MATH 453
Primality Testing

We have seen a few primality tests in previous chapters: Sieve of Eratosthenes (Trivial division), Wilson's Test, and Fermat's Test.

- **Sieve of Eratosthenes (or Trivial division)**
  Let $n \in \mathbb{N}$ with $n > 1$.
  If n is not divisible by any integer $d \leq \sqrt{n}$, then n is prime.
  If n is divisible by some integer $d \leq \sqrt{n}$, then n is composite.

- **Wilson Test**
  Let $n \in \mathbb{N}$ with $n > 1$.
  If $(n-1)! \not\equiv -1 \mod n$, then n is composite.
  If $(n-1)! \equiv -1 \mod n$, then n is prime.

- **Fermat Test**
  Let $n \in \mathbb{N}$ and $a \in \mathbb{Z}$ with $n > 1$ and $(a, n) = 1$.
  If $a^{n-1} \not\equiv 1 \mod n$, then n is composite.
  If $a^{n-1} \equiv 1 \mod n$, then the test is inconclusive.

  Remark 1. *Using the same assumption as above, if n is composite and $a^{n-1} \equiv 1 \mod n$, then n is said to be a* **pseudoprime to base** *a. If n is a pseudoprime to base a for all $a \in \mathbb{Z}$ such that $(a, n) = 1$, then n is called a* **Carmichael number**. *It is known that there are infinitely Carmichael numbers (hence infinitely many pseudoprimes to any base a). However, pseudoprimes are generally very rare. For example, among the first 10^{10} positive integers, $14,882$ integers ($\approx 0.00015\%$) are pseudoprimes (to base 2), compared with $455,052,511$ primes ($\approx 4.55\%$)*

In reality, the primality tests listed above are computationally inefficient. For instance, it takes up to $\sqrt{n}$ divisions to determine whether n is prime using the Trivial Division method. Similarly, there is no efficient way to compute $(n-1)!$ modulo n if n is very large. Although computing a^{n-1} modulo n is relatively easy, Fermat test can only be used as a test for compositeness, rather than primality, since false positives (i.e. pseudoprimes) exist. The next primality test fixes this hole in Fermat test.

- **Lucas Test**
  Let $n \in \mathbb{N}$ and $a \in \mathbb{Z}$ with $n > 1$.
  Suppose the following two conditions hold:
  (1) $a^{n-1} \equiv 1 \mod n$,
  (2) $a^{\frac{n-1}{q}} \not\equiv 1 \mod n$ for every prime $q \mid n-1$.
  Then n is prime.

- **Corollary to Lucas Test**
  Let $n > 1$ be an odd integer and $a \in \mathbb{Z}$.
  Suppose the following two conditions hold:
  (1) $a^{\frac{n-1}{2}} \equiv -1 \mod n$,
  (2) $a^{\frac{n-1}{q}} \not\equiv 1 \mod n$ for every prime $q \mid n-1$.
  Then n is prime.

(The proofs of these two tests can be found on pages 239-240 of the textbook.)

Example 1. *Let* $n = 997$. *Then* $n - 1 = 996 = 2^2 \cdot 3 \cdot 83$. *We have*

$$7^{996} \equiv 1 \mod 997,$$
$$7^{\frac{996}{2}} \equiv 7^{498} \equiv -1 \not\equiv 1 \mod 997,$$
$$7^{\frac{996}{3}} \equiv 7^{332} \equiv 304 \not\equiv 1 \mod 997,$$
$$7^{\frac{996}{83}} \equiv 7^{12} \equiv 9 \not\equiv 1 \mod 997.$$

Since 997 *passes Lucas test, it is prime.*

Remark 2. *Modular exponentiation can be computed easily in most computer algebra systems like* `Maple`, `Mathematica`, *or online computational tools like Wolfram Alpha. For example, if we enter* $Mod[7\hat{}498, 997]$ *or* $7\hat{}498 \mod 997$ *in Wolfram Alpha, it immediately returns* 996 *as the answer. Without the aid of computer algebra systems, there is also a systematic (but tedious) way to compute* a^k *modulo* n. *See Student Project 1 on page 73 of the textbook.*

A major drawback of Lucas test is that one needs to find all prime divisors of $n-1$ first. Unfortunately, factoring is usually much harder than testing for primality, so Lucas test is somewhat useless unless the prime divisors of $n-1$ are already known. Typical examples of integers n for which the prime divisors of $n-1$ are explicitly known are Fermat numbers $F_m = 2^{2^m} + 1$. We can apply Lucas test to deduce the following result.

- **Pépin Test**
  Let $m \in \mathbb{N}$ and $F_m = 2^{2^m} + 1$. Then F_m is prime if and only if
  $$3^{\frac{F_m - 1}{2}} \equiv -1 \mod F_m.$$
  (The proof is outlined in Problem 14 on page 241 of the textbook.)

Example 2. *We have* $F_3 = 2^{2^3} + 1 = 257$. *Since*

$$3^{\frac{F_3-1}{2}} = 3^{128} \equiv 256 \equiv -1 \mod 257,$$

it follows from Pépin test that F_3 *is prime.*

In theory, we can use Pépin Test to determine whether F_m is prime or composite for any $m \geq 1$. However, since F_m grows very rapidly, only a handful of Fermat numbers can be tested in a reasonable amount of time. Due to this computational limitation, very little is known about primality and compositeness of F_m. (As of today, only $F_0, F_1, F_2, F_3,$ and F_4 are known to be prime and only 288 Fermat numbers are known to be composite.)

The next test is similar to Fermat test in the sense that it can be used to test for compositeness rather than primality. Nevertheless, it serves as a very efficient probabilistic test for primality due to the fact that composite integers passing this test are much scarcer than pseudoprimes.

- **Miller-Rabin Test**
  Let $n > 2$ be an odd integer and $n - 1 = 2^k m$, where $k, m \in \mathbb{N}$ and m is odd.
  If n is prime, then $\forall a \in \{1, 2, \ldots, n-1\}$,

(1) $$a^m \equiv 1 \mod n \text{ OR } a^{2^j m} \equiv -1 \mod n \text{ for some } 0 \leq j \leq k-1.$$

  Equivalently, if there exists $a \in \{1, 2, \ldots, n-1\}$ such that

$$a^m \not\equiv 1 \mod n \text{ AND } a^{2^j m} \not\equiv -1 \mod n \text{ for all } 0 \leq j \leq k-1,$$

  then n is composite.

Proof. Consider a factorization of the polynomial $x^{n-1} - 1$:

$$\begin{aligned} x^{n-1} - 1 = x^{2^k m} - 1 &= \left(x^{2^{k-1}m}\right)^2 - 1 \\ &= (x^{2^{k-1}m} - 1)(x^{2^{k-1}m} + 1) \\ &= (x^{2^{k-2}m} - 1)(x^{2^{k-2}m} + 1)(x^{2^{k-1}m} + 1) \\ &= \cdots \\ &= (x^m - 1)(x^m + 1)(x^{2m} + 1)(x^{4m} + 1) \cdots (x^{2^{k-1}m} + 1). \end{aligned}$$

If n is prime and $1 \leq a \leq n-1$, then it follows from the factorization above and Fermat's Theorem that

$$(a^m - 1)(a^m + 1)(a^{2m} + 1)(a^{4m} + 1) \cdots (a^{2^{k-1}m} + 1) \equiv a^{n-1} - 1 \equiv 0 \mod n.$$

Hence $a^m - 1 \equiv 0 \mod n$ or $a^{2^j m} + 1 \equiv 0 \mod n$ for some $0 \leq j \leq k-1$, which is equivalent to (1). □

Remark 3. *An odd integer n is said to* **pass the Miller-Rabin test for base** *a if it satisfies* (1). *Hence every prime number passes the Miller-Rabin test for all bases $a \in \{1, 2, \ldots, n-1\}$. However, if n passes the Miller-Rabin test for some base a, then n is not necessarily prime. A composite integer passing the test for base a is called* **a strong pseudoprime to base a.** *It is easily seen that every strong pseudoprime to base a is a pseudoprime to base a, though the converse is not true. See a below example.*

Example 3. *Let $n = 2201$. Then $n - 1 = 2^3 \cdot 275$. Working modulo 2201, we have*

$$2^{275} \equiv 1582 \not\equiv 1, \quad 2^{550} \equiv 187 \not\equiv -1, \quad 2^{1100} \equiv 1954 \not\equiv -1.$$

Hence 2201 fails the Miller-Rabin test for base 2. Consequently, 2201 is composite.

Let $n = 2047$. Then $n - 1 = 2 \cdot 1023$. Since

$$2^{1023} \equiv 1 \mod 2047,$$

2047 passes the Miller-Rabin test for base 2. However, 2047 is composite since $2047 = 23 \cdot 89$. Hence 2047 is a strong pseudoprime to base 2.

Let $n = 341$. Then $n - 1 = 2^2 \cdot 85$. Working modulo 341, we have

$$2^{85} \equiv 32 \not\equiv 1, \quad 2^{170} \equiv 1 \not\equiv -1.$$

Hence 341 fails the Miller-Rabin test for base 2. Consequently, 341 is composite and 341 is not a strong pseudoprime to base 2. On the other hand, we have

$$2^{340} \equiv \left(2^{170}\right)^2 \equiv 1 \mod 341,$$

so 341 is a pseudoprime to base 2.

Remark 4. *It can be proven that a composite integer n is a strong pseudoprime to at most one quarter of bases $1, 2, \ldots, n-1$. In other words, given a random base $1 \le a \le n-1$, the probability that a composite integer n passes the Miller-Rabin test for base a is at most $1/4$. As a consequence, if we randomly choose k integers $a_1, a_2, \ldots, a_k \in \{1, 2, \ldots, n-1\}$ and n survives the test for all bases a_i, then the probability that n is prime is at least $1 - \left(\frac{1}{4}\right)^k$. (Note that if $k = 100$ then $1 - \left(\frac{1}{4}\right)^k \approx 0.\underbrace{99\ldots9}_{59 \text{ digits}}$.)*

The next (and the last) test has been used to locate many of the largest primes known to date. In particular, it gives an algorithm specialized to testing Mersenne primes.

- **Lucas-Lehmer test**
  Let $M_p = 2^p - 1$ be a Mersenne number, where p is an odd prime. Define a sequence $\{s_n\}_{n=0}^{\infty}$ by

$$s_n = \begin{cases} 4, & \text{if } n = 0 \\ s_{n-1}^2 - 2, & \text{otherwise.} \end{cases}$$

  Then M_p is prime if and only if $s_{p-2} \equiv 0 \mod M_p$.

Remark 5. *The first few values of s_n are $s_0 = 4, s_1 = 14, s_2 = 194, s_3 = 37634, \ldots$ Closed forms of s_n are also known. For instance, we have $s_n = (2+\sqrt{3})^{2^n} + (2-\sqrt{3})^{2^n}$ for $n \geq 0$. (This formula can be proven by induction.)*

Example 4. *Consider $M_7 = 2^7 - 1 = 127$. We have*

$$\begin{aligned} s_2 &= 194 \equiv 67 \mod 127 \\ s_3 &\equiv 67^2 - 2 \equiv 42 \mod 127 \\ s_4 &\equiv 42^2 - 2 \equiv 111 \equiv -16 \mod 127 \\ s_5 &\equiv 16^2 - 2 \equiv 0 \mod 127. \end{aligned}$$

Therefore, M_7 is prime.

Final remark The Lucas-Lehmer test has actively been used in the Great Internet Mersenne Prime Search (GIMPS) project. The largest prime known to date, discovered on January 7, 2016, is $M_{74207281}$, which is the 49th Mersenne prime and has $22,338,618$ decimal digits. GIMPS currently offers a $\$3,000$ award for those who discover a new Mersenne prime having fewer than 100 million digits.

It will be another million years, at least, before we understand the primes.

Paul Erdös

(1913-1996)