A SURVEY ON PRIMES IN ARITHMETIC PROGRESSIONS

KYLE PRATT

ABSTRACT. I will give a survey talk on primes in arithmetic progressions. The talk should be accessible to any graduate student, number theorist or not. Any errors are my own.

1. NOTATION AND PREHISTORY

Throughout, we always let $a$ and $q$ be coprime integers, and we are interested in the arithmetic progression $a \pmod{q}$. That is, we study the sequence of integers $a, a + q, a + 2q, a + 3q, \ldots$. We let $\varphi(q)$ be the Euler totient function, which counts how many integers less than $q$ are coprime to $q$. For example, $\varphi(4) = 2$ and $\varphi(10) = 4$. We denote by $o(1)$ a quantity that goes to zero as some other parameter goes to infinity.

The general conjecture that there are infinitely many primes $p$ with $p \equiv a \pmod{q}$ was first stated by Legendre. He assumed some version of this conjecture in an attempt to prove quadratic reciprocity. The great mathematician Gauss would later become greatly enamored of quadratic reciprocity, and would go on to give many proofs of quadratic reciprocity over his lifetime.

It was known since the days of Euclid in antiquity that there are infinitely many primes numbers. Euclid’s proof is very short and clever, but it seems hard to generalize to proving that there are infinitely many primes in arithmetic progressions. In fact, it is known that a “Euclidean proof” exists for the arithmetic progression $a \pmod{q}$ if and only if $a^2 \equiv 1 \pmod{q}$.

One key breakthrough occurred with Euler, in 1737, when he gave a different, more analytic, proof that there are infinitely many primes. Since his proof gives rise to the epoch-making work of Dirichlet, we pause briefly now to discuss it.

For a real number $s > 1$, we define the Riemann zeta function $\zeta(s)$ by

$$
\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}.
$$

Euler observed that, by the fundamental theorem of arithmetic, one may rewrite this infinite sum as an infinite product over primes:

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

This product over primes occurs in many other contexts, and is now referred to as an Euler product.

Roughly speaking, Euler’s proof now works like this. As $s \to 1^+$, we must have $\zeta(s) \to +\infty$, since the harmonic series diverges. Thus, we have $\log \zeta(s) \to +\infty$ as well. Taking the
logarithm of the Euler product and expanding in Taylor series, we obtain

$$\log \zeta(s) = \sum_p - \log \left(1 - \frac{1}{p^s}\right) = \sum_p \sum_{k} \frac{1}{kp^ks}.$$  

The contribution from \(k \geq 2\) is bounded by an absolute constant, so we have

$$\sum_p \frac{1}{p^s} \geq \log \zeta(s) - C$$

for some constant \(C\). Since the right side tends to infinity as \(s \to 1^+\) it follows that there are infinitely many primes.

2. **Dirichlet**

Dirichlet saw in Euler’s zeta function proof the ideas needed to study primes in arithmetic progressions. In 1837, Dirichlet succeeded in proving the long-sought result.

**Theorem 2.1** (Dirichlet, 1837). There are infinitely many primes \(p\) with \(p \equiv a \pmod{q}\).

In proving this theorem, Dirichlet also had to simultaneously invent the field of analytic number theory (not too shabby!). His key idea was to study a generalization of the Riemann zeta function, now called a Dirichlet \(L\)-function. The Dirichlet \(L\)-function \(L(s, \chi)\) is given by

$$L(s, \chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s},$$

where \(\chi\), called a Dirichlet character, is some kind of multiplicative homomorphism. The key, deep, input in Dirichlet’s proof is that \(L(1, \chi) \neq 0\).

3. **Generalizations of the PNT**

Let \(\pi(x)\) denote the number of primes \(p \leq x\). The prime number theorem (PNT), proved in 1896, is that

$$\pi(x) = (1 + o(1)) \frac{x}{\log x}.$$  

Actually, it is more convenient to count primes with a weight, and we define

$$\vartheta(x) = \sum_{p \leq x} \log p.$$  

The PNT is equivalent to \(\vartheta(x) = (1 + o(1))x\).

We can ask similar questions for primes in arithmetic progressions. Define

$$\vartheta(x; q, a) = \sum_{\substack{p \leq x \\ p \equiv a \pmod{q}}} \log p.$$  

By Theorem 2.1 we know \(\vartheta(x; q, a) \to \infty\) as \(x \to \infty\). One is naturally interested in obtaining a precise asymptotic formula for \(\vartheta(x; q, a)\), in analogy with the PNT. By adapting the techniques used to prove the PNT, one may prove the following result.
Theorem 3.1. Let $a$ and $q$ be fixed. Then

$$\vartheta(x; q, a) = (1 + o(1)) \frac{x}{\varphi(q)}$$

as $x \to \infty$.

On the one hand, Theorem 3.1 is very satisfactory, since it says, roughly, that the primes
are equidistributed in the $\varphi(q)$ residue classes $a$ modulo $q$. On the other hand, the result
is deeply unsatisfactory, because here $a$ and $q$ are required to be fixed. In applications it is
often very important to be able to vary $a$ and $q$ with $x$. The best result we know in this
Dirichlet was proved by Walfisz in 1936, using a result of Siegel on $L(1, \chi)$.

Theorem 3.2 (Siegel-Walfisz theorem). Let $N > 0$ be a fixed real number, and let $x$ be large.
For any $q \leq (\log x)^{N}$ and any $a \pmod{q}$ we have

$$\vartheta(x; q, a) = \frac{x}{\varphi(q)} + E(x; q, a),$$

where $E(x; q, a)$ is an error term satisfying

$$|E(x; q, a)| \leq c_1(N) x \exp(-c_2(N) \sqrt{\log x}).$$

The constants $c_1(N)$ and $c_2(N)$ are positive and depend only on $N$, but there is no way to
compute them if $N \geq 2$.

A couple of remarks about Theorem 3.2 are in order. First, the Siegel-Walfisz theorem
allows us to obtain some uniformity in $a$ and $q$. Still, the uniformity is not very great, since
$q$ is limited to being small compared to $x$. Second, we should remark on the quality of the
error term. The factor $x \exp(-\sqrt{\log x})$ might cause some confusion. The basic comparison
is that, for any large fixed $A > 0$ and any small fixed $\delta > 0$, we have

$$x^{1-\delta} < x \exp(-\sqrt{\log x}) < \frac{x}{(\log x)^{A}}.$$  

(1)

Third remark: the fact that we cannot compute the constants $c_1$ and $c_2$ is a great defect
of Theorem 3.2. We say that the constants $c_1$ and $c_2$ are ineffective. This has hampered
progress on a number of important problems.

4. The least prime in an arithmetic progression

One very natural question to ask, once we have Theorem 2.1 in hand, is: how long do you
have to wait before finding the first prime $p$ with $p \equiv a \pmod{q}$. A number of researchers
have worked on this important problem. We denote the least prime $p \equiv a \pmod{q}$ by
$P(a, q)$.

Before pressing on, let us first see what Theorem 3.2 allows one to deduce. If $\vartheta(x; q, a) > 0$,
then clearly $x \geq P(a, q)$. For any $N > 0$ we have

$$\vartheta(x; q, a) \geq x \left( \frac{1}{q} - c_1(N) \exp(-c_2(N) \sqrt{\log x}) \right).$$

(2)

Recalling that $q \leq (\log x)^{N}$, we see the lower bound in (2) is positive provided $x$ is sufficiently
large in terms of $N$. Since $N$ may be taken arbitrarily large, we have therefore proved the
following result.
Theorem 4.1. Let $\varepsilon > 0$ be small and fixed. For $q$ sufficiently large compared to $\varepsilon$ and any $a \pmod{q}$, we have

$$P(a, q) \leq \exp(q^{\varepsilon}).$$

Theorem 4.1 is okay, but the upper bound is exponential in $q$, and this leaves a lot to be desired. The Generalized Riemann Hypothesis implies $P(a, q) \leq q^{2 + \varepsilon}$, and it is conjectured that $P(a, q) \leq q^{1 + \varepsilon}$. It was therefore surprising that the mathematician Linnik was able to prove the following unconditional result.

Theorem 4.2 (Linnik, 1944). There exist absolute constants $c, L > 0$ such that the following is true: given $q$ large and $a \pmod{q}$, one has

$$P(a, q) \leq cq^L.$$

Linnik did not give a specific value to his constant $L$, but numerous researchers after him have worked hard to make $L$ as small as possible. Heath-Brown (1992) introduced a number of new ideas over previous researchers, and obtained $L \leq 5.5$. The current record is $L \leq 5$, due to Xylouris (2011).

Thus, upper bounds on $P(a, q)$ are well-studied. The question of lower bounds for $P(a, q)$ has received less attention. In this context, the appropriate quantity to consider is

$$P(q) = \max_{(a, q) = 1} P(a, q).$$

One can think of $P(q)$ as being “the largest least prime” modulo $q$. Since trivially $P(q)$ is larger than the $\varphi(q)$-th prime $p_{\varphi(q)}$, and since the PNT yields $p_n \approx n \log n$, we have the trivial lower bound

$$P(q) \geq (1 - o(1)) \varphi(q) \log \varphi(q) = (1 - o(1)) \varphi(q) \log q.$$

This trivial lower bound is surprisingly difficult to improve upon. In 1980 Pomerance showed

$$P(q) \geq (e^\gamma - o(1)) \varphi(q) \log q,$$

and this is still the best result that is known.

One can do slightly better if one asks for results that hold for almost all $q$. Pomerance showed

$$P(q) \geq (e^\gamma - o(1)) \varphi(q)(\log q)(\log \log q)\log \log \log \log \log q,$$

except for $q$ in a set of asymptotic density zero. Pomerance’s work is based on ideas coming from techniques in the study of large gaps between primes.

Recently, Ford, Green, Konyagin, Maynard, and Tao made a breakthrough in large gaps between primes. Junxian Li, George Shakan, and I were able to adapt their techniques and thereby answer a question raised by FGKMT.

Theorem 4.3 (Li-P.-Shakan, 2017). There exists an absolute constant $c > 0$ such that

$$P(q) \geq c \varphi(q)(\log q)(\log \log q)^2 \log \log \log \log q,$$

except for $q$ in a set of asymptotic density zero.

The improvement is a factor of $\log \log \log q$, and this seems to be the limit of present techniques.
5. PRIMES IN ARITHMETIC PROGRESSIONS TO LARGE MODULI

We saw earlier that the Siegel-Walfisz theorem has value, but has limited utility because of the constraint \( q \leq (\log x)^N \). In many applications, however, it suffices to obtain results that only hold on average over \( q \). The presence of an extra variable opens up many new techniques and possibilities. The most important theorem in this direction is due to Bombieri and Vinogradov (mid 1960s).

**Theorem 5.1.** Let \( A > 0 \) be large and fixed. Then for some constant \( B = B(A) > 0 \), we have

\[
\sum_{q \leq x^{1/2}/(\log x)^{A}} \max_{(a,q)=1} \left| \vartheta(x; q, a) - \frac{x}{\varphi(q)} \right| \leq c(A) \frac{x}{(\log x)^A}.
\]

The constant \( c(A) \) is ineffective.

The Bombieri-Vinogradov theorem says, essentially, that for most \( q \) up to \( x^{1/2-o(1)} \) we have \( \vartheta(x; q, a) \approx x/\varphi(q) \) for all \( a \) (mod \( q \)). Observe that the trivial bound for the quantity on the left side of Theorem 5.1 is \( \ll x(\log x)^2 \), say. The constant \( c(A) \) is ineffective because the Siegel-Walfisz theorem is used in the proof of Theorem 5.1.

In applications, the Bombieri-Vinogradov theorem is as strong, on average, as the Generalized Riemann Hypothesis. For, on GRH, we have

\[
\vartheta(x; q, a) = \frac{x}{\varphi(q)} + O(\sqrt{x}(\log x)^2),
\]

and if we insert this into the sum in Theorem 5.1 we get essentially the same result, up to some logarithmic factors.

There are many instances where the Bombieri-Vinogradov theorem, as fantastic as it is, does not suffice. Actually, we expect the following conjecture to be true.

**Conjecture 5.1 (Elliott-Halberstam conjecture).** For any \( \varepsilon, A > 0 \) we have

\[
\sum_{q \leq x^{1/4}} \max_{(a,q)=1} \left| \vartheta(x; q, a) - \frac{x}{\varphi(q)} \right| \leq c(A, \varepsilon) \frac{x}{(\log x)^A}.
\]

We are a long ways off from proving the Elliott-Halberstam conjecture. But there has been some limited success in improving the range of \( q \) over the Bombieri-Vinogradov theorem. Bombieri, Friedlander, and Iwaniec wrote a series of papers on this topic in the 80s. For instance, they proved the following result.

**Theorem 5.2 (Bombieri-Friedlander-Iwaniec, 1986).** Let \( a \neq 0 \) be a fixed integer. For any fixed \( A > 0 \) there exists \( B = B(A) > 0 \) such that

\[
\left| \sum_{q \leq x/(\log x)^{B}} \left( \vartheta(x; q, a) - \frac{x}{\varphi(q)} \right) \right| \leq c(a, A) \frac{x}{(\log x)^A}.
\]

Observe that the constant depends on the residue class \( a \), and this is a serious limitation.

More recently there has been renewed interest in the problem of improving upon the Bombieri-Vinogradov theorem, because of the connection to bounded gaps between primes.
In 2014, Yitang Zhang famously showed that
\[
\liminf_{n} (p_{n+1} - p_n) \leq 70 \cdot 10^6,
\]
where \( p_n \) denotes the \( n \)-th prime. This was followed by a flurry of activity and further improvements. The key input in Zhang’s work on bounded gaps between primes was something like the following.

**Theorem 5.3.** Let \( A > 0 \) be large and fixed. Let \( a \neq 0 \) be an integer. There exists a small, absolute \( \varepsilon > 0 \) such that
\[
\sum_{q \leq x^{1/2+\varepsilon}, \text{squarefree} \atop p | q \Rightarrow p \text{ "small"}} \left| \vartheta(x; q, a) - \frac{x}{\varphi(q)} \right| \leq c(A) \frac{x}{(\log x)^A}.
\]

The fact that the constant only depends on \( A \), and not on the residue class \( a \), is one of the key innovations of Zhang.