_1} \cdots z_t^{k_t} \leq z$$

Invoking (Ω) and taking logarithms, we have

$$L_j = \sum_{z_{j+1} < p \leq z_j} -\log(1 - g(p)) \leq \kappa \log 4 + \frac{B}{\log z_{j+1}} \leq \kappa_0 \log 4 + \frac{B_0}{\log 2} =: L.$$

Therefore, in the notation of Theorem 2.3,

$$(2.11) \quad E \leq \sum_{j=1}^t e^{L_j} \frac{L_j^{k_j}}{k_j!} \leq e^L \sum_{j=1}^{\infty} \frac{L^{2^j+1}}{2^{j-1}!} \ll_{\kappa_0, B_0} 1.$$

The theorem now follows from Theorem 2.3. \square

2.2. Applications of the upper bound sieve. Theorem (2.4) is very easy to apply in practice. It suffices to verify that the sifting function $g(p)$ has regular behavior ((Ω) or (Ω_0)) and that the remainders r_d are small on average in some reasonable range.

2.2.1. Primes. Take the Eratosthenes sieve $\Omega = [1, x] \cap \mathbb{N}$, $\mathcal{A}_p = \{n \in \Omega : p|n\}$, $X = x$, $g(p) = 1/p$, $z = X^{1/2}$. Then, by Theorem 2.4,

$$\pi(x) \leq S(\mathcal{A}, z) + z \ll XV(z) + O(z) \ll \frac{x}{\log x},$$

matching Chebyshev's bound.

2.2.2. Prime k -tuples.

Theorem 2.5. *Let a_1, \dots, a_k be non-zero integers and b_1, \dots, b_k integers. Let $\rho(d)$ be the number of solutions modulo d of*

$$(a_1 n + b_1) \cdots (a_k n + b_k) \equiv 0 \pmod{d},$$

and assume that $\rho(p) < p$ for all primes p (that is, the linear forms $a_i n + b_i$, $1 \leq i \leq k$, are admissible). Also assume that $E \neq 0$, where

$$E = \left| \prod_{i=1}^k a_i \prod_{i < j} (a_i b_j - a_j b_i) \right|.$$

Then $\rho(p) \neq k$ if and only if $p|E$, and furthermore,

$$\begin{aligned} \#\{n \leq x : a_i n + b_i \text{ prime}, 1 \leq i \leq k\} &\ll_k \frac{\mathfrak{S}x}{\log^k x} \\ &\ll_k \frac{x}{\log^k x} \prod_{p|E} \left(1 - \frac{1}{p}\right)^{\rho(p)-k} \\ &\ll_k \frac{x}{\log^k x} \left(\frac{E}{\phi(E)}\right)^k, \end{aligned}$$

where

$$\mathfrak{S} = \prod_p \left(1 - \frac{\rho(p)}{p}\right) \left(1 - \frac{1}{p}\right)^{-k}$$

and the implied constants may depend on k alone.

Proof. Define our sieve problem as follows. Let $\Omega = [1, x] \cap \mathbb{Z}$ and

$$\mathcal{A}_p = \{n \in \Omega : p|(a_1 n + b_1) \cdots (a_k n + b_k)\}$$

for each prime p . Let $X = x$ and put $z = X^{1/2}$. For squarefree d , let $\rho(d)$ be the number of solutions n mod d of the congruence

$$(a_1 n + b_1) \cdots (a_k n + b_k) \equiv 0 \pmod{d}.$$

By the Chinese remainder theorem, ρ is multiplicative. Now let p be prime and consider $\rho(p)$. Since $\rho(p) < p$, it follows that $(a_i, b_i) = 1$ for all i . Then the congruence $a_i n + b_i \equiv 0 \pmod{p}$ has a solution if and only if $p \nmid a_i$. Hence, if $p|a_i$ for some i , then $\rho(p) < k$. Now suppose that $p \nmid a_1 \cdots a_k$, and for each i let r_i be the unique residue class modulo p with $a_i r_i + b_i \equiv 0 \pmod{p}$. It is clear that $r_i = r_j$ if and only if $p|(a_i b_j - a_j b_i)$. Thus, if $p|E$ then $\rho(p) < k$, and if $p \nmid E$ then r_1, \dots, r_k all exist and are distinct, so $\rho(p) = k$. This proves the first claim.

Setting $g(p) = \rho(p)/p$, we see that (Ω_0) holds with $\delta = 1/(k+1)$ and $\kappa = k$. Then (Ω) holds with $\kappa = k$ and some B depending only on k . Moreover,

$$A_d = x \frac{\rho(d)}{d} + r_d, \quad |r_d| \leq \rho(d),$$

and thus

$$\sum_{d \leq z} |r_d| \leq \sum_{d \leq x^{1/2}} \rho(d) \leq x^{1/2} \sum_{d \leq x^{1/2}} \frac{\rho(d)}{d} \leq x^{1/2} \prod_{p \leq z} \left(1 + \frac{k}{p}\right) \ll_k x^{1/2} (\log x)^k$$

by Mertens' theorem. By Theorem 2.4 plus the easy bound

$$V(z) \gg_k \prod_{2k < p \leq z} (1 - k/p) \gg_k \frac{1}{\log^k z} \gg_k \frac{1}{\log^k x},$$

we have

$$S(\mathcal{A}, z) \ll_k xV(z) + x^{1/2}(\log x)^k \ll xV(z).$$

There are at most z values of $n \leq x$ such that $a_i n + b_i$ are all prime and $\leq z$. Thus,

$$\#\{n \leq x : a_i n + b_i \text{ prime}, 1 \leq i \leq k\} \leq z + S(\mathcal{A}, z) \ll x^{1/2} + xV(z) \ll xV(z).$$

Next,

$$\begin{aligned} V(z) &= \prod_{p \leq z} \left(1 - \frac{\rho(p)}{p}\right) \\ &\ll_k \frac{1}{(\log z)^k} \prod_{p \leq z} \left(1 - \frac{\rho(p)}{p}\right) \left(1 - \frac{1}{p}\right)^{-k} \\ &= \frac{\mathfrak{S}}{(\log z)^k} \prod_{p > z} \left(1 - \frac{\rho(p)}{p}\right)^{-1} \left(1 - \frac{1}{p}\right)^k \\ &\ll_k \frac{\mathfrak{S}}{(\log x)^k} \prod_{p > 2k} \left(1 - \frac{k}{p}\right)^{-1} \left(1 - \frac{1}{p}\right)^k \\ &\ll_k \frac{\mathfrak{S}}{(\log x)^k}. \end{aligned}$$

Finally, since $\rho(p) = k$ if and only if $p \nmid E$, $(1 - k/p)(1 - 1/p)^{-k} = 1 + O_k(1/p^2)$ and $1 - \rho/p \leq (1 - 1/p)^k$, we have

$$\mathfrak{S} \ll_k \prod_{p|E} \left(1 - \frac{\rho(p)}{p}\right) \left(1 - \frac{1}{p}\right)^{-k} \leq \prod_{p|E} \left(1 - \frac{1}{p}\right)^{\rho(p)-k} \leq \left(\frac{E}{\phi(E)}\right)^k. \quad \square$$

Remarks. Examining the proof, we see that $\mathfrak{S} \gg_k 1$, that is, \mathfrak{S} is bounded away from zero. On the other hand, \mathfrak{S} is not bounded above as one of the following examples shows.

Corollary 2.6. *We have, for positive m ,*

$$\begin{aligned} \#\{p \leq x : p, p + 2m \text{ both prime}\} &\ll \frac{2m}{\phi(2m)} \frac{x}{\log^2 x}, \\ \#\{p \leq x : p, 2p + 1 \text{ both prime}\} &\ll \frac{x}{\log^2 x}, \\ \#\{p, q \text{ prime} : p + q = 2m\} &\ll \frac{\sigma(m)}{m} \frac{m}{\log^2 m}. \end{aligned}$$

Proof. The count of generalized twin primes is the special case $k = 2$ with the forms $n, n + 2m$. Here $\rho(p) = 1$ for $p|2m$ and $\rho(p) = 2$ otherwise, and we have

$$\mathfrak{S} \asymp \prod_{p|2m} \left(1 - \frac{1}{p}\right)^{-1} = \frac{2m}{\phi(2m)}.$$

Also, $E = 2m$. The count of Sophie Germain is easier: here we use the forms $n, 2n + 1$ and $E = 2$. For the application to Goldbach's Conjecture, take the forms $n, 2m - n$, which gives $E = 2m$. The final estimate comes from the elementary bound $\frac{m}{\phi(m)} \ll \frac{\sigma(m)}{m}$. \square

2.2.3. The Brun-Titchmarsh inequality. Denote by $\pi(x; q, a)$ the number of primes $p \leq x$ satisfying $p \equiv a \pmod{q}$.

Theorem 2.7 (Brun-Titchmarsh inequality). *There is a constant C so that uniformly for $1 \leq a \leq q < y \leq x$ and $(a, q) = 1$,*

$$\pi(x; q, a) - \pi(x - y; q, a) \leq C \frac{y}{\phi(q) \log(y/q)}.$$

Remarks. The case $a = q = 1$, that is, showing that $\pi(x) - \pi(x - y) \ll y/\log y$, was asserted by Hardy and Littlewood [72, p. 69] without proof, the authors claiming that it followed from the method of Brun [19]. Using the Eratosthenes sieve, Hardy and Littlewood [72, Theorem G] showed the weaker bound $\pi(x) - \pi(x - y) \ll \frac{y}{\log_2 y}$. The case $x = 0$ with an arbitrary a, q was shown by Titchmarsh [129]. The constant $C = 2$ is admissible by work of Montgomery and Vaughan [100]. The utility of this bound is its uniformity in x, y, a, q . If $\pi(x; q, a) := \#\{p \leq x : p \equiv a \pmod{q}\}$, the prime number theorem for arithmetic progressions implies that

$$\pi(x; q, a) \sim \frac{x}{\phi(q) \log x}$$

for every individual q, a . Issues of uniformity are crucially important, and are intimately connected to questions of the existence of zeros of L -functions lying off the critical line (especially so-called Siegel zeros, real zeros lying very close to 1). If one assumes the Generalized Riemann Hypothesis, then the above asymptotic holds uniformly for $q \leq \sqrt{x}$ or so, and in a smaller range if one considers primes in "short" intervals $(x - y, x]$. On the other hand, the Brun-Titchmarsh inequality gives an upper bound of the correct order even for very large moduli $q = x^{1-\varepsilon}$ and for very short intervals $y/q = x^\varepsilon$ ($\varepsilon > 0$ fixed).

Proof. WLOG assume that $y > 2q$, for otherwise trivially the left side is ≤ 2 while the right side is $\geq C/\log(y/q) \geq C/\log 2$. Write

$$\{x - y < n \leq x : n \equiv a \pmod{q}\} = \{q(h + 1) + a, \dots, q(h + m) + a\}.$$

Apply Theorem 2.5 with $k = 1$ and the single form $qn + (qh + a)$, where $1 \leq n \leq m$. Here $E = q$ and thus

$$\pi(x; q, a) - \pi(x - y; q, a) \ll \frac{q}{\phi(q)} \frac{m}{\log m}.$$

Since $m = y/q$, the theorem follows. \square

2.2.4. Romanoff's Theorem.

Theorem 2.8 (Romanoff [115], 1934). *A positive proportion³ of positive integers can be expressed as $p + 2^k$ where p is prime and k is a non-negative integer.*

Proof. We start with a common device for lower-bounding the size of a set defined by solutions of some equation. Let

$$r(n) = \#\{(p, k) : k \geq 1, n = p + 2^k\}$$

and $B(x) = \#\{n \leq x : r(n) > 0\}$. We need to show that $B(x) \gg x$ for large x . Assume that $x \geq 100$. By Cauchy-Schwarz,

$$\begin{aligned} \left(\sum_{n \leq x} r(n) \right)^2 &= \left(\sum_{n \leq x} r(n) \mathbb{1}_{r(n) > 0} \right)^2 \\ &\leq \sum_{\substack{n \leq x \\ r(n) > 0}} 1 \sum_{n \leq x} r(n)^2 \\ &= B(x) \sum_{n \leq x} r(n)^2. \end{aligned}$$

On the other hand,

$$\sum_{n \leq x} r(n) \geq \#\{(p, k) : p \leq x/2, 2^k \leq x/2\} \gg \pi(x/2) \log x \gg x$$

and, since $n \leq x$ implies that $p \leq x$ and $2^k \leq x$,

$$\begin{aligned} \sum_{n \leq x} r(n)^2 &= \sum_{n \leq x} \#\{(p_1, p_2, k_1, k_2) : p_1 + 2^{k_1} = p_2 + 2^{k_2} = n\} \\ &\leq D := \#\{(p_1, p_2, k_1, k_2) : p_j \leq x, 2^{k_j} \leq x \text{ for } j = 1, 2; p_1 + 2^{k_1} = p_2 + 2^{k_2}\}. \end{aligned}$$

It follows that

$$(2.12) \quad B(x) \gg \frac{x^2}{D}.$$

There are $O(x)$ quadruples (p_1, p_2, k_1, k_2) with $p_1 = p_2$ and $k_1 = k_2$. Thus,

$$D \ll x + \#\{(p_1, p_2, k_1, k_2) : p_1 < p_2 < x, 2^{k_j} \leq x \text{ for } j = 1, 2; p_2 = p_1 + 2^{k_1} - 2^{k_2}\}.$$

Now fix $k_1 > k_2 \geq 1$. Now apply Corollary 2.6 with $2m = 2^{k_1} - 2^{k_2}$. With k_1 and k_2 fixed, the number of possible pairs p_1, p_2 with $p_1 \leq x$ is

$$\ll \frac{2^{k_1} - 2^{k_2}}{\phi(2^{k_1} - 2^{k_2})} \frac{x}{\log^2 x}$$

³If A is a set of natural numbers with counting function $A(x) = \#\{a \leq x : a \in A\}$ satisfying $\liminf_{x \rightarrow \infty} A(x)/x > 0$, we say that A contains a positive proportion of all positive integers.

and hence

$$D \ll x + \frac{x}{\log^2 x} \sum_{0 < k_2 < k_1 \leq \frac{\log x}{\log 2}} \frac{2^{k_1} - 2^{k_2}}{\phi(2^{k_1} - 2^{k_2})}.$$

Factoring out 2^{k_2} we see that

$$\frac{2^{k_1} - 2^{k_2}}{\phi(2^{k_1} - 2^{k_2})} \ll \frac{2^l - 1}{\phi(2^l - 1)}, \quad l = k_1 - k_2.$$

Also,

$$\frac{2^l - 1}{\phi(2^l - 1)} \ll \frac{\sigma(2^l - 1)}{2^l - 1} = \sum_{d|2^l - 1} \frac{1}{d}.$$

For each l there are $O(\log x)$ pairs (k_1, k_2) with $k_1 - k_2 = l$ and thus

$$\begin{aligned} D &\ll x + \frac{x}{\log x} \sum_{1 \leq l \leq \frac{\log x}{\log 2}} \sum_{d|2^l - 1} \frac{1}{d} \\ &\ll x + \frac{x}{\log x} \sum_{\substack{d \leq x \\ d \text{ odd}}} \frac{1}{d} \sum_{\substack{1 \leq l \leq \frac{\log x}{\log 2} \\ d|2^l - 1}} 1. \end{aligned}$$

If $s(d)$ denotes the order of 2 modulo d , then the inner sum counts $l \leq \frac{\log x}{\log 2}$ which are divisible by $s(d)$ and is therefore $O(\frac{\log x}{s(d)})$. We arrive at

$$(2.13) \quad D \ll x + x \sum_{\substack{d \leq x \\ d \text{ odd}}} \frac{1}{ds(d)}.$$

Following Erdős, we show that the sum on d converges, when extended to a sum over all odd positive integers. To this end, define

$$t_k = \sum_{\substack{d \text{ odd} \\ s(d) \leq k}} \frac{1}{d},$$

which is finite since $s(d) \gg \log d$. Partial summation gives

$$(2.14) \quad \sum_d \frac{1}{ds(d)} = \sum_k \frac{t_k}{k(k+1)}.$$

Letting

$$N_k = \prod_{i \leq k} (2^i - 1),$$

we see that $s(d) \leq k$ implies that $d|N_k$. Also $N_k \leq 2^{1+2+\dots+k} < 2^{k^2}$, and so

$$t_k \leq \sum_{d|N_k} \frac{1}{d} = \frac{\sigma(N_k)}{N_k} \ll \log_2 N_k \ll \log k.$$

Thus, the sum on the right side of (2.14) converges, as desired. Consequently, by (2.13), $D \ll x$. Recalling (2.12), the proof is complete. \square

Remark 1. Evidently, almost all even integers are not of the form $p + 2^k$. Erdős [35] showed that a positive proportion of odd numbers are not of the form $p + 2^k$. This paper introduced the notion of covering systems of congruences.

2.2.5. *Sums of primes: Schnirelmann's theorem.* In the 1933, Schnirelmann [121] showed that there is a constant k so that every positive integer ≥ 2 is the sum of at most k primes. This was a huge step in the direction of Goldbach's Conjecture. His proof combined the sieve upper bound with a very elementary argument.

Given a set $\mathcal{A} \subset \mathbb{N} \cup \{0\}$, let $A(N)$ be the counting function of \mathcal{A} (excluding zero), that is, $A(N) = \#\{n \in \mathcal{A} : 1 \leq n \leq N\}$. The *Schnirelmann density* $\sigma(\mathcal{A})$ of \mathcal{A} is defined as

$$\sigma(\mathcal{A}) = \inf_{N \geq 1} \frac{A(N)}{N}.$$

Examples:

- $\sigma(\mathcal{A}) = 1$ if and only if $\mathcal{A} \supset \mathbb{N}$
- if $1 \notin \mathcal{A}$ then $\sigma(\mathcal{A}) = 0$.
- $\sigma(\{1, 3, 5, 7, 9, 11, \dots\}) = 1/2$.
- $\sigma(\{1, 4, 9, 16, 25, \dots\}) = 0$.

Given any two sets \mathcal{A}, \mathcal{B} of integers, define the *sumset* $\mathcal{A} + \mathcal{B}$ by

$$\mathcal{A} + \mathcal{B} = \{a + b : a \in \mathcal{A}, b \in \mathcal{B}\}.$$

We denote the k -fold subset $k\mathcal{A}$ inductively as $k\mathcal{A} = (k-1)\mathcal{A} + \mathcal{A}$, so that $k\mathcal{A}$ is the set of integers that can be written as the sum of k (not necessarily distinct) elements of \mathcal{A} .

Theorem 2.9 (Schnirelmann [121], 1933). (a) *Suppose that $0 \in \mathcal{B}$ and $1 \in \mathcal{A}$. Then*

$$\sigma(\mathcal{A} + \mathcal{B}) \geq \sigma(\mathcal{A}) + \sigma(\mathcal{B}) - \sigma(\mathcal{A})\sigma(\mathcal{B}).$$

(b) *If $0 \in \mathcal{A}, 0 \in \mathcal{B}$ and $\sigma(\mathcal{A}) + \sigma(\mathcal{B}) \geq 1$ then $\mathcal{A} + \mathcal{B} = \mathbb{N} \cup \{0\}$.*

The conclusion of part (a) is conveniently written as

$$1 - \sigma(\mathcal{A} + \mathcal{B}) \leq (1 - \sigma(\mathcal{A}))(1 - \sigma(\mathcal{B})).$$

In general, the conclusion is best possible, for example if

$$\mathcal{A} = \{1, 5, 6, 7, 8, 9, \dots\}, \quad \mathcal{B} = \{0, 1, 4, 5, 6, 7, 8, \dots\}$$

then $\mathcal{A} + \mathcal{B} = \{1, 2, 5, 6, 7, 8, 9, \dots\}$, $\sigma(\mathcal{A}) = \frac{1}{4}$, $\sigma(\mathcal{B}) = \frac{1}{3}$ and $\sigma(\mathcal{A} + \mathcal{B}) = \frac{1}{2}$.

Corollary 2.10 (Schnirelmann [121]). *Suppose that $0 \in \mathcal{A}$ and $\sigma(k\mathcal{A}) > 0$ for some $k \in \mathbb{N}$. Then for some $h \in \mathbb{N}$, $h\mathcal{A} = \mathbb{N} \cup \{0\}$.*

Proof that Theorem 2.9 implies Corollary 2.10. Let $\mathcal{B} = k\mathcal{A}$. Obviously $0 \in \mathcal{B}$. Since $\sigma(\mathcal{B}) > 0$, we have $1 \in \mathcal{B}$. Hence, $\{0, 1\} \subset r\mathcal{B}$ for all $r \in \mathbb{N}$. By Theorem 2.9 (a), for any $r \in \mathbb{N}$ we have

$$1 - \sigma((r+1)\mathcal{B}) \leq (1 - \sigma(\mathcal{B}))(1 - \sigma(r\mathcal{B})).$$

By induction,

$$1 - \sigma(r\mathcal{B}) \leq (1 - \sigma(\mathcal{B}))^r$$

Hence, for some r , $\sigma(r\mathcal{B}) \geq 1/2$. Then, by Theorem 2.9 (b), we conclude that $\sigma(2r\mathcal{B}) = 1$, that is,

$$2rk\mathcal{A} = 2r\mathcal{B} = \mathbb{N} \cup \{0\},$$

as required. \square

Proof of Theorem 2.9. We begin with (a). Let $N \in \mathbb{N}$ and enumerate the elements of $\mathcal{A} \cap [1, N]$ as $1 = a_1 < a_2 < \dots < a_r \leq N$. These integers are separated by gaps of $g_i = a_{i+1} - a_i - 1$ numbers not in \mathcal{A} , plus a final gap of $g_r = N - a_r$ integers from $a_r + 1$ to N . Let $\mathcal{C} = \mathcal{A} + \mathcal{B}$. Then $\mathcal{C} \cap [1, N]$ contains $\mathcal{A} \cap [1, N]$, plus additional numbers $a_i + b$, where $b \in \mathcal{B}$, $1 \leq b \leq g_i$. The number of such elements b is $\geq g_i \sigma(\mathcal{B})$. It follows that

$$\begin{aligned} C(N) &\geq A(N) + \sum_{i=1}^r \sigma(\mathcal{B})g_i \\ &= A(N) + \sigma(\mathcal{B})(N - A(N)) \\ &= A(N)(1 - \sigma(\mathcal{B})) + N\sigma(\mathcal{B}) \\ &\geq N\left(\sigma(\mathcal{A})(1 - \sigma(\mathcal{B})) + \sigma(\mathcal{B})\right). \end{aligned}$$

As this is true for every N , $\sigma(\mathcal{C}) \geq \sigma(\mathcal{A}) + \sigma(\mathcal{B}) - \sigma(\mathcal{A})\sigma(\mathcal{B})$.

To prove (b), first observe that $1 \in \mathcal{A} \cup \mathcal{B}$, so that $1 \in \mathcal{A} + \mathcal{B}$. Suppose that $\mathcal{A} + \mathcal{B} \neq \mathbb{N} \cup \{0\}$ and that $n \notin \mathcal{A} + \mathcal{B}$. Then $n \geq 2$, $n \notin \mathcal{A}$ and $n \notin \mathcal{B}$. Thus,

$$A(n-1) + B(n-1) = A(n) + B(n) \geq n(\sigma(\mathcal{A}) + \sigma(\mathcal{B})) \geq n.$$

Now let

$$\mathcal{C} = \{a \in \mathcal{A} : 1 \leq a \leq n-1\}, \quad \mathcal{D} = \{n-b : 1 \leq b \leq n-1, b \in \mathcal{B}\}.$$

Then $|\mathcal{C}| + |\mathcal{D}| \geq n$. But $\mathcal{C}, \mathcal{D} \subset [1, n-1]$, hence by the pigeonhole principle, \mathcal{C} and \mathcal{D} must have a common element, thus $n \in \mathcal{A} + \mathcal{B}$, a contradiction. Therefore, $\mathcal{A} + \mathcal{B} = \mathbb{N} \cup \{0\}$. \square

We now apply these results to primes. Let \mathcal{P} denote the set of primes and set $\mathcal{P}_0 = \mathcal{P} \cup \{0, 1\}$. Now $\sigma(\mathcal{P}_0) = 0$ by the prime number theorem. However, by Exercise 2.5 below, we have $\sigma(2\mathcal{P}_0) > 0$. Hence, by Corollary 2.10, there is an h so that $h\mathcal{P}_0 = \mathbb{N} \cup \{0\}$. We also have $h \geq 3$, since $27 \notin 2\mathcal{P}_0$. Thus, for any positive integer $n \geq 4$, we have

$$n - 2 = p_1 + \dots + p_r + s \cdot 1$$

where p_1, \dots, p_r are primes, $r \geq 0$, $s \geq 0$ and $r + s \leq h$. Now $2 + s = 2k + 3l$ where $k \geq 0, l \geq 0$ and $k + l \leq s + 1$. Thus, n is the sum of at most $r + s + 1 = h + 1$ primes. We conclude that

Theorem 2.11 (Schnirelmann [121], 1933). *For some $h \in \mathbb{N}$, every positive integer ≥ 2 is the sum of at most h primes.*

2.2.6. Primitive roots of primes. Are there infinitely many primes p for which the fraction $1/p$ has period $p-1$ in base 10? Equivalently, is 10 a primitive root of p for infinitely many primes p ? This question was addressed by Gauss in his *Disquisitiones Arithmeticae* (1801). In 1927, E. Artin conjectured an asymptotic formula for the number of primes $p \leq x$ for which a given squarefree integer a is a primitive root; his formula was later discovered not to hold up against numerical data by D. H. Lehmer, and a revised conjecture was later proposed by H. Heilbronn and others. In 1967, C. Hooley deduced the revised conjecture from the Generalized Riemann Hypothesis for certain Dedekind zeta functions $\zeta_K(s)$ [82]; see also [86, Ch. 3]. The theorem makes use of sieve methods. Here we will specialize to the case $a = 2$. For background on Dedekind zeta functions, see [89, Sec. 5.10].

Theorem 2.12 (Hooley [82]). *Assume the Generalized Riemann Hypothesis for $\zeta_K(s)$ for the number fields $K = \mathbb{Q}(\sqrt[k]{2}, e^{2\pi i/k})$, k running over all squarefree integers. Then*

$$\#\{p \leq x : 2 \text{ is a primitive root of } p\} \sim C\pi(x), \quad C = \prod_{q \text{ prime}} \left(1 - \frac{1}{q(q-1)}\right).$$

Proof. We set this up as a general sieve problem as follows. Let Ω be the set of primes $p \leq x$, and for any prime q , let

$$\mathcal{A}_q = \left\{p \in \Omega : q|p-1 \text{ and } 2^{(p-1)/q} \equiv 1 \pmod{p}\right\}.$$

Clearly, 2 is a primitive root of p (order $p-1$) if and only if $p \notin \mathcal{A}_q$ for all primes q (and it suffices to check for primes $q \leq p$). We need good, *uniform* bounds for A_d . Bounds for individual d , but with poor uniformity, are available unconditionally by the analog of the prime number theorem for the number fields K (the prime ideal theorem of Landau), but the uniformity is very poor, especially for $x^{o(1)} < d \leq \sqrt{x}$, and not good enough for our application.

Lemma 2.13 (Hooley [82]). *Assume the Generalized Riemann Hypothesis for the Dedekind zeta functions $\zeta_K(s)$ for all of the number fields $K = \mathbb{Q}(\sqrt[k]{2}, e^{2\pi i/k})$, k running over all squarefree integers. Then, uniformly for squarefree $d \leq x$,*

$$A_d = \frac{\text{li}(x)}{d\phi(d)} + O(\sqrt{x} \log x).$$

Define the cutoffs

$$z_1 = \frac{1}{6} \log x, \quad z_2 = \sqrt{x}(\log x)^{-2}, \quad z_3 = \sqrt{x} \log x.$$

Evidently,

$$(2.15) \quad S(\mathcal{A}, z_1) \geq \#\{p \leq x : 2 \text{ is a primitive root of } p\} \geq S(\mathcal{A}, z_1) - S_1 - S_2 - T,$$

where

$$S_1 = \sum_{z_1 < q \leq z_2} A_q, \quad S_2 = \sum_{z_2 < q \leq z_3} A_q, \quad T = \#\{p \leq x : p \in \mathcal{A}_q \text{ for some } q > z_3\}.$$

Using the Legendre sieve (Theorem 1.2) with $X = \text{li}(x)$ and with $g(d) = \frac{1}{d\phi(d)}$, Lemma 2.13 gives

$$\begin{aligned} S(\mathcal{A}, z_1) &= \text{li}(x) \prod_{q \leq z_1} \left(1 - \frac{1}{q(q-1)}\right) + O(\sqrt{x}(\log x)2^{\pi(z_1)}) \\ &= \left(C + O\left(\frac{1}{\log x}\right)\right) \text{li}(x) = \left(C + O\left(\frac{1}{\log x}\right)\right) \pi(x). \end{aligned}$$

For S_1 , we again use Lemma 2.13 and obtain

$$\begin{aligned} S_1 &= \sum_{z_1 < q \leq z_2} \left(\frac{\text{li}(x)}{q(q-1)} + O(\sqrt{x} \log x)\right) \\ &\ll \frac{\text{li}(x)}{\log x} + \sqrt{x}(\log x)\pi(z_2) \ll \frac{\pi(x)}{\log x}. \end{aligned}$$

For S_2 , the bounds from Lemma 2.13 are too poor, but we do better by observing that $A_q \leq \pi(x; q, 1)$ and using Theorem 2.7 (the Brun-Titchmarsh inequality):

$$\begin{aligned} S_2 &\leq \sum_{z_2 < q \leq z_3} \pi(x; q, 1) \ll \sum_{z_2 < q \leq z_3} \frac{x}{q \log x} \ll \frac{x}{\log^2 x} \sum_{z_2 < q \leq z_3} \frac{\log q}{q} \\ &\ll \frac{x}{\log^2 x} \log \frac{z_3}{z_2} \ll \frac{x \log_2 x}{\log^2 x} \ll \pi(x) \frac{\log_2 x}{\log x}. \end{aligned}$$

Finally, if $p \in \mathcal{A}_q$ for some $q > z_3$, then $p | (2^m - 1)$ for some positive integer $m \leq \sqrt{x}/\log x$. Thus, $p | M$, where

$$M = \prod_{m \leq \sqrt{x}/\log x} (2^m - 1).$$

Thus,

$$T \leq \#\{p | M : p \text{ prime}\} \leq \frac{\log M}{\log 2} \ll \left(\frac{\sqrt{x}}{\log x} \right)^2 = \frac{x}{\log^2 x} \ll \frac{\pi(x)}{\log x}.$$

Combining the estimates for $S(\mathcal{A}, z_1)$, S_1 , S_2 and T with (2.15) proves the theorem. \square

In 1986, Heath-Brown [80] showed that for all but at most two primes r ,

$$\{p : r \text{ is a primitive root of } p\}$$

is infinite. We cannot say which two prime might be exceptional, or even give a bound on the exceptional primes. We will revisit this type of result later.

2.3. Exercises.

Exercise 2.1. Assume condition (Ω_0) . Show that (Ω) holds with the same value of κ and with B depending only on δ, κ .

Exercise 2.2. For each prime, let \mathcal{I}_p denote a set of residue classes modulo p . Suppose that $|\mathcal{I}_p| \leq \kappa$ for all p . Show that

$$\#\{x < n \leq x + y : \forall p \leq z, n \pmod p \notin \mathcal{I}_p\} \ll_\kappa y \prod_{p \leq z} \left(1 - \frac{|\mathcal{I}_p|}{p}\right),$$

uniformly for $2 \leq z \leq y$ and all x .

Exercise 2.3. Let k be a positive, even integer. Assuming Conjecture 1.10 for the pair of linear forms $(n, n + k)$, prove that

$$\#\{n \leq x : n \text{ and } n + k \text{ are consecutive primes}\} \sim \frac{a(k)x}{\log^2 x} \quad (x \rightarrow \infty),$$

where

$$a(k) = C \prod_{p|k, p>2} \frac{p-1}{p-2}, \quad C = 2 \prod_{p \geq 3} \left(1 - \frac{1}{(p-1)^2}\right),$$

C being the ‘‘twin prime constant’’.

Exercise 2.4. Show that for any odd N ,

$$\#\{(p_1, p_2, p_3) : N = p_1 + p_2 + p_3\} \ll \frac{N^2}{\log^3 N},$$

the constant being absolute.

Exercise 2.5. We say that an even number k is a Goldbach number if there exists primes p_1, p_2 such that $k = p_1 + p_2$. Show that a positive proportion of all positive integers are Goldbach numbers.

Exercise 2.6. Let $\Xi(x, y, z)$ denote the number of integers $n \leq x$ which have no prime factor in $(y, z]$. Prove that uniformly in $1.5 \leq y \leq z \leq x$, we have

$$\Xi(x, y, z) \ll \frac{x \log y}{\log z}.$$

Exercise 2.7. Prove that

$$\sum_{p \leq x} \Omega(p-1) \ll \frac{x \log_2 x}{\log x},$$

where $\Omega(n)$ is the number of prime power divisors of n .

Exercise 2.8. Let \mathcal{S} denote the set of integers that are the sum of two squares.

- (a) Show that \mathcal{S} has counting function $O(x(\log x)^{-1/2})$.
 (b) Let $h \in \mathbb{N}$. Show that, uniformly in h ,

$$\#\{n \leq x : n \in \mathcal{S}, n+h \in \mathcal{S}\} \ll \prod_{\substack{p|h \\ p \equiv 3 \pmod{4}}} \left(1 + \frac{1}{p}\right) \frac{x}{\log x}.$$

Exercise 2.9. (Landau-Lehmer problem). Let $q \in \mathbb{N}$, $q \geq 2$, and let \mathcal{R} be a collection of reduced residue classes modulo q . Prove that the number of integers $n \leq x$ lacking any prime factor that lies in one of the congruence classes of \mathcal{R} is bounded above by

$$\ll_q \frac{x}{(\log x)^{|\mathcal{R}|/\phi(q)}}.$$

Exercise 2.10. Let \mathcal{A} denote the set of positive, squarefree integers.

- (a) Show that the Schnirelmann density $\sigma(\mathcal{A}) > 1/2$.
 (b) Show that every integer $n \geq 2$ is the sum of exactly two squarefree integers. (This does not follow immediately from Theorem 2.9 (b)).

Exercise 2.11. Let \mathcal{B} be the set of primes that are of the form $a^2 + b^4$ for some integers a, b . Prove that

$$\#\{p \leq x : p \in \mathcal{B}\} \ll \frac{x^{3/4}}{\log x}.$$

Exercise 2.12. Let $1 \leq a \leq q$, $(a, q) = 1$. Prove that uniformly in a, q and $x \geq 10$ we have

$$\sum_{\substack{q \leq p \leq x \\ p \equiv a \pmod{q}}} \frac{1}{p} \ll \frac{\log_2 x}{\phi(q)}.$$

Note that the condition $p \geq q$ is necessary, as the least prime that is $\equiv a \pmod{q}$ might be a , which could be very small.

2.4. The Brun-Hooley sieve: lower bounds. Our lower bound for $S(\mathcal{A}, z)$ is derived from the upper bound in Lemma 2.2 by subtracting off appropriate quantities. We use the following simple inequality:

Lemma 2.14. *Suppose that $0 \leq x_j \leq y_j$ for $1 \leq j \leq t$. Then*

$$x_1 \cdots x_t \geq y_1 \cdots y_t - \sum_{\ell=1}^t (y_\ell - x_\ell) \prod_{\substack{j=1 \\ j \neq \ell}}^t y_j.$$

Proof. The inequality is an equality when $t = 1$, and follows by induction on t using

$$\begin{aligned} y_1 \cdots y_t - x_1 \cdots x_t &= (y_1 \cdots y_{t-1} - x_1 \cdots x_{t-1})y_t + x_1 \cdots x_{t-1}(y_t - x_t) \\ &\leq (y_1 \cdots y_{t-1} - x_1 \cdots x_{t-1})y_t + y_1 \cdots y_{t-1}(y_t - x_t). \end{aligned} \quad \square$$

As before, partition the primes in $[2, z]$ into sets $\mathcal{P}_1, \dots, \mathcal{P}_t$ and let k_1, \dots, k_t be nonnegative even integers. We apply Lemma 2.14 with

$$x_j = \sum_{d|(n, P_j)} \mu(d), \quad y_j = \sum_{\substack{d|(n, P_j) \\ \omega(d) \leq k_j}} \mu(d) \quad (1 \leq j \leq t),$$

where k_1, \dots, k_t are even, nonnegative integers. From Lemma 1.6 (with $f(p) = 1$ for each p) we have that

$$0 \leq y_\ell - x_\ell \leq \sum_{\substack{d|(n, P_\ell) \\ \omega(d) = k_\ell + 1}} 1.$$

Hence by Lemma 2.2 and Lemma 2.14, for any n with $P^+(n) \leq z$ we obtain

$$(2.16) \quad \mathbb{1}_{n=1} = \sum_{d|n} \mu(d) \geq \prod_{j=1}^t \sum_{\substack{d_j|(n, P_j) \\ \omega(d_j) \leq k_j}} \mu(d_j) - \sum_{\ell=1}^t \left(\sum_{\substack{d_\ell|(n, P_\ell) \\ \omega(d_\ell) = k_\ell + 1}} 1 \right) \prod_{\substack{j=1 \\ j \neq \ell}}^t \sum_{\substack{d_j|(n, P_j) \\ \omega(d_j) \leq k_j}} \mu(d_j).$$

Thus, we have a lower bound sieve with coefficients (here $d = d_1 \cdots d_t$ with $d_i = (d, P_i)$ for each i)

$$(2.17) \quad \lambda_d^- = \begin{cases} \mu(d) & \text{if } d_j | P_j, \omega(d_j) \leq k_j \quad (1 \leq j \leq t) \\ \mu(d) & \text{if } d_j | P_j \quad (1 \leq j \leq t), \exists \ell : \omega(d_j) \leq k_j \quad (j \neq \ell), \omega(d_\ell) = k_\ell + 1 \\ 0 & \text{otherwise.} \end{cases}$$

From (1.6),

$$S(\mathcal{A}, z) \geq \sum_{\substack{d_1, \dots, d_t \\ \forall j: d_j | P_j, \omega(d_j) \leq k_j}} \mu(d_1) \cdots \mu(d_t) A_{d_1 \cdots d_t} - \sum_{\ell=1}^t \sum_{\substack{d_1, \dots, d_t \\ d_j | P_j, \omega(d_j) \leq k_j \quad (j \neq \ell) \\ d_\ell | P_\ell, \omega(d_\ell) = k_\ell + 1}} \mu\left(\frac{d_1 \cdots d_t}{d_\ell}\right) A_{d_1 \cdots d_t}.$$

As before, introduce the conditions (g) and (r), and the shorthand notation (V). Adopting our previous notation (2.3) for quantities U_j , we can rewrite this as

$$S(\mathcal{A}, z) \geq XU_1 \cdots U_t \left(1 - \sum_{\ell=1}^t \frac{1}{U_\ell} \sum_{\substack{d_\ell | P_\ell \\ \omega(d_\ell) = k_\ell + 1}} g(d_\ell) \right) - \tilde{R},$$

where

$$\tilde{R} = \sum_{d \in \mathcal{D}} |r_d|,$$

and \mathcal{D} is the set of squarefree numbers d that satisfy $P^+(d) \leq z$, $\omega((d, P_j)) \leq k_j + 1$ for all j and $\omega((d, P_j)) = k_j + 1$ for at most one j . Define V_j and L_j by (2.4). By Lemma 1.6, $U_i \geq V_i$ for every i , thus in particular

$$U_1 \cdots U_t \geq V(z), \quad 1/U_\ell \leq e^{L_\ell \mathbb{1}_{k_\ell > 0}}.$$

Another invocation of the Erdős trick (cf., the proof of Lemma 1.6) gives

$$\sum_{\substack{d_\ell | P_\ell \\ \omega(d_\ell) = k_\ell + 1}} g(d_\ell) \leq \frac{1}{(k_\ell + 1)!} \left(\sum_{p \in P_\ell} g(p) \right)^{k_\ell + 1} \leq \frac{L_\ell^{k_\ell + 1}}{(k_\ell + 1)!}.$$

We partition the primes in $[2, z]$ as in (2.9). Then

$$\tilde{R} \leq \sum_{\substack{P^+(d) \leq z \\ d \leq D}} \mu^2(d) |r_d|, \quad D = z_1^{k_1 + 1} z_2^{k_2} \cdots z_t^{k_t}.$$

We arrive at a first general lower bound sieve.

Theorem 2.15. *Let \mathcal{A} be a sieve problem and assume (g) , (r) and (V) . Partition the set of primes in $[2, z]$ as in (2.9) and let k_1, \dots, k_t be nonnegative even integers. Then*

$$S(\mathcal{A}, z) \geq XV(z)(1 - E) - R'',$$

where E is given by (2.6) and

$$(2.18) \quad R'' = \sum_{\substack{P^+(d) \leq z \\ d \leq z_1^{k_1 + 1} z_2^{k_2} \cdots z_t^{k_t}}} \mu^2(d) |r_d|,$$

In terms of the lower bound sieve coefficients (2.17), we have shown that

$$(2.19) \quad (1 - E)V(z) \leq \sum_d \lambda_d^- g(d) \leq V(z),$$

where E is given by (2.6) and the upper bound comes from (1.7).

Incorporating (Ω) , we can derive a lower bound of general utility.

Theorem 2.16. *Let \mathcal{A} be a sieve problem and assume (g) , (r) and (V) . Assume also (Ω) with $\kappa > 0$. Then, if z is large enough as a function of κ, B , we have*

$$S(\mathcal{A}, z) \geq 0.0001XV(z) - \sum_{\substack{P^+(d) \leq z \\ d \leq z^{f(\kappa)}}} \mu^2(d) |r_d|,$$

where

$$f(\kappa) = 1 + \sum_{m=1}^{\infty} \frac{2m}{\exp\{0.26249m^2/\kappa\}}.$$

Moreover, we have $f(\kappa) \leq 1 + 3.81\kappa$ for all $\kappa > 0$, $f(\kappa) \leq \frac{5}{6} + 3.81\kappa$ for $\kappa \geq 0.05$ and $f(\kappa) \rightarrow 1$ as $\kappa \rightarrow 0^+$.

Proof. Let $\xi = 0.26249$ and define $\alpha_j = \exp\{\xi(j-1)^2/\kappa\}$ and

$$z_j = z^{1/\alpha_j} \quad (1 \leq j \leq t)$$

in (2.9), where t is maximally chosen satisfying the first line of (2.9). Also take $k_j = 2j - 2$ for all j . By (2.4) and (Ω) ,

$$(2.20) \quad L_j \leq \kappa \log \alpha_{j+1} - \kappa \log \alpha_j + \frac{B}{\log z_{j+1}} = \xi(2j-1) + \frac{\alpha_{j+1}B}{\log z}.$$

We bound E by separating the sum appearing in (2.6) into those summands with $\alpha_{j+1} \leq \sqrt{\log z}$ and those with $\alpha_{j+1} > \sqrt{\log z}$. The former summands contribute

$$\begin{aligned} &\leq e^{B/\sqrt{\log z}} \sum_{j=1}^{\infty} e^{\xi(2j-1)\mathbb{1}_{j>1}} \frac{(\xi(2j-1) + B/\sqrt{\log z})^{2j-1}}{(2j-1)!} \\ &= \sum_{j=1}^{\infty} e^{\xi(2j-1)\mathbb{1}_{j>1}} \frac{(\xi(2j-1))^{2j-1}}{(2j-1)!} + O_{B,\kappa} \left(\frac{1}{\sqrt{\log z}} \right) \\ &< 0.99967 + O_{B,\kappa} \left(\frac{1}{\sqrt{\log z}} \right). \end{aligned}$$

Since $\alpha_{j+1} > \sqrt{\log z}$ implies that $j \gg \sqrt{\log_2 z}$, and $e^\xi(\xi e) \leq 0.95$, the terms with $\alpha_{j+1} > \sqrt{\log z}$ contribute

$$\leq e^{B/\log 2} \sum_{\alpha_{j+1} > \sqrt{\log z}} e^{\xi(2j-1)} \frac{(\xi(2j-1) + B/\log 2)^{2j-1}}{(2j-1)!} = o_{\kappa,B}(1) \quad (z \rightarrow \infty).$$

Therefore, for large enough z ,

$$E \leq 0.9999.$$

Finally, for R'' we have

$$z_1^{k_1+1} z_2^{k_2} z_3^{k_3} \dots \leq z^{1+2/\alpha_2+4/\alpha_3+6/\alpha_4+\dots} = z^{f(\kappa)}.$$

Invoking Theorem 2.15, the proof is complete. The bounds on $f(\kappa)$ are straightforward, and given as Exercise 2.15 (a). \square

2.4.1. Application: twin primes. We take $\Omega = [1, x] \cap \mathbb{Z}$, $\mathcal{A}_p = \{n \in \Omega : p|n(n+2)\}$, $X = x$. As we saw previously, $g(p) = \rho(p)/p$ with $\rho(2) = 1$, $\rho(p) = 2$ for $p > 2$, so (Ω_0) holds with $\kappa = 2$, as does Ω . Here, $f(2) \leq 8.46$. Taking $z = x^{1/8.5}$ we have

$$\sum_{d \leq z^{f(2)}} \mu^2(d) |r_d| \leq \sum_{d \leq z^{f(2)}} \tau(d) \ll z^{f(2)} \log z \ll x^{0.996},$$

which is negligible. Since $V(z) \gg 1/\log^2 z \gg 1/\log^2 x$ we conclude from Theorem 2.16 that

$$S(\mathcal{A}, z) \gg \frac{x}{\log^2 x}.$$

We conclude that there are $\gg x/\log^2 x$ integers $n \leq x$, such that each of n and $n+2$ have at most 8 prime factors, as these factors are $> z$.

Now we approach the problem as in Example (c) (this is A. R enyi's approach), taking

$$\Omega = \{p+2 : p \text{ prime} \leq x\}, \quad X = \text{li}(x),$$

and $\mathcal{A}_p = \{n \in \Omega : p|n\}$. Here

$$A_d = \pi(x; d, -2) = \frac{\text{li}(x)}{\phi(d)} + r_d,$$

where r_d is expected to be small by the prime number theorem for arithmetic progressions. Taking $g(d) = 1/\phi(d)$, we easily verify the (Ω) holds with $\kappa = 1$. Indeed, for $y \geq 3$, Mertens' bounds give

$$\begin{aligned} \prod_{y \leq p \leq w} (1 - g(p))^{-1} &= \prod_{y \leq p \leq w} \left(1 - \frac{1}{p-1}\right)^{-1} = \prod_{y \leq p \leq w} \left(1 - \frac{1}{p}\right)^{-1} \left(1 - \frac{1}{(p-1)^2}\right)^{-1} \\ &\leq \frac{\log w}{\log y} \left(1 + O\left(\frac{1}{\log y}\right)\right). \end{aligned}$$

For the error terms r_d , we use the famous theorem of Bombieri and Vinogradov:

Theorem 2.17 (Bombieri-A.I. Vinogradov, 1965). *For every $A > 0$ there is a $B > 0$ so that*

$$\sum_{q \leq x^{1/2} (\log x)^{-B}} \max_{y \leq x} \max_{(a,q)=1} \left| \pi(y; q, a) - \frac{\text{li}(y)}{\phi(q)} \right| \ll \frac{x}{(\log x)^A}.$$

In Theorem 2.16, we have $f(1) \leq 4.65$. Take $z = x^{\frac{1}{9.4}}$ so that $z^{f(1)} \leq x^{0.499}$. Hence, Theorem BV implies

$$\sum_{d \leq z^{f(1)}} |r_d| = \sum_{d \leq z^{f(1)}} \left| \pi(x; d, -2) - \frac{\text{li}(x)}{\phi(d)} \right| \ll \frac{x}{(\log x)^{10}}.$$

We conclude that for large x ,

$$S(\mathcal{A}, z) \gg XV(z) \gg \frac{x}{\log^2 x}.$$

Finally, we observe that $S(\mathcal{A}, z)$ counts primes p such that $p+2$ has no prime factor $\leq z$; in particular, $p+2$ has at most 9 prime factors.

2.4.2. *Prime values of polynomials.* Generalizing greatly the study of twin primes, we can use the sieve to study prime values of arbitrary polynomials.

Theorem 2.18. *Let F_1, \dots, F_k be distinct, irreducible polynomials in $\mathbb{Z}[x]$, each with positive leading coefficient. Put $F = F_1 \cdots F_k$, $\ell = \deg(F)$. Suppose (F_1, \dots, F_k) is admissible. Then*

$$(2.21) \quad \#\{n \leq x : F_i(n) \text{ prime for every } i\} \ll_F \frac{x}{\log^k x}.$$

Further, there is an integer $m = O(k\ell)$ such that for large x ,

$$(2.22) \quad \#\{n \leq x : \Omega(F_i(n)) \leq m \ (1 \leq i \leq k)\} \gg_F \frac{x}{\log^k x}.$$

Proof. We will show the upper bound (2.21), leaving (2.22) as an exercise (cf., Exercise 2.13 below). Let x be large, $\Omega = [1, x] \cap \mathbb{N}$, $\mathcal{A}_p = \{n \in \Omega : p|F(n)\}$ for primes p , $X = x$, $z = x^{1/2}$. Generically write

$$\rho_G(d) = \#\{0 \leq n < d : G(n) \equiv 0 \pmod{d}\},$$

where G is any polynomial. As with twin primes, we have

$$A_d = \frac{\rho_F(d)}{d} X + r_d, \quad |r_d| \leq \rho_F(d),$$

and so we set $g(d) = \rho_F(d)/d$. Now ρ_F is multiplicative by the Chinese remainder theorem. Also,

$$\begin{aligned} \rho_F(p) &< p \quad \text{by hypothesis,} \\ \rho_F(p) &\leq \ell \quad \text{by Lagrange's theorem.} \end{aligned}$$

In particular, (Ω_0) holds with $\kappa = \ell$ and $\delta = 1/\ell$. Thus,

$$\begin{aligned} \sum_{d \leq z} |r_d| &\leq \sum_{d \leq x^{1/2}} dg(d) \leq x^{1/2} \sum_{d \in \mathcal{P}(z)} g(d) = x^{1/2} \prod_{p \leq z} (1 + g(p)) \\ &\leq x^{1/2} \prod_{p \leq z} \left(1 + \frac{\ell}{p}\right) \ll_{\ell} x^{1/2} (\log x)^{\ell} \ll_{\ell} x^{2/3}. \end{aligned}$$

By Theorem 2.4 and the trivial lower bound $V(z) \gg_F (\log x)^{-\ell}$, we have

$$S(\mathcal{A}, z) \ll XV(z).$$

As before, the left side is at least as large as the count of $k \leq x$ such that each $F_i(k)$ is prime and $> z$ (and there are $O_F(z)$ values of k with each of $F_i(k)$ prime, and one of them is $\leq z$). It remains to bound $V(z)$ from above. To do this, we need the following two facts:

$$(2.23) \quad \rho_F(p) = \rho_{F_1}(p) + \cdots + \rho_{F_k}(p) \text{ for all but finitely many } p,$$

$$(2.24) \quad \sum_{p \leq y} \frac{\rho_{F_i}(p)}{p} = \log_2 y + C(F_i) + O_{F_i} \left(\frac{1}{\log y} \right) \quad (1 \leq i \leq k)$$

where $C(F_i)$ is a constant depending on F_i . From (2.23) and (2.24) we deduce that

$$\begin{aligned} \log V(z) &= \sum_{p \leq z} \log \left(1 - \frac{\rho_F(p)}{p} \right) = O_F(1) - \sum_{p \leq z} \frac{\rho_F(p)}{p} \\ &= O_F(1) - \sum_{p \leq z} \sum_{j=1}^k \frac{\rho_{F_j}(p)}{p} = -k \log_2 z + O_F(1), \end{aligned}$$

and thus $V(z) \asymp_F (\log z)^{-k}$. In fact, (2.23) and (2.24) imply that (Ω) holds with $\kappa = k$ (this will be needed in the lower bound argument). In conclusion,

$$\#\{k \leq x : F_i(k) \text{ prime for every } i\} \leq O_F(z) + S(\mathcal{A}, z) \ll_F \frac{x}{(\log x)^k}.$$

Proof of (2.23): Suppose the equation in (2.23) does not hold. Then there are $i \neq j$ and some n with $p|F_i(n)$ and $p|F_j(n)$, i.e., $p|(F_i(n), F_j(n))$. As F_i and F_j are distinct, irreducible and have no fixed prime factor (in particular, neither is a multiple of the other), $(F_i, F_j) = 1$ over $\mathbb{Q}[x]$. Hence, there are $G, H \in \mathbb{Q}[x]$ such that $F_i G + F_j H = 1$. Clearing denominators gives $\tilde{G}, \tilde{H} \in \mathbb{Z}[x]$ with $F_i \tilde{G} + F_j \tilde{H} = C_{ij}$, where $C_{ij} \in \mathbb{Z}$. It follows that $p|C_{ij}$. As there are only finitely many pairs i, j , there are finitely many possible p .

Comments on (2.24): this is a consequence of the Prime Ideal Theorem of Landau [93]; see also [22, p. 33–38]. In some special cases, it follows from Mertens theorem for primes in arithmetic progressions, e.g. if $F(x) = x^2 + 1$, then

$$\sum_{p \leq x} \frac{\rho_F(p)}{p} = 1 + 2 \sum_{\substack{p \leq x \\ p \equiv 1 \pmod{4}}} \frac{1}{p} = \log_2 x + O(1).$$

□

2.5. Sieving limits. One sees from Theorem 2.16 the effect of the dimension κ on the quality of the estimates. In order to ensure the remainder terms $\sum |r_d|$ are small, one needs $z^{f(\kappa)}$ to be smaller than the sieving limit for the sieve problem \mathcal{A} (this is generally less than x), hence the range of permissible z is limited by the value of $f(\kappa)$.

Definition 2. In the literature, the sieve limit (or sifting limit) $\beta(\kappa)$, for a given κ , is the infimum of exponents u so that for any sieve problem \mathcal{A} satisfying (g), (r), and (Ω) , we have for some positive c the bound

$$S(\mathcal{A}, z) \geq cXV(z) - \sum_{d \leq z^u} |r_d|.$$

Some authors, e.g. Selberg, refer to $1/\beta(\kappa)$ as the *sieve limit*.

Theorem (2.16) implies that $\beta(\kappa) \leq f(\kappa) \leq 1 + 3.841\kappa$ for all κ and that $\beta(\kappa) \leq 1 + o(1)$ as $\kappa \rightarrow 0^+$. Choosing the parameters α_j in a more optimal manner leads to better bounds for large κ , namely $\beta(\kappa) \leq (c + o(1))\kappa$ where $c = 3.59112\dots$ is the solution of $e^{1+1/c} = c$. See Exercise 2.15 below. This matches the asymptotic upper bound for $\beta(\kappa)$ achievable from the very complicated “ β -sieve”; see [57, Ch. 11].

The exact value of $\beta(\kappa)$ is known only for $\kappa \in [0, 1/2] \cup \{1\}$, in these cases $\beta(\kappa) = 1$ for $\kappa \leq 1/2$ and $\beta(1) = 2$. See [57, Ch. 11] for details. The lower bound $\beta(1) \geq 2$ is clear from Selberg’s examples in Section 1.7.4. The very complicated combinatorial sieves given in [26] give the best known upper bounds on $\beta(\kappa)$ for small κ (less than 10, say), see Table 1. Selberg [124, eq. (14.40)] showed that $\beta(\kappa) \leq 2\kappa + 0.4454$ for sufficiently large κ . The exact value of $\beta(\kappa)$ is unknown in all cases $\kappa > 1/2$ except for $\kappa = 1$.

κ	$\beta(\kappa) \leq$
0.5	1.0
1.0	2.0
2.0	4.2665
3.0	6.6409

TABLE 1. Known upper bounds on the sieving limit $\beta(\kappa)$

2.6. The small z case. Asymptotic formula for the sifting function (Fundamental Lemma). We combine the upper and lower bound sieve theorems to achieve an asymptotic formula for the sifting function when z is small compared with x . The bounds below are of the same strength, as s becomes large, as [70, Theorem 2.5], which is derived from a later, complicated sieve developed by Brun. In particular, this gives the promised asymptotic formula in (1.4) as long as κ is fixed, $z = x^{o(1)}$ and the remainders $|r_d|$ are small enough on average.

Theorem 2.19 (Fundamental Lemma). (a) For any pair (z, D) of positive integers with $2 \leq z \leq D$, there are sieves λ^+ and λ^- satisfying (λ^+) and (λ^-) , respectively, satisfying $|\lambda_d^\pm| \leq 1$ for all d , with support in $\mathcal{D}(z, D) := \{d \in \mathbb{N} : \mu^2(d) = 1, P^+(d) \leq z, d \leq D\}$, and such that for any multiplicative function g satisfying (Ω) , we have

$$\sum_d \lambda^\pm(d)g(d) = \left(1 + O\left(e^{-s \log s + s \log_3 s + O_{\kappa, B}(s)}\right)\right) \prod_{p \leq z} (1 - g(p)),$$

where $s = \frac{\log D}{\log z}$.

(b) Let $\kappa_0 > 0$ and $B_0 > 0$. Assume \mathcal{A} is a sieve problem, such that (g), (r) and that (Ω) holds for some constants $0 \leq \kappa \leq \kappa_0$ and $0 \leq B \leq B_0$. For any $2 \leq z \leq D$, we have

$$S(\mathcal{A}, z) = XV(z) \left(1 + O \left(e^{-s \log s + s \log_3 s + O_{\kappa_0, B_0}(s)} \right) \right) + \Delta \sum_{\substack{d \leq D \\ P^+(d) \leq z}} |r_d|,$$

where $s = \frac{\log D}{\log z}$ and $|\Delta| \leq 1$.

Proof. Firstly, we observe that part (b) is immediate from part (a), the bound $|\lambda_d^\pm| \leq 1$ and (1.8). To prove (a), we take Brun-Hooley sieves, that is, sieves given in Lemma (2.2) (upper bound sieve) and (2.17) (lower bound sieve) and additionally supported on $\mathcal{D}(z, D)$. In light of (2.8), (2.11) and (2.19), it suffices to prove that there is a choice of parameters z_j and k_j such that

$$(2.25) \quad E \ll e^{-s \log s + s \log_3 s + O_{\kappa_0, B_0}(s)}.$$

As before, we will partition the primes in $[2, z]$ as in (2.9) and let k_1, \dots, k_t be nonnegative even integers. Let $s_0(\kappa_0, B_0) \geq 100$ be sufficiently large. When $s \leq s_0(\kappa_0, B_0)$, the trivial lower bound $S(\mathcal{A}, z) \geq 0$ is good enough, and thus we need only establish $E \ll 1$ in the upper bound sieve. We'll take, similar to the proof of Theorem 2.4, the parameters $k_1 = 0$, $k_j = 2^{j-1}$ ($j \geq 2$), and $z_j = z^{1/4^{j-1}}$ for each $j \geq 1$. Then and $d \leq z_1^{k_1} z_2^{k_2} \dots \leq z \leq D$. As before, $L_j \leq L$ for all j , where L is a constant that depends only on κ_0, B_0 . It then follows from (2.6) that $E \ll_{\kappa_0, B_0} 1$, and this implies (2.25) in this case.

When $s > s_0(\kappa_0, B_0)$ we take the parameters

$$\theta = \log s, \quad z_j = z^{1/\theta^{j-1}}, \quad (1 \leq j \leq t),$$

where t is maximally chosen to satisfy (2.9), and

$$k_j = 2 \left\lfloor \frac{s}{2} \left(1 - \frac{1}{\theta} \right) \right\rfloor - 6 + 2j \quad (1 \leq j \leq t).$$

Note that $\theta \geq \log 100 > 4$ and $k_j \leq s(1 - 1/\theta) - 6 + 2j$ for all j . These sieves are supported on integers d satisfying

$$d \leq z_1^{k_1+1} z_2^{k_2} \dots z_t^{k_t} \leq z^{1+(s(1-1/\theta)-6)/(1-1/\theta)+2/(1-1/\theta)^2} \leq z^s = D.$$

In the notation (2.4), we have by (Ω) the bound

$$L_j \leq \kappa \log \theta + \frac{B}{\log z_{j+1}} \leq \kappa_0 \log \theta + 2B_0 =: L.$$

For large enough $s_0(\kappa_0, B_0)$, if $s > s_0(\kappa_0, B_0)$ then

$$k_1 \geq s(1 - 1/\theta) - 6 \geq 3s/4 - 6 \geq 2L.$$

Thus, using Stirling's formula, we find that

$$\begin{aligned}
E &\leq e^L \sum_{j=1}^t \frac{L^{k_j+1}}{(k_j+1)!} \\
&\ll e^L \frac{L^{k_1+1}}{(k_1+1)!} \leq e^L \left(\frac{eL}{k_1+1} \right)^{k_1+1} \\
&\ll e^{O(B_0)} (\log s)^{\kappa_0} \exp \left\{ -k_1 \log k_1 + O(k_1) + k_1 \log(\kappa_0 \log \theta + 2B_0) \right\} \\
&\ll e^{-s \log s + s \log_3 s + O_{\kappa_0, B_0}(s)}.
\end{aligned}$$

This gives (2.25) and completes the proof. \square

2.6.1. Application: Buchstab's function. Buchstab's function

$$\Phi(x, z) = \#\{n \leq x : P^-(n) > z\}$$

is perhaps the most basic sieve function. Here we take $g(p) = 1/p$ for all p so that (Ω) holds with $\kappa = 1$.

Theorem 2.20 (No small prime factors). (i) *Uniformly for $x \geq 0$ and $2 \leq z \leq y$, we have*

$$\Phi(x+y, z) - \Phi(x, z) \ll \frac{y}{\log z};$$

(ii) *Uniformly for $x \geq 2z \geq 4$ we have*

$$\Phi(x, z) \gg \frac{x}{\log z}.$$

(iii) *Uniformly for $\exp\{(\log_2 x)^2\} \leq z \leq x$, we have*

$$\Phi(x, z) = \left(1 + O(e^{-u \log u + O(u \log_3 u)})\right) x \prod_{p \leq z} (1 - 1/p),$$

where $u = \frac{\log x}{\log z}$.

Proof. For (i), we may suppose that $z \leq \sqrt{y}$, for the estimate with $z > \sqrt{y}$ follows from that for $z = \sqrt{y}$. We let $\Omega = (x, x+y] \cap \mathbb{N}$, $X = y$, $\mathcal{A}_p = \{n \in \Omega : p|n\}$, $g(d) = 1/d$ and then (Ω) holds with $\kappa = 1$. Part (i) is then immediate from Theorem 2.4. For parts (ii) and (iii), let $\Omega = [1, x] \cap \mathbb{N}$, $X = x$, $\mathcal{A}_p = \{n \in \Omega : p|n\}$, $g(d) = 1/d$ and again (Ω) holds with $\kappa = 1$. Part (ii) follows from (2.16) when $z \leq x^{1/5}$ and x is large, since $f(1) < 5$ and thus $\sum_{d \leq z^{f(1)}} |r_d| \ll x^{f(1)/5}$. When $x^{1/5} < z \leq x/2$ and x is large, the Prime number theorem implies

$$\Phi(x, z) \geq \pi(x) - \pi(z) \gg \frac{x}{\log x} \gg \frac{x}{\log z}.$$

Finally, when x is small, we have $\Phi(x, z) \geq 1 \gg x/\log z$. This proves (ii).

For part (iii), take $D = \frac{x}{\log x} e^{-u \log u}$ in Theorem 2.19, and define s by $D = z^s$. Then the error terms satisfy

$$\sum_{d \leq D} |r_d| \leq D \ll e^{-u \log u} X V(z)$$

since $V(z) \asymp 1/\log z$. By hypothesis, $u \leq \frac{\log x}{(\log_2 x)^2} \leq \frac{\log x}{\log u}$ and hence

$$s = \frac{u}{\log x} (\log x - \log_2 x - u \log u) = u \left(1 - O\left(\frac{1}{\log u}\right) \right).$$

Inserting this into the conclusion of Theorem 2.19 completes the proof of (iii). \square

2.7. Small κ The petite sieve. In the previous sections, we showed an asymptotic formula for $S(\mathcal{A}, z)$ whenever κ, B are bounded and $\frac{\log D}{\log z} \rightarrow \infty$. In this section, we show an asymptotic formula for $S(\mathcal{A}, z)$ when $D = z^{O(1)}$ and $\kappa \rightarrow 0$. First, we mention a very general principle.

Definition 3. Let \mathcal{A} be a sieve problem, and let p be a prime and $p > w \geq 2$. Then

$$S(\mathcal{A}_p, w) := M\mathbb{P}\left(\mathcal{A}_p \setminus \bigcup_{q \leq w} \mathcal{A}_q\right).$$

This corresponds to $S(\tilde{\mathcal{A}}, w)$, where $\tilde{\mathcal{A}}$ is the sieve problem with space $(\tilde{\Omega}, \mathcal{F}, \mathbb{P})$ inherited from \mathcal{A} , that is, $\tilde{\Omega} = \mathcal{A}_p$, $\tilde{\mathcal{A}}_d = \mathcal{A}_p \cap \mathcal{A}_d$, $\tilde{X} = g(p)X$, $\tilde{g}(d) = g(d)$ and $\tilde{r}_d = r_{pd}$.

In the case where Ω is a finite set, $S(\mathcal{A}_p, w)$ counts those elements of Ω which have property \mathcal{A}_p but not any of the properties \mathcal{A}_q for $q \leq w$.

Lemma 2.21 (Buchstab's identity). Let \mathcal{A} be a sieve problem, and $z > w \geq 2$. Then

$$(2.26) \quad S(\mathcal{A}, z) = S(\mathcal{A}, w) - \sum_{w < p \leq z} S(\mathcal{A}_p, p-1).$$

Proof. Suppose that \mathcal{A}_q does not occur for all primes $q \leq w$, but \mathcal{A}_p does hold for some $p \in (w, z]$. Letting p be the largest such prime and summing over p yields the lemma. \square

Theorem 2.22 (The petite sieve). Let \mathcal{A} be a sieve problem and assume (g) , (r) and define $V(z)$ by (V). Assume g satisfies (Ω) for some $\kappa \in (0, 1]$ and $B > 0$. Then, uniformly for $2 \leq s \leq \log z$ with $\kappa \log s \leq 1$ we have

$$S(\mathcal{A}, z) = \left(1 + O_B\left(\kappa \log s + \frac{s}{\log z} + e^{-\frac{1}{2}s \log s}\right)\right) XV(z) + O\left(\sum_{d \leq z^{1+1/s}} |r_d|\right).$$

Proof. Let

$$w = z^{1/s}$$

so that $w \geq e > 2$. By Buchstab's identity (2.26) and the fact that $S(\mathcal{A}_p, z)$ is decreasing in z , we have

$$S(\mathcal{A}, w) \geq S(\mathcal{A}, z) \geq S(\mathcal{A}, w) - \sum_{w < p \leq z} S(\mathcal{A}_p, w).$$

By Theorem 2.19, with $\kappa_0 = 1$ and $B_0 = B$, we have

$$S(\mathcal{A}, w) = (1 + O_B(e^{-\frac{1}{2}s \log s}))XV(w) + \Delta \sum_{d \leq z} |r_d|$$

where $|\Delta| \leq 1$. By Theorem 2.4, again with $\kappa_0 = 1$ and $B_0 = B$ we have

$$S(\mathcal{A}_p, w) \leq O_B(Xg(p)V(w)) + \sum_{d \leq w} |r_{pd}|.$$

Summing over all $p \in (w, z]$ we use that

$$\begin{aligned} \sum_{w < p \leq z} g(p) &\leq - \sum_{w < p \leq z} \log(1 - g(p)) \\ &\leq \kappa \log\left(\frac{\log z}{\log w}\right) + \frac{B}{\log w} \\ &= \kappa \log s + \frac{Bs}{\log z}. \end{aligned}$$

We conclude that

$$(2.27) \quad S(\mathcal{A}, z) = \left(1 + O_B \left(e^{-\frac{1}{2}s \log s} + \kappa \log s + \frac{s}{\log z} \right)\right) XV(w) + O \left(\sum_{d \leq zw} |r_d| \right).$$

Finally,

$$\begin{aligned} V(z) &\leq V(w) = V(z) \frac{V(w)}{V(z)} \leq V(z) \left(\frac{\log z}{\log w} \right)^\kappa (1 + O_B(1/\log w)) \\ &= V(z) s^\kappa (1 + O_B(1/\log w)) \\ &= V(z) (1 + O_B(\kappa \log s + s/\log z)). \end{aligned}$$

Inserting this into (2.27) completes the proof. \square

Corollary 2.23. *Assume that $z \rightarrow \infty$, $\kappa \rightarrow 0$, and that the remainders satisfy*

$$\sum_{d \leq z^{1+\delta}} |r_d| = o(XV(z))$$

for some fixed $\delta > 0$. Then

$$S(\mathcal{A}, z) \sim XV(z)$$

Proof. Take $s = 2 + \min(\log(1/\kappa), \log_2 z)$ in Theorem 2.22. For large z , $s \geq 1/\delta$. By hypothesis, $s \rightarrow \infty$ and $\frac{s}{\log z} \rightarrow 0$, and $\kappa \log s \rightarrow 0$. \square

2.8. Exercises.

Exercise 2.13. *Prove the lower bound (2.22) in Theorem 2.18.*

Exercise 2.14. *Prove the bounds claimed for $f(\kappa)$ in Theorem 2.16.*

Exercise 2.15. (a) *Let $\gamma(\kappa)$ be the infimum of*

$$k_1 + 1 + \alpha_2 k_2 + \alpha_3 k_3 + \dots$$

over all choices of non-negative, even integers k_i and real numbers $1 = \alpha_1 > \alpha_2 > \dots$ satisfying

$$\sum_{j=1}^{\infty} \left(\frac{\alpha_j}{\alpha_{j+1}} \right)^\kappa \frac{\left(\kappa \log(\alpha_j/\alpha_{j+1}) \right)^{k_j+1}}{(k_j+1)!} < 1.$$

Show that $\beta(\kappa) \leq \gamma(\kappa)$.

(b) *Let $\kappa = 1$. Find more efficient choice of k_1, \dots and α_1, \dots which shows that $\beta(1) < 4.5$. You may use a computer search. Use this to show that there are infinitely many primes p such that $\Omega(p+2) \leq 8$.*

(c) *Prove the asymptotic upper bound $\beta(\kappa) \leq (c + o(1))\kappa$, where $c = 3.59112\dots$ is the solution of $e^{1+c} = c$.*

Exercise 2.16. *Show that for all sufficiently large even N , there is a prime p and a number q with $\Omega(q) \leq 9$ such that $N = p + q$.*

Exercise 2.17. Almost primes in short intervals. *Prove that for every $\delta > 0$, there is a natural number k so that whenever $x \geq x_0(\delta)$, then the interval $(x, x + x^\delta]$ contains an integer q with $\Omega(q) \leq k$.*

Exercise 2.18. Show the equivalence of the following two forms of the Bombieri-Vinogradov Theorem:

$$\forall A > 0 \exists B : \sum_{q \leq x^{1/2}/\log^B x} \max_{(a,q)=1} \max_{2 \leq y \leq x} \left| \pi(y; q, a) - \frac{li(y)}{\phi(q)} \right| \ll_A \frac{x}{(\log x)^A},$$

and

$$\forall A > 0 \exists B : \sum_{q \leq x^{1/2}/\log^B x} \max_{(a,q)=1} \max_{2 \leq y \leq x} \left| \psi(y; q, a) - \frac{y}{\phi(q)} \right| \ll_A \frac{x}{(\log x)^A}.$$

Here

$$\psi(x; q, a) = \sum_{\substack{n \leq x \\ n \equiv a \pmod{q}}} \Lambda(n).$$

Exercise 2.19 (*). Let \mathcal{S} denote the set of integers which are the sum of two squares

- (a) Show that a positive proportion of integers have the form $a^2 + b^2 + 2c^2$ for non-negative integers a, b, c . You may use as a fact that the counting function of \mathcal{S} is $\gg x/\sqrt{\log x}$.
- (a) Show that a positive proportion of integers **do not** have the form $a^2 + b^2 + 2c^2$ for non-negative integers a, b, c .

3. SELBERG'S SIEVE

For any real numbers $\lambda(d)$ satisfying $\lambda(1) = 1$, and for any natural number m , we have

$$\mathbb{1}_{m=1} = \sum_{d|m} \mu(d) \leq \left(\sum_{d|m} \lambda(d) \right)^2.$$

Thus, any choice of $\lambda(d)$ produces a valid upper bound sieve λ^+ with

$$\lambda_e^+ = \sum_{[d_1, d_2]=e} \lambda(d_1)\lambda(d_2).$$

Selberg calls this the Λ^2 -sieve, terminology used also by Friedlander and Iwaniec [57]. Our goal is to optimize the choice of $(\lambda(d))_{d \geq 1}$. Let \mathcal{A} be a sieve problem, and assume (g) and (r) . Then

$$\begin{aligned} S(\mathcal{A}, z) &\leq \sum_{\substack{d_1, d_2 \\ P^+(d_1 d_2) \leq z}} \lambda(d_1)\lambda(d_2) A_{[d_1, d_2]} \\ &\leq X \sum_{\substack{d_1, d_2 \\ P^+(d_1 d_2) \leq z}} \lambda(d_1)\lambda(d_2) g([d_1, d_2]) + \sum_{\substack{d_1, d_2 \\ P^+(d_1 d_2) \leq z}} |\lambda(d_1)\lambda(d_2) r_{[d_1, d_2]}| \\ &=: XG + R, \end{aligned}$$

say. Minimizing $XG + R$ is quite difficult. However, if we restrict the support of $\lambda(d)$ to $d \leq \sqrt{D}$, it is relatively easy to minimize G . Since primes with $g(p) = 0$ do not contribute anything to G , we let

$$P = \prod_{\substack{p \leq z \\ g(p) > 0}} p$$

and restrict the support of $\lambda(d)$ to $d|P$. Define

$$(3.1) \quad h(d) = \prod_{p|d} \frac{g(p)}{1 - g(p)} \quad \text{for } d|P.$$

Since $[d_1, d_2] = \frac{d_1 d_2}{(d_1, d_2)}$ is squarefree, we have

$$g([d_1, d_2]) = \frac{g(d_1)g(d_2)}{g((d_1, d_2))}.$$

Inverting (3.1) gives

$$\frac{1}{g(m)} = \prod_{p|m} \left(1 + \frac{1}{h(p)} \right) = \sum_{d|m} \frac{1}{h(d)} \quad (m|P),$$

so that

$$\begin{aligned} G &= \sum_{d_1|P, d_2|P} \lambda(d_1)\lambda(d_2) g(d_1)g(d_2) \sum_{d|(d_1, d_2)} \frac{1}{h(d)} \\ &= \sum_{d|P} \frac{1}{h(d)} \sum_{\substack{d_1|P, d_2|P \\ d|d_1, d|d_2}} \lambda(d_1)\lambda(d_2) g(d_1)g(d_2) = \sum_{d|P} \frac{1}{h(d)} \left(\sum_{d|m} \lambda(m)g(m) \right)^2. \end{aligned}$$

If we define

$$(3.2) \quad \xi(d) = \frac{\mu(d)}{h(d)} \sum_{d|m} \lambda(d)g(m) \quad (d|P(z), d \leq \sqrt{D}),$$

then we have

$$G = \sum_d h(d)\xi(d)^2.$$

This quadratic form in the $\lambda(d)$ is minimized using Cauchy's inequality. First, we invert (3.2). Since

$$\begin{aligned} \sum_k h(kl)\xi(kl) &= \mu(l) \sum_k \mu(k) \sum_{kl|m} \lambda(m)g(m) \\ &= \mu(l) \sum_{l|m} \lambda(m)g(m) \sum_{k|m/l} \mu(k) = \mu(l)\lambda(l)g(l), \end{aligned}$$

and thus

$$(3.3) \quad \lambda(l) = \frac{\mu(l)}{g(l)} \sum_{l|d} h(d)\xi(d) \quad (l|P).$$

In particular, by Cauchy's inequality,

$$1 = \lambda(1)^2 = \left(\sum_{d \leq \sqrt{D}} h(d)^{1/2} \xi(d) h(d)^{1/2} \right)^2 \leq \left(\sum_{d \leq \sqrt{D}} h(d)\xi(d)^2 \right) J = GJ, \quad J = \sum_{d \leq \sqrt{D}} h(d),$$

with equality if and only if $\xi(d)$ is constant; i.e., $\xi(d) = 1/J$ for every $d \leq \sqrt{D}, d|P$. By (3.3), this is attained by taking

$$(3.4) \quad \lambda(l) = \frac{\mu(l)}{Jg(l)} \sum_{l|d} h(d) = \frac{\mu(l)h(l)}{Jg(l)} \sum_{\substack{m \leq \sqrt{D}/l \\ (m,l)=1}} h(m).$$

We conclude that

$$S(\mathcal{A}, z) \leq \frac{X}{J} + R.$$

To handle R , we need an upper bound on $\lambda(l)$. Observe that for any $l \geq 1$,

$$\begin{aligned} J &= \sum_{k|l} \sum_{\substack{d \leq \sqrt{D} \\ (d,l)=k}} h(d) = \sum_{k|l} h(k) \sum_{\substack{m \leq \sqrt{D}/k \\ (m,l/k)=1}} h(m) \\ &\geq \sum_{k|l} h(k) \sum_{\substack{m \leq \sqrt{D}/l \\ (m,l)=1}} h(m) = \frac{h(l)}{g(l)} \sum_{\substack{m \leq \sqrt{D}/l \\ (m,l)=1}} h(m). \end{aligned}$$

Comparing with (3.4), we see that $|\lambda(l)| \leq 1$ for all l , and therefore that

$$(3.5) \quad R \leq \sum_{\substack{d_1, d_2 \leq \sqrt{D} \\ P^+(d_1 d_2) \leq z}} |r_{[d_1, d_2]}| \leq \sum_{\substack{d \leq D \\ P^+(d) \leq z}} 3^{\omega(d)} |r_d|.$$

Since $h(d) = 0$ for $d \nmid P$, we arrive at the following general theorem.

Theorem 3.1 (Selberg's sieve). *Let \mathcal{A} be a sieve problem, and assume (g) , (r) . Let $z \geq 2$ and $D \geq 1$. Then*

$$S(\mathcal{A}, z) \leq \frac{X}{J} + \sum_{\substack{d_1, d_2 \leq \sqrt{D} \\ P^+(d_1 d_2) \leq z}} |r_{[d_1, d_2]}| \leq \frac{X}{J} + \sum_{\substack{d \leq D \\ P^+(d) \leq z}} 3^{\omega(d)} |r_d|,$$

where $J = \sum_{n \leq \sqrt{D}} \mu^2(n) h(n)$, and h is the multiplicative function defined on primes $p \leq z$ by $h(p) = \frac{g(p)}{1-g(p)}$.

3.1. Application. The Brun-Titchmarsh inequality revisited.

Theorem 3.2 (Brun-Titchmarsh inequality, v.2). *For $x \geq y \geq q \geq 1$ and $(a, q) = 1$, we have*

$$\pi(x; q, a) - \pi(x - y; q, a) \leq \frac{2y}{\phi(q) \log(5y/q)} \left(1 + O\left(\frac{\log_2(5y/q)}{\log(5y/q)}\right) \right).$$

We need the following auxiliary lemma.

Lemma 3.3. *For $k \in \mathbb{N}$ and $x \geq 1$, define*

$$H_k(x) := \sum_{\substack{d \leq x \\ (d, k) = 1}} \frac{\mu^2(d)}{\phi(d)}.$$

Then

- (i) $H_k(x) \geq \frac{\phi(k)}{k} H_1(x)$ for all k, x ;
- (ii) $H_1(x) \geq \log x$ for $x \geq 1$.

Proof. We first write

$$H_1(x) = \sum_{\ell|k} \sum_{\substack{d \leq x \\ (d, k) = \ell}} \frac{\mu^2(d)}{\phi(d)}.$$

Write $d = \ell h$ and observe that any nonzero summand corresponds to squarefree d , so $(h, \ell) = 1$ and $(h, k/\ell) = 1$. Thus, $(h, k) = 1$ and we have

$$H_1(x) = \sum_{\ell|k} \frac{\mu^2(\ell)}{\phi(\ell)} \sum_{\substack{h \leq x/\ell \\ (h, k) = 1}} \frac{\mu^2(h)}{\phi(h)} = \sum_{\ell|k} \frac{\mu^2(\ell)}{\phi(\ell)} H_k(x/\ell) \leq H_k(x) \sum_{\ell|k} \frac{\mu^2(\ell)}{\phi(\ell)}.$$

Inequality (i) follows from the identity

$$\sum_{\ell|k} \frac{\mu^2(\ell)}{\phi(\ell)} = \prod_{p|k} \left(1 + \frac{1}{p-1} \right) = \frac{k}{\phi(k)}.$$

Next, define $s(d) = \prod_{p|d} p$ to be the squarefree kernel of d . Then

$$\sum_{s(d)=m} \frac{1}{d} = \prod_{p|m} \left(\frac{1}{p} + \frac{1}{p^2} + \dots \right) = \frac{\mu^2(m)}{\phi(m)}.$$

Hence, for $x \geq 2$ we have

$$H_1(x) = \sum_{m \leq x} \sum_{s(h)=m} \frac{1}{h} = \sum_{s(h) \leq x} \frac{1}{h} \geq \sum_{h \leq x} \frac{1}{h} \geq \int_1^{\lfloor x+1 \rfloor} \frac{dt}{t} = \log \lfloor x+1 \rfloor \geq \log x. \quad \square$$

Proof of Theorem 3.2. As with the proof of Theorem 2.7, let

$$\Omega = \{x - y < n \leq x : n \equiv a \pmod{q}\}, \quad X = y/q,$$

and let $g(p) = 1/p$ for $p \nmid q$ and $g(p) = 0$ for $p|q$. Then

$$A_d = g(d)X + r_d, \quad |r_d| \leq 1$$

Also

$$S(\mathcal{A}, z) \geq \pi(x; q, a) - \pi(x - y; q, a) - z.$$

In the notation of Theorem 3.1, we have

$$h(d) = \frac{\mu^2(d)}{\phi(d)} \quad \text{for } (d, q) = 1.$$

Let $z = \sqrt{D}$. By Lemma 3.3,

$$J = H_q(\sqrt{D}) \geq \frac{\phi(q)}{2q} \log D.$$

By Theorem 3.1,

$$S(\mathcal{A}, z) \leq \frac{X}{J} + \sum_{d_1, d_2 \leq \sqrt{D}} 1 \leq \frac{X}{J} + D \leq \frac{2y}{\phi(q) \log D} + D,$$

hence

$$\pi(x; q, a) - \pi(x - y; q, a) \leq \frac{2y}{\phi(q) \log D} + D + \sqrt{D}.$$

A near-optimal choice for D is

$$D = \max\left(2, \frac{5y/q}{\log^2(5y/q)}\right),$$

and this gives the theorem upon using that

$$\frac{1}{\log D} = \frac{1}{\log(5y/q)} \left(1 + O\left(\frac{\log_2(5y/q)}{\log(5y/q)}\right)\right).$$

□

3.2. Asymptotic formulas. It is possible, under two-sided bounds on $g(p)$, to obtain an asymptotic formula for J . The theorem below illustrates some useful techniques for analyzing sums of multiplicative functions.

Theorem 3.4. *Let $A_1, A_2, L, \kappa > 0$, and let g be a multiplicative function supported on squarefree integers satisfying*

$$(3.6) \quad 0 \leq g(p) \leq 1 - A_1 \quad (p \text{ prime})$$

and

$$(3.7) \quad -L \leq \sum_{w \leq p \leq y} g(p) \log p - \kappa \log \frac{y}{w} \leq A_2 \quad (2 \leq w \leq y).$$

Let h be the multiplicative function supported on squarefree integers and defined by

$$h(p) = \frac{g(p)}{1 - g(p)} \quad (p \text{ prime}).$$

Then, uniformly for $x \geq 2$,

$$\sum_{n \leq x} \mu^2(n) h(n) = \mathfrak{S}(g) \frac{(\log x)^\kappa}{\Gamma(\kappa + 1)} + O_{\kappa, A_1, A_2}(\mathfrak{S}(g) [(L + 1)(\log x)^{\kappa-1} + (L + 1)^\kappa]),$$

where

$$\mathfrak{S}(g) = \prod_p (1 - g(p))^{-1} (1 - 1/p)^\kappa.$$

Remarks. It is important that the dependence on L be made explicit in the error term, as in many applications L is not uniformly bounded, whereas κ, A_1, A_2 are usually uniformly bounded. That is, we may wish to apply the result with a sequence of functions g_1, g_2, \dots , and typically the same κ, A_1, A_2 will work for every g_i but the corresponding numbers L (call them L_i , say) may not be bounded; see Theorem TP2 below for an example.

The sum on the left side depends only on $g(p)$ for primes $p \leq x$, whereas the singular series is defined in terms of $g(p)$ for all primes p . It might seem more natural to replace the infinite product defining $\mathfrak{S}(g)$ with a finite product over primes $p \leq x$, but the given form of the theorem is easier to apply in practice. The inclusion of “extraneous factors” in $\mathfrak{S}(g)$ does force us to include the additional error term $\mathfrak{S}(g)(L+1)^\kappa$, which is in fact best possible as the following example shows: fix $\kappa > 0$, consider a large L (say going to ∞ as $x \rightarrow \infty$), $g(p) = 0$ for $p < e^{L/2\kappa}$ and $g(p) = \kappa/p$ for $p \geq e^{L/2\kappa}$. One easily verifies (3.6) and (3.7), and computes that $\mathfrak{S}(g) \ll L^{-\kappa}$. If $1 < x < e^{o(L)}$, then the sum in the lemma is just $h(1) = 1$, while the “main term” and first error term on the right side are both $o(1)$.

The second error term $\mathfrak{S}(g)(L+1)^\kappa$ is frequently missing in versions of Theorem 9h appearing in the literature, e.g. some of the recent work on prime gaps [61, Lemma 4], [97, Lemma 6.1]. These two works ultimately depend on [70, Lemma 5.3 (2.5)], which claims, in our notation, that

$$\prod_{p \leq z} (1 - g(p)) = \mathfrak{S}(g)^{-1} \frac{e^{-\gamma\kappa}}{(\log z)^\kappa} \left(1 + O\left(\frac{L+1}{\log z}\right) \right)$$

for all $z \geq 2$. The above example clearly shows this claim to be false in some cases when $2 \leq z < e^{o(L)}$. The error in the proof can be traced to [70, p. 146], two lines after (2.7), where it is written that $(1 + O(L/\log z))^{-1} = (1 + O(L/\log z))$, a relation which is only true when $z > e^{CL}$ for some positive constant C .

Proof. We will use a technique due to E. Wirsing. Assume throughout that g and h are supported on squarefree integers, so that all sums are over squarefree integers, and let

$$H(x) = \sum_{n \leq x} h(n).$$

By partial summation,

$$H(x) \log x = \sum_{n \leq x} h(n) \left(\log n + \log \frac{x}{n} \right) = \sum_{n \leq x} h(n) \log n + \int_1^x \frac{H(u)}{u} du.$$

We rewrite the right hand sum as

$$\sum_{n \leq x} h(n) \log n = \sum_{n \leq x} h(n) \sum_{p \leq x} \log p = \sum_{p \leq x} \log p \sum_{\substack{m \leq x/p \\ p \nmid m}} h(p)h(m).$$

Using the relation $h(p) = g(p) + g(p)h(p)$, the right side transforms into

$$\begin{aligned}
&= \sum_{p \leq x} g(p) \log p \left\{ \sum_{m \leq x/p} h(m) - \sum_{\substack{m \leq x/p \\ p|m}} h(m) + h(p) \sum_{\substack{m \leq x/p \\ p \nmid m}} h(m) \right\} \\
&= \sum_{p \leq x} g(p) \log p \left\{ \sum_{m \leq x/p} h(m) - h(p) \sum_{\substack{l \leq x/p^2 \\ p \nmid l}} h(l) + h(p) \sum_{\substack{m \leq x/p \\ p \nmid m}} h(m) \right\} \\
&= \sum_{p \leq x} g(p) \log p \left\{ \sum_{m \leq x/p} h(m) + h(p) \sum_{\substack{x/p^2 < m \leq x/p \\ p \nmid m}} h(m) \right\}.
\end{aligned}$$

Interchanging the order of summation yields

$$(3.8) \quad \sum_{n \leq x} h(n) \log n = \sum_{m \leq x} h(m) \left\{ \sum_{p \leq x/m} g(p) \log p + \sum_{\substack{\sqrt{x/m} < p \leq x/m \\ p \nmid m}} g(p) h(p) \log p \right\}.$$

Applying (3.7) (with $y = w = p$) followed by (3.6), we see that for every p ,

$$g(p) \leq \frac{A_2}{\log p} \quad \text{and} \quad h(p) \leq \frac{A_2 / \log p}{A_1}.$$

Hence, by another application of (3.7), we obtain

$$\sum_{\sqrt{x/m} \leq p \leq x/m} g(p) h(p) \log p \leq \frac{A_2 / A_1}{\log \sqrt{x/m}} \sum_{\sqrt{x/m} \leq p \leq x/m} g(p) \log p \ll 1 \quad (m \leq x/4),$$

the sum being trivially $O(1)$ when $m > x/4$ (here and throughout the proof, constants implied by O -symbols may depend on κ, A_1, A_2 but not on any other parameter). By (3.7),

$$\sum_{p \leq x/m} g(p) \log p = \kappa \log \frac{x}{m} + O(L + 1),$$

and thus relation (3.8) becomes

$$\sum_{n \leq x} h(n) \log n = \sum_{m \leq x} h(m) \left\{ \kappa \log \frac{x}{m} + O(L + 1) \right\} = \kappa \int_1^x \frac{H(u)}{u} du + O((L + 1)H(x)).$$

Hence

$$H(x) \log x = (\kappa + 1) \int_1^x \frac{H(u)}{u} du + \Delta^*(x), \quad \Delta^*(x) \ll (L + 1)H(x).$$

It is convenient to slightly alter this relation, using the fact that $H(u) = 1$ for $1 \leq u < 2$. Thus

$$(3.9) \quad H(x) \log x = (\kappa + 1) \int_2^x \frac{H(u)}{u} du + \Delta(x) \quad (x \geq 2), \quad \Delta(x) \ll (L + 1)H(x).$$

We treat $\Delta(x)$ like an error term, and consider the integral equation for H given by (3.9). The ‘‘unperturbed’’ equation $f(x) \log x = (\kappa + 1) \int_2^x f(u)/u du$ has general solution $f(t) = C(\log t)^\kappa$ for some constant C , and our aim is to prove an asymptotic of this shape for $H(x)$. First, we bound $\Delta(x)$ using the crude estimate

$$(3.10) \quad H(x) \leq \prod_{p \leq x} (1 + h(p)) = S(x) \prod_{p \leq x} \left(1 - \frac{1}{p}\right)^{-\kappa} \ll (\log x)^\kappa \mathfrak{S}(x),$$

where

$$S(x) = \prod_{p \leq x} (1 - g(p))^{-1} (1 - 1/p)^\kappa.$$

We must relate $S(x)$ to $\mathfrak{S}(g)$ by estimating the contribution of the large primes $p > x$ to $\mathfrak{S}(g)$; that is, the “extraneous” primes that are not involved in the sum $\sum_{n \leq x} h(n)$ (cf. the Remarks). Let $x \geq 2$. Now

$$\log(S(x)/\mathfrak{S}(g)) = \log \prod_{p > x} (1 - g(p))(1 - 1/p)^{-\kappa} \leq \sum_{p > x} \left(\frac{\kappa}{p} - g(p) + \frac{\kappa}{p^2} \right).$$

By (3.7) and partial summation, when $x \geq e^{L+1}$ we get

$$\sum_{p > x} \frac{\kappa}{p} - g(p) = \sum_{p > x} \frac{\frac{\kappa \log p}{p} - g(p) \log p}{\log p} = \int_x^\infty \sum_{x < p \leq t} \left(\frac{\kappa \log p}{p} - g(p) \log p \right) \frac{dt}{t \log^2 t} \ll \frac{L+1}{\log x} \ll 1.$$

When $x < e^{L+1}$, however, we do better using the trivial observation $g(p) \geq 0$:

$$\sum_{p > x} \frac{\kappa}{p} - g(p) \leq \sum_{x < p \leq e^{L+1}} \frac{\kappa}{p} + \sum_{p > e^{L+1}} \frac{\kappa}{p} - g(p) = \kappa \log \left(\frac{L+1}{\log x} \right) + O(1).$$

Therefore we have

$$(3.11) \quad S(x) = \mathfrak{S}(g) \frac{S(x)}{\mathfrak{S}(g)} \ll \left(1 + \left(\frac{L+1}{\log x} \right)^\kappa \right) \mathfrak{S}(g).$$

The example described in the Remarks shows that (3.11) is in fact best possible. Combining (3.11) with (3.10) yields the estimates

$$(3.12) \quad H(x) \ll ((\log x)^\kappa + (L+1)^\kappa) \mathfrak{S}(g) \quad (x \geq 2),$$

$$(3.13) \quad \Delta(x) \ll ((L+1)(\log x)^\kappa + (L+1)^{\kappa+1}) \mathfrak{S}(g) \quad (x \geq 2).$$

Returning to (3.9), we replace x with t , divide through by $t(\log t)^{\kappa+2}$ and integrate from 2 to x . This gives

$$\int_2^x \frac{H(t)}{t(\log t)^{\kappa+1}} dt - \int_2^x \frac{\kappa+1}{t(\log t)^{\kappa+2}} \int_2^t \frac{H(u)}{u} du = \int_2^x \frac{\Delta(t)}{t(\log t)^{\kappa+2}} dt.$$

After interchanging the order of integration, we see that the double integral equals

$$\int_2^x \frac{H(u)}{u} \left(\frac{1}{(\log u)^{\kappa+1}} - \frac{1}{(\log x)^{\kappa+1}} \right) du,$$

which implies that

$$\int_2^x \frac{H(u)}{u} du = (\log x)^{\kappa+1} \int_2^x \frac{\Delta(t)}{t(\log t)^{\kappa+2}} dt.$$

Comparing this with (3.9) yields

$$(3.14) \quad H(x) = (\kappa+1)(\log x)^\kappa \int_2^x \frac{\Delta(t)}{t(\log t)^{\kappa+2}} dt + \frac{\Delta(x)}{\log x} \quad (x \geq 2).$$

By (3.13), the integral above converges as $x \rightarrow \infty$ (the tail being $\ll (L+1)\mathfrak{S}(g)/\log x$ for $x > e^{L+1}$), thus

$$\int_2^\infty \frac{\Delta(t)}{t(\log t)^{\kappa+2}} dt = C$$

for some constant C . Therefore, combining (3.14) and (3.13) (when $x \geq e^{L+1}$) and (3.12) (when $x < e^{L+1}$), we conclude that

$$(3.15) \quad H(x) = C(\kappa + 1)(\log x)^\kappa + O\left(\mathfrak{S}(g) \left[(L+1)(\log x)^{\kappa-1} + (L+1)^\kappa \right]\right) \quad (x \geq 2).$$

It remains to determine C . For real $s > 0$ let

$$\zeta_h(s) := \sum_{m=1}^{\infty} h(m)m^{-s} = s \int_1^{\infty} H(x)x^{-s-1} dx = s \int_0^{\infty} H(e^t)e^{-st} dt.$$

By (3.15), as $s \rightarrow 0^+$ we have

$$\zeta_h(s) \sim sC(\kappa + 1) \int_0^{\infty} t^\kappa e^{-st} dt = s^{-\kappa}C(\kappa + 1) \int_0^{\infty} u^\kappa e^{-u} du = s^{-\kappa}C(\kappa + 1)\Gamma(\kappa + 1).$$

Since $\zeta(s+1) \sim \frac{1}{s}$ as $s \rightarrow 0^+$, we obtain

$$\lim_{s \rightarrow 0^+} \zeta(s+1)^{-\kappa} \zeta_h(s) = C(\kappa + 1)\Gamma(\kappa + 1).$$

On the other hand,

$$\zeta(s+1)^{-\kappa} \zeta_h(s) = \prod_p \left(1 - \frac{1}{p^{s+1}}\right)^\kappa \left(1 + \frac{h(p)}{p^s}\right).$$

Using (3.7), we see that the Euler product is uniformly convergent for $s \geq 0$ (Exercise). Therefore,

$$C(\kappa + 1)\Gamma(\kappa + 1) = \lim_{s \rightarrow 0^+} \prod_p \left(1 - \frac{1}{p^{s+1}}\right)^\kappa \left(1 + \frac{h(p)}{p^s}\right) = \prod_p \left(1 - \frac{1}{p}\right)^\kappa (1 + h(p)) = \mathfrak{S}(g). \quad \square.$$

3.3. Application: twin primes.

Theorem 3.5. *Let k be an even, positive integer. Then, uniformly in $k \leq x$,*

$$\#\{p \leq x : p+k \text{ prime}\} \leq C \prod_{\substack{p|k \\ p>2}} \left(\frac{p-1}{p-2}\right) \frac{x}{\log^2 x} \left(4 + O\left(\frac{\log_2 x}{\log x}\right)\right),$$

where

$$C = 2 \prod_p \left(1 - \frac{1}{(p-1)^2}\right)$$

is the “twin prime constant”.

Proof. Let $\Omega = \{p+k : p \leq x\}$. Then

$$A_d = Xg(d) + r_d, \quad X = \text{li}(x), \quad g(d) = \begin{cases} 1/\phi(d) & \text{if } (d, k) = 1 \\ 0 & \text{if } (d, k) > 1. \end{cases}$$

Let $D = z = x^{1/2}(\log x)^{-B}$, where B is sufficiently large. We have $|r_d| \ll x/d$ trivially, and therefore by the Bombieri-Vinogradov theorem and Cauchy's inequality,

$$\begin{aligned} \sum_{d \leq D} 3^{\omega(d)} \mu^2(d) |r_d| &\ll \sum_{d \leq D} \mu^2(d) 3^{\omega(d)} \left(\frac{x}{d}\right)^{1/2} |r_d|^{1/2} \\ &\leq x^{1/2} \left(\sum_{d \leq D} \frac{\mu^2(d) 9^{\omega(d)}}{d} \right)^{1/2} \left(\sum_{d \leq D} |r_d| \right)^{1/2} \\ &\ll x^{1/2} \left(\prod_{p \leq D} \left(1 + \frac{9}{p}\right) \right)^{1/2} \left(\frac{x}{(\log x)^{20}} \right)^{1/2} \ll \frac{x}{(\log x)^5}. \end{aligned}$$

Since $g(p) = \frac{1}{p-1}$ for primes $p \nmid k$, the hypotheses of Theorem 3.4 hold with $\kappa = 1$, A_1 and A_2 absolute constants, and with

$$L = O(1) + \sum_{p|k} \frac{\log p}{p-1} \ll \sum_{p=O(\log k)} \frac{\log p}{p-1} \ll \log_2 k.$$

We also have $h(p) = \frac{1}{p-2}$ for $p \nmid k$. Theorem 3.4 implies that

$$J = \mathfrak{S}(g) \left(\log \sqrt{D} + O(\log_2 k) \right) = \mathfrak{S}(g) \left(\frac{1}{4} \log x + O(\log_2 x) \right),$$

where

$$\mathfrak{S}(g) = \frac{1}{2C} \prod_{\substack{p|k \\ p > 2}} \frac{p-2}{p-1}.$$

Finally, Theorem 3.1 gives

$$\begin{aligned} \#\{p \leq x : p+k \text{ prime}\} &\leq D + S(\mathcal{A}, D) \leq D + \frac{X}{J} + \sum_{d \leq D} \mu^2(d) 3^{\omega(d)} |r_d| \\ &\leq C \prod_{\substack{p|k \\ p > 2}} \left(\frac{p-1}{p-2} \right) \frac{x}{\log^2 x} \left(4 + O\left(\frac{\log_2 x}{\log x} \right) \right). \quad \square \end{aligned}$$

Remarks. Assuming the Elliott-Halberstam conjecture, we may take $D = x^{1-\varepsilon}$ for any positive ε in the above argument, and replace the 4 with $2 + o(1)$ in the conclusion. This is only a factor two worse than the Hardy-Littlewood conjectured asymptotic formula for the left hand side.

For *fixed* k , Bombieri, Friedlander and Iwaniec showed that one may replace 4 with 3.5 (the error term is not uniform in k).

Using the very same analysis, one can also prove, for even $N \geq 4$,

$$\#\{p_1, p_2 : N = p_1 + p_2\} \leq C \prod_{\substack{p|N \\ p > 2}} \frac{p-1}{p-2} \frac{N}{\log^2 N} \left(4 + O\left(\frac{\log_2 N}{\log N} \right) \right).$$

We leave this as an exercise.

3.4. Selberg's sieve is best possible in dimension 1. Consider Selberg's example $\Omega = \{n \leq x : \lambda(n) = -1\}$, where λ is Liouville's function. As before, we saw that $(R(\theta, A))$ holds for all $\theta < 1$ and $A > 0$, $X = x/2$, $g(d) = 1/d$ and thus $h(p) = 1/(p-1)$. Take $z = D = x^{1/2-\varepsilon}$ for small, positive ε . In Theorem 3.4, we have $\mathfrak{S} = 1$, and so by Theorem 3.1,

$$S(\mathcal{A}, z) \leq \frac{X}{J} + O\left(\frac{x}{\log^5 x}\right) = \frac{x}{(1-2\varepsilon)\log x} + O\left(\frac{x}{\log^2 x}\right).$$

But $S(\mathcal{A}, z) = \pi(x) - \pi(\sqrt{x}) + 1 \sim x/\log x$ by the prime number theorem. Thus, Selberg's upper bound sieve cannot be improved, in general, for $\kappa = 1$.

3.5. Exercises.

Exercise 3.1. As in the proof of Lemma 3.3, let

$$H_1(x) = \sum_{n \leq x} \frac{\mu^2(n)}{\phi(n)}.$$

Show that $H_1(x) = \log x + c + o(1)$, where

$$c = \gamma + \sum_p \frac{\log p}{p(p-1)} = 1.332\dots$$

and $\gamma = 0.5772\dots$ is Euler's constant.

Exercise 3.2. Prove that for even $N \geq 4$,

$$\#\{p_1, p_2 : N = p_1 + p_2\} \leq C \prod_{\substack{p|N \\ p>2}} \frac{p-1}{p-2} \frac{N}{\log^2 N} \left(4 + O\left(\frac{\log_2 N}{\log N}\right)\right).$$

Exercise 3.3. (Asymptotic for J in Selberg's sieve). Let $A_1, A_2, L, \kappa > 0$, and let g be a multiplicative function satisfying (3.6) and (3.7). Let h be the multiplicative function defined by $h(p) = \frac{g(p)}{1-g(p)}$ for prime p .

(i) Prove that uniformly for $2 \leq w \leq y$ and $s \geq 0$,

$$\prod_{w \leq p \leq y} \left(1 - \frac{1}{p^{s+1}}\right)^\kappa \left(1 + \frac{h(p)}{p^s}\right) = 1 + O\left(\frac{L+1}{\log w}\right).$$

The implied constant in the O -term may depend only on A_1, A_2, L, κ . Hint: be careful. You may want to consider separately the cases $w < e^{L+1}$ and $w \geq e^{L+1}$.

(ii) Use (i) to show that

$$\lim_{s \rightarrow 0^+} \prod_p \left(1 - \frac{1}{p^{s+1}}\right)^\kappa \left(1 + \frac{h(p)}{p^s}\right) = \prod_p \left(1 - \frac{1}{p}\right)^\kappa (1 + h(p)).$$

4. SMOOTH NUMBERS

In what follows we will need the Erdős notation for iterates of the logarithm:

$$\log_k x = \underbrace{\log \cdots \log x}_k.$$

The basic function

$$\Psi(x, y) = \#\{n \leq x : P^+(n) \leq y\}$$

is widely used in number theory. In contrast with $\Phi(x, z)$, which eliminates numbers with small prime factors, $\Psi(x, y)$ eliminates numbers with large prime factors. One can use the small sieve (Theorem 2.4) to bound $\Psi(x, y)$ but we obtain only

$$\Psi(x, y) \ll x \frac{\log y}{\log x}$$

with no lower bound. The truth, however, is very different, owing to the non-independence of large primes dividing n , e.g. the events $p|n$ and $p'|n$ are exclusive if $p > p' > \sqrt{x}$.

Theorem 4.1. *Uniformly for $x \geq 10$ and $\log x \leq y \leq x$ we have*

$$\Psi(x, y) = xe^{-u \log u + O(u \log_2(10u))}, \quad u = \frac{\log x}{\log y}.$$

Remarks. There is a change of behavior around $y = \log x$, due to the fact that for smaller y , $\prod_{p \leq y} p < x$, and this forces at least some of the exponents of prime dividing n to be large.

We note some special cases which we will find useful for applications:

$$(4.1) \quad \Psi(x, \log x) = \exp \left\{ O \left(\frac{(\log x) \log_3 x}{\log_2 x} \right) \right\} = x^{o(1)} \quad (x \rightarrow \infty),$$

$$(4.2) \quad \Psi(x, (\log x)^c) = x^{1-1/c+o(1)} \quad (x \rightarrow \infty)$$

for any fixed $c \geq 1$, and

$$(4.3) \quad \Psi(x, x^{c(\log_3 x)/\log_2 x}) = \frac{x}{(\log x)^{c+o(1)}} \quad (x \rightarrow \infty).$$

We first need a combinatorial lemma, which is similar to devices we used to develop the Brun-Hooley sieve.

Lemma 4.2. *Let I be a finite set of positive integers, and $k \in \mathbb{N}$. Then*

$$\sum_{\substack{n_1, \dots, n_k \in I \\ n_1 < n_2 < \dots < n_k}} \frac{1}{n_1 \cdots n_k} \geq \frac{1}{k!} \left(\sum_{n \in I} \frac{1}{n} - \frac{k-1}{\min I} \right)^k,$$

provided that the expression in parentheses is ≥ 0 .

Proof. This is straightforward. We have

$$\begin{aligned} \sum_{\substack{n_1, \dots, n_k \in I \\ n_1 < n_2 < \dots < n_k}} \frac{1}{n_1 \cdots n_k} &= \frac{1}{k!} \sum_{\substack{n_1, \dots, n_k \in I \\ \text{distinct}}} \frac{1}{n_1 \cdots n_k} \\ &= \frac{1}{k!} \sum_{n_1 \in I} \frac{1}{n_1} \sum_{\substack{n_2 \in I \\ n_2 \neq n_1}} \frac{1}{n_2} \cdots \sum_{\substack{n_k \in I \\ n_k \notin \{n_1, \dots, n_{k-1}\}}} \frac{1}{n_k}. \end{aligned}$$

Each sum over n_i is at least $\sum_{n \in I} 1/n - (i-1)/\min I$, independent of the choice of n_1, \dots, n_{i-1} , and the proof is complete. \square

Proof of Theorem 4.1. We begin with the upper bound, and we will in fact prove a stronger bound

$$(4.4) \quad \Psi(x, y) \leq x e^{-u \log u + O(u)}.$$

Define

$$\alpha = 1 - \frac{\log u}{\log y}.$$

By our hypothesis that $\log x \leq y \leq x$,

$$(4.5) \quad 1 \leq u \leq \frac{\log x}{\log_2 x}, \quad \frac{\log_3 x}{\log_2 x} \leq \alpha \leq 1.$$

For all $w > 0$, $\log(w^\alpha) \leq w^\alpha$ and thus $\log w \leq \alpha^{-1} w^\alpha$. Hence,

$$(4.6) \quad (\log x) \Psi(x, y) = \sum_{\substack{n \leq x \\ P^+(n) \leq y}} \log(x/n) + \log n \leq \alpha^{-1} x^\alpha S + \sum_{\substack{n \leq x \\ P^+(n) \leq y}} \sum_{p^a | n} \log p,$$

where

$$S = \sum_{P^+(n) \leq y} \frac{1}{n^\alpha}.$$

In the double-sum on the right side of (4.6), let $n = p^a m$, and separate into cases depending on $a = 1$ or $a > 1$. The $a = 1$ terms contribute

$$\leq \sum_{\substack{m \leq x \\ P^+(m) \leq y}} \sum_{p \leq \min(y, x/m)} \log p \ll \sum_{\substack{m \leq x \\ P^+(m) \leq y}} \min(y, x/m) \leq \sum_{P^+(m) \leq y} y^{1-\alpha} \left(\frac{x}{m}\right)^\alpha = u x^\alpha S.$$

The terms with $a > 1$ contribute

$$\leq \sum_{\substack{p \leq y \\ 2 \leq a \ll \log x}} \log p \sum_{\substack{m \leq x/p^a \\ P^+(m) \leq y}} 1 \leq \sum_{\substack{p \leq y \\ 2 \leq a \ll \log x}} \log p \sum_{P^+(m) \leq y} \left(\frac{x}{p^a m}\right)^\alpha = x^\alpha S T,$$

where

$$T = \sum_{\substack{p \leq y \\ 2 \leq a \ll \log x}} \frac{\log p}{p^{a\alpha}}.$$

If $\alpha \geq 2/3$ then clearly $T \ll 1$. If $0 < \alpha < 2/3$ then $y \leq (\log x)^3$ and $u \geq \frac{\log x}{3 \log_2 x}$, thus crudely

$$T \ll (\log x) \sum_{p \leq y} \log p \ll y \log x \ll (\log x)^4 \ll u^5.$$

Putting together the $a = 1$ and $a > 1$ terms, we conclude from (4.5) and (4.6) that

$$(4.7) \quad (\log x) \Psi(x, y) \ll x^\alpha S (\alpha^{-1} + u + u^5) \ll u^5 x^\alpha S = x u^5 e^{-u \log u} S.$$

It remains to bound S . We have

$$S = \prod_{p \leq y} \left(1 + \frac{1}{p^\alpha} + \frac{1}{p^{2\alpha}} + \dots\right) = \prod_{p \leq y} \left(1 + \frac{1}{p^\alpha - 1}\right) \leq \exp \left\{ \sum_{p \leq y} \frac{1}{p^\alpha - 1} \right\}.$$

First consider the case $\alpha \geq 2/3$. For any $0 \leq z \leq 1$ and $c \geq 0$ we have

$$e^{cz} = \sum_{k=0}^{\infty} \frac{(cz)^k}{k!} \leq 1 + z \sum_{k=1}^{\infty} \frac{c^k}{k!} \leq 1 + e^c z,$$

hence

$$\frac{1}{p^\alpha} = \frac{1}{p} e^{(\log u) \frac{\log p}{\log y}} \leq \frac{1}{p} \left(1 + e^{\log u} \frac{\log p}{\log y} \right).$$

Thus, by Mertens bounds,

$$\begin{aligned} \log S &\leq O(1) + \sum_{p \leq y} \frac{1}{p^\alpha} \\ &\leq O(1) + \sum_{p \leq y} \frac{1}{p} + \frac{u}{\log y} \sum_{p \leq y} \frac{\log p}{p} \\ &\leq \log_2 y + O(u + 1). \end{aligned}$$

Thus, $S \ll (\log y) e^{O(u)}$. Combining this with (4.7), we get (4.4) in this case.

Now assume $0 < \alpha < 2/3$. Then $y \leq u^3 \leq \log^3 x$ and $u \asymp \frac{\log x}{\log_2 x}$. We then have, using (4.5) again,

$$\begin{aligned} \log S &\ll \sum_{p \leq 2^{1/\alpha}} \frac{1}{\alpha \log p} + \int_1^y \frac{dt}{t^\alpha} \\ &\ll \alpha^{-1} 2^{1/\alpha} + \frac{y^{1-\alpha}}{1-\alpha} \\ &\ll (\log x)^{o(1)} + u \ll u. \end{aligned}$$

Again, plugging this into (4.7) yields the claimed upper bound in (4.4).

Now we prove the lower bound in Theorem 4.1. This breaks into two cases,

- (i) $\log x \leq y \leq \exp\{(\log_2 x)^{10}\}$;
- (ii) $\exp\{(\log_2 x)^{10}\} \leq y \leq x$.

In each case we may assume that $x \geq x_0$, a sufficiently large constant, since for $x \leq x_0$, $\Psi(x, y) \geq 1$ and the result follows.

We begin with the easier case (i), following ideas from Tenenbaum [127, Ch. III.5.1]. Here

$$(4.8) \quad \frac{\log x}{(\log_2 x)^{10}} \leq u \leq \frac{\log x}{\log_2 x}.$$

Let $v = [u]$ and $k = \pi(y)$. Let p_1, \dots, p_k be the primes $\leq y$. Then $\Psi(x, y)$ counts at least every number of the form $p_1^{\nu_1} \cdots p_k^{\nu_k}$ where $\nu_1 + \cdots + \nu_k \leq v$. Thus,

$$\Psi(x, y) \geq \binom{k+v}{v}.$$

By (4.8), $u \ll y/\log y \asymp k$. Thus, by Stirling's formula and $v = u + O(1)$, we deduce

$$\begin{aligned} \log \Psi(x, y) &\geq (k+v) \log(k+v) - k \log k - v \log v + O(\log(k+v)) \\ &= (k+u) \log(k+u) - k \log k - u \log u + O(\log y) \\ &= -u \log u + u \log k + (k+u) \log(1+u/k) + O(\log y). \end{aligned}$$

Again, (4.8) implies that $\log_2 y \ll \log_3 x \ll \log_2 u$, hence

$$u \log k = u \log y + O(u \log_2 y) = \log x + O(u \log_2 u).$$

Also,

$$(k+u) \log(1+u/k) \leq \frac{(k+u)u}{k} \leq u + \frac{u^2}{k} \ll u.$$

Hence,

$$\log \Psi(x, y) \geq \log x - u \log u + O(u \log_2 u),$$

as desired.

In case (ii), we will first show a weaker bound

$$(4.9) \quad \Psi(x, y) \gg x e^{-3u \log u} \quad (1 \leq y \leq x).$$

If $y < \log x$ then $3u \log u > \log x$ and (4.9) is trivial, and if $\log x \leq y \leq \exp\{(\log_2 x)^{10}\}$ then (4.9) follows from the bound proved in case (i). Now suppose $y > \exp\{(\log_2 x)^{10}\}$. Let $k = \lfloor u \rfloor + 1$ and let $I = \mathbb{N} \cap (x^{\frac{1}{k+1}}, x^{\frac{1}{k}}]$. Then $\Psi(x, y)$ counts all numbers of the form $n = p_1 \cdots p_k m \leq x$ with $p_i \in I$ (these numbers are distinct since $m \leq x^{\frac{1}{k+1}}$). We observe that

$$x^{\frac{1}{k+1}} \geq x^{\frac{1}{u+2}} \geq x^{\frac{1}{3u}} = y^{1/3} > \exp\{(\log_2 x)^9\}.$$

By the Prime Number Theorem, we thus have for some constant $c > 0$

$$\sum_{p \in I} \frac{1}{p} = \log \left(\frac{k+1}{k} \right) + O\left(e^{-c\sqrt{\log x^{1/(k+1)}}}\right) = \log \left(\frac{k+1}{k} \right) + O(1/\log^{10} x).$$

Hence, by Lemma 4.2,

$$\begin{aligned} \Psi(x, y) &\geq \sum_{\substack{p_1, \dots, p_k \in I \\ p_1 < p_2 < \dots < p_k}} \left\lfloor \frac{x}{p_1 \cdots p_k} \right\rfloor \geq \sum_{\substack{p_1, \dots, p_k \in I \\ p_1 < p_2 < \dots < p_k}} \frac{x}{2p_1 \cdots p_k} \\ &\geq \frac{x/2}{k!} \left(\sum_{p \in I} \frac{1}{p} - \frac{k}{x^{\frac{1}{k+1}}} \right)^k \\ &\geq \frac{x}{k!} \left(\log(1+1/k) - O\left(\frac{1}{k^2 \log^2 x}\right) \right)^k \\ &\gg \frac{x}{k^k k!} \gg x e^{-2k \log k + O(k)} \end{aligned}$$

and (4.9) follows.

Now we use (4.9) as a bootstrap for a better estimate. Suppose that $\exp\{(\log_2 x)^{10}\} \leq y \leq x$. Assume $u \geq e^4$, since the desired lower bound in Theorem 4.1 follows from (4.9) for $1 \leq u \leq e^4$. Let $k = \lfloor u \rfloor + 1$, let $\eta = \frac{1}{\log u} \leq \frac{1}{4}$ and $I = \mathbb{N} \cap (y^{1-2\eta}, y^{1-\eta}]$. Consider integers $n = p_1 \cdots p_k m$, where $p_i \in I$ for all i , $p_1 < \dots < p_k$ and $P^+(m) \leq y^{1-2\eta}$. These integers are distinct and counted by $\Psi(x, y)$. Then

$$\Psi(x, y) \geq \sum_{\substack{p_1, \dots, p_k \in I \\ p_1 < \dots < p_k}} \Psi\left(\frac{x}{p_1 \cdots p_k}, y^{1-2\eta}\right).$$

Now $p_1 \cdots p_k \geq y^{k(1-2\eta)} \geq y^{u(1-2\eta)} = x^{1-2\eta}$ and thus

$$\frac{x}{p_1 \cdots p_k} \leq x^{2\eta} = y^{2\eta u} \leq (y^{1-2\eta})^{4\eta u},$$

using that $\eta \leq \frac{1}{4}$. Hence, by (4.9),

$$\begin{aligned} \Psi(x, y) &\gg x \sum_{\substack{p_1, \dots, p_k \in I \\ p_1 < \dots < p_k}} \frac{1}{p_1 \cdots p_k} e^{-12\eta u \log(4\eta u)} \\ &\gg x e^{-O(u)} \sum_{\substack{p_1, \dots, p_k \in I \\ p_1 < \dots < p_k}} \frac{1}{p_1 \cdots p_k}. \end{aligned}$$

Invoking Lemma 4.2 and using the Prime Number Theorem as in case (i), we conclude that

$$\begin{aligned} \Psi(x, y) &\gg \frac{x e^{-O(u)}}{k!} \left(\sum_{p \in I} \frac{1}{p} + O\left(\frac{1}{k^{100} \log x}\right) \right)^k \\ &\gg \frac{x e^{-O(u)}}{k!} \left(\frac{1}{2 \log u} \right)^k \\ &= x e^{-u \log u + O(u \log_2(10u))}. \end{aligned}$$

This completes the proof of the lower bound in Theorem 4.1. □

Exercise 4.1. (a) Show, using elementary estimates, that

$$\Psi(x, x^{1/u}) = x(1 - \log u) + O(x/\log x)$$

uniformly for $1 \leq u \leq 2$.

(b) Show that for $y < z < x$ that

$$\Psi(x, y) = \Psi(x, z) - \sum_{y < p \leq z} \Psi(x/p, p).$$

(c) Let $\rho(u)$ be the Dickman-de Bruijn function, defined recursively by

$$\rho(u) = 1 \quad (0 \leq u \leq 1), \quad \rho(u) = 1 - \int_1^u \frac{\rho(v-1)}{v} dv \quad (u > 1).$$

Using (b) and induction on $\lfloor u \rfloor$, show that for any $k > 1$, uniformly for $1 \leq u \leq k$ we have

$$\Psi(x, x^{1/u}) = \rho(u)x + O_k\left(\frac{x}{\log x}\right).$$

Exercise 4.2. Prove that uniformly for $10 \leq \log z \leq y \leq z \leq x$,

$$\Theta(x, y, z) := \#\left\{n \leq x : \prod_{\substack{p^v \parallel n \\ p \leq y}} p^v > z\right\} = x e^{-u \log u + O(u \log_2(3u))}, \quad u = \frac{\log z}{\log y}.$$

That is, counting numbers which have a large y -smooth part.

Exercise 4.3. Let \mathcal{S} denote the set of integers with $(P^+(n))^2 | n$. Show that

$$\#\{n \leq x : n \in \mathcal{S}\} \ll x \exp\left\{-\left(\sqrt{2} + o(1)\right)\sqrt{\log x \log_2 x}\right\}.$$

5. COUNTING PRIME FACTORS

Let

$$\pi_k(x) = \#\{n \leq x : \omega(n) = k\}.$$

Using the Prime Number Theorem, Landau proved an asymptotic for $\pi_k(x)$ for each fixed k .

Theorem (Landau, 1900). For every fixed k ,

$$\pi_k(x) \sim \frac{x}{\log x} \frac{(\log_2 x)^{k-1}}{(k-1)!}.$$

This already suggests that $\omega(n)$ has a Poisson distribution, although Landau never wrote this explicitly. It was Hardy and Ramanujan in 1917 who analyzed the behavior of $\pi_k(x)$ uniformly in k , showing

Theorem (Hardy-Ramanujan, 1917). Uniformly for $x \geq 2$ and $k \geq 1$,

$$\pi_k(x) \leq C_1 \frac{x}{\log x} \frac{(\log_2 x + C_2)^{k-1}}{(k-1)!},$$

where C_1, C_2 are certain absolute constants.

Summing the upper bound for $k \geq (1 + \varepsilon) \log_2 x$ and $k \leq (1 - \varepsilon) \log_2 x$, with $\varepsilon > 0$ fixed, and using standard bounds on the tail of the Poisson distribution (see Lemma 5.3 below), one obtains a sum of $o(x)$. Consequently, most $n \leq x$ have close to $\log_2 x$ distinct prime factors. This result is sometimes referred to as the birth of probabilistic number theory.

Motivated by the fact that the Poisson distribution tends to the Gaussian as the parameter tends to infinity, Erdős and Kac proved their celebrated “Central Limit Theorem” for $\omega(n)$ in 1939:

Theorem (Erdős-Kac, 1939 [42]). For any real z ,

$$\frac{1}{x} \#\left\{n \leq x : \frac{\omega(n) - \log_2 x}{\sqrt{\log_2 x}} \leq z\right\} \rightarrow \Phi(z) := \frac{1}{\sqrt{2\pi}} \int_{-\infty}^z e^{-\frac{1}{2}t^2} dt \quad (x \rightarrow \infty).$$

Much further work was done starting in the 1940s, examining the distribution of the entire *sequence of prime factors* of integers (equivalently, studying the distribution of arbitrary *additive functions*). Perhaps the most notable was the work of Kubilius, who developed a probabilistic model of integers which provides a kind of meta-tool for studying all kinds of statistical questions about the distribution of prime factors. A key concept in the theory is *independence*, the idea that if p and q are small primes, then the “events” $p|n$ and $q|n$ are nearly independent, from a probabilistic viewpoint; this idea also played a prominent role in the development of sieve methods. The theory leads to a “Poisson model” of prime factors; namely that the number of prime factors in an interval $(e^{e^a}, e^{e^b}]$ has roughly Poisson($b - a$) distribution, with disjoint intervals having independent distributions.

Denote by $\omega(n, \mathcal{T})$ the number of distinct prime factors of n that lie in \mathcal{T} .

Lemma 5.1. Let \mathcal{T} be a finite set of primes, and $m \geq 0$. Then

$$\frac{1}{m!} \left(\sum_{p \in \mathcal{T}} \frac{1}{p} - \frac{m}{\min \mathcal{T}} \right)^m \leq \sum_{\substack{n: p|n \Rightarrow p \in \mathcal{T} \\ \omega(n; \mathcal{T}) = m}} \frac{1}{n} \leq \frac{1}{m!} \left(\sum_{p \in \mathcal{T}} \frac{1}{p-1} \right)^m.$$

Proof. The first inequality follows from Lemma 4.2 upon considering squarefree n . By grouping products, we see that

$$\left(\sum_{p \in \mathcal{T}} \frac{1}{p} + \frac{1}{p^2} + \cdots \right)^m$$

is at least $m!$ times the sum on the left. This gives the second inequality. \square

Theorem 5.2 (Prime factors in sets). *Let $\mathcal{T}_1, \dots, \mathcal{T}_r$ be arbitrary disjoint, nonempty subsets of the primes $\leq x$. For any $k_1, \dots, k_r \geq 0$ we have*

$$\begin{aligned} \#\{n \leq x : \omega(n; \mathcal{T}_j) = k_j \ (1 \leq j \leq r)\} &\ll x \prod_{j=1}^r \left(\frac{H_j^{k_j}}{k_j!} e^{-H_j} \right) \left(1 + \sum_{j=1}^r \frac{k_j}{H_j} \right) \\ &\leq x \prod_{j=1}^r e^{-H_j} \left(\frac{H_j^{k_j-1}}{(k_j-1)!} + \frac{H_j^{k_j}}{k_j!} \right), \end{aligned}$$

where, for each j ,

$$H_j = \sum_{p \in \mathcal{T}_j} \frac{1}{p-1}.$$

When $k_j = 0$ the corresponding term $H_j^{k_j-1}/(k_j-1)!$ is to be omitted.

Proof. Let

$$L = \sum_{\substack{h \leq x \\ \omega(h; \mathcal{T}_j) = k_j \ (1 \leq j \leq r)}} \frac{1}{h}, \quad L_t = \sum_{\substack{h \leq x \\ \omega(h; \mathcal{T}_j) = k_j \ (j \neq t) \\ \omega(h; \mathcal{T}_t) = k_t - 1}} \frac{1}{h}.$$

We use the “log-trick” again (due to E. Wirsing). For any $n \leq x$ write

$$\log x = \log n + \log(x/n) = \sum_{p^a \parallel n} \log p^a + \log(x/n) \leq \sum_{p^a \parallel n} \log p^a + x/n.$$

This gives

$$(\log x) \#\{n \leq x : \omega(n; \mathcal{T}_j) = k_j \ (1 \leq j \leq r)\} \leq xL + \sum_{\substack{n \leq x \\ \omega(n; \mathcal{T}_j) = k_j \ (1 \leq j \leq r)}} \sum_{p^a \parallel n} \log p^a.$$

In the double sum, let $n = p^a h$ and observe that $\omega(h, \mathcal{T}_j) = k_j - 1$ if $p \in \mathcal{T}_j$ and $\omega(h, \mathcal{T}_j) = k_j$ otherwise (note that the former case is only possible if $k_j > 0$). That is, h is either counted by L or h is counted by L_t for some $t, 1 \leq t \leq r$. Hence

$$(\log x) \#\{n \leq x : \omega(n; \mathcal{T}_j) = k_j \ (1 \leq j \leq r)\} \leq 2xL + \sum_{t: k_t > 0} \sum_{\substack{h \leq x \\ \omega(h; \mathcal{T}_j) = k_j - \mathbb{1}_{j=t} \ (1 \leq j \leq r)}} \sum_{p^a \leq x/h} \log p^a.$$

Using Chebyshev’s Estimate for primes, the innermost sum over p^a is $O(x/h)$ and thus

$$\#\{n \leq x : \omega(n; \mathcal{T}_j) = k_j \ (1 \leq j \leq r)\} \ll \frac{x}{\log x} \left(L + \sum_{1 \leq j \leq r: k_j > 0} L_j \right).$$

To bound the sum in L and in L_t , write the denominator $h = h_1 \cdots h_r h'$, where, for $1 \leq j \leq r$, h_j is composed only of primes from \mathcal{T}_j , $\omega(h_j; \mathcal{T}_j) = k_j - \mathbb{1}_{t=j}$, and h' is composed of primes in $[2, x] \setminus (\mathcal{T}_1 \cup$

$\dots \cup \mathcal{T}_r$). For brevity, write $m_j = \omega(h; \mathcal{T}_j)$. Using Lemma 5.1 and Mertens, we obtain

$$\begin{aligned} \sum_{\substack{h \leq x \\ \omega(h; \mathcal{T}_j) = m_j \ (\forall j)}} \frac{1}{h} &\leq \prod_{j=1}^r \sum_{\substack{\omega(h_j; \mathcal{T}_j) = m_j \\ p|h_j \implies p \in \mathcal{T}_j}} \frac{1}{h_j} \prod_{\substack{p \leq x \\ p \notin \mathcal{T}_1 \cup \dots \cup \mathcal{T}_r}} \left(1 + \frac{1}{p} + \frac{1}{p^2} + \dots\right) \\ &\leq \prod_{j=1}^r \frac{H_j^{m_j}}{m_j!} \prod_{\substack{p \leq x \\ p \notin \mathcal{T}_1 \cup \dots \cup \mathcal{T}_r}} \left(1 - \frac{1}{p}\right)^{-1} \\ &\ll (\log x) \prod_{j=1}^r \frac{H_j^{m_j}}{m_j!} \prod_{p \in \mathcal{T}_1 \cup \dots \cup \mathcal{T}_r} \left(1 - \frac{1}{p}\right). \end{aligned}$$

We conclude that

$$\#\{n \leq x : \omega(n; \mathcal{T}_j) = k_j \ (1 \leq j \leq r)\} \ll x \prod_{j=1}^r \frac{H_j^{k_j}}{k_j!} \left(1 + \sum_{j=1}^r \frac{k_j}{H_j}\right) \prod_{p \in \mathcal{T}_1 \cup \dots \cup \mathcal{T}_r} \left(1 - \frac{1}{p}\right).$$

Finally, using the elementary inequality $1 + y \leq e^y$, we see that

$$\begin{aligned} \prod_{p \in \mathcal{T}_1 \cup \dots \cup \mathcal{T}_r} \left(1 - \frac{1}{p}\right) &\leq \exp \left\{ - \sum_{p \in \mathcal{T}_1 \cup \dots \cup \mathcal{T}_r} \frac{1}{p} \right\} \\ &= \exp \left\{ O(1) - \sum_{p \in \mathcal{T}_1 \cup \dots \cup \mathcal{T}_r} \frac{1}{p-1} \right\} \\ &\ll e^{-H_1 - \dots - H_r}, \end{aligned}$$

and the proof is complete. \square

Remark. Theorem 5.2 is similar to [130, Theorem 2].

In the special case of a single set of primes, we have

$$(5.1) \quad \#\{n \leq x : \omega(n; \mathcal{T}) = k\} \ll x e^{-H} \left(\frac{H^{k-1}}{(k-1)!} + \frac{H^k}{k!} \right), \quad H = \sum_{p \in \mathcal{T}} \frac{1}{p-1}.$$

In particular,

$$\#\{n \leq x : \omega(n; \mathcal{T}) = 0\} \ll x e^{-H} \asymp x \prod_{p \in \mathcal{T}} \left(1 - \frac{1}{p}\right).$$

This matches the sieve upper bound in Theorem 2.4 in the special case $\Omega = [1, x] \cap \mathbb{N}$, $\mathcal{A}_p = \{n \in \Omega : p|n\}$ for $p \in \mathcal{T}$.

To use (5.1), one often sums up the bound for k_j in an interval. The bound in Theorem 5.2 looks like the product of independent Poisson distributions with parameters H_j .

Lemma 5.3 (Poisson tails). *Let X be a Poisson random variable with parameter λ . Then*

$$\mathbb{P}(X \leq \alpha \lambda) \leq e^{-Q(\alpha)\lambda} \quad (0 \leq \alpha \leq 1), \quad \mathbb{P}(X \geq \alpha \lambda) \leq e^{-Q(\alpha)\lambda} \quad (\alpha \geq 1),$$

where

$$(5.2) \quad Q(x) = x \log x - x + 1.$$

Proof. We use the idea behind Chernoff's inequality, Markov's inequality, and the easy identity $\mathbb{E}c^X = e^{(c-1)\lambda}$ for $c > 0$. Let $b = \log \alpha$. Then

$$\mathbb{P}(X \leq \alpha\lambda) = \mathbb{P}\left(e^{bX} \geq e^{b\alpha\lambda}\right) \leq \frac{\mathbb{E}e^{bX}}{e^{b\alpha\lambda}} = \frac{e^{(e^b-1)\lambda}}{e^{b\alpha\lambda}} = e^{-Q(\alpha)\lambda}.$$

Similarly,

$$\mathbb{P}(X \geq \alpha\lambda) = \mathbb{P}\left(e^{bX} \geq e^{b\alpha\lambda}\right) \leq \frac{\mathbb{E}e^{bX}}{e^{b\alpha\lambda}} = \frac{e^{(e^b-1)\lambda}}{e^{b\alpha\lambda}} = e^{-Q(\alpha)\lambda}. \quad \square$$

We record frequently needed bounds on the function $Q(x)$.

Lemma 5.4 (Q bounds). *We have*

$$(5.3) \quad Q(x) = \int_1^x \log t \, dt \quad (\text{all } x) = \sum_{k=2}^{\infty} \frac{(-1)^k}{k(k-1)} (x-1)^k \quad (|x-1| < 1),$$

and

$$(5.4) \quad \frac{x^2}{3} \leq Q(1+x) \leq x^2 \quad (|x| \leq 1).$$

Corollary 5.5 (Prime factors in intervals). *Let $\omega(n, t) = \#\{p|n : p \leq t\}$.*

(a) *Uniformly for $3 \leq t \leq x$ and $0 \leq \lambda \leq 1$, we have*

$$\#\{n \leq x : \omega(n, t) \leq \lambda \log_2 t\} \ll x(\log t)^{-Q(\lambda)}.$$

Let $\lambda_0 > 1$.

(b) *Uniformly for $3 \leq t \leq x$ and $1 \leq \lambda \leq \lambda_0$, we have*

$$\#\{n \leq x : \omega(n, t) \geq \lambda \log_2 t\} \ll_{\lambda_0} x(\log t)^{-Q(\lambda)}.$$

(c) *Uniformly for $3 \leq t \leq x$ and $0 \leq \psi \leq \sqrt{\log_2 t}$, we have*

$$\#\{n \leq x : |\omega(n, t) - \log_2 t| > \psi \sqrt{\log_2 t}\} \ll x e^{-\frac{1}{3}\psi^2}.$$

Proof. Let \mathcal{T} denote the set of primes in $[2, t]$. By Mertens, $H = \log_2 t + O(1)$. The given bounds now follow from Theorem 5.2 together with the tail bounds in Lemma 5.3. For (a),

$$\begin{aligned} \#\{n \leq x : \omega(n, t) \leq \lambda \log_2 t\} &\ll \frac{x}{\log t} \sum_{k \leq \lambda \log_2 t} \frac{(\log_2 t + O(1))^k}{k!} \\ &= \frac{x}{\log t} \sum_{k \leq \lambda \log_2 t} \frac{(\log_2 t)^k (1 + O(1/\log_2 t))^k}{k!} \\ &\ll \frac{x}{\log t} \sum_{k \leq \lambda \log_2 t} \frac{(\log_2 t)^k}{k!} \\ &\leq x(\log t)^{-Q(\lambda)}. \end{aligned}$$

For (b), there is some C such that

$$\begin{aligned} \#\{n \leq x : \omega(n, t) \geq \lambda \log_2 t\} &\ll \frac{x}{\log t} \sum_{k \geq \lambda \log_2 t - 1} \frac{(\log_2 t + C)^k}{k!} \\ &= \frac{x}{\log t} \sum_{k \geq \lambda^*(\log_2 t + C)} \frac{(\log_2 t + C)^k}{k!}, \end{aligned}$$

where $\lambda^* = \lambda + O(1/\log_2 t)$. Since $Q(\lambda^*) = Q(\lambda) + O_{\lambda_0}(1/\log_2 t)$, applying Lemma 5.3 gives

$$\#\{n \leq x : \omega(n, t) \geq \lambda \log_2 t\} \ll x e^{-(\log_2 t + C)Q(\lambda^*)} \ll_{\lambda_0} x (\log t)^{-Q(\lambda)}.$$

Part (c) follows from (a) and (b) plus Lemma 5.4. \square

5.1. Primes counted with multiplicity. The results of the previous section may be extended to the distribution of the function $\Omega(n)$. There is, however, a change of behavior of $\#\{n \leq x : \Omega(n) = k\}$ in the vicinity of $k = 2 \log_2 x$, due to the influence of powers of 2.

Lemma 5.6. *Uniformly for $x \geq 2$ and $0 \leq y < 2$ we have*

$$\sum_{n \leq x} y^{\Omega(n)} \ll \frac{x}{(2-y)} (\log x)^{y-1}.$$

Proof. Again, use the log-trick. We have

$$\begin{aligned} (\log x) \sum_{n \leq x} y^{\Omega(n)} &\leq \sum_{n \leq x} y^{\Omega(n)} (x/n + \log n) \\ &\leq xS + \sum_{n \leq x} y^{\Omega(n)} \sum_{q|n} \Lambda(q), \quad S = \sum_{n \leq x} \frac{y^{\Omega(n)}}{n}. \end{aligned}$$

Write $n = qm$ and note that $\Omega(n) = \Omega(q) + \Omega(m)$. Then

$$\begin{aligned} \sum_{n \leq x} y^{\Omega(n)} \sum_{q|n} \Lambda(q) &= \sum_{m \leq x} y^{\Omega(m)} \sum_{q \leq x/m} \Lambda(q) y^{\Omega(q)} \\ &\ll \sum_{m \leq x} y^{\Omega(m)} (x/m) = xS. \end{aligned}$$

Therefore,

$$\begin{aligned} \sum_{n \leq x} y^{\Omega(n)} &\ll \frac{x}{\log x} S \leq \frac{x}{\log x} \prod_{p \leq x} \left(1 + \frac{y}{p} + \frac{y^2}{p^2} + \dots\right) \\ &= \frac{x}{\log x} \prod_{p \leq x} \left(1 + \frac{y}{p-y}\right) \ll \frac{x}{2-y} (\log x)^{y-1}. \end{aligned} \quad \square$$

Theorem 5.7. (a) *Uniformly for $0 \leq \lambda \leq 1$ we have*

$$\#\{n \leq x : \Omega(n) \leq \lambda \log_2 x\} \ll \frac{x}{(\log x)^{Q(\lambda)}}.$$

(b) *Uniformly for $1 \leq \lambda < 2$ we have*

$$\#\{n \leq x : \Omega(n) \geq \lambda \log_2 x\} \ll \frac{x}{(2-\lambda)(\log x)^{Q(\lambda)}}.$$

(c) Uniformly for $k \geq 1$ we have

$$\#\{n \leq x : \Omega(n) \geq k\} \ll \frac{xk \log x}{2^k}.$$

Remarks. Estimate (c) is most useful when $k \geq 2 \log_2 x$. Estimates (b) and (c) smoothly interpolate, since $Q(2) = \log 4 - 1$, and thus when $k = 2 \log_2 x + O(1)$ both bounds take the form

$$\ll \frac{x \log_2 x}{(\log x)^{\log 4 - 1}}.$$

Proof. (a) Take $y = \lambda$ in Lemma 5.6, obtaining

$$\#\{n \leq x : \Omega(n) \leq \lambda \log_2 x\} \leq \sum_{n \leq x} \lambda^{\Omega(n) - \lambda \log_2 x} \ll x(\log x)^{-Q(\lambda)}.$$

(b) Similarly, apply Lemma 5.6 with $y = \lambda$:

$$\#\{n \leq x : \Omega(n) \geq \lambda \log_2 x\} \leq \sum_{n \leq x} \lambda^{\Omega(n) - \lambda \log_2 x} \ll \frac{x}{(2 - \lambda)(\log x)^{Q(\lambda)}}.$$

(c) Take $y = 2 - 1/k$ in Lemma 5.6. Then

$$\begin{aligned} \#\{n \leq x : \Omega(n) \geq k\} &\leq \sum_{n \leq x} y^{\Omega(n) - k} \\ &\ll y^{-k} \frac{x}{2 - y} (\log x)^{y-1} \\ &\leq \frac{xk}{2^k (1 - \frac{1}{2k})^k} (\log x)^{1-1/k} \ll \frac{xk \log x}{2^k}. \quad \square \end{aligned}$$

5.2. Application: Erdős' multiplication table problem. In 1955, Erdős [36] posed the following problem: Estimate the number, $A(N)$, of *distinct* products of the form ab with $a \leq N$, $b \leq N$. Erdős proved that $A(N) = o(N^2)$, and later in 1960 [38] refined the estimates to prove that $A(N) = N^2(\log N)^{-\mathcal{E} + o(1)}$, where

$$\mathcal{E} = Q(1/\log 2) = 1 - \frac{1 + \log \log 2}{\log 2} = 0.08607 \dots$$

Theorem 5.8. We have $A(N) \ll \frac{N^2}{(\log N)^{\mathcal{E}}}$.

Proof. Let $k_0 = \frac{\log_2(N^2)}{\log 2} = \frac{\log_2 N}{\log 2} + 1$. By Theorem 5.7, the number of distinct products with $\Omega(ab) \geq k_0$ is bounded above by

$$\#\{m \leq N^2 : \Omega(m) \geq k_0\} \ll N^2(\log N)^{-Q(1/\log 2)} = N^2(\log N)^{-\mathcal{E}}.$$

If $\Omega(ab) < k_0$, then $\omega(a) = h$, $\omega(b) = j$ with $h + j = k < k_0$. The number of pairs (a, b) with $h \leq \frac{1}{2} \log_2 N$ or $j \leq \frac{1}{2} \log_2 N$ is

$$\leq 2N \#\{a \leq N : \omega(a) \leq \frac{1}{2} \log_2 N\} \ll N^2(\log N)^{-Q(1/2)} \ll N^2(\log N)^{-0.15} \ll N^2(\log N)^{-\mathcal{E}}.$$

If h and j are fixed, and both larger than $\frac{1}{2} \log_2 N$, we apply Theorem 5.2, taking \mathcal{T} as the set of all primes $\leq N$, so that $H = \log_2 N + O(1)$. The number of pairs (a, b) is thus

$$\ll \frac{N^2(\log_2 N)^{h+j}}{(\log N)^2 h! j!}.$$

Summing first over all j, h with $h + j = k$ using the binomial theorem, and then over $k < k_0$ using Lemma 5.3, we obtain an upper bound for the total number of pairs a, b with $\Omega(ab) < k_0$ of

$$\ll \frac{N^2}{\log^2 N} \sum_{k < k_0} \frac{(2 \log_2 N)^k}{k!} \ll N^2 (\log^2 N)^{-Q(1/\log 4)} = N^2 (\log N)^{-\varepsilon}. \quad \square$$

The upper bound in Theorem 5.8 is close to the truth. In fact [47],

$$A(N) \asymp \frac{N^2}{(\log N)^\varepsilon (\log_2 N)^{3/2}}.$$

5.3. Exercises.

Exercise 5.1. Let \mathcal{S} denote the set of numbers that are the sum of two squares. Show that for any $\varepsilon \in (0, 1]$,

$$\#\{n \leq x, n \in \mathcal{S} : |\omega(n) - \frac{1}{2} \log_2 x| > \varepsilon \log_2 x\} \ll \frac{x}{(\log x)^{1/2 + \varepsilon^2/6}}.$$

6. STRUCTURE OF SHIFTED PRIMES

Throughout, we will work with sets $\mathcal{P}_a = \{p + a : p \text{ prime}\}$, for a fixed nonzero a . The structure of these sets have numerous applications, particularly when $a = -1$ or $a = 1$. These include

- (1) The study of Euler's totient function $\phi(n)$;
- (2) The study of the sum-of-divisors function $\sigma(n)$;
- (3) Problems about orders and primitive roots modulo primes;
- (4) Carmichael numbers; analyzing primality tests

6.1. The number of prime factors of shifted primes. In 1935, Erdős [31] showed that for any fixed $a \neq 0$, the function $\omega(p + a)$ has normal order $\log_2 p$. To accomplish this, Erdős proved an upper bound of Hardy-Ramanujan type for the number of primes $p \leq x$ with $\omega(p + a) = k$. Here we prove a best-possible version of this estimate. Theorem 6.2 below improves the uniformity of Theorem 1 of Timofeev [128], who showed this bound uniformly for $k \leq b \log_2 x$ for any fixed b .

Lemma 6.1. *Fix $b \geq 0$. Uniformly for $x \geq 2$ and $\ell \geq 0$ we have*

$$\sum_{\substack{\omega(r)=\ell \\ rP^+(r) \leq x}} \frac{1}{\phi(r) \log^b(x/r)} \ll_b \frac{(\log_2 x + O(1))^\ell}{\ell! \log^b x}.$$

Proof. If $\ell = 0$ then $r = 1$ and the result is trivial. Now suppose $\ell \geq 1$. Then $2 \leq r \leq x/2$. We separately consider r in log-dyadic ranges. Let $Q_j = x^{1/2^j}$ for $j \geq 0$ and define

$$\mathcal{T}_j = \left\{ 2 \leq r \leq x/2 : \omega(r) = \ell, rP^+(r) \leq x, \frac{x}{Q_{j-1}} < r \leq \frac{x}{Q_j} \right\}.$$

For $r \in \mathcal{T}_j$, $P^+(r) \leq x/r \leq Q_{j-1}$. Also, if \mathcal{T}_j is nonempty then $Q_{j-1} \geq 2$. We have

$$\sum_{r \in \mathcal{T}_j} \frac{1}{\phi(r) \log^b(x/r)} \leq \frac{1}{\log^b Q_j} \sum_{r \in \mathcal{T}_j} \frac{1}{\phi(r)}.$$

For the sum on the right side, we'll use a trick that was useful in the study of $\Psi(x, y)$. Let $\alpha = \frac{1}{10 \log Q_j}$. Since $Q_{j-1} \geq 2$, $Q_j \geq \sqrt{2}$ and thus $0 < \alpha \leq \frac{1}{3}$. We'll encode the condition $r \geq x/Q_{j-1}$ with

$$\frac{1}{\phi(r)} = \frac{1}{\phi(r)^\alpha \phi(r)^{1-\alpha}} \ll \frac{1}{r^{\alpha/2} \phi(r)^{1-\alpha}} \ll \frac{1}{x^{\alpha/2} \phi(r)^{1-\alpha}},$$

since $(x/r)^{\alpha/2} \leq Q_{j-1}^{\alpha/2} = Q_j^\alpha = e^{1/10}$. Now

$$\begin{aligned} \sum_{\substack{P^+(r) \leq Q_{j-1} \\ \omega(r)=\ell}} \frac{1}{\phi(r)^{1-\alpha}} &\leq \frac{1}{\ell!} \left\{ \sum_{p \leq Q_{j-1}} \frac{1}{(p-1)^{1-\alpha}} + \frac{1}{(p(p-1))^{1-\alpha}} + \dots \right\}^\ell \\ &= \frac{1}{\ell!} \left\{ O(1) + \sum_{p \leq Q_{j-1}} \frac{1}{p^{1-\alpha}} \right\}^\ell. \end{aligned}$$

Since $\log p \leq \log Q_{j-1} = 2 \log Q_j$, we have $p^\alpha = 1 + O(\alpha \log p)$. It follows that

$$\sum_{p \leq Q_{j-1}} \frac{1}{p^{1-\alpha}} \leq \sum_{p \leq Q_{j-1}} \frac{1}{p} + O\left(\frac{\alpha \log p}{p}\right) \leq \log_2 Q_{j-1} + O(1) \leq \log_2 x + O(1).$$

Putting everything together, we see that

$$\begin{aligned} \sum_{r \in \mathcal{F}_j} \frac{1}{\phi(r) \log^b(x/r)} &\ll \frac{1}{x^{\alpha/2} \log^b Q_j} \sum_{\substack{P^+(r) \leq Q_{j-1} \\ \omega(r) = \ell}} \frac{1}{\phi(r)^{1-\alpha}} \\ &\ll \frac{1}{x^{\alpha/2} \log^b Q_j} \frac{(\log_2 x + O(1))^\ell}{\ell!} \\ &= \frac{2^{bj} \exp\left\{-\frac{1}{20} \cdot 2^j\right\}}{\log^b x} \frac{(\log_2 x + O(1))^\ell}{\ell!}. \end{aligned}$$

Summing over j completes the proof. \square

Theorem 6.2. Fix $a \neq 0$. Uniformly for $x \geq 4|a|$ and $k \in \mathbb{N}$ we have

$$\#\{2 + |a| < p \leq x : \omega(p+a) = k\} \ll_a \frac{x}{\log^2 x} \frac{(\log_2 x + O(1))^{k-1}}{(k-1)!} \quad (2|a)$$

and

$$\#\{2 + |a| < p \leq x : \omega\left(\frac{p+a}{2}\right) = k\} \ll_a \frac{x}{\log^2 x} \frac{(\log_2 x + O(1))^{k-1}}{(k-1)!} \quad (2 \nmid a).$$

Proof. Let

$$s = \begin{cases} 1 & 2|a \\ 2 & 2 \nmid a. \end{cases}$$

Suppose $p > 2 + |a| \geq 3$ is prime and $\omega\left(\frac{p+a}{s}\right) = k$. Define $q = P^+\left(\frac{p+a}{s}\right)$ and write $\frac{p+a}{s} = qr$. Either $\omega(r) = k-1$ or $\omega(r) = k$, and r is odd if $2|a$. Also, $rP^+(r) \leq rq \leq (x+a)/s$. Define, for $\ell \geq 0$,

$$\mathcal{R}_\ell = \{r \in \mathbb{N} : rP^+(r) \leq \frac{x+a}{s}, \omega(r) = \ell; r \text{ odd if } 2|a\}.$$

We separately consider two cases. First, suppose that $1 \leq k \leq \log_2 x$. Let $L = \exp\{\sqrt{\log x}\}$. Using Theorem 4.1, we have

$$(6.1) \quad \#\{2 + |a| < p \leq x : q^2 \mid \frac{p+a}{s}\} \leq \underbrace{\Psi(x+a, L)}_{q \leq L} + \sum_{q > L} \frac{x+a}{q^2} \ll_a \frac{x}{L}.$$

We use Theorem 2.5 to bound the contribution of those p with $q \parallel (p+a)$ thus:

$$\begin{aligned} \#\{2 + |a| < p \leq x : \omega\left(\frac{p+a}{s}\right) = k, q^2 \nmid \frac{p+a}{s}\} &\leq \sum_{r \in \mathcal{R}_{k-1}} \#\{q \leq \frac{x+a}{rs} : \underbrace{q, qsr - a}_{E=|rsa|} \text{ both prime}\} \\ &\ll \sum_{r \in \mathcal{R}_{k-1}} \frac{|ars|}{\phi(|ars|)} \frac{x+a}{rs \log^2 \frac{x+a}{rs}} \\ &\ll_a x \sum_{r \in \mathcal{R}_{k-1}} \frac{1}{\phi(r) \log^2 \frac{x+a}{r}}. \end{aligned}$$

Invoking Lemma 6.1, we conclude that

$$\#\{2 + |a| < p \leq x : \omega\left(\frac{p+a}{s}\right) = k\} \ll_a \frac{x}{\log^2 x} \frac{(\log_2 x + O(1))^{k-1}}{(k-1)!} + \frac{x}{L}.$$

The final term x/L is negligible since $k \leq \log_2 x$ implies that the first term on the right is $\gg x/\log^2 x$. This concludes the proof when $k \leq \log_2 x$.

Now assume $k > \log_2 x$. Here we do not separately consider the case $q^2 | \frac{p+a}{s}$ and do not use (6.1). We must then retain both cases $\omega(r) = k - 1$ and $\omega(r) = k$. Arguing as before, we obtain from Theorem 2.5 and Lemma 6.1 the estimate

$$\begin{aligned} \#\{2 + |a| < p \leq x : \omega\left(\frac{p+a}{s}\right) = k\} &\ll_a \sum_{r \in \mathcal{R}_{k-1} \cup \mathcal{R}_k} \frac{x}{\phi(r) \log^2((x+a)/r)} \\ &\ll_a \frac{x}{\log^2 x} \left(\frac{(\log_2 x + O(1))^{k-1}}{(k-1)!} + \frac{(\log_2 x + O(1))^k}{k!} \right) \\ &= \frac{x}{\log^2 x} \frac{(\log_2 x + O(1))^{k-1}}{(k-1)!} \left(1 + \frac{(\log_2 x + O(1))}{k} \right) \end{aligned}$$

Recalling that $k \geq \log_2 x$, this concludes the proof. \square

6.2. Large prime factors of shifted primes. It is conjectured that $P^+(p+a)$ has a distribution roughly the same as the distribution of $P^+(n)$ over all integers $n \leq x$. We are far from proving this, in fact the following is not known:

Conjecture 6.3. *For any $0 < u < 1$, there are infinitely many primes p with $P^+(p+a) < p^u$ and infinitely many primes p with $P^+(p+a) > p^u$.*

The second assertion measures progress toward a special case of the Prime k -tuples conjecture 1.3. Letting $s = 1$ for even a and $s = 2$ for odd a , it's conjectured that infinitely often, $\frac{p+a}{s}$ is prime.

At present, it is known that $P^+(p+a) < p^{0.2961}$ infinitely often and $P^+(p+a) \geq p^{0.677}$ infinitely often. The first result in this direction is due to Erdős.

Theorem 6.4 (Erdős [31], 1935). *For some $u < 1$ there are infinitely many primes p with $P^+(p+a) < p^u$.*

Definition 4. Let μ_1 denote the infimum of all real numbers μ such that for all $a \neq 0$,

$$\#\{p \leq x : P^+(p+a) \leq x^\mu\} > x^{1-o(1)}.$$

Upper bounds on μ_1 have been given in a series of papers, see Table 2.

Upper bound on μ_1	Author	year
$2\sqrt{2} - 2 = 0.82842\dots$	Wooldridge [133]	1979
$\frac{625}{512e} = 0.44907\dots$	Pomerance [110]	1980
$\frac{1}{2}e^{-1/2.73} = 0.34664\dots$	Balog [4]	1984
$\frac{1}{2}e^{-1/2} = 0.30326\dots$	Friedlander [54]	1989
0.2961	Baker and Harman [7]	1998

TABLE 2. Progression of results on smooth shifted primes

Here, we present an argument due to Balog which gives quantitatively better constants. The main input is a hypothesis known as the *Brun-Titmarsh on average hypothesis*. Here $N = N(x)$ is some function of x .

Hypothesis BT($x, N, -a; \lambda$). For all but $o(N)$ moduli $n \in (N, 2N]$ (as $N \rightarrow \infty$), we have

$$(6.2) \quad \pi(x; n, -a) \leq \lambda \frac{x}{\phi(n) \log x}.$$

By Theorem 3.2, for any $\varepsilon > 0$, any $1 < N < x$ with x sufficiently large (depending on ε), and any a , we have (6.2) with $\lambda = (2 + \varepsilon) \frac{\log x}{\log(x/N)}$. The first result showing Hypothesis BT($x, N, -a; \lambda$) with a value of λ smaller than that achievable pointwise (that is, for *all* n, a) is due to Hooley [83], with further improvements due to Hooley [85], Fouvry [53], Bombieri, Friedlander and Iwaniec [14] and Baker and Harman [6, 7].

Theorem 6.5 (Balog [4], 1984). *Let x be large, $M = x^\xi \geq x^{1/2} \log^A x$, where A is a large enough constant. Assume that $\lambda \geq 1$ and Hypothesis BT($x, N; \lambda$) holds for all $M < N \leq M \log x$. Then for any u satisfying*

$$(6.3) \quad \xi > u > (e^{-1} \xi^\lambda (1 - \xi))^{\frac{1}{1+\lambda}},$$

there are $\gg_u x / \log^5 x$ primes $p \leq x$ so that $P^+(p + a) < x^u$.

Take $\xi > 1/2$, then BT($x, x^\xi; a, 4 + \varepsilon$) holds, where $\varepsilon \rightarrow 0$ as $\xi \rightarrow 1/2$ and $x \rightarrow \infty$. We conclude that

Corollary 6.6. *For any $u > \frac{1}{2} e^{-1/5} = 0.409365\dots$, there are $\gg_u x / \log^5 x$ primes $p \leq x$ with $P^+(p + a) < x^u$.*

Bombieri, Friedlander and Iwaniec [14] showed that Hypothesis BT($x, x^{1/2} \log^A x, a; 1 + \varepsilon$) holds for all $A > 0$ and all $\varepsilon > 0$, if x is sufficiently large. It follows that (6.3) holds for all $u > \frac{1}{2} e^{-1/2} = 0.303\dots$, giving Friedlander's result [54].

Proof of Theorem 6.5. Let $y = x^u$, and for $|a| < p \leq x$ let

$$g(p) = \#\{(m, n) : p + a = mn, P^+(mn) \leq y, M < n \leq M \log x\}.$$

By Cauchy-Schwarz (see §2.2.4) we have

$$(6.4) \quad \#\{p \leq x : P^+(p + a) \leq y\} \geq \frac{\left(\sum_{p \leq x} g(p)\right)^2}{\sum_{p \leq x} g(p)^2}.$$

We bound the denominator crudely as

$$(6.5) \quad \sum_{p \leq x} g(p)^2 \leq \sum_{p \leq x} (\#\{m | p + a\})^2 \leq \sum_{n \leq x+a} \tau(n)^2 \ll x \log^3 x.$$

Evidently,

$$g(p) \geq \#\{(m, n) : p + a = mn, P^+(m) \leq y, M < n \leq M \log x\} \\ - \#\{(m, n) : p + a = mn, M < n \leq M \log x, P^+(n) > y\},$$

where we have ignored the condition $P^+(m) \leq y$ in the subtracted term. Thus

$$(6.6) \quad \sum_{p \leq x} g(p) \geq S_1 - S_2,$$

where, ignoring the terms with $m \leq \frac{x+a}{M \log x}$, which are negligible,

$$S_1 \geq \sum_{\substack{P^+(m) \leq y \\ \frac{x+a}{M \log x} < m \leq \frac{x+a}{M}}} \pi(x; m, -a) - \pi(Mm - a; m, -a)$$

and, writing $n = q\ell$ with $q = P^+(n)$,

$$S_2 = \sum_{y < q \leq M \log x} \sum_{\substack{M/q < \ell \leq (M \log x)/q \\ P^+(\ell) \leq q}} \pi(x; \ell q, -a).$$

Since $\frac{x+a}{M} \ll x^{1/2}(\log x)^{-A}$, we use the Bombieri-Vinogradov theorem for S_1 , obtaining

$$\begin{aligned} S_1 &\geq \sum_{\substack{P^+(m) \leq y \\ \frac{x+a}{M \log x} < m \leq \frac{x+a}{M}}} \frac{x - Mm}{\phi(m) \log x} + O\left(\frac{x}{\log x}\right) \\ &\geq \frac{x}{\log x} \sum_{\substack{P^+(m) \leq y \\ \frac{x+a}{M \log x} < m \leq \frac{x+a}{M}}} \frac{1}{\phi(m)} + O\left(\frac{x}{\log x}\right) \end{aligned}$$

using the elementary bound

$$\sum_{m \leq z} \frac{m}{\phi(m)} = O(z).$$

We will also need the asymptotic

$$(6.7) \quad \sum_{m \leq z} \frac{1}{\phi(m)} = C_1 \log z + O(1)$$

for some constant $C_1 > 0$. If $P^+(m) > y$ write $m = qm'$ where $q = P^+(m)$. Then

$$\sum_{\substack{P^+(m) \leq y \\ \frac{x+a}{M \log x} < m \leq \frac{x+a}{M}}} \frac{1}{\phi(m)} \geq \sum_{\substack{\frac{x+a}{M \log x} < m \leq \frac{x+a}{M}}} \frac{1}{\phi(m)} - \sum_{y < q \leq \frac{x+a}{M}} \frac{1}{q-1} \sum_{\substack{\frac{x+a}{Mq \log x} < m' \leq \frac{x+a}{Mq}}} \frac{1}{\phi(m')}.$$

The contribution from primes $q > x/(M \log x)$ is $\ll \frac{(\log_2 x)^2}{\log x}$ by Mertens' theorem and (6.7). For $y < q \leq x/(M \log x)$ we use (6.7) again and see that the sum on m' is $C_1 \log_2 x + O(1)$. Therefore,

$$\begin{aligned} (6.8) \quad S_1 &\geq \frac{x}{\log x} (C_1 \log_2 x) \left(1 - \log \frac{\log(x/M)}{\log y} + o(1)\right) \\ &= \frac{x}{\log x} (C_1 \log_2 x) \left(1 - \log \frac{1-\xi}{u} + o(1)\right). \end{aligned}$$

Now we bound S_2 from above. The terms corresponding to $M < q \leq M \log x$ contribute, by the Brun-Titchmarsh inequality,

$$\ll \frac{x}{\log x} \sum_{M < q \leq M \log x} \frac{1}{q} \sum_{M/q < \ell \leq (M \log x)/q} \frac{1}{\phi(\ell)} \ll \frac{x(\log_2 x)^2}{\log^2 x}.$$

Let E denote the set of $n \in (M, M \log x]$ such that $\pi(x; n, -a) > \lambda \frac{x}{\phi(n) \log x}$. By our hypothesis (6.2) and the Brun-Titchmarsh inequality,

$$\sum_{n \in E} \pi(x; n, -a) \ll \frac{x}{\log x} \sum_{n \in E} \frac{1}{\phi(n)} = o\left(\frac{x \log_2 x}{\log x}\right).$$

Using (6.7) again, the terms with $q \leq M$ and $q\ell \notin E$ contribute

$$\begin{aligned} &\leq \frac{\lambda x}{\log x} \sum_{y < q \leq M} \sum_{\substack{M/q < \ell \leq (M \log x)/q \\ q\ell \notin E}} \frac{1}{\phi(q\ell)} \\ &\leq (\lambda \log(\xi/u) + o(1)) \frac{x}{\log x} (C_1 \log_2 x). \end{aligned}$$

Therefore,

$$(6.9) \quad S_2 \leq (\lambda \log(\xi/u) + o(1)) \frac{x}{\log x} (C_1 \log_2 x).$$

Combining (6.8) and (6.9), we conclude that

$$\sum_{p \leq x} g(p) \geq \frac{x}{\log x} (C_1 \log_2 x) \left(1 - \log \frac{1-\xi}{u} - \lambda \log \frac{\xi}{u} + o(1) \right)$$

as $x \rightarrow \infty$. The hypothesis (6.3) implies that

$$1 - \log \frac{1-\xi}{u} - \lambda \log \frac{\xi}{u} > 0.$$

Inserting the lower bound for $\sum_{p \leq x} g(p)$ into (6.4) and recalling (6.5), the proof is complete. \square

Now we turn to the problem of showing that $P^+(p+a)$ is often large.

Definition 5. Let μ_2 denote the supremum of all real numbers μ such that for any $a \neq 0$

$$\#\{p \leq x : P^+(p+a) > x^\mu\} \gg_\mu \frac{x}{\log x}$$

The progression of records for the lower bound on μ_2 is given in Table 3.

Lower bound on μ_2	Author	year
$1 - \frac{1}{2}e^{-1/4} = 0.6105\dots$	Goldfeld [58]	1969
$1 - \frac{1}{2}e^{-1/4} = 0.6105\dots$	Motohashi [101]	1970
$\frac{1}{2} + \frac{3}{2}(1 - e^{-1/12}) = 0.61993\dots$	Hooley [83]	1972
$5/8 = 0.625$	Hooley [84]	1973
0.6683	Fouvry [53] ⁴	1985
0.676	Baker and Harman [6]	1996
0.677	Baker and Harman [7]	1998

TABLE 3. Progression of results on large prime factors of shifted primes

Here we show the theorem proved independently by Goldfeld and Motohashi. We will then indicate where in the proof the further improvements come from.

Theorem 6.7. We have $\mu_2 \geq 1 - \frac{1}{2}e^{-1/4}$.

Proof. We use a device due to Chebyshev, in connection with the largest prime factor of polynomials. Let $1/2 < \theta < 1 - \frac{1}{2}e^{-1/4}$ and define

$$M = \log \prod_{|a| < p \leq x} (p+a).$$

Let B be the exponent in the Bombieri-Vinogradov Theorem (Theorem 2.17) corresponding to $A = 2$, and let $Q = x^{1/2}(\log x)^{-B}$. Let \mathcal{P} denote the set of primes $|a| < p \leq x$ so that there is a prime power $q^b > Q$ with $b \geq 2$ and $q^b | (p+a)$. Define exponents $\alpha(q)$ by the prime factorization

$$\prod_{\substack{|a| < p \leq x \\ p \notin \mathcal{P}}} (p+a) = \prod_{q \leq x+a} q^{\alpha(q)}.$$

Then

$$M = M_1 + M_2 + M_3 + M_4,$$

where

$$M_1 = \log \prod_{p \in \mathcal{P}} (p + a),$$

$$M_2 = \log \prod_{q \leq Q} q^{\alpha(q)}.$$

$$M_3 = \log \prod_{Q < q \leq x^\theta} q^{\alpha(q)},$$

$$M_4 = \log \prod_{x^\theta < q \leq x+a} q^{\alpha(q)}.$$

Our goal is to prove that $M_4 \gg x$. We accomplish this by first observing that

$$(6.10) \quad M \sim x$$

by the Prime Number Theorem, and then upper bounding M_1, M_2, M_3 . For M_1 , if $p \in \mathcal{P}$ then $p + a$ is divisible by d^2 for some $d > Q^{1/3}$. Hence

$$M_1 \ll (\log x) \sum_{d > Q^{1/3}} \frac{x}{d^2} \ll x^{6/7}.$$

We handle M_2 with the Bombieri-Vinogradov Theorem. Letting $E(x; s, c) = \pi(x; s, c) - \text{li}(x)/\phi(s)$ we have

$$\begin{aligned} M_2 &= \sum_{q^b \leq Q} (\log q) \pi(x; q^b, -a) \\ &= \sum_{q^b \leq Q} (\log q) \left(\frac{\text{li}(x)}{\phi(q^b)} + E(x; q^b, -a) \right) \\ &\sim \text{li}(x) \log Q \sim \frac{x}{2}. \end{aligned}$$

We cannot evaluate M_3 asymptotically, but a good upper bound will suffice. The most crude method is to use the Brun-Titchmarsh inequality, Theorem 3.2 with explicit constant. This gives

$$\begin{aligned} M_3 &= \sum_{Q < q \leq x^\theta} (\log q) \pi(x; q, -a) \\ &\leq (2 + o(1)) \sum_{Q < q \leq x^\theta} \frac{x \log q}{(q-1) \log(x/q)} \\ &= (2 + o(1)) x \int_Q^{x^\theta} \frac{dt}{t \log(x/t)} \\ &\sim \left(2 \log \frac{1}{2-2\theta} \right) x. \end{aligned}$$

Combining the estimates for M_1, M_2 and M_3 , we find that

$$M_1 + M_2 + M_3 \leq (1 + o(1)) \left(\frac{1}{2} + 2 \log \frac{1}{2-2\theta} \right) x.$$

Recalling the bound on θ , and comparing this with (6.10), we find that $M_4 \gg_\theta x$. As each number $p + a$ is divisible by at most one prime $> x^\theta$ we see that

$$\#\{p \leq x : P^+(p + a) > x^\theta\} \geq \frac{M_4}{\log(x + a)} \gg_\theta \frac{x}{\log x},$$

as desired. \square

Remarks. Most improvements to Theorem 6.7 come from better estimates of M_3 using Hypothesis $\text{BT}(x, N, a; \lambda)$ (an exception is the work of Hooley [84], which makes use of a Selberg-type sieve). These in turn rely on a variety of tools, from complicated sieves to bounds on Kloosterman sums.

The bound $\mu_2 > 2/3$ of Fouvry enabled Adleman and Heath-Brown [1] to deduce that the first case of Fermat's Last Theorem is true for infinitely many primes p ; this is now a historical point in light of Wiles's proof 10 years later.

The bound on μ_2 also played an important role in the original AKS polynomial-time algorithm [2] for determining the primality of numbers.

6.3. Application to Carmichael numbers. A composite number n is a *Carmichael number* if for all $(a, n) = 1$, $a^{n-1} \equiv 1 \pmod{n}$. Such a number mimics a prime w.r.t. the Fermat congruence. An old criteria of Korselt says that n is a Carmichael number if and only if n is squarefree and $(p-1) | (n-1)$ for every prime $p | n$. The smallest Carmichael numbers are 561, 1105 and 1729. One way to construct Carmichael numbers is to observe that if $k \in \mathbb{N}$, and $6k + 1$, $12k + 1$ and $18k + 1$ are all prime, then $n = (6k + 1)(12k + 1)(18k + 1)$ is a Carmichael number. By the Prime k -tuples conjecture (Conjecture 1.3), there are $\sim C \frac{x}{\log^3 x}$ such numbers $k \leq x$.

Alford, Granville and Pomerance showed unconditionally in 1994 [3] that there are infinitely many Carmichael numbers. Moreover, they showed a lower bound $C(x) \gg x^{2/7}$ for the counting function $C(x)$ of Carmichael numbers. A key ingredient is finding many smooth shifted primes $p - 1$. In fact, Alford, Granville and Pomerance proved that

$$C(x) \gg x^{\frac{5}{12}(1-\mu_1)-o(1)}.$$

With Baker and Harman's [7] value $\mu_1 \leq 0.2961$, we get an exponent of $0.29329\dots$. The $\frac{5}{12}$ fraction comes from lower bounds for prime in progressions to "virtually all" moduli. Harman [75, 77] improved the exponent, showing

$$C(x) \gg x^{0.4736(1-\mu_1)-o(1)},$$

where now the exponent is a bit larger than $1/3$.

6.4. Applications to Euler's function and the sum of divisors function.

6.4.1. Popular values of Euler's function. Let $A(m) = \#\{m : \phi(m) = n\}$. Erdős [31] showed that there is a constant $c > 0$ such that $A(m) > m^c$ infinitely often. A key ingredient in the proof is Theorem 6.4. The argument was sharpened by Pomerance [110], to connect c with the exponent in Theorem 6.4.

Theorem 6.8 (Erdős; Pomerance). *For every $\varepsilon > 0$ there are infinitely many n such that $A(n) > n^{1-\mu_1-\varepsilon}$.*

Currently, the best bound we know is $\mu_1 \leq 0.2961$ due to Baker and Harman [7], while it is conjectured that $\mu_1 = 0$. The conclusion then would be best possible since trivially

$$A(m) \leq \#\{n : \phi(n) \leq m\} \asymp m \log_2 m.$$

Proof. Fix $\mu_1 < \nu < 1$ and let z be large. Let

$$\mathcal{P} = \{p \leq (\log z)^{1/\nu} : P^+(p-1) \leq \log z\}.$$

By hypothesis, $\#\mathcal{P} \geq (\log z)^{1/\nu - o(1)}$ as $z \rightarrow \infty$. Let

$$M = \left\lfloor \frac{\nu \log z}{\log \log z} \right\rfloor,$$

and let \mathcal{N} denote the set of all integers which are the product of M distinct primes from \mathcal{P} . Note that for all $n \in \mathcal{N}$, $\phi(n) \leq n \leq z$ and $P^+(\phi(n)) \leq \log z$. Hence, there is an $m \in \{\phi(n) : n \in \mathcal{N}\}$ such that

$$A(m) \geq \frac{\#\mathcal{N}}{\Psi(z, \log z)}$$

By Theorem 4.1 (inequality (4.1)), $\Psi(z, \log z) = z^{o(1)}$. Also, as $z \rightarrow \infty$, we have

$$\begin{aligned} \#\mathcal{N} &= \binom{\#\mathcal{P}}{M} \geq \left(\frac{\#\mathcal{P}}{M}\right)^M \geq \left(\frac{(\log z)^{(1-o(1))/\nu}}{M}\right)^M \\ &\geq (\log z)^{\left[\frac{1}{\nu} - 1 - o(1)\right] \cdot \left[\frac{\nu \log z}{\log 2} - 1\right]} \\ &= z^{1-\nu - o(1)}. \end{aligned}$$

Hence there is an $m \leq z$ with $A(m) \geq z^{1-\nu - o(1)}$. Taking ν arbitrarily close to μ_1 , the theorem follows. \square

6.4.2. *The range of Euler's function.* Let

$$\mathcal{V} = \{\phi(n) : n \in \mathbb{N}\} = \{1, 2, 4, 6, 8, 10, 12, 16, 18, 20, 22, 24, 28, \dots\}$$

denote the range of Euler's totient function $\phi(n)$, and let $V(x) = \#\{m \in \mathcal{V} : m \leq x\}$ be its counting function. Evidently \mathcal{V} contains only one odd number, namely 1, but what can we say about the growth of $V(x)$? Since $\phi(p) = p - 1$ for all primes p , trivially

$$V(x) \geq \pi(x) \sim \frac{x}{\log x}.$$

Pillai [105] gave the first non-trivial upper bound on $V(x)$, namely

$$V(x) \ll \frac{x}{(\log x)^{(\log 2)/e}}.$$

Using sieve methods, Erdős [31] improved this to

$$V(x) = \frac{x}{(\log x)^{1-o(1)}} \quad (x \rightarrow \infty).$$

Upper and lower bounds for $V(x)$ were sharpened in a series of papers by Erdős [34], Erdős and Hall [40, 41], Pomerance [111], Maier and Pomerance [95], and finally by Ford [45]. The exact order of $V(x)$ is now known [45, Theorem 1], namely

$$V(x) = \frac{x}{\log x} \exp\{C(\log_3 x - \log_4 x)^2 + D \log_3 x - (D + 1/2 - 2C) \log_4 x + O(1)\},$$

where $C = 0.81781464640083632231\dots$ and $D = 2.17696874355941032173\dots$ are specific constants defined in [45]. Sieve methods played a crucial role in these investigations. Below we use the results about the normal behavior of $\omega(n)$ and $\omega(p+a)$ to provide nontrivial upper and lower bounds for $V(x)$.

Theorem 6.9. *We have*

$$V(x) \gg \frac{x \log_2 x}{\log x}.$$

Proof. Let $y = \exp\{\sqrt{\log x}\}$ and let

$$\mathcal{B} = \{pq : q \leq y < p \leq x/q, p \text{ and } q \text{ prime}\}.$$

Evidently $\phi(m) \leq x$ for $m \in \mathcal{B}$. Our goal is to show that there is little overlap among the numbers $\phi(m)$. By simple inclusion-exclusion,

$$(6.11) \quad V(x) \geq |\mathcal{B}| - Z, \quad Z := \#\{m_1, m_2 \in \mathcal{B} : m_1 \neq m_2, \phi(m_1) = \phi(m_2)\}.$$

By Mertens,

$$|\mathcal{B}| = \sum_{q \leq y} \pi(x/q) - \pi(y) \gg \sum_{q \leq y} \frac{x}{q \log x} \gg \frac{x \log_2 x}{\log x}.$$

Also, Z is the number of solutions of

$$(p-1)(q-1) = (p'-1)(q'-1) \quad (p \neq p', pq \in \mathcal{B}, p'q' \in \mathcal{B}).$$

Fix q and q' , and write

$$g = (q-1, q'-1), \quad r = \frac{q-1}{g}, \quad s = \frac{q'-1}{g}.$$

Then the above equation reduces to

$$(p-1)r = (p'-1)s,$$

where $(r, s) = 1$. Thus, for some $n \leq x/(qs)$ we have $p = 1 + rn$ and $p' = 1 + sn$. Apply Theorem 2.5 with the pair of linear forms $rn + 1, sn + 1$. Here $E = rs|r - s| \ll x^3$. Hence

$$\begin{aligned} \#\{n \leq x/(qs) : nr + 1, ns + 1 \text{ both prime}\} &\ll \frac{x/(qs)}{\log^2(x/(qs))} (\log_2 x)^2 \\ &\ll \frac{x(\log_2 x)^2}{\log^2 x} \frac{g}{qq'} \end{aligned}$$

We now sum over q, q' using Exercise 2.12. This gives

$$\begin{aligned} \sum_{\substack{q, q' \leq y \\ q \neq q'}} \frac{(q-1, q'-1)}{qq'} &\leq \sum_{g \leq y/2} g \left(\sum_{\substack{q \leq y \\ q \equiv 1 \pmod{g}}} \frac{1}{q} \right)^2 \\ &\ll (\log_2 x)^2 \sum_{g \leq y/2} \frac{g}{\phi(g)^2} \\ &\leq (\log_2 x)^2 \prod_{p \leq y/2} \left(1 + \frac{p}{(p-1)^2} + O\left(\frac{1}{p^2}\right) \right) \\ &\ll (\log_2 x)^2 \sqrt{\log x}. \end{aligned}$$

It follows that

$$Z \ll \frac{x(\log_2 x)^4}{(\log x)^{3/2}}.$$

Combined with (6.11), this completes the proof. \square

Theorem 6.10. *We have*

$$V(x) \ll \frac{x}{\log x} \exp \{33(\log_3 x)^2\}.$$

Proof. Let

$$\varepsilon = 0.001, \quad \delta = Q(1 - \varepsilon) \geq \varepsilon^2/3.$$

Let

$$\mathcal{S} = \{p : \omega(p-1) \leq (1 - \varepsilon) \log_2 p\}$$

and let $S(x)$ be the counting function of \mathcal{S} . By Theorem 6.2, and Lemma 5.3,

$$\begin{aligned} (6.12) \quad S(x) &\leq \#\{p \leq x : \omega(p-1) \leq (1 - \varepsilon) \log_2 x\} \\ &\ll \frac{x}{\log^2 x} \sum_{k \leq (1-\varepsilon) \log_2 x} \frac{(\log_2 x + O(1))^{k-1}}{(k-1)!} \\ &\ll \frac{x}{\log^2 x} \sum_{k \leq (1-\varepsilon) \log_2 x} \frac{(\log_2 x)^{k-1}}{(k-1)!} \\ &\ll \frac{x}{(\log x)^{1+\delta}}. \end{aligned}$$

Also define

$$W(x) = \max_{y \leq x} \frac{\log y}{y} V(y).$$

Although $\frac{\log y}{y} V(y)$ may not be monotone, $W(x)$ is and this will be convenient in the proof.

Let x be large. Then there is a $y \leq x$ with

$$W(x) = \frac{\log y}{y} V(y).$$

By Theorem 6.9, $W(x) \rightarrow \infty$ as $x \rightarrow \infty$ and hence $y \rightarrow \infty$ as $x \rightarrow \infty$. We now bound $V(y)$. Let

$$\theta = 0.97, \quad y_1 = \exp \left\{ \frac{(\log y)^\theta}{3 \log_2 y} \right\}.$$

Associate to each $v \in \mathcal{V}$ with $v \leq y$ a preimage n , that is, $\phi(n) = v$. We have $n \ll y \log_2 y$ by a classical estimate.

We divide these v into four classes:

- (a) $V_1 = \{v : \Omega(v) \geq 2.9 \log_2 y \text{ or } \Omega(n) \geq 2.9 \log_2 y\}$;
- (b) $V_2 = \{v : p^2 | n \text{ for some } p > y_1\}$;
- (c) $V_3 = \{v \notin V_1 \cup V_2 : p | n \text{ for some } p > y_1, p \in \mathcal{S}\}$;
- (d) $V_4 = \mathcal{V} \cap [1, x] \setminus (V_1 \cup V_2 \cup V_3)$ (the remaining v).

Theorem 5.7 (c) implies immediately that

$$(6.13) \quad |V_1| \ll \frac{y(\log_2 y)^2}{(\log y)^{2.9 \log_2 y - 1}} \ll \frac{y}{(\log y)^{1.01}}.$$

Trivially,

$$(6.14) \quad |V_2| \ll \sum_{p > y_1} \frac{y \log_2 y}{p^2} \ll \frac{y}{(\log y)^{100}}.$$

Now suppose that $v \in V_3$. Then $p|n$ for some $p \in \mathcal{S}, p > y_1$. Since $v \notin V_2, v = (p-1)\phi(n/p) = (p-1)w$ for some $w \in \mathcal{V}, w \leq \frac{y}{p-1}$. Thus,

$$|V_3| \leq \sum_{\substack{y_1 < p \leq y \\ p \in \mathcal{S}}} V\left(\frac{y}{p-1}\right) \ll \underbrace{S(y)}_{p > y/2} + W(y)y \sum_{\substack{y_1 < p \leq y/2 \\ p \in \mathcal{S}}} \frac{1}{p \log(y/p)}.$$

A standard partial summation argument, together with (6.12), yields

$$\begin{aligned} \sum_{\substack{y_1 < p \leq y/2 \\ p \in \mathcal{S}}} \frac{1}{p \log(y/p)} &\ll \frac{S(y)}{y} + \int_{y_1}^{y/2} \frac{S(t)}{t^2 \log(y/t)} dt \\ &\ll \frac{1}{(\log y)^{1+\delta}} + \frac{1}{(\log y_1)^\delta} \int_{y_1}^{y/2} \frac{dt}{t(\log t) \log(y/t)} \\ &\ll \frac{(\log_2 y)^2}{(\log y)^{1+\delta\theta}}. \end{aligned}$$

Therefore, by the monotonicity of $W(\cdot)$ and (6.12),

$$(6.15) \quad |V_3| \ll W(y) \frac{(\log_2 y)^2}{y(\log y)^{1+\delta\theta}} \ll \frac{yW(x)}{(\log y)^{1+\delta\theta/2}}.$$

Finally, suppose that $v \in V_4$. Let

$$y_2 = y_1^{3 \log_2 y} = \exp\{(\log y)^\theta\}.$$

We claim that

$$v = w, \quad v = (p-1)w \quad \text{or} \quad v = (p-1)(p'-1)w \quad (w \in \mathcal{V}, w \leq y_2),$$

where p, p' are primes $> y_1$. Since $v \notin V_3$, any prime factor of n which is $> y_1$ is not in \mathcal{S} . This implies that n has at most two prime factors which are $> y_1$. If n has three or more such factors, then none of them is in \mathcal{S} and thus

$$\Omega(v) \geq 3(1-\varepsilon) \log_2 y_1 > 3(1-\varepsilon)(\theta - o(1)) \log_2 y > 2.9 \log_2 y,$$

contradicting that $v \notin V_1$. Thus, $n = qm$, where q is 1, a prime $> y_1$ or the product of two primes $> y_1$, and $P^+(m) \leq y_1$. But then $m \leq y_1^{\Omega(m)} \leq y_1^{\Omega(n)} \leq y_2$ since $v \notin V_1$ and $\phi(n) = \phi(q)\phi(m)$. This proves the claim with $w = \phi(m)$. Thus,

$$|V_4| \leq V(y_2) + \sum_{p-1 \leq y} V\left(\min\left(y_2, \frac{y}{p-1}\right)\right) + \sum_{(p-1)(p'-1) \leq y} V\left(\min\left(y_2, \frac{y}{(p-1)(p'-1)}\right)\right).$$

For $t \leq y_2, V(t) = \frac{t}{\log t} W(t) \leq \frac{t}{\log t} W(y_2)$. again separating out the terms with $p > y/2$ or with $pp' > y/2$ we find that

$$\begin{aligned} |V_4| &\ll W(y_2) \left[\frac{y}{\log y} + \sum_{p \leq y/2} \frac{y}{p \log(y/p)} + \sum_{pp' \leq y/2} \frac{y}{pp' \log(y/pp')} \right] \\ &\ll W(y_2) \frac{y(\log_2 y)^2}{\log y}. \end{aligned}$$

Combining this with (6.13), (6.14) and (6.15) gives

$$W(x) \ll \frac{1}{(\log y)^{0.01}} + \frac{W(x)}{(\log y)^{\delta\theta/2}} + W(y_2)(\log_2 y)^2.$$

Again, using the monotonicity of $W(\cdot)$,

$$W(y_2) \leq W(\exp\{(\log x)^\theta\}).$$

Also recall that $W(x) \rightarrow \infty$ as $x \rightarrow \infty$, and we obtain

$$W(x) \leq K(\log_2 x)^2 W(\exp\{(\log x)^\theta\})$$

for some absolute constant $K > 0$. Iterating this expression yields

$$W(x) \leq K^k \theta^{k(k-1)} (\log_2 x)^{2k} W(\exp\{(\log x)^{\theta^k}\})$$

provided that $(\log x)^{\theta^k} \gg 1$. Taking

$$k = \left\lfloor \frac{\log_3 x}{-\log \theta} \right\rfloor$$

produces

$$W(x) \leq \exp\{(-1/\log(\theta))(\log_3 x)^2 + O(\log_3 x)\} \ll \exp\{33(\log_2 x)^2\}.$$

This completes the proof. □

6.5. Exercises.

Exercise 6.1. Show that for every $\alpha < \frac{1}{2}$, a positive proportion of primes p satisfy both $P^+(p-1) > p^\alpha$ and $P^+(p+1) > p^\alpha$.

Exercise 6.2. Improve the upper estimate (6.5) for $\sum_{p \leq x} g(p)^2$.

Exercise 6.3 (Ford, 1995 - see [45]). (a) Suppose that $A(m) = k$. Also suppose that $p > 2m+1$ is a prime such that

- (i) $2p+1$ and $2mp+1$ are both prime;
- (ii) $dp+1$ is composite for all $d|2m$ except for $d=2, d=2m$.

Show that $A(2mp) = k+2$.

(b) Assume the Prime k -tuples conjecture, Conjecture 1.3. Show that a prime p satisfying the above conditions always exists. Conclude that for any $k \geq 2$ that there is a number m with $A(m) = k$. [This is a conjecture of Sierpiński (see [116] and [37]), which was proved for even k by Ford and Konyagin [52] and for odd k by Ford [46].]

Exercise 6.4. Carmichael [20, 21] conjectured that $A(m) = 1$ is impossible. Assume that $A(m) = 1$ and $\phi(n) = m$.

- (a) (Carmichael-Klee) Show that if $d \prod_{p|d} p|n$ and $q = 1+d$ is prime, then $q^2|n$.
- (b) Show that $2^2 3^2 7^2 43^2|n$.
- (c) Show that either $13^2|n$ or $19^2|n$. Hint: consider the two cases $3^2||n$ and $3^3|n$.

7. SMALL GAPS BETWEEN PRIMES

7.1. Introduction. Prior to 2005, there were only weak results known about small gaps between primes. Let p_n denote the n -th prime, and set

$$\Delta = \liminf_{n \rightarrow \infty} \frac{p_{n+1} - p_n}{\log n}.$$

The Prime Number Theorem implies $\Delta \leq 1$. Prior to 2005, it was not known that $\Delta = 0$, which is itself a very weak bound in the direction of the Twin Prime Conjecture. Here we summarize the major events:

- Hardy-Littlewood, 1926 [73] (unpublished): $\Delta \leq 2/3$ assuming the Extended Riemann Hypothesis for Dirichlet L -functions.
- Erdős, 1940 [33]: $\Delta < 1$ unconditionally.
- Bombieri and Davenport, 1966 [13]: $\Delta \leq \frac{2+\sqrt{3}}{8} = 0.466\dots$
- Maier, 1988 [94]: $\Delta \leq 0.248$.

We begin by showing Erdős' argument from 1940, which incorporated a basic sieve bound.

Theorem 7.1. *Suppose that, uniformly for all even $h \leq 2 \log x$ we have*

$$(7.1) \quad \#\{x/2 < n \leq x : n \text{ and } n+h \text{ are both prime}\} \leq (B + o(1))C_h \frac{x/2}{\log^2 x}$$

where

$$C_h = C \prod_{\substack{p|h \\ p>2}} \frac{p-1}{p-2}, \quad C = 2 \prod_{p>2} \left(1 - \frac{1}{(p-1)^2}\right).$$

Then $\Delta \leq 1 - \frac{1}{2B}$.

Basic upper bound sieves, such as Theorem 2.5, show that (7.1) holds for some finite B , while Theorem 3.5 implies that $B = 4$ is admissible.

Proof. The basic idea is that the Prime Number Theorem implies that the average gap between primes up to x is $\sim \log x$, but (7.1) implies that there are not many gaps that are extremely close to $\log x$.

Let x be large and let $p_{n+1}, \dots, p_{n+m+1}$ be the primes in $(x/2, x]$. Put $d_j = p_{j+1} - p_j$ for all j . Fix $\frac{1}{3B} < \varepsilon < \frac{1}{2B}$ and let

$$I = [(1 - \varepsilon) \log x, (1 + \varepsilon) \log x].$$

Assume that $d_j > (1 - \varepsilon) \log x$ for all $n + 1 \leq j \leq n + m$. For each even $k \in I$, let

$$N_k = \#\{n + 1 \leq j \leq n + m : d_j = k\},$$

so that by (7.1), we have

$$(7.2) \quad N_k \leq (B + o(1))C_k \frac{x/2}{\log^2 x}.$$

Now

$$\begin{aligned}
\frac{x}{2} &\geq \sum_{j=n+1}^{n+m} d_j = \sum_{k > (1-\varepsilon) \log x} k N_k \\
&\geq \sum_{k \in I} k N_k + (1 + \varepsilon) \log x \left(m - \sum_{k \in I} N_k \right) \\
&= (1 + \varepsilon) m \log x - \sum_{k \in I} N_k ((1 + \varepsilon) \log x - k).
\end{aligned}$$

The Prime Number Theorem gives $m \sim \frac{x/2}{\log x}$. Hence, by (7.2),

$$(7.3) \quad \frac{x}{2} \geq \left(\frac{1 + \varepsilon}{2} + o(1) \right) x - \frac{(B/2 + o(1))x}{\log^2 x} \sum_{k \in I} C_k ((1 + \varepsilon) \log x - k).$$

We claim that

$$(7.4) \quad \sum_{k \leq y} C_k = y + O(\log^2 y).$$

Assuming the claim, partial summation gives

$$\sum_{k \in I} k C_k \sim 2\varepsilon \log^2 x,$$

and we conclude from (7.3) that

$$0 \geq \frac{\varepsilon}{2} - (B/2)(2\varepsilon(1 + \varepsilon) - 2\varepsilon) + o(1) = \frac{\varepsilon}{2} - B\varepsilon^2 + o(1).$$

This is a contradiction if $\varepsilon < \frac{1}{2B}$, and proves the theorem.

Now we prove the claim (7.4). Write $C_k = C \sum_{d|k} g(d)$, where g is multiplicative, supported on square-free integers, $g(2) = 0$ and $g(p) = \frac{1}{p-2}$ for primes $p > 2$. Thus,

$$g(d) \ll \frac{1}{d} \left(\frac{d}{\phi(d)} \right)^2 \ll \frac{(\log_2 d)^2}{d} \ll \frac{\log d}{d}.$$

We then compute

$$\begin{aligned}
\sum_{k \leq y} C_k &= C \sum_{\substack{d \leq y \\ d \text{ odd}}} g(d) \sum_{\substack{k \leq y \\ (2d)|k}} 1 = C \sum_{\substack{d \leq y \\ d \text{ odd}}} g(d) \left\lfloor \frac{y}{2d} \right\rfloor \\
&= \frac{Cy}{2} \sum_d \frac{g(d)}{d} + O\left(y \sum_{d > y} \frac{g(d)}{d} + \sum_{d \leq y} g(d) \right) \\
&= \frac{Cy}{2} \prod_{p > 2} \left(1 + \frac{g(p)}{p} \right) + O(\log^2 y) \\
&= y + O(\log^2 y),
\end{aligned}$$

which proves (7.4). □

7.2. Improved gap detectors: GPY-Zhang-Maynard-Tao. In 2005 (the paper appeared in 2009), Goldston, Pintz and Yıldırım[59] showed that $\Delta = 0$ using a new type of prime detector. Let (h_1, \dots, h_k) be an *admissible* k -tuple of non-negative integers; that is, the set of linear forms $(n + h_1, \dots, n + h_k)$ is admissible in the sense of Definition 1. For some non-negative “weight function” $w(n)$, consider

$$(7.5) \quad S = \sum_{N < n \leq 2N} \left(\sum_{j=1}^k \mathbb{1}_{n+h_j \text{ prime}} - 1 \right) w(n).$$

If $S > 0$ then there is an $n \in (N, 2N]$ such that at least two of the forms $n + h_j$ are simultaneously prime. The object is to choose $w(n)$ so that

- (a) $w(n)$ is small when there are few primes among the $n + h_j$
- (b) $w(n)$ is large when $n + h_j$ is prime (or nearly prime) for many j ;
- (c) We can find a good upper bound for $\sum_{N < n \leq 2N} w(n)$ and, for every j , a good lower bound for the sum $\sum_{N < n \leq 2N} w(n) \mathbb{1}_{n+h_j \text{ prime}}$.

A naive choice is

$$w(n) = \mathbb{1}_{n+h_j \text{ prime}} \forall j.$$

This satisfies (a) and (b) but not (c), because we need something like the Hardy-Littlewood conjectures (Conjecture 1.3) to get the required lower bounds. Motivated by Selberg’s sieve, Goldston, Pintz and Yıldırım make the choice

$$w(n) = \left(\sum_{d|(n+h_1)\dots(n+h_k)} \lambda_d \right)^2, \quad \lambda_d = \mu(d) \left(\frac{\log(z/d)}{\log z} \right)^{k+\ell}, \quad \ell \geq 0.$$

Elaborating on the ideas in [59], they proved in [60] that

$$\liminf_{n \rightarrow \infty} \frac{p_{n+1} - p_n}{\sqrt{\log n} (\log_2 n)^2} < \infty.$$

More interestingly, they showed that any exponent improvement in the Bombieri-Vinogradov Theorem would imply that bounded gaps exist infinitely often. More precisely,

Theorem 7.2 (Goldston-Pintz-Yıldırım, 2007). *Assume that for some $\theta > \frac{1}{2}$ we have*

$$(7.6) \quad EH(\theta) : \forall A > 0, \sum_{q \leq x^\theta} \max_{(a,q)=1} \max_{y \leq x} \left| \pi(y; q, a) - \frac{\text{li}(y)}{\phi(q)} \right| \ll_A \frac{x}{\log^A x}.$$

Then there is a constant $C(\theta)$ such that $p_{n+1} - p_n \leq C(\theta)$ infinitely often. In particular, $C(0.971) = 16$.

Unconditionally, the Bombieri-Vinogradov Theorem (Theorem 2.17) implies $EH(\theta)$ for all $\theta < 1/2$, while Elliott and Halberstam [30] conjectured $EH(\theta)$ for all $\theta < 1$.

Conjecture 7.3 (Elliott-Halberstam Conjecture). *We have $EH(\theta)$ for every $\theta < 1$.*

Motohashi and Pintz [102] showed in fact that the bounded gaps conclusion would follow from a version of (7.6) restricted to smooth moduli up to x^θ , where $\theta > 1/2$, that is moduli with $P^+(q) \leq x^\delta$. Yitang Zhang [135] then surprised the world in May, 2013 by supplying such a proof of the modified version of (7.6).

Theorem 7.4 (Yitang Zhang, 2013 [135]). *For infinitely many n , $p_{n+1} - p_n \leq 70000000$.*

A large on-line collaborative Polymath project [108] refined Zhang's ideas in the summer of 2013 and subsequently reduced the bound to about 4600. Then, in October, 2013, James Maynard [97] introduced a better weight function $w(n)$, which reduced the bound further to 600 and furthermore showed that bounded gaps could contain arbitrarily many primes. Around the same time, Terence Tao (unpublished) had a similar idea for improving the weight function.

Theorem 7.5 (Maynard-Tao). *For any m there is a number $C_m \ll m^2 e^{4m}$ such that $p_{n+m} - p_n \leq C_m$ infinitely often. Assuming the Elliott-Halberstam Conjecture, we have $C_2 \leq 12$ and $C_m \ll m^2 e^{2m}$.*

A second Polymath project [109] resulted in further numerical improvements, culminating in the bound $p_{n+1} - p_n \leq 246$ infinitely often. This is the current world record.

7.3. Bounded gaps between primes. We now prepare the ground for the proof of Theorem 7.5. The method is robust enough to handle general linear forms (not only those of type $n + h_i$), and moreover the bounds can be made uniform in the coefficients of the forms, as in [98], with little additional effort.

Theorem 7.6. *For every $m \in \mathbb{N}$ there is a number K_m such that the following holds. Fix $k \in \mathbb{N}$ with $k \geq K_m$. Uniformly over all $N \geq 100$ and every admissible set $(a_1 n + b_1, \dots, a_k n + b_k)$ of linear forms, with $1 \leq a_i \leq (\log N)^{100}$ and $-a_i N/2 \leq b_i \leq N(\log N)^{100}$ for all i , we have*

$$\#\left\{N < n \leq 2N : \sum_{j=1}^k \mathbb{1}_{a_j n + b_j \text{ prime}} \geq m\right\} \geq \frac{N}{(\log N)^{c_k}}$$

for some constant c_k depending only on k . Moreover, we have

- (a) $K_m \ll m e^{4m}$ for all $m \geq 2$.
- (b) Assuming the Elliott-Halberstam Conjecture, we have $K_m \ll m e^{2m}$.

The PolyMath8b project [109] implies⁵ that $K_2 = 50$ is admissible. Also, Maynard [97] showed $K_2 = 5$ is admissible assuming the Elliott-Halberstam conjecture.

Proof of Theorem 7.5 from Theorem 7.6. Let $k = K_m$. Fix $h_1 < \dots < h_k$ so that $n + h_1, \dots, n + h_k$ is an admissible set of linear forms (we say that the tuple (h_1, \dots, h_k) is admissible). Apply Theorem 7.6, we see that

$$\liminf_{n \rightarrow \infty} p_{n+m-1} - p_n \leq h_k - h_1.$$

When $m = 2$, there is an admissible tuple with $h_{50} - h_1 = 246$, proved in [109]. For general m , let h_1, \dots, h_k be the k smallest primes greater than k . Then $n + h_1, \dots, n + h_k$ is clearly admissible, and by the Prime Number Theorem,

$$h_k - h_1 \sim k \log k = K_m \log K_m \ll m^2 e^{4m}.$$

Assuming the Elliott-Halberstam Conjecture, the above calculation yields $C_m \ll m^2 e^{2m}$. When $m = 2$, we may take $k = 5$, and we apply Theorem 7.6 with the 5-tuple $(0, 2, 6, 8, 12)$. \square

⁵The theorems in [109] are stated only in the case $a_i = 1$ and b_i fixed, however it is clear from the proof that the same quantitative bounds hold in the range of uniformity of Theorem 7.6. The relevant parts of [109] to be adjusted are Theorems 19 (i), 20 (i) and 26.

We now describe the prime-detector which we will use to prove Theorem 7.6. Let $N \geq 100$, assume $\text{EH}(\theta)$ for some $\theta \in [1/3, 1)$, and define

$$(7.7) \quad s = \log_2 N, \quad R = N^{\frac{\theta}{2} - \frac{1}{s}}, \quad D = N^{1/s}, \quad z = D^{1/s} = N^{1/s^2}.$$

For each $k \in \mathbb{N}$ we will construct a special sequence $\lambda(\mathbf{d})$ (which depends only on N and k) for $\mathbf{d} = (d_1, \dots, d_k) \in \mathbb{N}^k$, which is supported on the set

$$(7.8) \quad \mathcal{D} = \mathcal{D}(N) := \{\mathbf{d} \in \mathbb{N}^k : d_1 \cdots d_k \leq R, \mu^2(d_1 \cdots d_k) = 1, P^-(d_1 \cdots d_k) > z\}.$$

We will frequently use the fact that \mathcal{D} is *divisor-closed*, that is, if $\mathbf{d} \in \mathcal{D}$ and $r_j | d_j$ for all j then $\mathbf{r} \in \mathcal{D}$.

Let μ^+ denote an upper bound sieve which is guaranteed by Theorem 2.19 (with respect to the parameters z, D). In particular we have

$$(7.9) \quad |\mu^+(t)| \leq 1 \quad (t \in \mathbb{N}).$$

Now let $(a_1 n + b_1, \dots, a_k n + b_k)$ be an arbitrary admissible set of linear forms (in particular, $a_i \neq 0$ and $(a_i, b_i) = 1$ for all i), with respect to Definition 1. Let

$$(7.10) \quad E = E(\mathbf{a}, \mathbf{b}) = \prod_{i=1}^k a_i \prod_{i < j} (a_i b_j - a_j b_i), \quad \mathcal{E} = \mathcal{E}(\mathbf{a}, \mathbf{b}) = \left\{ \mathbf{d} \in \mathbb{N}^k : (d_1 \cdots d_k, E) = 1 \right\}.$$

Let

$$\rho(d) = \#\{n \pmod{d} : (a_1 n + b_1) \cdots (a_k n + b_k) \equiv 0 \pmod{d}\},$$

and note that $\rho(p) < p$ for all p (because the set of forms is admissible) and $\rho(p) = k$ for all $p \nmid E$; see Theorem 2.5. Let

$$(7.11) \quad V = \prod_{p \leq z} \left(1 - \frac{\rho(p)}{p} \right).$$

Finally, motivated by Selberg's sieve and using an idea from Koukoulopoulos [92, Ch. 28], let

$$(7.12) \quad w(n) = \left(\sum_{t | (a_1 n + b_1) \cdots (a_k n + b_k)} \mu^+(t) \right) \left(\sum_{\substack{\mathbf{d} \in \mathcal{D} \cap \mathcal{E} \\ \forall j: d_j | a_j n + b_j}} \lambda(\mathbf{d}) \right)^2.$$

By Theorem 2.19, $w(n) \geq 0$ for all n . The first factor is a familiar upper bound sieve that we used in Theorem 2.5, for example, and very efficiently sieves out those n for which some $a_i n + b_i$ has a prime factor $\leq z$. The second factor is the new ingredient, a kind of k -dimensional version of the Selberg method. We will optimize $\lambda(\mathbf{d})$ later, and at this point only impose the normalizing condition

$$(7.13) \quad |\lambda(\mathbf{d})| \leq 1 \quad (\mathbf{d} \in \mathcal{D}).$$

The purpose of imposing $\mathbf{d} \in \mathcal{E}$ is to ensure that d_1, \dots, d_k are pairwise relatively prime.

Lemma 7.7. *Suppose that $m_j | a_j n + b_j$ for every j and $\mathbf{m} \in \mathcal{E}$. Then m_1, \dots, m_k are pairwise relative prime, and $(m_j, a_j) = 1$ for all j .*

Proof. If $p | m_i$ and $p | m_j$ then p divides $a_i(a_j n + b_j) - a_j(a_i n + b_i) = a_i a_j - a_j a_i$, and so $p | E$. This proves the first claim. Since $(a_1 n + b_1, \dots, a_k n + b_k)$ is an admissible set, $(a_j, b_j) = 1$ for all j . Hence, if p is prime, $p | m_j | (a_j n + b_j)$ and $p | a_j$ then $p | b_j$, a contradiction. Thus, $(a_j, m_j) = 1$. \square

Notational Convention. Throughout the remainder of this section, constants implied by O and \ll symbols may depend on k and θ , but not on any other parameter. We also suppose that N is sufficiently large, in terms of k and θ . In particular, our bounds are uniform in the coefficients a_i, b_i in some range.

Proposition 7.8. *Adopt the notation (7.7), (7.8), and let μ^+ be an upper bound sieve function from Theorem 2.19 with parameters z, D . Let $\lambda(\mathbf{d})$ satisfy (7.13) and be supported on \mathcal{D} . For $\mathbf{r} \in \mathcal{D}$ define*

$$(7.14) \quad \xi(\mathbf{r}) = \sum_{\mathbf{d}} \frac{\lambda(r_1 d_1, \dots, r_k d_k)}{d_1 \cdots d_k}.$$

Let $(a_1 n + b_1, \dots, a_k n + b_k)$ be an admissible set of linear forms, with $k \geq 2$ and such that

$$(7.15) \quad 1 \leq |a_i| \leq N^2, \quad |b_i| \leq N^2 \quad (1 \leq i \leq k).$$

Define E, \mathcal{E} by (7.10), V by (7.11) and $w(n)$ by (7.12). Then

$$\sum_{N < n \leq 2N} w(n) = VN \sum_{\mathbf{r} \in \mathcal{D}} \frac{\xi(\mathbf{r})^2}{r_1 \cdots r_k} + O\left(\frac{N}{(\log N)^{99k}}\right).$$

Proof. From (7.12), we have

$$\sum_{N < n \leq 2N} w(n) = \sum_{t \leq D} \mu^+(t) \sum_{\mathbf{d}, \mathbf{e} \in \mathcal{D} \cap \mathcal{E}} \lambda(\mathbf{d}) \lambda(\mathbf{e}) \sum_{\substack{N < n \leq 2N \\ t|(a_1 n + b_1) \cdots (a_k n + b_k) \\ \forall j: [d_j, e_j] | (a_j n + b_j)}} 1.$$

Since $\mathbf{d}, \mathbf{e} \in \mathcal{E}$, by Lemma 7.7 the inner sum is empty unless $(d_i e_i, d_j e_j) = 1$ for all $i \neq j$. In this case, the simultaneous conditions $[d_j, e_j] | (a_j n + b_j)$, $1 \leq j \leq k$, define a single residue class n modulo $\prod_{j=1}^k [d_j, e_j]$. Also, the condition $t | (a_1 n + b_1) \cdots (a_k n + b_k)$ defines $\rho(t)$ residue classes modulo t . But $P^+(t) \leq z < P^-(d_j e_j)$ for each j , hence n runs over $\rho(t)$ residue classes modulo $t[d_1, e_1] \cdots [d_k, e_k]$. Hence,

$$(7.16) \quad \begin{aligned} \sum_{N < n \leq 2N} w(n) &= \sum_{t \leq D} \mu^+(t) \sum_{\substack{\mathbf{d}, \mathbf{e} \in \mathcal{D} \cap \mathcal{E} \\ (d_i e_i, d_j e_j) = 1 \ (i \neq j)}} \lambda(\mathbf{d}) \lambda(\mathbf{e}) \left(\frac{\rho(t) N}{t[d_1, e_1] \cdots [d_k, e_k]} + O(\rho(t)) \right) \\ &= NV^+ B + T, \end{aligned}$$

where

$$V^+ = \sum_{t \leq D} \frac{\mu^+(t) \rho(t)}{t}, \quad B = \sum_{\substack{\mathbf{d}, \mathbf{e} \in \mathcal{D} \cap \mathcal{E} \\ (d_i e_i, d_j e_j) = 1 \ (i \neq j)}} \frac{\lambda(\mathbf{d}) \lambda(\mathbf{e})}{[d_1, e_1] \cdots [d_k, e_k]},$$

and, by (7.13) and (7.9),

$$|T| \ll |\mathcal{D}|^2 \sum_{t \leq D} \rho(t).$$

We begin with the error terms T . We have

$$\begin{aligned} |\mathcal{D}| &\leq \sum_{\substack{r \leq R \\ P^-(r) > z}} k^{\omega(r)} \mu^2(r) \leq R \sum_{\substack{r \leq R \\ P^-(r) > z}} \frac{k^{\omega(r)} \mu^2(r)}{r} \\ &\leq R \prod_{z < p \leq R} \left(1 + \frac{k}{p}\right)^2 \ll R (\log_2 N)^{2k}, \end{aligned}$$

and

$$\sum_{t \leq D} \rho(t) \leq D \sum_{t \leq D} \frac{\rho(t)}{t} \leq D \prod_{p \leq D} \left(1 + \frac{k}{p}\right) \ll D(\log N)^k.$$

Hence,

$$(7.17) \quad T \ll R^2 D (\log N)^{3k} \ll N^\theta.$$

The function $g(t) = \rho(t)/t$ satisfies (Ω) with $\kappa = k$ since $\rho(p) \leq k$ for all p . Therefore, by the Fundamental Lemma (Theorem 2.19),

$$(7.18) \quad V^+ = V(1 + O(e^{-\frac{1}{2}s \log s})) = V + O\left(\frac{1}{(\log N)^{100k}}\right).$$

We now record a very crude bound for B . For any $m_i = [d_i, e_i]$, there are at most $3^{\omega(m_i)}$ choices for d_i, e_i . Hence, from (7.13),

$$(7.19) \quad \left| \sum_{\mathbf{d}, \mathbf{e} \in \mathcal{D}} \frac{\lambda(\mathbf{d})\lambda(\mathbf{e})}{m_1 \cdots m_k} \right| \leq \prod_{i=1}^k \sum_{\substack{m_i \leq R^2 \\ P^-(m_i) > z}} \frac{3^{\omega(m_i)}}{m_i} \leq \prod_{z < p \leq R^2} \left(1 + \frac{3}{p}\right)^k \ll s^{6k} \ll \log N.$$

To asymptotically bound B , we first remove the conditions $\mathbf{d}, \mathbf{e} \in \mathcal{E}$ and $(d_i e_i, d_j e_j) = 1$. Now from (7.10) and (7.15),

$$E \ll N^{2k+4(k^2/2)}.$$

Hence there are $\ll \frac{\log N}{\log z} \ll s^2$ prime factors of E which are $> z$. If $\mathbf{d} \notin \mathcal{E}$ or $\mathbf{e} \notin \mathcal{E}$ then there is a $p|E$ with $p|m_j$ for some j . Write $m_j = pm$, then analogously to (7.19) we have

$$\left| \sum_{\substack{\mathbf{d}, \mathbf{e} \in \mathcal{D} \\ \mathbf{d} \notin \mathcal{E} \text{ or } \mathbf{e} \notin \mathcal{E}}} \frac{\lambda(\mathbf{d})\lambda(\mathbf{e})}{m_1 \cdots m_k} \right| \leq \sum_{i=1}^k \sum_{\substack{p|E \\ p > z}} \sum_{\substack{m \leq R^2 \\ P^-(m) > z}} \frac{3^{\omega(m)+1}}{mp} \prod_{j \neq i} \sum_{\substack{m_j \leq R^2 \\ P^-(m_j) > z}} \frac{3^{\omega(m_j)}}{m_j} \ll \frac{s^2}{z} s^{6k} \ll \frac{\log N}{z}.$$

Similarly, for each $i \neq j$ we have

$$\sum_{\substack{\mathbf{d}, \mathbf{e} \in \mathcal{D} \\ (d_i e_i, d_j e_j) > 1}} \frac{\lambda(\mathbf{d})\lambda(\mathbf{e})}{m_1 \cdots m_k} \leq \sum_{z < p \leq R^2} \frac{1}{p^2} \prod_{z < p \leq R^2} \left(1 + \frac{3}{p}\right)^k \ll \frac{s^{6k}}{z \log z} \ll \frac{1}{z}.$$

Therefore,

$$(7.20) \quad B = O\left(\frac{\log N}{z}\right) + B', \quad B' = \sum_{\mathbf{d}, \mathbf{e} \in \mathcal{D}} \frac{\lambda(\mathbf{d})\lambda(\mathbf{e})}{[d_1, e_1] \cdots [d_k, e_k]}.$$

Combining (7.16) with (7.17), (7.18) and (7.20), plus the crude bound (7.19), we find that

$$(7.21) \quad \begin{aligned} \sum_{N < n \leq 2N} w(n) &= NVB' + T + O\left(\frac{NV \log N}{z} + \frac{NB'}{(\log N)^{100k}}\right) \\ &= NVB' + O\left(\frac{N}{(\log N)^{99k}}\right). \end{aligned}$$

It remains to bound B' . Write

$$(7.22) \quad \frac{1}{[d, e]} = \frac{(d, e)}{de} = \frac{1}{de} \sum_{r|(d, e)} \phi(r).$$

Then

$$\begin{aligned} B' &= \sum_{\mathbf{r} \in \mathcal{D}} \phi(r_1) \cdots \phi(r_k) \left(\sum_{\forall j: r_j | d_j} \frac{\lambda(\mathbf{d})}{d_1 \cdots d_k} \right) \left(\sum_{\forall j: r_j | e_j} \frac{\lambda(\mathbf{e})}{e_1 \cdots e_k} \right) \\ &= \sum_{\mathbf{r} \in \mathcal{D}} \frac{\phi(r_1) \cdots \phi(r_k)}{r_1^2 \cdots r_k^2} \xi(\mathbf{r})^2. \end{aligned}$$

For any $r \leq R$, r has at most s^2 prime factors $> z$. Hence, for all r_i ,

$$(7.23) \quad \frac{\phi(r_i)}{r_i} = \prod_{p|r_i} (1 - 1/p) = 1 + O\left(\frac{s^2}{z}\right) = 1 + \left(\frac{\log N}{z}\right).$$

Similar to (7.19) we have

$$(7.24) \quad \xi(\mathbf{r}) \leq \prod_{z < p \leq R} \left(1 + \frac{1}{p}\right)^k \ll s^{2k} \ll \log N.$$

Therefore,

$$B' = \sum_{\mathbf{r} \in \mathcal{D}} \frac{\xi(\mathbf{r})^2}{r_1 \cdots r_k} + O\left(\frac{\log^3 N}{z}\right).$$

Combining this with (7.21) completes the proof. \square

Proposition 7.9. *Assume $EH(\theta)$. Adopt the notation (7.7), (7.8), and let μ^+ be an upper bound sieve function from Theorem 2.19 with parameters z, D . Let $\lambda(\mathbf{d})$ satisfy (7.13) and be supported on \mathcal{D} . For $\mathbf{r} \in \mathcal{D}$ and $1 \leq m \leq k$ define*

$$(7.25) \quad \zeta_m(\mathbf{r}) = \mathbb{1}_{r_m=1} \sum_{\substack{\mathbf{d} \in \mathcal{D} \\ d_m=1}} \frac{\lambda(r_1 d_1, \dots, r_k d_k)}{d_1 \cdots d_k}.$$

Let $(a_1 n + b_1, \dots, a_k n + b_k)$ be an admissible set of linear forms, with $k \geq 2$, such that

$$(7.26) \quad \begin{aligned} 1 \leq a_m \leq (\log N)^{100}, \quad -\frac{N}{2} a_m \leq b_m \leq N \log^{100} N \\ 1 \leq |a_i| \leq N^2, \quad |b_i| \leq N^2 \quad (i \neq m). \end{aligned}$$

Define E, \mathcal{E} by (7.10), V by (7.11) and $w(n)$ by (7.12). Then, for $1 \leq m \leq k$ we have

$$\sum_{N < n \leq 2N} w(n) \mathbb{1}_{a_m n + b_m \text{ prime}} = \frac{V Y_m}{\prod_{p \leq z} (1 - 1/p)} \sum_{\mathbf{r} \in \mathcal{D}} \frac{\zeta_m(\mathbf{r})^2}{r_1 \cdots r_k} + O\left(\frac{N}{(\log N)^{40k^2}}\right),$$

where

$$Y_m := \frac{\text{li}(2a_m N + b_m) - \text{li}(a_m N + b_m)}{a_m} \sim \frac{N}{\log N}.$$

Proof. We begin with

$$(7.27) \quad \sum_{N < n \leq 2N} w(n) \mathbb{1}_{a_m n + b_m \text{ prime}} = \sum_{t \leq D} \mu^+(t) \sum_{\mathbf{d}, \mathbf{e} \in \mathcal{D} \cap \mathcal{E}} \lambda(\mathbf{d}) \lambda(\mathbf{e}) \sum_{\substack{N < n \leq 2N \\ t|(a_1 n + b_1) \cdots (a_k n + b_k) \\ \forall j: [d_j, e_j] | (a_j n + b_j) \\ a_m n + b_m \text{ prime}}} 1.$$

As in the proof of Proposition 7.8, $\mathbf{d} \in \mathcal{E}$ and $\mathbf{e} \in \mathcal{E}$ implies that $(d_i e_i, d_j e_j) = 1$ for all $i \neq j$. Also, since $[d_m, e_m] \leq R^2 = N^{\theta-2/s}$, $p = a_m n + b_m$ is prime and

$$(7.28) \quad p = a_m n + b_m \geq \frac{a_m N}{2} \geq \frac{N}{2},$$

we see that

$$d_m = e_m = 1.$$

The range of n implies that

$$a_m N + b_m < p \leq 2a_m N + b_m.$$

For each $i \neq m$, the condition $[d_i, e_i] | a_i n + b_i$ is equivalent to

$$p \equiv a_i^{-1}(a_i b_m - a_m b_i) \pmod{[d_i, e_i]},$$

Again, $\mathbf{d} \in \mathcal{E}$ and $\mathbf{e} \in \mathcal{E}$ implies that this defines a single residue class modulo $[d_i, e_i]$, and moreover this residue class is coprime to $[d_i, e_i]$. By (7.28), the condition $t | (a_1 n + b_1) \cdots (a_k n + b_k)$ is equivalent to

$$\prod_{i \neq m} (a_i n + b_i) \equiv 0 \pmod{t}, \quad (a_m n + b_m, t) = 1.$$

This defines $\rho^*(t)$ residue classes for n modulo t , where ρ^* is multiplicative by the Chinese Remainder Theorem, and moreover for primes q we have

$$(7.29) \quad \rho^*(q) = \begin{cases} \rho(q) & \text{if } q | a_m \\ \rho(q) - 1 & \text{if } q \nmid a_m. \end{cases}$$

To see this, note that when $q | a_m$, the congruence $a_m n + b_m \equiv 0 \pmod{q}$ has no solutions, and for any n we have $(a_m n + b_m, q) = 1$ since $(a_m, b_m) = 1$. When $q \nmid a_m$, there are $\rho(q)$ solutions of

$$(a_1 n + b_1) \cdots (a_k n + b_k) \equiv 0 \pmod{q},$$

including the single solution of $a_m n + b_m \equiv 0 \pmod{q}$, which must be removed.

Therefore, there are $\rho^*(t)$ residue classes for p modulo $a_m t$. By assumption, $1 \leq a_m \leq \log^{100} N < z$, and so $a_m t$ is coprime to $[d_1, e_1] \cdots [d_k, e_k]$. Hence, the inner sum in (7.27) defines precisely $\rho^*(t)$ reduced residue classes for the prime p modulo $a_m t [d_1, e_1] \cdots [d_k, e_k]$. Define $E(u)$ by

$$E(u) = \max_{(u,s)=1} \left| \pi(2a_m N + b_m; u, s) - \pi(a_m N + b_m; u, s) - \frac{\text{li}(2a_m N + b_m) - \text{li}(a_m N + b_m)}{\phi(u)} \right|$$

and write $u = a_m t [d_1, e_1] \cdots [d_k, e_k]$. Then, by (7.27),

(7.30)

$$\begin{aligned} \sum_{N < n \leq 2N} w(n) \mathbb{1}_{a_m n + b_m \text{ prime}} &= \sum_{t \leq D} \mu^+(t) \sum_{\substack{\mathbf{d}, \mathbf{e} \in \mathcal{D} \cap \mathcal{E} \\ (d_i e_i, d_j e_j) = 1 \ (i \neq j) \\ d_m = e_m = 1}} \lambda(\mathbf{d}) \lambda(\mathbf{e}) \left[\rho^*(t) \frac{a_m Y_m}{\phi(u)} + O(\rho^*(t) E(u)) \right] \\ &= a_m Y_m V^* B^* + T^*, \end{aligned}$$

where, since $P^+(a_mt) \leq z < P^-([d_1, e_1] \cdots [d_k, e_k])$,

$$\begin{aligned} V^* &= \sum_{t \leq D} \frac{\mu^+(t) \rho^*(t)}{\phi(a_mt)}, \\ B^* &= \sum_{\substack{\mathbf{d}, \mathbf{e} \in \mathcal{D} \cap \mathcal{E} \\ (d_i e_i, d_j e_j) = 1 \ (i \neq j) \\ d_m = e_m = 1}} \frac{\lambda(\mathbf{d}) \lambda(\mathbf{e})}{\phi([d_1, e_1] \cdots [d_k, e_k])}, \\ |T^*| &\ll \sum_{\substack{t \leq D \\ P^+(t) \leq z}} \rho^*(t) \sum_{\substack{\mathbf{d}, \mathbf{e} \in \mathcal{D} \cap \mathcal{E} \\ (d_i e_i, d_j e_j) = 1 \ (i \neq j)}} E(u). \end{aligned}$$

We use Hypothesis EH(θ) to handle the error term T^* . Note that $x := 2a_m N + b_m > N$ by hypothesis, and since $\mathbf{d}, \mathbf{e} \in \mathcal{D}$, the moduli satisfy

$$u \leq a_m t d_1 \cdots d_k e_1 \cdots e_k \leq a_m D R^2 \leq N^\theta \leq x^\theta$$

if N is large enough. For each squarefree $q = [d_1, e_1] \cdots [d_k, e_k]$, there are $\leq (3k)^{\omega(q)}$ ways to choose $d_1, e_1, \dots, d_k, e_k$. Also, $\rho^*(t) \leq k^{\omega(t)}$. Thus, by Cauchy-Schwarz and the trivial bound $E(u) \ll \frac{2a_m N + |b_m|}{u}$,

$$\begin{aligned} |T^*| &\ll \sum_{\substack{t \leq D \\ P^+(t) \leq z}} \mu^2(t) k^{\omega(t)} \sum_{\substack{P^-(q) > z \\ q \leq R^2}} \mu^2(q) (3k)^{\omega(q)} E(a_m t q) \\ &\leq \sum_{r \leq D R^2} \mu^2(r) (3k)^{\omega(r)} E(a_m r) \\ &\ll (N + |b_m|)^{1/2} \left(\sum_{P^+(r) \leq N} \frac{\mu^2(r) (3k)^{2\omega(r)}}{r} \right)^{1/2} \left(\sum_{r \leq D R^2} E(a_m r) \right)^{1/2} \\ &\ll (N \log^{100} N)^{1/2} (\log N)^{9k^2/2} \left(\frac{2a_m N + b_m}{(\log N)^{1000k^2}} \right)^{1/2}. \end{aligned}$$

Invoking the bounds on a_m and b_m , we conclude that

$$(7.31) \quad T^* \ll \frac{N}{(\log N)^{100k^2}}.$$

As in the proof of Proposition 7.8, we have

$$\prod_{i=1}^m \frac{[d_i, e_i]}{\phi([d_i, e_i])} = 1 + O\left(\frac{\log N}{z}\right).$$

Hence, by the argument in (7.19),

$$B^* = O\left(\frac{\log^2 N}{z}\right) + \sum_{\substack{\mathbf{d}, \mathbf{e} \in \mathcal{D} \cap \mathcal{E} \\ (d_i e_i, d_j e_j) = 1 \ (i \neq j) \\ d_m = e_m = 1}} \frac{\lambda(\mathbf{d}) \lambda(\mathbf{e})}{[d_1, e_1] \cdots [d_k, e_k]}.$$

As in the proof of Proposition 7.8, the ‘‘missing terms’’, those with $\mathbf{d} \in \mathcal{D}, \mathbf{e} \in \mathcal{D}$ and with either $(d_i e_i, d_j e_j) > 1$, $\mathbf{d} \in \mathcal{E}$, or $\mathbf{e} \in \mathcal{E}$, have total $O(\frac{\log N}{z})$. Using (7.22) and (7.23) again, we get

$$(7.32) \quad B^* = O\left(\frac{\log^2 N}{z}\right) + \sum_{\mathbf{r} \in \mathcal{D}} \frac{\zeta_m(\mathbf{r})^2}{r_1 \cdots r_k}.$$

Finally, apply the Fundamental Lemma of the sieve (Theorem 2.19) with the function

$$g(t) = \frac{\rho^*(t)\phi(a_m)}{\phi(a_mt)},$$

where, by (7.29), for primes p we have

$$g(p) = \begin{cases} \frac{\rho^*(p)}{p} = \frac{\rho(p)}{p} & \text{if } p|a_m, \\ \frac{\rho^*(p)}{p-1} = \frac{\rho(p)-1}{p-1} & \text{if } p \nmid a_m. \end{cases}$$

Again, $g(p) \leq 2k/p$ for all p , thus (Ω) holds with $\kappa = 2k$. Then, by Theorem 2.19,

$$V^* = \frac{1}{\phi(a_m)} \left(1 + O(e^{-\frac{1}{2}s \log s})\right) \prod_{p \leq z} (1 - g(p)) = \left(1 + O\left(\frac{1}{(\log N)^{100k^2}}\right)\right) V^{**},$$

where, using (7.29),

$$\begin{aligned} V^{**} &= \frac{1}{\phi(a_m)} \prod_{p|a_m} \left(1 - \frac{\rho(p)}{p}\right) \prod_{\substack{p \leq z \\ p \nmid a_m}} \left(1 - \frac{\rho(p)-1}{p-1}\right) \\ &= \frac{V}{\phi(a_m)} \prod_{p \leq z} \left(1 - \frac{1}{p}\right)^{-1} \prod_{p|a_m} \left(1 - \frac{1}{p}\right) \\ &= \frac{V}{a_m} \prod_{p \leq z} \left(1 - \frac{1}{p}\right)^{-1}. \end{aligned}$$

Therefore,

$$(7.33) \quad V^* = \frac{V}{a_m} \prod_{p \leq z} \frac{p}{p-1} + O\left(\frac{1}{(\log N)^{90k^2}}\right).$$

The same argument leading to (7.19) yields $B^* \ll \log N$. Combining (7.30) with (7.31), (7.32) and (7.33) yields the claimed asymptotic. \square

Next, we prove two relatively easy inversion formulas.

Lemma 7.10. *For all $\mathbf{r} \in \mathcal{D}$ and $1 \leq m \leq k$,*

$$\zeta_m(\mathbf{r}) = \mathbb{1}_{r_m=1} \sum_{b \in \mathbb{N}} \frac{\mu(b)\xi(r_1, \dots, r_{m-1}, b, r_{m+1}, \dots, r_k)}{b}.$$

Proof. Let $r_m = 1$. By (7.14), the right side equals

$$\begin{aligned} &= \sum_b \frac{\mu(b)}{b} \sum_{\mathbf{d}} \frac{\lambda(r_1 d_1, \dots, r_{m-1} d_{m-1}, \mathbf{d}_m b, r_{m+1} d_{m+1}, \dots)}{d_1 \cdots d_k} \\ &= \sum_{d_i: i \neq m} \frac{1}{\prod_{i \neq m} d_i} \sum_{\ell \in \mathbb{N}} \frac{\lambda(r_1 d_1, \dots, r_{m-1} d_{m-1}, \ell, r_{m+1} d_{m+1}, \dots)}{\ell} \sum_{b|\ell} \mu(b) = \zeta_m(\mathbf{r}). \quad \square \end{aligned}$$

Lemma 7.11. *For all \mathbf{d} ,*

$$\lambda(\mathbf{d}) = \mathbb{1}_{\mathbf{d} \in \mathcal{D}} \sum_{\mathbf{b}} \frac{\mu(b_1) \cdots \mu(b_k)\xi(b_1 d_1, \dots, b_k d_k)}{b_1 \cdots b_k}.$$

Proof. Let $\mathbf{d} \in \mathcal{D}$. By (7.14), the right side is

$$\begin{aligned} &= \sum_{\mathbf{b}} \frac{\mu(b_1) \cdots \mu(b_k)}{b_1 \cdots b_k} \sum_{\mathbf{e}} \frac{\lambda(b_1 d_1 e_1, \dots, b_k d_k e_k)}{e_1 \cdots e_k} \\ &= \sum_{\mathbf{l}} \frac{\lambda(l_1 d_1, \dots, l_k d_k)}{l_1 \cdots l_k} \prod_{i=1}^k \sum_{b_i | l_i} \mu(b_i) = \lambda(\mathbf{d}). \end{aligned} \quad \square$$

Now we describe how we will construct the functions $\xi(\cdot)$ and $\lambda(\cdot)$. Let \mathcal{F}_k denote the set of functions $F(\mathbf{x})$ that are continuously differentiable, symmetric and supported on the set

$$(7.34) \quad \mathcal{R}_k = \{\mathbf{x} \in [0, 1]^k : x_1 + \cdots + x_k \leq 1\},$$

and such that

$$(7.35) \quad |F(\mathbf{x})| \leq 1 \quad (\mathbf{x} \in \mathcal{R}_k),$$

and F is not identically zero on \mathcal{R}_k . For such an F , we then take

$$(7.36) \quad \xi(\mathbf{r}) = \mathbb{1}_{\mathbf{r} \in \mathcal{D}} \mu(r_1) \cdots \mu(r_k) \underbrace{\prod_{z < p \leq R} (1 + k/p)^{-1}}_{\text{constant}} F\left(\frac{\log r_1}{\log R}, \dots, \frac{\log r_k}{\log R}\right).$$

In this way, by Lemma 7.11, for any $\mathbf{d} \in \mathcal{D}$ we have

$$\left| \lambda(\mathbf{d}) \prod_{z < p \leq R} (1 + k/p) \right| \leq \sum_{\mathbf{b} \in \mathcal{D}} \frac{1}{b_1 \cdots b_k} \leq \sum_{\substack{P^-(\ell) > z \\ P^+(\ell) \leq R}} \frac{\mu^2(\ell) k^{\omega(\ell)}}{\ell} = \prod_{z < p \leq R} (1 + k/p),$$

that is, $|\lambda(\mathbf{d})| \leq 1$ for all $\mathbf{d} \in \mathcal{D}$, as required by (7.35).

We next insert the definition (7.36) into Propositions 7.8 and 7.9, thus relating the sums in question to integrals over F . We first need some general tools, first relating a sum over a 1-variable function to an integral, and using it to handle multivariate functions.

Lemma 7.12. *Suppose $g \in C^1[a, b]$, $0 \leq a < b \leq 1$, with $|g(t)| \leq 1$ and $|g'(t)| \leq \log R$ throughout $[a, b]$. Suppose that $e^{\sqrt{\log R}} \leq z \leq R$ and write $R = z^u$. Then*

$$\sum_{\substack{R^a < n \leq R^b \\ P^-(n) > z}} \frac{1}{n} g\left(\frac{\log n}{\log R}\right) = e^{-\gamma} \frac{\log R}{\log z} \left(\int_a^b g(t) dt + O\left(\frac{\log u}{u}\right) \right).$$

Proof. Let $\delta = \frac{\log u}{u}$ and $a' = \max(\delta, a)$. We separate the sum into two parts:

$$S_1 = \sum_{\substack{R^a < n \leq R^{a'} \\ P^-(n) > z}} \frac{1}{n} g\left(\frac{\log n}{\log R}\right), \quad S_2 = \sum_{\substack{R^{a'} < n \leq R^b \\ P^-(n) > z}} \frac{1}{n} g\left(\frac{\log n}{\log R}\right),$$

If $\delta < a$ then $S_1 = 0$, otherwise we have the crude bound

$$|S_1| \leq \sum_{\substack{P^+(n) \leq R^\delta \\ P^-(n) > z}} \frac{1}{n} \ll \frac{\log R^\delta}{\log z} = \delta \frac{\log R}{\log z}.$$

We use partial summation on S_2 , first writing

$$S_2 := \sum_{\substack{R^{a'} < n \leq R^b \\ P^-(n) > z}} \frac{1}{n} g\left(\frac{\log n}{\log R}\right) = \int_{R^{a'}}^{R^b} \frac{1}{t} g\left(\frac{\log t}{\log R}\right) d\Phi(t, z).$$

By Hypothesis, $\frac{\log t}{\log z} \leq \sqrt{\log t}$ for $t \leq R$. Hence, by Theorem 2.20 (iii),

$$\Phi(t, z) = \frac{e^{-\gamma t}}{\log z} + E(t), \quad E(t) = O\left(\frac{t}{e^{u\delta} \log z}\right).$$

Therefore,

$$\begin{aligned} S_2 &= \frac{e^{-\gamma}}{\log z} \int_{R^{a'}}^{R^b} g\left(\frac{\log t}{\log R}\right) \frac{dt}{t} + \frac{E(t)g\left(\frac{\log t}{\log R}\right)}{t} \Big|_{R^{a'}}^{R^b} - \int_{R^{a'}}^{R^b} E(t) \left[\frac{g'\left(\frac{\log t}{\log R}\right)}{t^2 \log R} - \frac{g\left(\frac{\log t}{\log R}\right)}{t^2} \right] dt \\ &= \frac{e^{-\gamma} \log R}{\log z} \int_{a'}^b g(y) dy + O\left(\frac{\log R}{e^{u\delta} \log z}\right). \end{aligned}$$

Recalling that $\delta = \frac{\log u}{u}$ and our bound on S_1 , the lemma follows; if $\delta < a$ then $S = S_2$ and otherwise we use that $\int_a^{a'} |g| \leq \int_0^\delta 1 = \delta$. \square

Lemma 7.13. *Suppose that $f \in C^1(\mathcal{R}_k)$, $|f(\mathbf{x})| \leq 1$ on \mathcal{R}_k , and*

$$\max_{\mathbf{x} \in \mathcal{R}_k} \max_i \left| \frac{\partial f}{\partial x_i}(\mathbf{x}) \right| \leq \log R.$$

Let $R = z^u$, where $3 \leq u \leq \sqrt{\log R}$. then

$$\sum_{\substack{P^-(n_1 \cdots n_k) > z \\ \mu^2(n_1 \cdots n_k) = 1}} \frac{f\left(\frac{\log n_1}{\log R}, \dots, \frac{\log n_k}{\log R}\right)}{n_1 \cdots n_k} = \left(\frac{e^{-\gamma} \log R}{\log z} \right)^k \left[\int_{\mathcal{R}_k} f + O_k\left(\frac{\log u}{u}\right) \right].$$

Proof. We first insert “missing” summands corresponding to $\mu^2(n_1 \cdots n_k) = 0$. These have total at most

$$\sum_{\substack{P^-(n_1 \cdots n_k) > z \\ \mu^2(n_1 \cdots n_k) = 0}} \frac{1}{n_1 \cdots n_k} \leq k^2 \sum_{p > z} \frac{1}{p^2} \left(\sum_{\substack{P^-(m) > z \\ m \leq R}} \frac{1}{m} \right)^k \ll_k \frac{1}{z} \left(\frac{\log R}{\log z} \right)^k,$$

which is tiny. Repeated application of Lemma 7.12 (each time with $a = 0$) shows that

$$\sum_{P^-(n_1 \cdots n_k) > z} \frac{f\left(\frac{\log n_1}{\log R}, \dots, \frac{\log n_k}{\log R}\right)}{n_1 \cdots n_k} = \left(\frac{e^{-\gamma} \log R}{\log z} \right)^k \left[\int_{\mathcal{R}_k} f + O_k\left(\frac{\log u}{u}\right) \right],$$

which implies the desired conclusion. \square

Proposition 7.14. *Let $F \in \mathcal{F}_k$. Define ξ by (7.36).*

(i) *Under the hypotheses of Proposition 7.8, we have*

$$\sum_{N < n \leq 2N} w(n) \sim VN \left(e^{-\gamma} \frac{\log z}{\log R} \right)^k I(F) \quad (N \rightarrow \infty),$$

where

$$(7.37) \quad I(F) = \int_{\mathcal{R}_k} F^2(\mathbf{x}) d\mathbf{x}.$$

(ii) Under the hypotheses of Proposition 7.9, we have

$$\sum_{N < n \leq 2N} \sum_{m=1}^k w(n) \mathbb{1}_{a_m n + b_m \text{ prime}} \sim VN \left(e^{-\gamma} \frac{\log z}{\log R} \right)^k \frac{k\theta}{2} J(F) \quad (N \rightarrow \infty),$$

where

$$(7.38) \quad J(F) = \int \cdots \int \left(\int F(\mathbf{x}) dx_1 \right)^2 dx_2 \cdots dx_k.$$

Proof. From the definitions (7.7), we have $R = z^u$, where

$$u = s^2 \left(\frac{\theta}{2} - \frac{1}{s} \right) \asymp s^2.$$

(i) From Proposition 7.8, the definition (7.36) of ξ and Lemma 7.13, we have

$$\sum_{N < n \leq 2N} w(n) = \sigma^2 VN \left(e^{-\gamma} \frac{\log R}{\log z} \right)^k I(F) \left(1 + O\left(\frac{\log s}{s^2} \right) \right) + O\left(\frac{N}{(\log N)^{99k}} \right),$$

where

$$\sigma = \prod_{z < p \leq R} (1 + k/p)^{-1} \sim \left(\frac{\log z}{\log R} \right)^k.$$

The final error term is negligible since

$$V\sigma^2 \geq \prod_{p \leq 2k} \left(1 - \frac{p-1}{p} \right) \prod_{2k < p \leq R} \left(1 - \frac{k}{p} \right)^3 \gg_k \frac{1}{(\log N)^{3k}}.$$

(ii) From the symmetry of F , we see that $\zeta_m(\mathbf{r})$ is independent of m . By Lemma 7.10,

$$\sum_{\mathbf{r}} \frac{\zeta_1^2(\mathbf{r})}{r_1 \cdots r_k} = \sigma^2 \sum_{r_2, \dots, r_k} \frac{1}{r_2 \cdots r_k} \left(\sum_{r_1} \frac{1}{r_1} F\left(\frac{\log r_1}{\log R}, \dots, \frac{\log r_k}{\log R} \right) \right)^2.$$

For each i set $x_i = \frac{\log r_i}{\log R}$. With x_2, \dots, x_k fixed we have $0 \leq x_1 \leq 1 - (x_2 + \cdots + x_k)$.

By Lemma 7.12, the sum on r_1 is equal to

$$e^{-\gamma} \frac{\log R}{\log z} \left[\underbrace{\int_0^{1-x_2-\cdots-x_k} F(\mathbf{x}) dx_1}_{f(x_2, \dots, x_k)} + O_F\left(\frac{\log s}{s^2} \right) \right], \quad x_i = \frac{\log r_i}{\log R} \quad (2 \leq i \leq k).$$

Lemma 7.13 then implies that

$$\sum_{\mathbf{r}} \frac{\zeta_1^2(\mathbf{r})}{r_1 \cdots r_k} \sim \sigma^2 \left(e^{-\gamma} \frac{\log R}{\log z} \right)^{k+1} J(F).$$

Recalling Proposition 7.9, we have

$$\sum_{m=1}^k \sum_{N < n \leq 2N} w(n) \mathbb{1}_{a_m n + b_m \text{ prime}} \sim \frac{kVN/\log N}{\prod_{p \leq z} (1 - 1/p)} \sum_{\mathbf{r} \in \mathcal{D}} \frac{\zeta_1(\mathbf{r})^2}{r_1 \cdots r_k}.$$

Now $\prod_{p \leq z} (1 - 1/p) \sim e^{-\gamma} / \log z$ by Mertens, and $\frac{\log R}{\log N} \sim \frac{\theta}{2}$, and the desired asymptotic follows. \square

Armed with Proposition 7.14, we can now apply these results to prime gaps and prime k -tuples.

Theorem 7.15. *Fix $k \in \mathbb{N}$ and $m \in \mathbb{N}$, and assume Hypothesis $EH(\theta)$. There is a constant c_k such that the following holds. Suppose that there is a function $F \in \mathcal{F}_k$ and such that*

$$M_k(F) := \frac{kJ(F)}{I(F)} > \frac{2(m-1)}{\theta},$$

where $I(F), J(F)$ are defined in (7.37) and (7.38), respectively. Then, for all sufficiently large N , and all admissible tuples $(a_1n + b_1, \dots, a_kn + b_k)$ of linear forms, with

$$1 \leq a_i \leq \log^{100} N, \quad -a_iN/2 < b_i \leq N \log^{100} N \quad (1 \leq i \leq k),$$

there are $\gg N/(\log N)^{c_k}$ integers $n \in (N, 2N]$ for which at least m of the numbers $a_1n + b_1, \dots, a_kn + b_k$ are prime.

In particular, unconditionally the conclusion holds provided that $M_k(F) > 4(m-1)$.

Proof. Let

$$S = \sum_{N < n \leq 2N} v(n)w(n), \quad v(n) := \sum_{j=1}^k \mathbb{1}_{a_jn + b_j \text{ prime}} - (m-1).$$

By the two parts of Proposition 7.14, we have

$$S \sim VN \left(e^{-\gamma} \frac{\log z}{\log R} \right)^k \left[\frac{kJ(F)\theta}{2} - (m-1)I(F) \right].$$

By hypothesis, the bracketed expression is positive. From (7.11) we have

$$V \geq \prod_{p \leq z} \left(1 - \frac{\min(k, p-1)}{p} \right) \gg (\log z)^{-k},$$

and thus

$$S' := \sum_{\substack{N < n \leq 2N \\ v(n) \geq 1}} w(n) \geq \sum_{N < n \leq 2N} \frac{v(n)w(n)}{k} = \frac{S}{k} \gg \frac{N}{(\log N)^k}.$$

It follows that there are many values of n with $v(n) > 0$. More precisely, by Cauchy-Schwarz,

$$(S')^2 \leq \#\{N < n \leq 2N : v(n) \geq 1\} \left(\sum_{N < n \leq 2N} w(n)^2 \right).$$

Thus,

$$(7.39) \quad \#\{N < n \leq 2N : v(n) \geq 1\} \gg \frac{N^2}{(\log N)^{2k}} \left(\sum_{N < n \leq 2N} w(n)^2 \right)^{-1}$$

By (7.12),

$$0 \leq w(n) \leq \prod_{j=1}^k \tau(a_jn + b_j)^3.$$

Hence, by Hölder's inequality and the bound $a_i n + b_i \leq 3N(\log N)^{100}$,

$$\begin{aligned} \sum_{N < n \leq 2N} w(n)^2 &\leq \sum_{N < n \leq 2N} \prod_{j=1}^k \tau(a_j n + b_j)^6 \\ &\leq \prod_{j=1}^k \left(\sum_{N < n \leq 2N} \tau(a_j n + b_j)^{6k} \right)^{1/k} \\ &\leq \sum_{d \leq 3N(\log N)^{100}} \tau^{6k}(d) \\ &\ll N(\log N)^{100+2^{6k}-1}. \end{aligned}$$

Combined with (7.39), this completes the proof of the first claim, with $c_k = 2k + 100 + 2^{6k} - 1$.

The final statement follows from the Bombieri-Vinogradov Theorem, which implies Hypothesis EH(θ) for all $\theta < 1/2$. \square

7.4. Bounds on $M_k(F)$.

Definition 6. Let

$$M_k := \sup_{F \in \mathcal{F}_k} M_k(F) = \sup_{F \in \mathcal{F}_k} \frac{kJ(F)}{I(F)}.$$

We begin with a simple upper bound for M_k from [109].

Theorem 7.16 ([109]). *We have $M_k \leq \frac{k}{k-1} \log k = \log k + O(\frac{\log k}{k})$.*

Proof. Let x_2, \dots, x_k be given and set $y = 1 - (x_2 + \dots + x_k)$. The integral over those \mathbf{x} with $y = 0$ has measure zero and can be discarded. Thus, we may assume that $y > 0$. For any $A > 0$, by Cauchy-Schwarz we have

$$\begin{aligned} \left(\int_0^y F(\mathbf{x}) dx_1 \right)^2 &\leq \int_0^y (1 + Ax_1) F(\mathbf{x})^2 dx_1 \int_0^y \frac{dx_1}{1 + Ax_1} \\ &= \frac{\log(1 + Ay)}{A} \int_0^y (1 + Ax_1) F(\mathbf{x})^2 dx_1. \end{aligned}$$

Put $A = B/y$ for some constant B to be determined, then integrate over x_2, \dots, x_k . We get

$$J(F) \leq \frac{\log(1 + B)}{B} \int_{\mathcal{R}_k} (1 - x_2 - \dots - x_k + Bx_1) F(\mathbf{x})^2 dx.$$

Since $F(\mathbf{x})$ is symmetric, we may interchange x_1 and x_i . Doing this for each i and summing gives

$$kJ(F) \leq \frac{\log(1 + B)}{B} \int_{\mathcal{R}_k} (k - (k-1) \sum x_i + B \sum x_i) F(\mathbf{x})^2 dx.$$

Taking $B = k - 1$, the integral above equals $kI(F)$ and this completes the proof. \square

Theorem 7.17. *We have*

$$M_k \geq \log k - \log_2 k - O(1).$$

Proof. Let $\delta > 0$, and let $g : [0, \delta] \rightarrow [0, \infty)$ be a function with $|g(t)| \leq 1$ for all t . We'll specialize to functions of the type

$$F(\mathbf{x}) = g(x_1) \cdots g(x_k).$$

For short, let

$$m_1 = \int_0^\delta g(t) dt, \quad m_2 = \int_0^\delta g^2(t) dt.$$

We interpret $I(F)$ and $J(F)$ probabilistically. Let Z_1, \dots, Z_k be independent random variables with density function $\frac{1}{m_2}g^2(t)$, $0 \leq t \leq \delta$. Then

$$I(F) = \int_{\mathcal{R}_k} g^2(x_1) \cdots g^2(x_k) d\mathbf{x} = m_2^k \mathbb{P}(Z_1 + \cdots + Z_k \leq 1).$$

Also,

$$\begin{aligned} J(F) &\geq \int_{x_2 + \cdots + x_k \leq 1 - \delta} \cdots \int g^2(x_2) \cdots g^2(x_k) \left(\int_0^\delta g(x_1) dx_1 \right)^2 dx_2 \cdots dx_k \\ &= m_1^2 m_2^{k-1} \mathbb{P}(Z_2 + \cdots + Z_k \leq 1 - \delta). \end{aligned}$$

Thus,

$$(7.40) \quad M_k(F) \geq \frac{km_1^2}{m_2} \cdot \frac{\mathbb{P}(Z_2 + \cdots + Z_k \leq 1 - \delta)}{\mathbb{P}(Z_1 + \cdots + Z_k \leq 1)} \geq \frac{km_1^2}{m_2} \mathbb{P}(Z_2 + \cdots + Z_k \leq 1 - \delta).$$

We will choose g so that the probability on the RHS is about 1. If

$$\mu := \mathbb{E}Z_i = \frac{1}{m_2} \int_0^\delta t g^2(t) dt,$$

then we want

$$(7.41) \quad \mu < \frac{1 - \delta}{k - 1}$$

so that

$$\mathbb{E}(Z_2 + \cdots + Z_k) = (k - 1)\mu < 1 - \delta.$$

We can bound the probability of a large deviation from the mean using Chebyshev's inequality and the calculated variance

$$\sigma^2 := \mathbb{E}(Z_i - \mu)^2 = \mathbb{E}Z_i^2 - \mu^2 = \frac{1}{m_2} \int_0^\delta t^2 g^2(t) dt - \mu^2.$$

Then

$$\mathbb{E}(Z_2 + \cdots + Z_k - (k - 1)\mu)^2 = (k - 1)\sigma^2.$$

Thus, under the assumption of (7.41), we have

$$(7.42) \quad \begin{aligned} \mathbb{P}(Z_2 + \cdots + Z_k \geq 1 - \delta) &\leq \mathbb{P}(|Z_2 + \cdots + Z_k - (k - 1)\mu| \geq 1 - \delta - (k - 1)\mu) \\ &\leq \frac{(k - 1)\sigma^2}{(1 - \delta - (k - 1)\mu)^2}. \end{aligned}$$

We will choose parameters so that the right side of (7.42) is very small.

It then remains to maximize m_1^2/m_2 subject to $\mu \lesssim 1/k$. Motivated by the proof of Theorem 7.16, for any $A > 0$ we have

$$m_1^2 \leq \left(\int_0^\delta (1 + At)g^2(t) dt \right) \left(\int_0^\delta \frac{dt}{1 + At} \right) = (m_2 + Am_2\mu) \frac{\log(1 + A\delta)}{A}.$$

Moreover, equality holds only for $g(t) = \frac{1}{1+At}$. That is,

$$(7.43) \quad \frac{m_1^2}{m_2} \leq \min_{A>0} \left(\frac{1}{A} + \mu \right) \log(1 + A\delta).$$

The minimum occurs when

$$\left(\frac{1}{A} + \mu \right) \frac{\delta}{1 + A\delta} = \frac{\log(1 + A\delta)}{A^2},$$

and then taking $g(t) = \frac{1}{1+At}$ gives equality in (7.43). With this function $g(t)$ and assuming that $A\delta$ is large, we compute

$$m_1 = \frac{\log(1 + A\delta)}{A}, \quad m_2 = \frac{\delta}{1 + A\delta} \approx \frac{1}{A},$$

and

$$\mu = \frac{1}{m_2 A^2} \left(\log(1 + A\delta) - 1 + \frac{1}{1 + A\delta} \right) \approx \frac{\log(1 + A\delta)}{A}.$$

We will take a convenient choice of A, δ satisfying the simpler relation

$$(7.44) \quad A = k \log(1 + A\delta).$$

Then

$$\mu = \frac{1}{k} - \frac{1}{A} + \frac{1}{kA\delta}$$

and

$$\frac{m_1^2}{m_2} = \frac{1}{k^2} \left(A + \frac{1}{\delta} \right) > \frac{A}{k^2}.$$

Thus, by (7.40) and (7.42),

$$(7.45) \quad M_k(F) \geq \frac{A}{k} \left(1 - \frac{(k-1)\sigma^2}{(1-\delta-(k-1)\mu)^2} \right).$$

Crudely,

$$\sigma^2 \leq \mathbb{E}Z_i^2 \leq \frac{1}{m_2} \left(\frac{A\delta}{1 + A\delta} \right)^2 \int_0^\delta \frac{t^2 dt}{(At)^2} = \frac{\delta^2}{1 + A\delta} < \frac{\delta}{A}.$$

Also, using (7.44), we compute (after some algebra)

$$1 - \delta - (k-1)\mu = (k - e^{A/k}) \left(\frac{1}{A} - \frac{1}{k(e^{A/k} - 1)} \right).$$

In particular, for this to be positive, we need $A < k \log k$. Combined with (7.45), we conclude that

$$M_k(F) \geq \frac{A}{k} \left(1 - \frac{(k-1)(e^{A/k} - 1)}{(k - e^{A/k})^2 \left(1 - \frac{A}{k(e^{A/k} - 1)} \right)^2} \right).$$

A good choice for A is

$$A = k(\log k - \log_2 k).$$

(this gives $\delta \sim \frac{1}{\log^2 k}$). Then $e^{A/k} = k/\log k$ and we see that

$$M_k \geq (\log k - \log_2 k) \left(1 - O\left(\frac{1}{\log k}\right) \right) = \log k - \log_2 k + O(1),$$

as required. \square

Together with Theorem 7.15, Theorem 7.17 immediately implies Theorem 7.6. To obtain the claimed bounds on K_m , notice that by Theorem 7.17 there is a $k \ll me^{4m}$ with $M_k > 4(m-1)$.

The PolyMath8b project provides better bounds on M_k , as well as numerical bounds when k is small.

Theorem [109, Theorem 3.9 (vii), (xi)]. We have

- (i) $M_{54} > 4$;
- (ii) $M_k = \log k - O(1)$.

Also, Maynard [97] proved that

$$(7.46) \quad M_5 > 2.$$

Consequently, assuming the Elliott-Halberstam conjecture, or any admissible 5-tuple, infinitely often at least two of the forms are prime.

7.5. Consecutive integers with large prime factors. One special case of the prime k -tuples conjecture, Conjecture 1.3 states that for infinitely many primes p , $p+1 = 2q$ for a prime q . In this direction, we prove

Theorem 7.18 (K. Ford and J. Maynard, 2014; unpublished). *There is a constant B so that for infinitely many $n \in \mathbb{N}$, $P^+(n) \geq n/B$ and $P^+(n+1) \geq (n+1)/B$.*

Lemma 7.19 (Heath-Brown [79]). *For any k there is a set of k positive integers a_1, \dots, a_k such that*

$$(7.47) \quad a_i - a_j = (a_i, a_j) \quad (i > j).$$

Examples are

$$\begin{aligned} k = 4 : & \quad \{6, 8, 9, 12\} \\ k = 5 : & \quad \{60, 63, 64, 66, 72\}. \end{aligned}$$

The condition (7.47) is equivalent to $(a_i - a_j) | a_i$ for all $i \neq j$. Thus, Lemma 7.19 is one of the assertions in Lemma 1 of Heath-Brown [79]. As we do not require the other properties of the a_i from [79], our proof is much shorter.

Proof. By induction. If $\{a_1, \dots, a_k\}$ satisfies (7.47), then so does the $k+1$ element set

$$\{M, M - a_1, \dots, M - a_k\}, \quad M = a_1 \cdots a_k \prod_{i < j} |a_i - a_j|. \quad \square$$

Proof of Theorem 7.18. By Theorem 7.17, for some k we have $M_k > 4$. Thus, by Theorem 7.6, in any set of k admissible linear forms, two are prime infinitely often. Let a_1, \dots, a_k satisfy (7.47), which exist by Lemma 7.19. The set of forms $a_1 n + 1, \dots, a_k n + 1$ is admissible since for any prime p , $\prod (a_i n + 1) \not\equiv 0 \pmod{p}$ when $p|n$. By Theorem 7.6, for some pair $i < j$, infinitely often $a_i n + 1$ and $a_j n + 1$ are prime. By (7.47), $a_j - a_i = (a_i, a_j)$ and hence

$$\frac{a_j}{(a_i, a_j)}(a_i n + 1) \quad \text{and} \quad \frac{a_i}{(a_i, a_j)}(a_j n + 1)$$

are consecutive integers. Thus the theorem follows with

$$B = \max_{i \neq j} \frac{a_i}{(a_i, a_j)}.$$

□

7.6. Locally repeated values of Euler's function. We partially solve a longstanding conjecture about the solubility of

$$(7.48) \quad \phi(n+k) = \phi(n),$$

where ϕ is Euler's function and k is a fixed positive integer.

Hypothesis \mathcal{S}_k . The equation (7.48) holds for infinitely many n .

Erdős conjectured in 1945 that for any m , the simultaneous equations

$$(7.49) \quad \phi(n) = \phi(n+1) = \dots = \phi(n+m-1)$$

has infinitely many solutions n . If true, this would immediately imply hypothesis \mathcal{S}_k for every k . However, there is only one solution of (7.49) known when $m \geq 3$, namely $n = 5186, m = 3$. In 1956, Sierpiński [125] showed that for any k , (7.48) has at least one solution n (e.g. take $n = (p-1)k$, where p is the smallest prime not dividing k). This was extended by Schinzel [117] and by Schinzel and Wakulicz [120], who showed that for any $k \leq 2 \cdot 10^{58}$ there are at least two solutions of (7.48). In 1958, Schinzel [117] explicitly conjectured that \mathcal{S}_k is true for every $k \in \mathbb{N}$. There is good numerical evidence for \mathcal{S}_k , at least when $k = 1$ or k is even [63]. Information about solutions for $k \in \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12\}$ can also be found in OEIS [104] sequences A001274, A001494, A330251, A179186, A179187, A179188, A179189, A179202, A330429, A276503, A276504 and A217139, respectively. Below 10^{11} there are very few solutions of (7.48) when $k \equiv 3 \pmod{6}$ [63], e.g. only the two solutions $n \in \{3, 5\}$ for $k = 3$ are known. A further search by G. Resta (see [104], sequence A330251) reveals 17 more solutions in $[10^{12}, 10^{15}]$.

There is a close connection between Hypothesis \mathcal{S}_k for even k and generalized prime twins.

Hypothesis $\mathcal{P}(a, b)$: there are infinitely many $n \in \mathbb{N}$ such that both $an + 1$ and $bn + 1$ are prime.

Hypothesis $\mathcal{P}(a, b)$ is a special case of the Prime k -tuples conjecture, Conjecture 1.3. Schinzel [117] observed that Hypothesis $\mathcal{P}(1, 2)$ implies \mathcal{S}_k for every even k . The proof is simple: if $n + 1$ and $2n + 1$ are prime and larger than k , then

$$\phi(k(2n+1)) = \phi((n+1)2k) = 2n\phi(k).$$

Graham, Holt and Pomerance [63] generalized this idea, showing the following.

Lemma 7.20 ([63, Theorem 1]). *For any k and any number j such that j and $j+k$ have the same prime factors, Hypothesis $\mathcal{P}(\frac{j}{(j, j+k)}, \frac{j+k}{(j, j+k)})$ implies \mathcal{S}_k .*

This also has an easy proof: if $\frac{j}{(j, j+k)}r + 1$ and $\frac{j+k}{(j, j+k)}r + 1$ are both prime, then $n = j(\frac{j+k}{(j, j+k)}r + 1)$ satisfies (7.48). Note that for odd k there are no such numbers j , and for each even k there are finitely many such j (see [63], Section 3). Extending a bound of Erdős, Pomerance and Sárkőzy [44] in the case $k = 1$, Graham, Holt and Pomerance showed that the solutions of (7.48) not generated from Lemma 7.20 are very rare, with counting function $O_k(x \exp\{-(\log x)^{1/3}\})$. Yamada [134] sharpened this bound to $O_k(x \exp\{-(1/\sqrt{2} + o(1))\sqrt{\log x \log \log \log x}\})$. Assuming the Hardy-Littlewood conjectures [72], when k is even we conclude that there are $\sim C_k x / \log^2 x$ solutions $n \leq x$ of (7.48), where $C_k > 0$.

Using the fact that $K_2 = 50$ is admissible in Theorem 2.5, we will prove the following.

Theorem 7.21 (Ford [48], 2020). *We have*

- (a) *For any k that is a multiple of 442720643463713815200, \mathcal{S}_k is true;*
- (b) *There is some even $\ell \leq 3570$ such that \mathcal{S}_k is true whenever $\ell|k$; consequently, the number of $k \leq x$ for which \mathcal{S}_k is true is at least $x/3570$.*

Under the assumption of the Elliott-Halberstam Conjecture (Conjecture 7.3), Maynard [97] showed that $K_2 \leq 5$, improving the bound $K_2 \leq 6$ proved by Goldston, Pintz and Yıldırım[59] under the same hypothesis. A generalized version of the Elliott-Halberstam conjecture (in the notation of [109], this is the statement that $\text{GEH}[\theta]$ holds for all $\theta < 1$), implies that $K_2 \leq 3$ [109, Theorem 16 (xii)]. Improvements to K_2 allow us to improve significantly on Theorem 7.21.

Theorem 7.22 (Ford [48], 2020). *If $K_2 \leq 5$, then \mathcal{S}_k is true for all k with $30|k$. If $K_2 \leq 4$, then \mathcal{S}_k is true for all k with $6|k$. In particular, the Elliott-Halberstam conjecture implies \mathcal{S}_k for all k with $30|k$, and the Generalized Elliott-Halberstam conjecture implies \mathcal{S}_k for all k with $6|k$.*

Incidentally, the conclusion of Theorem 7.22 when $K_2 \leq 4$ is not improved if we have the stronger bound $K_2 \leq 3$.

Using Theorem 7.6, we also make progress toward Erdős' conjecture that (7.49) has infinitely many solutions.

Theorem 7.23 (Ford [48], 2020). *For any $m \geq 3$ there is a tuple of distinct positive integers h_1, \dots, h_m so that for any $\ell \in \mathbb{N}$, the simultaneous equations*

$$\phi(n + \ell h_1) = \phi(n + \ell h_2) = \dots = \phi(n + \ell h_m)$$

have infinitely many solutions n .

Very recently, Sungjin Kim [91] proved weaker statements in the direction of Theorem 7.21. He used Theorem 2.5 to show that \mathcal{S}_k holds for some $k \in \{B, 2B, \dots, 50B\}$, with $B = \prod_{p \leq 50} p$. He also proved that the set of k for which \mathcal{S}_k holds has counting function $\gg \log \log x$.

Now we get to the proofs. Throughout, $1 \leq a < b$ are integers. We first show that $\mathcal{P}(a, b)$ implies \mathcal{S}_k for certain k , inverting Lemma 7.20. Define

$$(7.50) \quad \kappa(a, b) = (b' - a') \prod_{p|a'b'} p, \quad a' = \frac{a}{(a, b)}, \quad b' = \frac{b}{(a, b)}.$$

We observe that $\kappa(a, b)$ is always even.

Lemma 7.24. *Assume $\mathcal{P}(a, b)$. Then \mathcal{S}_k holds for every k which is a multiple of $\kappa(a, b)$.*

Proof. Define $a' = \frac{a}{(a, b)}$, $b' = \frac{b}{(a, b)}$ and observe that $\mathcal{P}(a, b) \Rightarrow \mathcal{P}(a', b')$. Let $s = \prod_{p|a'b'} p$, and suppose that $r > \max(a', b')$ such that $a'r + 1$ and $b'r + 1$ are both prime. Let $\ell \in \mathbb{N}$ and set

$$m_1 = b'\ell s(a'r + 1), \quad m_2 = a'\ell s(b'r + 1).$$

As all of the prime factors of $a'b'$ divide ℓs , we have $\phi(b'\ell s) = b'\phi(\ell s)$ and $\phi(a'\ell s) = a'\phi(\ell s)$, and it follows that $\phi(m_1) = \phi(m_2)$. Finally, $m_1 - m_2 = (b' - a')\ell s = \kappa(a, b)$. \square

Proof of Theorem 7.21. Let

$$\{a_1, \dots, a_{50}\} = \{1, 2, 4, 5, 6, \dots, 48, 49, 52, 56\},$$

By Theorem 7.6, for some i, j with $1 \leq i < j \leq 50$, $\mathcal{P}(a_i, a_j)$ is true. We compute

$$\text{lcm}\{\kappa(a_i, a_j) : 1 \leq i < j \leq 50\} = 442720643463713815200 = 2^5 3^3 5^2 \prod_{7 \leq p \leq 47} p,$$

and thus (a) follows from Lemma 7.24.

For part (b), we take

$$\begin{aligned} \{a_1, \dots, a_{50}\} = \{ & 15, 20, 30, 36, 40, 45, 60, 72, 75, 80, 90, 96, 100, 108, 120, 135, 144, 150, 180, 192, 200, \\ & 216, 225, 240, 250, 270, 288, 300, 320, 324, 360, 375, 384, 400, 405, 450, 480, 500, 540, 600, \\ & 720, 750, 810, 900, 960, 1080, 1200, 1440, 1500, 1800\}, \end{aligned}$$

numbers that only have prime factors 2, 3, 5. We also compute that

$$\max_{1 \leq i < j \leq 50} \kappa(a_i, a_j) = 3570,$$

and again invoke Lemma 7.24. This proves (b). \square

Remarks. For any choice of a_1, \dots, a_{50} , $\frac{442720643463713815200}{6} | L(\mathbf{a})$, where

$$L(\mathbf{a}) = \text{lcm}\{\kappa(a_i, a_j) : i < j\}.$$

Without loss of generality, assume $(a_1, \dots, a_{50}) = 1$. For a prime $7 \leq p \leq 47$, if $p | a_i$ for some i then $p \nmid a_j$ for some j and thus $p | \kappa(a_i, a_j)$. If $p \nmid a_i$ for all i , by the pigeonhole principle, there are two indices with $a_i \equiv a_j \pmod{p}$. Again, $p | \kappa(a_i, a_j)$. Thus, $p | L(\mathbf{a})$. Now we show that $5^2 | L(\mathbf{a})$. Let $S_b = \{a_i : 5^b || a_i\}$ for $b \geq 0$. Then $|S_0| \geq 1$. If $|S_b| \geq 1$ for some $b \geq 2$, then there are i, j with $5^2 | a_i$ and $5 \nmid a_j$, and then $5^2 | \kappa(a_i, a_j)$. Otherwise, we have $|S_b| \geq 21$ for some $b \in \{0, 1\}$. By the pigeonhole principle, there is $i \neq j$ with $5^b || a_i, 5^b || a_j$ and $5^{b+2} | (a_i - a_j)$. This also implies that $5^2 | \kappa(a_i, a_j)$. Similarly, let $T_b = \{a_i : 3^b || a_i\}$. Then we have either $|T_b| \geq 1$ for some $b \geq 2$, or $|T_i| \geq 7$ for some $i \in \{0, 1\}$. Either way, $3^2 | L(\mathbf{a})$. Let $U_b = \{a_i : 2^b || a_i\}$. Then either $|U_b| \geq 1$ for some $b \geq 4$ or $|U_b| \geq 9$ for some $b \in \{0, 1, 2, 3\}$. Either way, $2^4 | L(\mathbf{a})$. It is easy to construct $\mathbf{a} = (a_1, \dots, a_{50})$ such that $3^3 \nmid L(\mathbf{a})$ and $2^5 \nmid L(\mathbf{a})$. However, such constructions seem to always produce $q | L(\mathbf{a})$ for some prime $q > 50$.

We believe that 3570 is the smallest number than can be produced for Theorem 7.21 (b). Using numbers divisible by 4 or more primes always produces some very large $\kappa(a, b)$, thus we limited our search to sets of numbers composed only of the primes 2,3,5. For a given finite set of integers $\{b_1, \dots, b_r\}$, the problem of minimizing $\max_{i,j \in I} \kappa(b_i, b_j)$ over all 50-element subsets $I \subset \{1, \dots, r\}$, is equivalent to that of finding the largest clique in a graph. Take vertex set $\{1, \dots, r\}$ and draw an edge from i to j if $\kappa(b_i, b_j) \leq t$. Using the Sage routine `clique_number()` with $t = 3569$ and $\{b_1, \dots, b_r\}$ being the smallest 800 numbers composed only of primes 2,3,5 (the largest being 12754584), we find that the largest clique has size 49.

Proof of Theorem 7.22. Same as the proof of Theorem 7.21 (a), but take $\{a_1, a_2, a_3, a_4, a_5\} = \{1, 2, 3, 4, 6\}$ if $K_2 \leq 5$ and $\{a_1, \dots, a_4\} = \{1, 2, 3, 4\}$ if $K_2 \leq 4$. \square

Proof of Theorem 7.23. Let $m \geq 2$, $k = K_m$ and consider any set $\{a_1, a_2, \dots, a_k\}$ of k positive integers. By Theorem 7.6, there are $1 \leq i_1 < i_2 < \dots < i_m \leq k$ such that for infinitely many r , the m numbers $a_{i_1}r + 1, \dots, a_{i_m}r + 1$ are all prime. Let r be such a number. Define

$$h_j = \frac{(a_{i_1} \cdots a_{i_m})^2}{a_{i_j}} \quad (1 \leq j \leq m).$$

Let $\ell \in \mathbb{N}$ and set $n = \ell(a_{i_1} \cdots a_{i_m})^2 r$. Then, since $a_{i_j} | h_j$ for all j , it follows that for any j ,

$$\phi(n + \ell h_j) = \phi(\ell h_j(a_{i_j} r + 1)) = \phi(\ell h_j) a_{i_j} r = \phi(\ell h_j a_{i_j}) r. \quad \square$$

7.7. Locally repeated values of σ . One can ask analogous questions about the sum of divisors function $\sigma(n)$. As $\sigma(p) = p + 1$ vs $\phi(p) = p - 1$, oftentimes one can port theorems about ϕ over to σ . This is not the case here, since our results depend heavily on the existence of solutions of

$$a\phi(b) = b\phi(a),$$

which is true if and only if a and b have the same set of prime factors. The analogous equation

$$a\sigma(b) = b\sigma(a) \Leftrightarrow \frac{\sigma(a)}{a} = \frac{\sigma(b)}{b}$$

has more sporadic solutions, e.g. if a, b are both perfect numbers or multiply perfect numbers.

Theorem 7.25 (Ford [48], 2020). *For a positive proportion of all $k \in \mathbb{N}$, the equation*

$$\sigma(n) = \sigma(n + k)$$

has infinitely many solutions n .

As we shall see from the proof, there is a specific number A and a finite set \mathcal{B} such that for some element $b \in \mathcal{B}$, the equation $\sigma(n) = \sigma(n + k)$ has infinitely many solutions for all numbers $k = \ell b$ where $(\ell, A) = 1$. Unfortunately, our methods cannot specify any particular k for which the conclusion holds. Our method requires finding, for $t = K_2$, numbers a_1, \dots, a_t so that

$$(7.51) \quad \frac{\sigma(a_1)}{a_1} = \dots = \frac{\sigma(a_t)}{a_t} = y.$$

Such collections of numbers are sometimes referred to as “friends” in the literature, e.g. [107]. Finding larger collections of a_i satisfying (7.51) leads to stronger conclusions.

Theorem 7.26 (Ford [48], 2020). *Let $m \geq 2$, let $t = K_m$ and assume that there is a y and positive integers a_1, \dots, a_t satisfying (7.51). Then there are positive integers $h_1 < h_2 < \dots < h_m$ so that for a positive proportion of integers ℓ , there are infinitely many solutions of*

$$\sigma(n + \ell h_1) = \dots = \sigma(n + \ell h_m).$$

It is known [103] that for $y = 9$, there is a set of 2095 integers satisfying (7.51). The number $y = 9$ has the largest known multiplicity of $\sigma(n)/n$. Also $K_2 \leq 50$ [109], and hence Theorem 7.25 follows from the case $m = 2$ of Theorem 7.26. We cannot make the conclusion unconditional when $m \geq 3$, since the best known bounds for K_3 is $K_3 \leq 35410$ [109, Theorem 3.2 (ii)].

Conjecture 7.27. *For any t , there is an y such that $\sigma(a)/a = y$ has at least t solutions. That is, there are arbitrarily large circles of friends.*

Clearly, Conjecture 7.27 implies the conclusion of Theorem 7.26 for all m . In [39], Erdős mentions Conjecture A and states that he doesn’t know of any argument that would lead to its resolution. In the opposite direction, Wirsing [132] showed that the number of $n \leq z$ with $\sigma(n)/n = y$ is $O(z^{c/\log \log z})$ for some c , uniformly in y . Pollack and Pomerance [107] studied the solutions of (7.51), gathering data on pairs, triples and quadruples of friends, but did not address Conjecture A.

Using (7.51) and prime pairs $an - 1$ and $bn - 1$, one can generate many solutions of $\sigma(n) = \sigma(n + k)$, analogous to Lemma 7.20; see Yamada [134, Theorem 1.1]. For example, one can generate solutions with $k = 1$ if there is an integer m with $\sigma(m)/m = \sigma(m + 1)/(m + 1) = y$ (the ratios need not be integers as claimed in [134]). Indeed, if $r > m + 1$, and $rm - 1$ and $r(m + 1) - 1$ are both prime, then

$$\begin{aligned}\sigma(m(r(m + 1) - 1)) &= \sigma(m)r(m + 1) = rm(m + 1)y, \\ \sigma((m + 1)(mr - 1)) &= \sigma(m + 1)rm = rm(m + 1)y.\end{aligned}$$

Yamada [134, Theorem 1.2] showed that there are $\ll x \exp\{-(1/\sqrt{2} + o(1))\sqrt{\log x \log \log x}\}$ solutions $n \leq x$ not generated in this way.

Proof of Theorem 7.26. Let $t = K_m$ and a_1, \dots, a_t satisfy (7.51). Put $A = \text{lcm}[a_1, \dots, a_t]$ and for each i define $b_i = A/a_i$. By Theorem 7.6 applied to the collection of linear forms $b_i n - 1$, $1 \leq i \leq t$, there exist i_1, \dots, i_m such that for infinitely many $r \in \mathbb{N}$, the m numbers $b_{i_j} r - 1$ are all prime. Let $r > A$ be such a number, and let $\ell \in \mathbb{N}$ such that $(\ell, A) = 1$ (this holds for a positive proportion of all ℓ). Let

$$t_j = \ell a_{i_j} (b_{i_j} r - 1) = \ell r - \ell a_{i_j} \quad (1 \leq j \leq m).$$

By (7.51), for every j we have

$$\sigma(t_j) = \sigma(\ell)\sigma(a_{i_j})b_{i_j}r = \sigma(\ell)ya_{i_j}b_{i_j}r = y\sigma(\ell)Ar. \quad \square$$

8. LARGE GAPS BETWEEN CONSECUTIVE PRIMES

8.1. Introduction. Let p_n denote the n^{th} prime, and let

$$G(X) := \max_{p_{n+1} \leq X} (p_{n+1} - p_n)$$

denote the maximum gap between consecutive primes less than X . It is clear from the prime number theorem that

$$G(X) \geq (1 + o(1)) \log X,$$

as the *average* gap between the prime numbers which are $\leq X$ is $\sim \log X$. Explicit gaps of (at least) this size may be constructed by observing that $P(n)+2, P(n)+3, \dots, P(n)+n$ is a sequence of $n-1$ composite numbers, where $P(n)$ is the product of the primes $\leq n$; by the prime number theorem, $P(n) = e^{(1+o(1))n}$.

In 1931, Westzynthius [131] proved that infinitely often the gap between consecutive prime numbers can be an arbitrarily large multiple of the average gap. His bound is⁶

$$G(X) \gg \frac{\log X \log_3 X}{\log_4 X}.$$

In 1934, Ricci [114] slightly improved this to $G(X) \gg \log X \log_3 X$. In 1935 Erdős [32] made a much larger improvement, showing

$$G(X) \gg \frac{\log X \log_2 X}{(\log_3 X)^2}$$

and in 1938 Rankin [112] added a quadruple-log, showing

$$(8.1) \quad G(X) \geq (c + o(1)) \frac{\log X \log_2 X \log_4 X}{(\log_3 X)^2}$$

with $c = \frac{1}{3}$. The constant c was increased several times [122, 113, 96, 106], ultimately getting to $c = 2e^\gamma$ by Pintz [106].

It was a well-known open problem (and Erdős prize problem) to show that one could take $c \rightarrow \infty$. In August 2014, in two independent papers of Ford-Green-Konyagin-Tao [49] and Maynard [99], it was shown that c could be taken to be arbitrarily large. The methods of proof in [49] and [99] are quite different. The arguments in [49] used recent results [66] on the number of solutions to linear equations in primes, whereas the arguments in [99] instead relied on a multidimensional prime-detecting sieve of the type introduced in [99] (but more complicated). Later, in [50], a quantitative improvement to Rankin's bound was given, namely

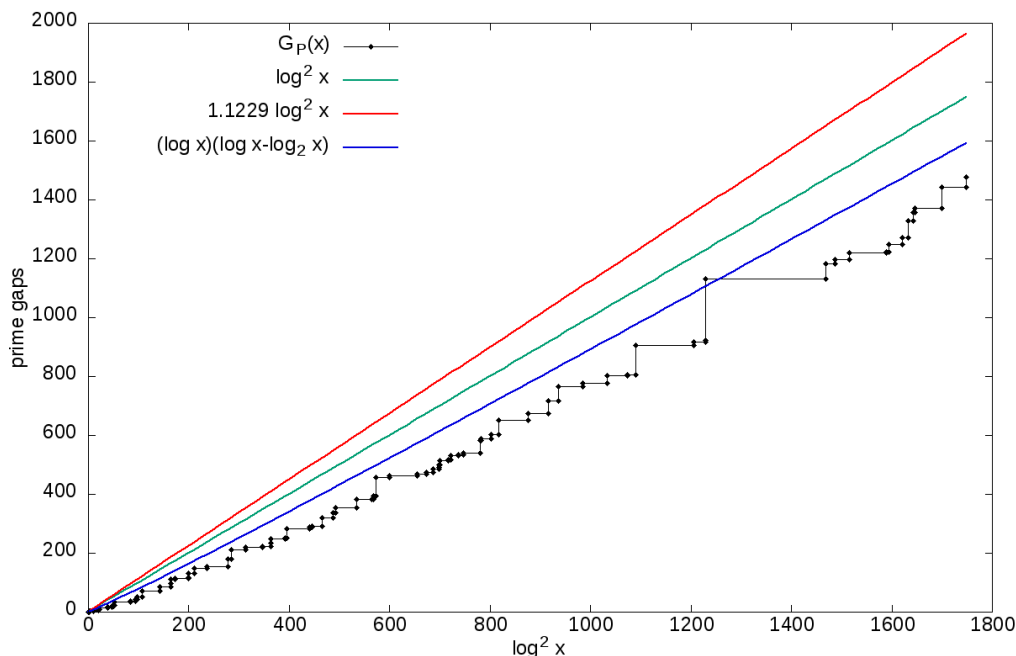
Theorem 8.1 (Ford-Green-Konyagin-Maynard-Tao [50, Theorem 1]). *For sufficiently large X , one has*

$$G(X) \gg \frac{\log X \log_2 X \log_4 X}{\log_3 X}.$$

Here we present a proof of the original theorem from [49] and [99] that the c in (8.1) may be taken arbitrarily large (without a specific rate of growth), which is much simpler than that in either of the two original papers. It is based on a hybrid approach, utilizing ideas worked out in [50], but without the need to make various estimates quantitative.

Theorem 8.2. *The bound (8.1) holds for any real number $c > 0$, if x is large enough, depending on c .*

⁶Recall that $\log_2 x = \log \log x$, $\log_3 x = \log \log \log x$, and so on.

FIGURE 1. $G(x)$ vs. various approximations

Based on a probabilistic model of primes, Cramér [24] conjectured that

$$\limsup_{X \rightarrow \infty} \frac{G(X)}{\log^2 X} = 1.$$

Granville [64] offered a refinement of Cramér's model and has conjectured that the lim sup above is in fact at least $2e^{-\gamma} = 1.1229\dots$. Recently, Banks, Ford and Tao [9] made a specific conjecture about the largest gap which is dependent on a problem called the *interval sieve*. These conjectures are well beyond the reach of our methods. Numerical evidence is inconclusive, in fact $\max_{X \leq 4 \cdot 10^{18}} G(X)/\log^2 X \approx 0.9206$, slightly below the predictions of Cramér and Granville. This bound is a consequence of the gap of size 1132 following the prime 1693182318746371. See also Figure 1 for a plot of $G(x)$ versus various approximations.

Unconditional upper bounds for $G(X)$ are far from the conjectured truth, the best being $G(X) \ll X^{0.525}$ and due to Baker, Harman and Pintz [8]. Even the Riemann Hypothesis only⁷ furnishes the bound $G(X) \ll X^{1/2} \log X$ [23].

8.1.1. *Notational conventions.* Our arguments will rely heavily on probabilistic arguments using discrete random variables. We will use boldface symbols such as \mathbf{X} or \mathbf{a} to denote random variables (and non-boldface symbols such as X or a to denote deterministic counterparts of these variables). Vector-valued random variables will be denoted in arrowed boldface, e.g. $\vec{\mathbf{a}} = (\mathbf{a}_s)_{s \in \mathcal{S}}$ might denote a random tuple of random variables \mathbf{a}_s indexed by some index set \mathcal{S} . The letters p and q will always denote primes.

⁷Some slight improvements are available if one also assumes some form of the pair correlation conjecture; see [78].

8.2. Overall plan of the proof. We construct many consecutive integers in $(X/2, X]$, each of which has a “very small” prime factor. By the Chinese Remainder Theorem, this is equivalent to sieving out an interval by progressions to small primes.

Definition 7 (Jacobsthal’s function). *Let x be a positive integer. Define $Y(x)$ to be the largest gap in the integers with no prime factor $\leq x$. Equivalently, $Y(x)$ is the largest integer y for which one may select residue classes $a_p \pmod p$, one for each prime $p \leq x$, which together “sieve out” (cover) a whole interval of the form $\{1, 2, \dots, y\}$.*

The equivalence of the two definitions of $Y(x)$ is easy by the Chinese remainder theorem. One consequence is that $(P(x), 2P(x)]$ contains $Y(x)$ consecutive numbers that have a prime factor $\leq x$, and thus these numbers are all composite. We conclude that

$$(8.2) \quad G(2P(x)) \geq Y(x).$$

Since $\log P(x) \sim x$ by the Prime Number Theorem, this essentially says that

$$G(X) \gtrsim Y(\log X).$$

All known lower bounds in $G(X)$ are based on lower bounds for $Y(x)$.

Fix a large, positive real number c , let x be a large integer and define

$$(8.3) \quad y := \left\lfloor cx \frac{\log x \log_3 x}{(\log_2 x)^2} \right\rfloor,$$

Also let

$$(8.4) \quad z := x^{\log_3 x / (5 \log_2 x)},$$

and introduce the three disjoint sets of primes

$$\mathcal{S} := \{s \text{ prime} : \log^{20} x < s \leq z\},$$

$$\mathcal{P} := \{p \text{ prime} : x/2 < p \leq x\},$$

$$\mathcal{Q} := \{q \text{ prime} : x < q \leq y\}.$$

We will show that $Y(x) \geq y - x$ by covering $(x, y]$ with residue classes modulo primes $\leq x$. Now $P(x) = e^{(1+o(1))x}$ by the prime number theorem, so (8.2) and (8.3) imply that

$$G(e^{(1+o(1))x}) \geq (1 + o(1))cx \log x \frac{\log_3 x}{(\log_2 x)^2}.$$

As G is monotone, Theorem 8.2 follows upon taking c arbitrarily large.

We first reduce the problem to finding residue classes modulo the primes in $\mathcal{S} \cup \mathcal{P}$ which cover most of the primes in \mathcal{Q} . For residue classes $\vec{a} = (a_s \pmod s)_{s \in \mathcal{S}}$ and $\vec{b} = (b_p \pmod p)_{p \in \mathcal{P}}$, define the sifted sets

$$S(\vec{a}) := \{n \in \mathbb{Z} : n \not\equiv a_s \pmod s \text{ for all } s \in \mathcal{S}\}$$

and likewise

$$T(\vec{b}) := \{n \in \mathbb{Z} : n \not\equiv b_p \pmod p \text{ for all } p \in \mathcal{P}\}.$$

Theorem 8.3 (Sieving primes). *Let $c > 0$ be arbitrary, let x be sufficiently large and suppose that y obeys (8.3). Then there are vectors $\vec{a} = (a_s \pmod s)_{s \in \mathcal{S}}$ and $\vec{b} = (b_p \pmod p)_{p \in \mathcal{P}}$, such that*

$$(8.5) \quad \#(\mathcal{Q} \cap S(\vec{a}) \cap T(\vec{b})) \leq \frac{x}{5 \log x}.$$

Proof of Theorem 8.3 implies Theorem 8.2. We will first take

$$a_p = 0 \quad (p \leq \log^{20} x, z < p \leq x/4).$$

This is a “big gun” and eliminates all numbers from $(x, y]$ except primes and a negligible set of z -smooth numbers. It dates from work of Westzynthius [131], Erdős [32] and Rankin [112]. Let \vec{a} and \vec{b} be as in Theorem 8.3, and consider the sifted set

$$\mathcal{U} := (x, y] \cap S(\vec{a}) \cap T(\vec{b}) \cap V,$$

where

$$V = \{n \in \mathbb{Z} : n \not\equiv 0 \pmod{p} \text{ for all } p \leq \log^{20} x \text{ and } z < p \leq x/4\}.$$

The elements of \mathcal{U} , by construction, are not divisible by any prime in $(0, \log^{20} x] \cup (z, x/4]$. Thus, each element must either be a z -smooth number (i.e., a number with all prime factors at most z), or must consist of a prime greater than $x/4$, possibly multiplied by some additional primes that are all at least $\log^{20} x$. However, from (8.3) we know that $y = o(x \log x)$. Thus, we see that an element of \mathcal{U} is either a z -smooth number or a prime in $(x/4, y]$. In the second case, the element lies in $\mathcal{Q} \cap S(\vec{a}) \cap T(\vec{b})$. Conversely, every element of $\mathcal{Q} \cap S(\vec{a}) \cap T(\vec{b})$ lies in \mathcal{U} . Thus, \mathcal{U} only differs from $\mathcal{Q} \cap S(\vec{a}) \cap T(\vec{b})$ by a set \mathcal{R} consisting of z -smooth numbers in $[1, y]$. Let $u := \frac{\log y}{\log z} \sim 5 \frac{\log_2 x}{\log_3 x}$. By Theorem 4.1 and (8.3),

$$(8.6) \quad \#\mathcal{R} \leq \Psi(y, z) \ll \frac{y}{(\log x)^{5+o(1)}} \ll \frac{x}{\log^2 x}.$$

Thus, we find that

$$\#\mathcal{U} \leq (1 + o(1)) \frac{x}{5 \log x}.$$

By matching each of these surviving elements to a distinct prime in $(x/4, x/2]$ and choosing congruence classes appropriately, we thus find congruence classes $a_p \pmod{p}$ for $p \leq x$ which cover *all* of the integers in $(x, y]$. This proves $Y(x) \geq y - x = (1 - o(1))y$, and hence Theorem 8.2. \square

8.2.1. *The Westzynthius-Erdős-Rankin argument giving (8.1) for some $c > 0$.* It is very easy to show that (8.5) holds for some value of $c > 0$. Indeed, by the pigeonhole principle, for any finite set \mathcal{R} and prime p there is a residue class a_p so that $|\mathcal{R} \cap (a_p \pmod{p})| \geq |\mathcal{R}|/p$. Consequently, there are choices of a_s for $s \in \mathcal{S}$ and b_p for $p \in \mathcal{P}$ such that

$$\begin{aligned} \# \left(\mathcal{Q} \cap S(\vec{a}) \cap T(\vec{b}) \right) &\leq |\mathcal{Q}| \prod_{s \in \mathcal{S}} \left(1 - \frac{1}{s} \right) \prod_{p \in \mathcal{P}} \left(1 - \frac{1}{p} \right) \\ &\ll |\mathcal{Q}| \frac{\log_2 x}{\log z} \\ &\ll \frac{y(\log_2 x)^2}{(\log x)^2 \log_3 x} \leq \frac{cx}{\log x}. \end{aligned}$$

Hence, if c is small enough, then (8.5) holds.

8.2.2. *Improving the Westzynthius-Erdős-Rankin method.* We argue in two stages:

Stage 1. For each prime $s \in \mathcal{S}$, we select each $\mathbf{a}_s \pmod{s}$ uniformly at random from $\mathbb{Z}/s\mathbb{Z}$, independently for each s . Let $\vec{\mathbf{a}} := (\mathbf{a}_s \pmod{s})_{s \in \mathcal{S}}$;

Stage 2. For each prime $p \in \mathcal{P}$, we select the residue class $b_p \pmod p$ also at random, but in a strategic way which is dependent on the choice of $\vec{\mathbf{a}}$; this is done in such a way so that each $b_p \pmod p$ covers many primes in \mathcal{Q} left uncovered by Stage 1.

What we gain in Stage 1 is only what is typical for residue classes for these primes, but the random choice will be advantageous for Stage 2, which is much more complicated. Greatly improving upon arguments from Maier and Pomerance [96] and Pintz [106], we show in Stage 2 that for any fixed r , there are residue classes $b_p \pmod p$ for $p \in \mathcal{P}$ which cover an average of at least r numbers left uncovered by Stage 1.

8.3. Concentration of $S(\vec{\mathbf{a}})$. The sifted set $S(\vec{\mathbf{a}})$ is a random periodic subset of \mathbb{Z} , each element surviving with probability

$$\sigma := \prod_{s \in \mathcal{S}} \left(1 - \frac{1}{s}\right) = \prod_{\log^{20} x < s \leq z} \left(1 - \frac{1}{s}\right).$$

From Mertens' bound and (8.4),

$$(8.7) \quad \sigma \sim \frac{\log(\log^{20} x)}{\log z} = \frac{100(\log_2 x)^2}{\log x \log_3 x}.$$

In particular, we have

$$(8.8) \quad \mathbb{E}\#\left(\mathcal{Q} \cap S(\vec{\mathbf{a}})\right) = \sum_{q \in \mathcal{Q}} \mathbb{P}(q \in S(\vec{\mathbf{a}})) = \sigma\#\mathcal{Q} \sim 100c \frac{x}{\log x}.$$

We now show that $\mathcal{Q} \cap S(\vec{\mathbf{a}})$ is concentrated about its mean. To accomplish this, we first show that for any reasonably sized integers n_1, \dots, n_t , the events $n_i \in S(\vec{\mathbf{a}})$ are close to being independent.

Lemma 8.4. *Let $t \leq \log x$, and let n_1, \dots, n_t be distinct integers in $[-x^2, x^2]$. Then*

$$\mathbb{P}(n_1, \dots, n_t \in S(\vec{\mathbf{a}})) = \left(1 + O\left(\frac{1}{\log^{16} x}\right)\right) \sigma^t.$$

Proof. For each $s \in \mathcal{S}$, the probability that n_1, \dots, n_t are all in $S(\vec{\mathbf{a}})$ is equal to $1 - \frac{m(s)}{t}$, where $m(s)$ is the number of distinct residue classes modulo s occupied by n_1, \dots, n_t . We have $m(s) = t$ unless s divides one of the numbers $n_i - n_j$ for $1 \leq i < j \leq t$. Since $|n_i - n_j| \leq 2x^2$, each difference $n_i - n_j$ has $O(\log x)$ prime factors. Therefore, $m(s) < t$ occurs for at most $O(t^2 \log x) = O(\log^3 x)$ primes $s \in \mathcal{S}$. By the independence of the choices \mathbf{a}_s for $s \in \mathcal{S}$, the events “ $\{n_1, \dots, n_t\}$ doesn't intersect $\mathbf{a}_s \pmod s$ ” are

independent. Thus,

$$\begin{aligned}
\mathbb{P}(n_1, \dots, n_t \in S(\vec{\mathbf{a}})) &= \prod_{s \in \mathcal{S}} \left(1 - \frac{m(s)}{s}\right) \\
&= \prod_{s \in \mathcal{S}} \left(1 - \frac{t}{s}\right) \prod_{\substack{s \in \mathcal{S} \\ m(s) < t}} \left(1 - \frac{t}{s}\right)^{-1} \left(1 - \frac{m(s)}{s}\right) \\
&= \left(1 + O\left(\frac{1}{\log^{19} x}\right)\right)^{O(\log^3 x)} \prod_{s \in \mathcal{S}} \left(1 - \frac{t}{s}\right) \\
&= \left(1 + O\left(\frac{1}{\log^{16} x}\right)\right) \sigma^t \prod_{s \in \mathcal{S}} \left(1 + O\left(\frac{t^2}{s^2}\right)\right) \\
&= \left(1 + O\left(\frac{1}{\log^{16} x}\right)\right) \sigma^t. \quad \square
\end{aligned}$$

Corollary 8.5. *With probability $\geq 1 - O(1/\log^6 x)$, we have*

$$(8.9) \quad \#(\mathcal{Q} \cap S(\vec{\mathbf{a}})) = \left(1 + O\left(\frac{1}{\log^4 x}\right)\right) \sigma \# \mathcal{Q} \sim 100c \frac{x}{\log x}.$$

Proof. From Lemma 8.4, we have

$$\begin{aligned}
\mathbb{E}(\#(\mathcal{Q} \cap S(\vec{\mathbf{a}})))^2 &= \sum_{q_1, q_2 \in \mathcal{Q}} \mathbb{P}(q_1, q_2 \in S(\vec{\mathbf{a}})) \\
&= \left(1 + O\left(\frac{1}{\log^{16} x}\right)\right) \left(\underbrace{\sigma \# \mathcal{Q}}_{q_1=q_2} + \underbrace{\sigma^2 (\# \mathcal{Q})(\# \mathcal{Q} - 1)}_{q_1 \neq q_2} \right),
\end{aligned}$$

and so by (8.8), (8.3), (8.7),

$$\mathbb{E}(\#(\mathcal{Q} \cap S(\vec{\mathbf{a}})) - \sigma \# \mathcal{Q})^2 = \mathbb{E} \#(\mathcal{Q} \cap S(\vec{\mathbf{a}}))^2 - (\sigma \# \mathcal{Q})^2 \ll \frac{x^2}{\log^{16} x} \ll \frac{(\sigma \# \mathcal{Q})^2}{\log^{14} x}.$$

Combining this last estimate with Chebyshev's inequality, we conclude that

$$\mathbb{P}\left(|\#(\mathcal{Q} \cap S(\vec{\mathbf{a}})) - \sigma \# \mathcal{Q}| \geq \frac{\sigma \# \mathcal{Q}}{\log^4 x}\right) \ll \frac{x^2/\log^{16} x}{(\sigma \# \mathcal{Q})^2 (\log x)^{-8}} \ll \frac{1}{\log^6 x}. \quad \square$$

8.4. The weight function $w(p, n)$. We will also choose the vector $\vec{\mathbf{b}}$ at random, but in a strategic way which is *dependent* on $\vec{\mathbf{a}}$. Each residue class $b_p \pmod p$ must cover many primes in \mathcal{Q} (in fact, many primes in $\mathcal{Q} \cap S(\vec{\mathbf{a}})$), and accomplishing this is the key to success of the whole enterprise. This is done via showing the existence of a good “weight” function $w(p, n)$.

Let k be a fixed positive integer, large in terms of the constant c (in fact, $k = \lfloor \exp(c^2) \rfloor$ will do), and let (h_1, \dots, h_k) be a fixed *admissible k -tuple* of positive integers (that is, for any prime, (h_1, \dots, h_k) does not cover $(\mathbb{Z}/p\mathbb{Z})$). For instance, $(1, 3^2, 5^2, \dots, (2k-1)^2)$.

Theorem 8.6 (Existence of good sieve weight). *Let k be a fixed positive integer and (h_1, \dots, h_k) a fixed admissible k -tuple. Suppose x is large and y is defined by (8.3). Then there are quantities τ, u satisfying*

$$(8.10) \quad \tau = x^{o(1)}, \quad u \gg \log k \quad (x \rightarrow \infty)$$

and a non-negative weight function $w(p, n)$ defined on $\mathcal{P} \times ([-y, y] \cap \mathbb{Z})$ satisfying

- Uniformly for every $p \in \mathcal{P}$, one has

$$(8.11) \quad \sum_{n \in \mathbb{Z}} w(p, n) \sim \tau \frac{y}{\log^k x}.$$

- Uniformly for every $q \in \mathcal{Q}$ and $i = 1, \dots, k$, one has

$$(8.12) \quad \sum_{p \in \mathcal{P}} w(p, q - h_i p) \sim \tau \frac{u}{k} \frac{x/2}{\log^k x}.$$

- Uniformly for all $p \in \mathcal{P}$ and $n \in \mathbb{Z}$,

$$(8.13) \quad w(p, n) \ll x^{o(1)} \quad (x \rightarrow \infty).$$

Remark 2. One should think of $w(p, n)$ as being a smoothed out indicator function for the event that $n + h_1 p, \dots, n + h_k p$ are all almost primes in $[1, y]$. It is thus natural to bring into play the technology from Section 7.

Proof. We first recall the construction of sieve weights from Section 7. Let

$$N = 2y.$$

Define s, R, D, z by (7.7) where $\theta = \frac{1}{3}$, define \mathcal{D} as in (7.8), and let μ^+ be an upper bound sieve guaranteed by the Fundamental Lemma (Theorem 2.19). Fix a prime $p \in \mathcal{P}$, and consider the forms

$$f_{i,p}(m) = m + (h_i p - 3y) \quad (1 \leq i \leq k),$$

where $2y = N < m \leq 2N = 4y$ (so that $h_i p - y < f_{i,p}(m) \leq h_i p + y$). Here we write $m = n + 3y$, which maps $(-y, y)$ to $(N, 2N)$. Define E, \mathcal{E} by (7.10), and define $w(p, n)$ as in (7.12), that is,

$$w(p, n) = \left(\sum_{t|(n+h_1 p) \cdots (n+h_k p)} \mu^+(t) \right) \left(\sum_{\forall j: d_j | n+h_j p} \lambda(\mathbf{d}) \mathbb{1}_{\mathbf{d} \in \mathcal{E}} \right)^2 \quad (-y < n \leq y),$$

where $\xi(\mathbf{r})$ is defined by (7.36), and $\lambda(\mathbf{d})$ is defined from Lemma 7.11. Here F is a symmetric, smooth function defined on \mathcal{R}_k , where \mathcal{R}_k is defined in (7.34). Moreover, we choose F so that

$$M_k(F) \geq 0.9M_k \geq (0.9 - o(1)) \log k$$

by Theorem 7.17. Also, since

$$E = \left| p^{k(k-1)/2} \prod_{i < j} (h_j - h_i) \right|,$$

the h_i are bounded and $p > x/2 > R$, the factor $\mathbb{1}_{\mathbf{d} \in \mathcal{E}}$ above is superfluous and may be removed.

By Proposition 7.14 (i),

$$\sum_{-y < n \leq y} w(p, n) = \sum_{N < m \leq 2N} w(p, m + 3y) \sim V(2y) \left(e^{-\gamma} \frac{\log z}{\log R} \right)^k I(F),$$

where $I(F)$ is defined in (7.37) and

$$V = \prod_{q \leq z} \left(1 - \frac{\rho(q)}{q} \right),$$

where, for prime $q \leq z$,

$$\begin{aligned} \rho(q) &= \#\left\{n \pmod q : \prod_{j=1}^k (n + h_j p) \equiv 0 \pmod q\right\} \\ &= \#\left\{n \pmod q : \prod_{j=1}^k (n + h_j) \equiv 0 \pmod q\right\} \end{aligned}$$

is independent of p (since $q < p$). This proves (8.11) with

$$(8.14) \quad \tau = 2V \left(e^{-\gamma} (\log x) \frac{\log z}{\log R} \right)^k I(F) = x^{o(1)}.$$

Next, fix a prime $q \in \mathcal{Q}$ and an index $i \in \{1, \dots, k\}$. Then

$$\sum_{p \in \mathcal{P}} w(p, q - h_i p) = \sum_{x/2 < p \leq x} \mathbb{1}_{p \text{ prime}} \left(\sum_{t \mid \prod_{j \neq i} (q + (h_j - h_i)p)} \mu^+(t) \right) \left(\sum_{d_j \mid q + (h_j - h_i)p \forall j} \lambda(\mathbf{d}) \right)^2.$$

The asymptotic (8.12) follows from Proposition 7.14 (ii) applied to the linear forms $a_j n + b_j$, $1 \leq j \leq k$, where $a_i = 1$, $b_i = 0$ and for $j \neq i$, $a_j = h_j - h_i$ and $b_j = q$. Here we have $N = x/2$, and technically the R, D values used to construct $w(p, n)$ with $N = x/2$ differ from those defined with $N = 2y$ by a logarithmic factor. However, the proof of Theorem 7.14 (ii) is robust under this kind of slight tweaking of R and D . Also, the quantity E has prime factors which are either bounded or $> x$ and as before, the factor $\mathbb{1}_{\mathbf{d} \in \mathcal{E}}$ is superfluous. Also, $|a_j| \ll 1$ and $q \leq y \ll x \log x \ll N \log N$, which are within the allowable bounds for Proposition 7.14 (ii). We also note that

$$u = \frac{\log R}{2 \log x} M_k(F) \gg \log k$$

by Theorem 7.17. Thus, (8.10) follows. Finally, (8.13) since the definition of $w(p, n)$ implies that $w(p, n)$ is bounded by a divisor function. \square

8.5. Strategic choice of \vec{b} . Our goal is to choose residue classes b_p modulo $p \in \mathcal{P}$ such that $b_p \pmod p$ contains many elements of $\mathcal{Q} \cap S(\vec{a})$.

For each $p \in \mathcal{P}$, let $\tilde{\mathbf{n}}_p$ denote the random integer with probability density

$$(8.15) \quad \mathbb{P}(\tilde{\mathbf{n}}_p = n) := \frac{w(p, n)}{\sum_{n' \in \mathbb{Z}} w(p, n')} \quad (-y \leq n \leq y),$$

and chosen independently for each $p \in \mathcal{P}$. Notice that the random numbers $\tilde{\mathbf{n}}_p$ are chosen independently of the vector \vec{a} . Roughly speaking, this gives more weight to n for which many of the numbers $n + h_i p$ are prime.

In order to capture the event that $b_p \pmod p$ contains many elements of $S(\vec{a})$, for each $p \in \mathcal{P}$ and fixed (non-random) \vec{a} , we consider the quantity

$$(8.16) \quad X_p(\vec{a}) := \mathbb{P}(\tilde{\mathbf{n}}_p + h_i p \in S(\vec{a}) \text{ for all } i = 1, \dots, k),$$

over the random integer $\tilde{\mathbf{n}}$. In light of Lemma 8.4, we expect that $X_p(\vec{a}) \sim \sigma^k$ for most choices of p and \vec{a} , and this will be confirmed below (Lemma 8.8). With this in mind, let $\mathcal{P}(\vec{a})$ denote the set of all the primes

$p \in \mathcal{P}$ such that

$$(8.17) \quad \left| X_p(\vec{a}) - \sigma^k \right| \leq \frac{\sigma^k}{\log^3 x}.$$

We now define the random variables \mathbf{n}_p . Suppose we are in the event $\vec{\mathbf{a}} = \vec{a}$. If $p \in \mathcal{P} \setminus \mathcal{P}(\vec{a})$, we set $\mathbf{n}_p = 0$. Otherwise, if $p \in \mathcal{P}(\vec{a})$, we define \mathbf{n}_p to be the random integer with conditional probability distribution

$$(8.18) \quad \mathbb{P}(\mathbf{n}_p = n | \vec{\mathbf{a}} = \vec{a}) := \frac{Z_p(\vec{a}; n)}{X_p(\vec{a})},$$

where, for any \vec{a} , any $p \in \mathcal{P}$ and any n ,

$$(8.19) \quad Z_p(\vec{a}; n) = \begin{cases} \mathbb{P}(\tilde{\mathbf{n}}_p = n) & \text{if } n + h_j p \in S(\vec{a}) \text{ for } j = 1, \dots, k \\ 0 & \text{otherwise,} \end{cases}$$

with the \mathbf{n}_p ($p \in \mathcal{P}(\vec{a})$) jointly independent, conditionally on the event $\vec{\mathbf{a}} = \vec{a}$. From (8.16) we see that these random variables are well defined.

Observe that the support of \mathbf{n}_p is contained in those n for which $n + h_i p \in S(\vec{a})$ for all i , that is, the residue class $n \pmod p$ contains at least k elements of $S(\vec{a})$. Also, recalling Remark 1, we see that, conditionally on $\vec{\mathbf{a}} = \vec{a}$, \mathbf{n}_p is very likely to be a number for which there are $\gg \log k$ of the numbers $n + h_1 p, \dots, n + h_k p$ which are prime (and hence in \mathcal{Q}). Thus, the residue class $\mathbf{n}_p \pmod p$ will likely have many elements of $\mathcal{Q} \cap S(\vec{a})$, as desired. Unlike $\tilde{\mathbf{n}}_p$, the random numbers \mathbf{n}_p are very much dependent on the vector $\vec{\mathbf{a}}$. However, conditional on $\vec{\mathbf{a}} = \vec{a}$, all of the \mathbf{n}_p ($p \in \mathcal{P}$) are independent.

Our main objective is a concentration bound for an average of $Z_p(\vec{\mathbf{a}}; q - h_i p)$.

Lemma 8.7. *Fix c, k , and let u be the value guaranteed by Theorem 8.6. Define $Z_p(\vec{a}; n)$ by (8.18). Then, as $x \rightarrow \infty$, with probability $1 - o(1)$ we have*

$$(8.20) \quad \sigma^{-k} \sum_{i=1}^k \sum_{p \in \mathcal{P}(\vec{\mathbf{a}})} Z_p(\vec{\mathbf{a}}; q - h_i p) \sim \frac{u}{\sigma} \frac{x}{2y} \sim \frac{u}{200c}$$

for all but at most $o(x/\log x)$ of the primes $q \in \mathcal{Q} \cap S(\vec{\mathbf{a}})$.

Proof of Theorem 8.3 from Lemma 8.7. By Corollary 8.5 and Lemma 8.7, there is some vector \vec{a} such that (8.9) holds and also (8.20) holds for almost all $q \in \mathcal{Q} \cap S(\vec{a})$. Fix this vector \vec{a} (it is no longer random), and choose random integers \mathbf{n}_p according to the laws (8.18). Suppose that $q \in \mathcal{Q} \cap S(\vec{a})$. Substituting definition (8.18) into the left hand side of (8.20), using (8.17), and observing that $q = \mathbf{n}_p + h_i p$ is only possible if $p \in \mathcal{P}(\vec{a})$, we find that

$$\begin{aligned} \sigma^{-k} \sum_{i=1}^k \sum_{p \in \mathcal{P}(\vec{a})} Z_p(\vec{a}; q - h_i p) &= \sigma^{-k} \sum_{i=1}^k \sum_{p \in \mathcal{P}(\vec{a})} X_p(\vec{a}) \mathbb{P}(\mathbf{n}_p = q - h_i p | \vec{\mathbf{a}} = \vec{a}) \\ &= \left(1 + O\left(\frac{1}{\log^3 x}\right) \right) \sum_{i=1}^k \sum_{p \in \mathcal{P}(\vec{a})} \mathbb{P}(\mathbf{n}_p = q - h_i p | \vec{\mathbf{a}} = \vec{a}) \\ &= \left(1 + O\left(\frac{1}{\log^3 x}\right) \right) \sum_{p \in \mathcal{P}} \mathbb{P}(q \in \mathbf{e}_p), \end{aligned}$$

where $\mathbf{e}_p = \{\mathbf{n}_p + h_i p : 1 \leq i \leq k\} \cap \mathcal{Q} \cap S(\vec{a})$. By (8.20), we conclude that

$$(8.21) \quad \sum_{p \in \mathcal{P}} \mathbb{P}(q \in \mathbf{e}_p) \sim \frac{ux}{2\sigma y} \sim \frac{u}{200c}.$$

Observe that each random set \mathbf{e}_p is contained in a single arithmetic progression modulo p . Now we set $\mathbf{b}_p = \mathbf{n}_p \pmod p$ for each $p \in \mathcal{P}$. Then, for any $q \in \mathcal{Q} \cap S(\vec{a})$, by the independence of the \mathbf{n}_p ,

$$(8.22) \quad \begin{aligned} \mathbb{P}(q \in T(\vec{\mathbf{b}})) &= \mathbb{P}(q \not\equiv \mathbf{b}_p \pmod p \ \forall p \in \mathcal{P}) \\ &= \prod_{p \in \mathcal{P}} (1 - \mathbb{P}(q \equiv \mathbf{b}_p \pmod p)) \\ &\leq \prod_{p \in \mathcal{P}} (1 - \mathbb{P}(q \in \mathbf{e}_p)) \\ &\leq \exp \left\{ - \sum_{p \in \mathcal{P}} \mathbb{P}(q \in \mathbf{e}_p) \right\} \\ &= \exp \left\{ - (1 + o(1)) \frac{u}{200c} \right\}. \end{aligned}$$

Hence, by (8.9),

$$\mathbb{E} \#(\mathcal{Q} \cap S(\vec{a}) \cap T(\vec{\mathbf{b}})) \leq \frac{200cx}{\log x} \exp \left\{ - \frac{u}{300c} \right\}.$$

The right hand side is $\leq \frac{x}{5 \log x}$ if k is large enough, thanks to (8.10) which states $u \gg \log k$. Therefore, there is some choice of the vector $\vec{\mathbf{b}}$ so that (8.5) holds, and this completes the proof of Theorem 8.3. \square

It remains to prove Lemma 8.7. We first confirm that $\mathcal{P} \setminus \mathcal{P}(\vec{\mathbf{a}})$ is small with high probability.

Lemma 8.8. *With probability $1 - O(1/\log^3 x)$, $\mathcal{P}(\vec{\mathbf{a}})$ contains all but $O(\frac{1}{\log^3 x} \frac{x}{\log x})$ of the primes $p \in \mathcal{P}$. In particular, $\mathbb{E} \# \mathcal{P}(\vec{\mathbf{a}}) = \# \mathcal{P}(1 + O(1/\log^3 x))$.*

Proof. It suffices to show that for each $p \in \mathcal{P}$, we have

$$(8.23) \quad \mathbb{P}(p \in \mathcal{P}(\vec{\mathbf{a}})) = 1 - O\left(\frac{1}{\log^6 x}\right).$$

From (8.23), we get

$$\mathbb{E} (\# \mathcal{P} \setminus \mathcal{P}(\vec{\mathbf{a}})) = \sum_{p \in \mathcal{P}} \mathbb{P}(p \notin \mathcal{P}(\vec{\mathbf{a}})) \ll \frac{\# \mathcal{P}}{\log^6 x} \ll \frac{x}{\log^7 x},$$

and then by Markov's inequality,

$$\mathbb{P}\left(\# \mathcal{P} \setminus \mathcal{P}(\vec{\mathbf{a}}) \geq \frac{x}{\log^4 x}\right) \leq \frac{\mathbb{E} (\# \mathcal{P} \setminus \mathcal{P}(\vec{\mathbf{a}}))}{x/\log^4 x} \ll \frac{1}{\log^3 x}.$$

We will prove (8.23) by computing first and second moments of $X_p(\vec{\mathbf{a}})$. Recall that, by (8.16),

$$X_p(\vec{\mathbf{a}}) := \sum_n 1_{n+h_i p \in S(\vec{a}) \ \forall i} \mathbb{P}(\tilde{\mathbf{n}}_p = n).$$

The right side is not random (unless we make $\vec{a} = \vec{\mathbf{a}}$ random), since $\mathbb{P}(\tilde{\mathbf{n}}_p = n)$ is a deterministic function of n which is independent of \vec{a} . Using Lemma 8.4,

$$(8.24) \quad \begin{aligned} \mathbb{E}X_p(\vec{\mathbf{a}}) &= \sum_n \mathbb{P}(n + h_i p \in S(\vec{\mathbf{a}}) \text{ for all } i = 1, \dots, k) \mathbb{P}(\tilde{\mathbf{n}}_p = n) \\ &= \left(1 + O\left(\frac{1}{\log^{16} x}\right)\right) \sigma^k \sum_n \mathbb{P}(\tilde{\mathbf{n}}_p = n) = \left(1 + O\left(\frac{1}{\log^{16} x}\right)\right) \sigma^k. \end{aligned}$$

Similarly,

$$\begin{aligned} \mathbb{E}X_p(\vec{\mathbf{a}})^2 &= \sum_{n_1, n_2} \mathbb{P}(n_l + h_i p \in S(\vec{\mathbf{a}}) \text{ for } 1 \leq i \leq k; l = 1, 2) \mathbb{P}(\tilde{\mathbf{n}}_p = n_1) \mathbb{P}(\tilde{\mathbf{n}}_p = n_2) \\ &= \left(1 + O\left(\frac{1}{\log^{16} x}\right)\right) \sigma^{2k} + O\left(y(y/p) \max_n (\mathbb{P}(\tilde{\mathbf{n}}_p = n))^2\right), \end{aligned}$$

since

$$\#\{n_l + h_i p : i = 1, \dots, k; l = 1, 2\} = 2k$$

unless $n_1 \equiv n_2 \pmod{p}$ and there are $O(y(y/p))$ such pairs (n_1, n_2) . From (8.15), (8.11), (8.13), and (8.10) one has $\mathbb{P}(\tilde{\mathbf{n}}_p = n) \ll x^{-1+o(1)}$ for all $p \in \mathcal{P}$ and $n \in \mathbb{Z}$. Also, $\sigma \gg x^{-o(1)}$ by (8.7), hence

$$(8.25) \quad \mathbb{E}X_p(\vec{\mathbf{a}})^2 = \left(1 + O\left(\frac{1}{\log^{16} x}\right)\right) \sigma^{2k}.$$

Combining (8.24) and (8.25), we compute

$$\mathbb{E} \left| X_p(\vec{\mathbf{a}}) - \sigma^k \right|^2 \ll \frac{\sigma^{2k}}{\log^{16} x}.$$

By Chebyshev's inequality, for any $p \in \mathcal{P}$,

$$\mathbb{P}(p \notin \mathcal{P}(\vec{\mathbf{a}})) = \mathbb{P} \left(\left| X_p(\vec{\mathbf{a}}) - \sigma^k \right| \geq \frac{1}{\log^3 x} \right) \ll \frac{1}{\log^{10} x},$$

which proves (8.23). □

Proof of Lemma 8.7. We first show that replacing $\mathcal{P}(\vec{\mathbf{a}})$ with \mathcal{P} has negligible effect on the sum, with high probability. The purpose is to set up an application of (8.12) and to decouple some expressions involving $\vec{\mathbf{a}}$.

Fix $i \in \{1, \dots, k\}$. By Lemma 8.4 and the definition (8.19) of $Z_p(\vec{a}, n)$, we have

$$\begin{aligned} \mathbb{E} \sum_n \sigma^{-k} \sum_{p \in \mathcal{P}} Z_p(\vec{\mathbf{a}}; n) &= \sigma^{-k} \sum_{p \in \mathcal{P}} \sum_n \mathbb{P}(\tilde{\mathbf{n}}_p = n) \mathbb{P}(n + h_j p \in S(\vec{\mathbf{a}}) \text{ for } j = 1, \dots, k) \\ &= \left(1 + O\left(\frac{1}{\log^{16} x}\right)\right) \sum_{p \in \mathcal{P}} \sum_n \mathbb{P}(\tilde{\mathbf{n}}_p = n) \\ &= \left(1 + O\left(\frac{1}{\log^{16} x}\right)\right) \#\mathcal{P}. \end{aligned}$$

Next, by (8.17) and Lemma 8.8 we have

$$\begin{aligned}
\mathbb{E} \sum_n \sigma^{-k} \sum_{p \in \mathcal{P}(\vec{\mathfrak{a}})} Z_p(\vec{\mathfrak{a}}; n) &= \sigma^{-k} \sum_{\vec{a}} \mathbb{P}(\vec{\mathfrak{a}} = \vec{a}) \sum_{p \in \mathcal{P}(\vec{a})} X_p(\vec{a}) \underbrace{\sum_n \mathbb{P}(\mathbf{n}_p = n | \vec{\mathfrak{a}} = \vec{a})}_{\text{equals 1}} \\
&= \left(1 + O\left(\frac{1}{\log^3 x}\right)\right) \sum_{\vec{a}} \mathbb{P}(\vec{\mathfrak{a}} = \vec{a}) \sum_{p \in \mathcal{P}(\vec{a})} 1 \\
&= \left(1 + O\left(\frac{1}{\log^3 x}\right)\right) \mathbb{E} \#\mathcal{P}(\vec{\mathfrak{a}}) = \left(1 + O\left(\frac{1}{\log^3 x}\right)\right) \#\mathcal{P}.
\end{aligned}$$

Subtracting these two expectations, we conclude that

$$(8.26) \quad \mathbb{E} \sum_n \sigma^{-k} \sum_{p \in \mathcal{P} \setminus \mathcal{P}(\vec{\mathfrak{a}})} Z_p(\vec{\mathfrak{a}}; n) \ll \frac{\#\mathcal{P}}{\log^3 x} \ll \frac{x}{\log^4 x}.$$

We substitute $n = q - h_i p$ and find that

$$\begin{aligned}
\mathbb{E} \sum_{q \in \mathcal{Q} \cap S(\vec{\mathfrak{a}})} \sigma^{-k} \sum_{i=1}^k \sum_{p \in \mathcal{P} \setminus \mathcal{P}(\vec{\mathfrak{a}})} Z_p(\vec{\mathfrak{a}}; q - h_i p) &\leq \mathbb{E} \sum_n \sigma^{-k} \sum_{p \in \mathcal{P} \setminus \mathcal{P}(\vec{\mathfrak{a}})} Z_p(\vec{\mathfrak{a}}; n) \\
&\ll \frac{x}{\log^4 x}.
\end{aligned}$$

By Markov's inequality, with probability $1 - O(1/\log x)$, we have

$$\sum_{q \in \mathcal{Q} \cap S(\vec{\mathfrak{a}})} \sigma^{-k} \sum_{i=1}^k \sum_{p \in \mathcal{P} \setminus \mathcal{P}(\vec{\mathfrak{a}})} Z_p(\vec{\mathfrak{a}}; q - h_i p) \leq \frac{x}{\log^3 x}.$$

Hence, with probability $1 - O(1/\log x)$, we have

$$\sigma^{-k} \sum_{i=1}^k \sum_{p \in \mathcal{P} \setminus \mathcal{P}(\vec{\mathfrak{a}})} Z_p(\vec{\mathfrak{a}}; q - h_i p) \leq \frac{1}{\log x}$$

for all but $O(x/\log^2 x)$ primes $q \in \mathcal{Q} \cap S(\vec{\mathfrak{a}})$. Recalling our goal (8.20), it therefore suffices to show that with probability $1 - o(1)$, for all but at most $o(x/\log x)$ primes $q \in \mathcal{Q} \cap S(\vec{\mathfrak{a}})$, one has

$$(8.27) \quad F(q; \vec{\mathfrak{a}}) := \sigma^{-k} \sum_{i=1}^k \sum_{p \in \mathcal{P}} Z_p(\vec{\mathfrak{a}}; q - h_i p) \sim \frac{xu}{2\sigma y}.$$

We accomplish this with another first-second moment calculation.

First, we note that from Theorem 8.6, (8.11) and (8.12), we have

$$(8.28) \quad \sum_{p \in \mathcal{P}} \mathbb{P}(q = \tilde{\mathbf{n}}_p + h_i p) \sim \frac{u}{k} \frac{x}{2y} \quad (q \in \mathcal{Q}, 1 \leq i \leq k).$$

Hence, combining (8.28) with Lemma 8.4 and (8.15), we get

$$\begin{aligned} \mathbb{E} \sum_{q \in \mathcal{Q} \cap S(\vec{\mathbf{a}})} F(q; \vec{\mathbf{a}}) &= \sigma^{-k} \sum_{q \in \mathcal{Q}} \sum_{i=1}^k \sum_{p \in \mathcal{P}} \mathbb{P}(q + (h_j - h_i)p \in S(\vec{\mathbf{a}}) \forall j) \mathbb{P}(\tilde{\mathbf{n}}_p = q - h_i p) \\ &= \left(1 + O\left(\frac{1}{\log^{16} x}\right)\right) \sum_{q \in \mathcal{Q}} \sum_{i=1}^k \sum_{p \in \mathcal{P}} \mathbb{P}(\tilde{\mathbf{n}}_p = q - h_i p) \\ &\sim \sigma^k \sum_{q \in \mathcal{Q}} \sum_{i=1}^k \frac{ux}{2ky} \sim \frac{\sigma y}{\log x} \left(\frac{xu}{2\sigma y}\right). \end{aligned}$$

This matches what we want, since by corollary (8.5), $\#(\mathcal{Q} \cap S(\vec{\mathbf{a}})) \sim \sigma y / \log x$ with high probability. Similarly,

$$\begin{aligned} \mathbb{E} \sum_{q \in \mathcal{Q} \cap S(\vec{\mathbf{a}})} F(q; \vec{\mathbf{a}})^2 &= \sum_{\substack{p_1, p_2 \in \mathcal{P} \\ q \in \mathcal{Q}}} \sum_{i_1, i_2} \mathbb{P}(q + (h_j - h_{i_\ell})p_\ell \in S(\vec{\mathbf{a}}) \text{ for } j = 1, \dots, k; \ell = 1, 2) \\ &\quad \times \mathbb{P}(\tilde{\mathbf{n}}_{p_1} = q - h_{i_1} p_1) \mathbb{P}(\tilde{\mathbf{n}}_{p_2} = q - h_{i_2} p_2) \\ &\sim \frac{\sigma y}{\log x} \left(\sigma^{k-1} \frac{ux}{2y}\right)^2, \end{aligned}$$

where in the last step we used the fact that the terms with $p_1 = p_2$ contribute negligibly (the argument is similar to that leading to (8.25)). Putting the first and second moment bounds together, and using (8.8), we get

$$\begin{aligned} \mathbb{E} \sum_{q \in \mathcal{Q} \cap S(\vec{\mathbf{a}})} \left(F(q; \vec{\mathbf{a}}) - \frac{xu}{2\sigma y}\right)^2 &= \mathbb{E} \sum_{q \in \mathcal{Q} \cap S(\vec{\mathbf{a}})} F(q; \vec{\mathbf{a}})^2 - 2\frac{xu}{2\sigma y} \mathbb{E} \sum_{q \in \mathcal{Q} \cap S(\vec{\mathbf{a}})} F(q; \vec{\mathbf{a}}) + \left(\frac{xu}{2\sigma y}\right)^2 \mathbb{E} \#(\mathcal{Q} \cap S(\vec{\mathbf{a}})) \\ &= o\left(\frac{\sigma y}{\log x} \left(\frac{xu}{2\sigma y}\right)^2\right). \end{aligned}$$

Using Chebyshev's inequality, we find that with probability $1 - o(1)$, $F(q; \vec{\mathbf{a}}) \sim \frac{xu}{2\sigma y}$ for all but $o(\sigma y / \log x)$ primes $q \in \mathcal{Q} \cap S(\vec{\mathbf{a}})$. Now $\sigma y / \log x \asymp x / \log x$, and the lemma follows. \square

8.6. Remarks: quantitative improvements. The proof described above may be adapted to the case where $k \rightarrow \infty$ ($x \rightarrow \infty$). The relevant estimates needed for the analog of Theorem 8.6 may be found in [98]. The error terms corresponding to bounds for primes in progressions from the sum (8.12) need to be of the form $x/(\log x)^{100k^2}$, and this is achieved (as in [98]) by a careful analysis of Siegel exceptional zeros. With $k \approx (\log x)^{1/5}$, the analog of Theorem 8.6 will have a factor $u \gg \log \log x$ in (8.12). Inserted into the final estimate (8.22) in the proof of Theorem 2, we find that to succeed we need

$$u \gg c \log c,$$

which means that we can improve $Y(x)$ by a factor $\gg u / \log u$ (and hence $G(x)$ improved by a factor $\gg \frac{\log u}{\log \log u}$). In light of (8.21), however, we may expect an improvement of order $\gg u$ for $Y(x)$, and of order $\gg \log u$ for $G(x)$. This is achieved by dealing effectively with overlaps among the random sets \mathbf{e}_p , using techniques from hypergraph covering (§4-5 of [50]).

REFERENCES

- [1] L. M. Adleman and D. R. Heath-Brown, *The first case of Fermat's last theorem*. Invent. Math. **79** (1985), no. 2, 409–416.
- [2] M. Agrawal, N. Kayal and N. Saxena, *PRIMES is in P*. Ann. of Math. (2) **160** (2004), no. 2, 781–793; errata: Ann. of Math. (2) **189** (2019), no. 1, 317–318.
- [3] W. R. Alford, A. Granville and C. Pomerance, *There are infinitely many Carmichael numbers*. Ann. of Math. **139** (1994), 703–722.
- [4] A. Balog, *$p + a$ without large prime factors*. Seminar on number theory, 1983–1984 (Talence, 1983/1984), Exp. No. 31, 5 pp., Univ. Bordeaux I, Talence, 1984.
- [5] ———, *Linear equations in primes*. Mathematika **39** (1992), no. 2, 367–378.
- [6] R. C. Baker and G. Harman, *The Brun-Titchmarsh theorem on average*, Analytic Number Theory (Proceedings in honor of Heini Halberstam), Birkhauser, Boston, 1996, 39–103.
- [7] ———, *Shifted primes without large prime factors*, Acta Arith. **83** (1998), 331–361.
- [8] R. C. Baker, G. Harman and J. Pintz, *The difference between consecutive primes. II.*, Proc. London Math. Soc. (3) **83** (2001), no. 3, 532–562.
- [9] W. Banks, K. Ford and T. Tao, *Large prime gaps and probabilistic models*, submitted. `Arxiv: 1908.08613`
- [10] P. T. Bateman and R. A. Horn, *Primes represented by irreducible polynomials in one variable*, Proc. Sympos. Pure Math., Vol. VIII, Amer. Math. Soc., Providence, R.I. (1965), 119–132.
- [11] P. Billingsly, *On the distribution of large prime divisors*, Collection of articles dedicated to the memory of Alfréd Rényi, I. Period. Math. Hungar. **2** (1972), 283–289.
- [12] E. Bombieri, *On the large sieve*. Mathematika **12** (1965), 201–225.
- [13] E. Bombieri and H. Davenport, *Small differences between prime numbers*. Proc. Roy. Soc. London Ser. A **293** (1966), 1–18.
- [14] E. Bombieri, J. Friedlander and H. Iwaniec, *Primes in arithmetic progressions to large moduli. II*, Math. Ann. **277** (1987), 361–393.
- [15] V. Y. Bouniakowsky, *Nouveaux théorèmes relatifs à la distinction des nombres premiers et à la décomposition des entiers en facteurs*, Mém. Acad. Sci. St. Pétersbourg (6) (1857), 305–329.
- [16] V. Brun, *Über das Goldbachsche Gesetz und die Anzahl der Primzahlpaare*, Archiv for Math. og Naturvid. B **34** (1915), no. 8, 19pp.
- [17] V. Brun, *Om fordelingen av primtallene i forskjellige talklasser. En ovre begrænsning*, Nyt Tidsskr. f. Math. **27** B (1916), 45–58.
- [18] V. Brun, *La série $1/5 + 1/7 + 1/11 + 1/13 + 1/17 + 1/19 + 1/29 + 1/31 + 1/41 + 1/43 + 1/59 + 1/61 + \dots$ où les dénominateurs sont “nombres premiers jumeaux” est convergente ou finie*, Bull. Sci. Math. (2) **43** (1919), 100–104, 124–128.
- [19] V. Brun, *Le crible d’Eratosthène et le théorème de Goldbach*, Skr. Norske Vid.-Akad. Kristiania I. **1920**, no. 3, 36 pp.
- [20] R. D. Carmichael, *On Euler's ϕ -function*, Bull. Amer. Math. Soc. **13** (1907), 241–243.
- [21] ———, *Note on Euler's ϕ -function*, Bull. Amer. Math. Soc. **28** (1922), 109–110.
- [22] A. C. Cojocaru and M. Ram Murty. *An introduction to sieve methods and their applications*. London Mathematical Society Student Texts, vol. **66**. Cambridge University Press, 2006.
- [23] H. Cramér, *Some theorems concerning prime numbers*, Ark. Mat. Astr. Fys. **15** (1920), 1–33.
- [24] H. Cramér, *On the order of magnitude of the difference between consecutive prime numbers*, Acta Arith. **2** (1936), 396–403.
- [25] H. Davenport, *Multiplicative number theory*, 3rd ed., Graduate Texts in Mathematics vol. 74, Springer-Verlag, New York, 2000.
- [26] H. Diamond, H. Halberstam and W. F. Galway, *A Higher-Dimensional Sieve Method: With Procedures for Computing Sieve Functions*, Cambridge Tracts in Mathematics, vol. 177, 2008.
- [27] L. E. Dickson, *A new extension of Dirichlet's theorem on prime numbers*, Messenger Math., **33** (1904), 155–161.
- [28] P. G. L. Dirichlet, *Beweis des Satzes, dass jede unbegrenzte arithmetische Progression, deren erstes Glied und Differenz ganze Zahlen ohne gemeinschaftlichen Factor sind, unendlich viele Primzahlen enthält* [Proof of the theorem that every unbounded arithmetic progression, whose first term and common difference are integers without common factors, contains infinitely many prime numbers], Abhandlungen der Königlich Preussischen Akademie der Wissenschaften zu Berlin, 48 (1837), 45–71.
- [29] P. Donnelly and G. Grimmett, *On the asymptotic distribution of large prime factors*, J. London Math. Soc. (2) **47** (1993), 395–404.
- [30] P. D. T. A. Elliott and H. Halberstam, *A conjecture in prime number theory*, Symp. Math. **4** (1968), 59–72.
- [31] P. Erdős, *On the normal number of prime factors of $p - 1$ and some related problems concerning Euler's ϕ -function*, Quart. J. Math. Oxford **6** (1935), 205–213.
- [32] ———, *On the difference of consecutive primes*, Quart. J. Math. Oxford Ser. **6** (1935), 124–128.

- [33] ———, *The difference of consecutive primes*. Duke Math. J. **6** (1940), 438–441.
- [34] ———, *Some remarks on Euler’s ϕ -function and some related problems*, Bull. Amer. Math. Soc. **51** (1945), 540–544.
- [35] ———, *On integers of the form $2^k + p$ and some related problems*, Summa Brasil. Math. **2** (1950), 113–123.
- [36] ———, *Some remarks on number theory*, Riveon Lematematika **9** (1955), 45–48, (Hebrew. English summary).
- [37] ———, *Some remarks on Euler’s ϕ -function*, Acta Arith. **4** (1958), 10–19.
- [38] ———, *An asymptotic inequality in the theory of numbers*, Vestnik Leningrad. Univ. **15** (1960), no. 13, 41–49, (Russian).
- [39] ———, *On the distribution of numbers of the form $\sigma(n)/n$ and on some related questions*, Pacific J. Math. **52** (1974), 59–65.
- [40] P. Erdős and R.R.Hall, *On the values of Euler’s ϕ -function*, Acta Arith. **22** (1973), 201–206.
- [41] ———, *Distinct values of Euler’s ϕ -function*, Mathematika **23** (1976), 1–3.
- [42] P. Erdős and M. Kac, *The Gaussian law of errors in the theory of additive number theoretic functions*. Amer. J. Math. **62** (1940), 738–742.
- [43] P. Erdős and C. Pomerance, *On the normal number of prime factors of $\phi(n)$* , Rocky Mountain J. of Math. **15** (1985), 343–352.
- [44] P. Erdős, C. Pomerance, and A. Sárközy, *On locally repeated values of certain arithmetic functions. III*. Proc. Amer. Math. Soc. **101** (1987), no. 1, 1–7.
- [45] K. Ford, *The distribution of totients*, Ramanujan J. (Paul Erdős memorial issue) **2** (1998), 67–151.
- [46] ———, *The number of solutions of $\phi(x) = m$* , Annals of Math. **150** (1999), 283–311.
- [47] ———, *The distribution of integers with a divisor in a given interval*, Ann. Math. (2) **168** (2008), 367–433.
- [48] ———, *Solutions of $\phi(n) = \phi(n+k)$ and $\sigma(n) = \sigma(n+k)$* , preprint, March 2020. arXiv:2002.12155
- [49] K. Ford, B. Green, S. Konyagin, T. Tao, *Large gaps between consecutive prime numbers*, Ann. Math. **183** (2016), 935–974.
- [50] K. Ford, B. Green, S. Konyagin, J. Maynard and T. Tao, *Long gaps between consecutive prime numbers*, J. Amer. Math. Soc., **31** (2018), no. 1, 65–105.
- [51] K. Ford and H. Halberstam, *The Brun-Hooley sieve*, J. Number Th. **81** (2000), 335–350.
- [52] K. Ford and S. Konyagin, *On two conjectures of Sierpiński concerning the arithmetic functions σ and ϕ* , Number Theory in Progress (Zakopane, Poland, 1997), vol. II, de Gruyter (1999), 795–803.
- [53] É. Fouvry, *Théorème de Brun-Titchmarsh: application au théorème de Fermat*. (French) [The Brun-Titchmarsh theorem: application to the Fermat theorem], Invent. Math. **79** (1985), no. 2, 383–407.
- [54] J. Friedlander, *Shifted primes without large prime factors*, in Number theory and applications (Banff, AB, 1988), Kluwer Acad. Publ., Dordrecht (1989), 393–401.
- [55] J. Friedlander and H. Iwaniec, *The polynomial $X^2 + Y^4$ captures its primes* Ann. of Math. (2), **148** (3) (1998), 945–1040.
- [56] ———, *The asymptotic sieve*, Ann. of Math. (2), **148** (3) (1998), 1041–1065.
- [57] J. Friedlander and H. Iwaniec, *Opera de Cribro*, American Math. Soc., 2010.
- [58] M. Goldfeld, *On the number of primes p for which $p+a$ has a large prime factor*. Mathematika **16** (1969), 23–27.
- [59] D. Goldston, J. Pintz and C. Yıldırım, *Primes in tuples. I*, Ann. of Math. **170** (2009), no. 2, 819–862.
- [60] ———, *Primes in tuples. II*. Acta Math. **204** (2010), no. 1, 1–47.
- [61] D. Goldston, S. Graham, J. Pintz and C. Yıldırım, *Small gaps between primes or almost primes*, Trans. Amer. Math. Soc. **361** (2009), no. 10, 5285–5330.
- [62] ———, *Small gaps between products of two primes*, Proc. London Math. Soc. (3) **98** (2009), 741–774.
- [63] S. W. Graham, J. J. Holt and C. Pomerance, *On the solutions to $\phi(n) = \phi(n+k)$* . Number theory in progress, Vol. 2 (Zakopane-Kościełisko, 1997), 867–882, de Gruyter, Berlin, 1999.
- [64] A. Granville, *Harald Cramér and the distribution of prime numbers*, Scandanavian Actuarial J. **1** (1995), 12–28.
- [65] B. J. Green and T. C. Tao, *The primes contain arbitrarily long arithmetic progressions*, Ann. of Math. **167** (2008), 481–547.
- [66] ———, *Linear equations in primes*, Annals of Math. **171** (2010), no. 3, 1753–1850.
- [67] ———, *The quantitative behaviour of polynomial orbits on nilmanifolds*, Annals of Math. **175** (2012), no. 2, 465–540.
- [68] B. J. Green and T. C. Tao and T. Ziegler, *An inverse theorem for the Gowers U^4 -norm*, Glasg. Math. J. **53** (2011), no. 1, 1–50.
- [69] ———, *An inverse theorem for the Gowers $U^{s+1}[N]$ -norm*, Annals of Math. **176** (2012), 1231–1372.
- [70] H. Halberstam and H.-E. Richert, *Sieve Methods*, Academic Press, London, 1974.
- [71] R. R. Hall, G. Tenenbaum, *Divisors*, Cambridge Tracts in mathematics vol. **90**, 1988.
- [72] G. H. Hardy and J. E. Littlewood, *Some problems of ‘partitio numerorum’; III: On the expression of a number as a sum of primes*, Acta Math., **114** (3) (1923), 215–273.
- [73] ———, *Some problems of ‘partitio numerorum’; VII.*, unpublished.
- [74] G. H. Hardy and S. Ramanujan, *The normal number of prime factors of a number n* , Quart. J. Math. **48** (1917), 76–92.
- [75] G. Harman, *On the number of Carmichael numbers up to x* . Bull. London Math. Soc. **37** (2005), no. 5, 641–650.
- [76] ———, *Prime detecting sieves*, London Math. Soc. monographs, 2006.
- [77] ———, *Watt’s mean value theorem and Carmichael numbers*. Int. J. Number Theory **4** (2008), no. 2, 241–248.

- [78] D. R. Heath-Brown, *Gaps between primes, and the pair correlation of zeros of the zeta function*, Acta Arith. **41** (1982), no. 1, 85–99.
- [79] ———, *The divisor function at consecutive integers* Mathematika **31** (1984), no. 1, 141–149.
- [80] ———, *Artin’s conjecture for primitive roots*, Quart. J. Math. Oxford Ser. (2) **37** (1986), no. 145, 27–38.
- [81] A. Hildebrand and G. Tenenbaum, *Integers without large prime factors*, J. Théor. Nombres Bordeaux **5** (1993), 411–484.
- [82] C. Hooley, *On Artin’s conjecture*, J. Reine Angew. Math. **225** (1967), 209–220.
- [83] ———, *On the Brun-Titchmarsh theorem*. J. Reine Angew. Math. **255** (1972), 60–79.
- [84] ———, *On the largest prime factor of $p + a$* . Mathematika **20** (1973), 135–143.
- [85] ———, *On the Brun-Titchmarsh theorem. II*. Proc. London Math. Soc. (3) **30** (1975), 114–128.
- [86] ———, *Applications of Sieve Methods to the Theory of Numbers*, Cambridge University Press, 1976.
- [87] ———, *On an almost-pure sieve*, Acta Arith. **LXVI** (1994), 359–368.
- [88] H. Iwaniec, *On the error term in the linear sieve*. Acta Arith. **19** (1971), 1–30.
- [89] H. Iwaniec and E. Kowalski, *Analytic number theory*, Amer. Math. Soc. Colloquium Publications vol. 53, 2004.
- [90] R. Jajte, *On random partitions of the segment*, Bull. Acad. Polon. Sci. **19** (1971), 231–233.
- [91] Sungjin Kim, *On the equations $\phi(n) = \phi(n + k)$ and $\phi(p - 1) = \phi(q - 1)$* , preprint.
- [92] D. Koukoulopoulos, *The distribution of prime numbers*, Graduate Studies in Math. vol. 203, Amer. Math. Soc., 2019.
- [93] E. Landau, *Neuer Beweis des Primzahlsatzes und Beweis des Primidealsatzes*. Mathematische Annalen. **56** (4) (1903), 645–670.
- [94] H. Maier, *Small differences between prime numbers*. Michigan Math. J. **35** (1988), no. 3, 323–344.
- [95] H. Maier and C. Pomerance, *On the number of distinct values of Euler’s ϕ -function*, Acta Arith. **49** (1988), 263–275.
- [96] ———, *Unusually large gaps between consecutive primes*. Trans. Amer. Math. Soc. **322** (1990), no. 1, 201–237.
- [97] J. Maynard, *Small gaps between primes*, Annals of Math. **181** (2015), 383–413.
- [98] J. Maynard, *Dense clusters of primes in subsets*, Compos. Math. **152** (2016), no. 7, to appear.
- [99] J. Maynard, *Large gaps between primes*, Ann. Math. **183** (2016), 915–933.
- [100] H. L. Montgomery and R. C. Vaughan, *On the large sieve*, Mathematika **20** (1973), 119–134.
- [101] Y. Motohashi, *A note on the least prime in an arithmetic progression with a prime difference*. Acta Arith. **17** (1970), 283–285.
- [102] Y. Motohashi and J. Pintz, *A smoothed GPY sieve*, Bull. Lond. Math. Soc. **40** (2008), no. 2, 298–310.
- [103] The Multiply Perfect Numbers Page, <http://wwwhomes.uni-bielefeld.de/achim/mpn.html>
- [104] The On-Line Encyclopedia of Integer Sequences, <https://oeis.org/>
- [105] S. Pillai, *On some functions connected with $\phi(n)$* , Bull. Amer. Math. Soc. **35** (1929), 832–836.
- [106] J. Pintz, *Very large gaps between consecutive primes*. J. Number Theory **63** (1997), no. 2, 286–301.
- [107] P. Pollack and C. Pomerance, *Some problems of Erdős on the sum-of-divisors function*, Trans. Amer. Math. Soc. Ser. B **3** (2016), 1–26.
- [108] D. H. J. Polymath, *New equidistribution estimates of Zhang type*, Algebra Number Theory **8** (2014), 2067–2199. See also http://michaelnielsen.org/polymath1/index.php?title=Bounded_gaps_between_primes
- [109] D. H. J. Polymath, *Variants of the Selberg sieve, and bounded gaps between primes*, Research in the Mathematical Sciences **1**:12 (2014).
- [110] C. Pomerance, *Popular values of Euler’s function*. Mathematika **27** (1980), no. 1, 84–89.
- [111] ———, *On the distribution of the values of Euler’s function*, Acta Arith. **47** (1986), 63–70.
- [112] R. A. Rankin, *The difference between consecutive prime numbers*, J. London Math. Soc. **13** (1938), 242–247.
- [113] R. A. Rankin, *The difference between consecutive prime numbers. V*, Proc. Edinburgh Math. Soc. (2) **13** (1962/63), 331–332.
- [114] G. Ricci, *Ricerche aritmetiche sui polinomi II (Intorno a una proposizione non vera di Legendre)*, Rend. Circ. Mat. di Palermo **58** (1934), 190–208.
- [115] N. P. Romanoff, *Über einige Sätze der additiven Zahlentheorie*, Math. Ann. **109** (1934), 668–678.
- [116] A. Schinzel, *Sur l’équation $\phi(x) = m$* , Elem. Math. **11** 1956, 75–78.
- [117] ———, *Sur l’équation $\phi(x + k) = \phi(x)$* . (French) Acta Arith **4** (1958), 181–184.
- [118] ———, *Remarks of the paper “Sur certaines hypothèses concernant les nombres premiers”*, Acta Arith. **7** (1961/62), 1–8.
- [119] A. Schinzel and W. Sierpiński, *Sur certaines hypothèses concernant les nombres premiers*, Acta Arith., **4** (1958), 185–208. erratum, **5** (1959), p. 259.
- [120] A. Schinzel and A. Wakulicz, *Sur l’équation $\phi(x + k) = \phi(x)$. II*. (French) Acta Arith. **5** (1959), 425–426.
- [121] L. Shnirelmann, *Über additive Eigenschaften von Zahlen*, Math. Ann. **107** (1933), 649–690.
- [122] A. Schönage, *Eine Bemerkung zur Konstruktion grosser Primzahllücken*, Arch. Math. **14** (1963), 29–30.
- [123] A. Selberg, *The general sieve-method and its place in prime number theory*. Proceedings of the International Congress of Mathematicians, Cambridge, Mass., 1950, vol. 1, pp. 286–292. Amer. Math. Soc., Providence, R. I., 1952.
- [124] A. Selberg, *Lectures on sieves*, A. Selberg’s collected papers, vol. II, Springer-Verlag, 1991, pp. 65–247.

- [125] W. Sierpiński, *Sur une propriété de la fonction $\phi(n)$* . (French) Publ. Math. Debrecen **4** (1956), 184–185.
- [126] T. Oliveira e Silva, S. Herzog, S. Pardi, *Empirical verification of the even Goldbach conjecture and computation of prime gaps up to 4×10^{18}* , Math. Comp. **83** (2014), 2033–2060.
- [127] G. Tenenbaum, *Introduction to Analytic and Probabilistic Number Theory*, 3rd ed., Amer. Math Soc., 2015
- [128] N. M. Timofeev, *Hardy-Ramanujan and Hálász type inequalities for shifted prime numbers*, Math. Notes **57** (1995), 522–535.
- [129] E. C. Titchmarsh, *A divisor problem*, Rend. Circ. Mat. Palermo **54** (1930), 414–429.
- [130] Christian Tudesq, Majoration de la loi locale de certaines fonctions additives. *Arch. Math. (Basel)*, 67(6):465–472, 1996.
- [131] E. Westzynthius, *Über die Verteilung der Zahlen, die zu den n ersten Primzahlen teilerfremd sind*, Commentationes Physico-Mathematicae, Societas Scientiarum Fennica, Helsingfors **5**, no. 25, (1931) 1–37.
- [132] E. Wirsing, Bemerkung zu der Arbeit über vollkommene Zahlen. (German) Math. Ann. **137** (1959), 316–318.
- [133] K. Wooldridge, *Values taken many times by Euler's phi-function*. Proc. Amer. Math. Soc. **76** (1979), no. 2, 229–234.
- [134] T. Yamada, *On equations $\sigma(n) = \sigma(n + k)$ and $\phi(n) = \phi(n + k)$* . J. Comb. Number Theory **9** (2017), no. 1, 15–21.
- [135] Yitang Zhang, *Bounded gaps between primes*. Annals of Mathematics **179** (2014), 1121–1174.

DEPARTMENT OF MATHEMATICS, 1409 WEST GREEN STREET, UNIVERSITY OF ILLINOIS AT URBANA-CHAMPAIGN,
URBANA, IL 61801, USA

Email address: ford@math.uiuc.edu