Chapter 5: Number Theory and Algebra

Lecture 24

Primality testing

Trial division

Pseudo-prime test

Lucas' test

Miller-Rabin test

AKS test

others...

Largest prime found: $2^{257885161} - 1$ (January 2014)

Trial division

Input: an integer n
Output: Answer to whether n is prime.

- Trial divide n by primes up to $\sqrt{n}$.

This is good for small n but slow ($O(\sqrt{n})$) in general.
Eratosthenes' Sieve implements this nicely.

Example

Is 11 prime?

We try to divide 11 by primes $2, 3 \leq \sqrt{11}$.
Neither are factors, so 11 is prime.

Pseudo-prime test

Input: an integer n
Output: No! if n is composite

- Let $a \in \mathbb{N}$.
- If $\gcd(a, n) \neq 1$, then n is composite; return No!
    - If $a^{n-1} \not\equiv 1 \pmod{n}$, then n is composite; return No!

Fermat's Little Theorem: $a^{n-1} \equiv 1 \pmod{n}$ if $\gcd(a, n) = 1$ for n prime.
The test might not return No!, in which case n is a pseudo-prime to base a.
If n passes this for many values of a, then it is likely that n is prime.
However, some composite integers n can pass this test for all integers a.
These are called Carmichael numbers.

Example

The number 561 is a Carmichael number.
For instance, $\gcd(5, 561) = 1$ and $5^{560} \equiv 1 \pmod{n}$.
However, 561 is clearly divisible by 3 and is thus not prime.

Pseudo-prime test

Input: an integer n
Output: No! if n is composite

- Let $a \in \mathbb{N}$.
- If $\gcd(a, n) \neq 1$, then n is composite; return No!
  - If $a^{n-1} \not\equiv 1 \pmod{n}$, then n is composite; return No!

Fermat's Little Theorem: $a^{n-1} \equiv 1 \pmod{n}$ if $\gcd(a, n) = 1$ for n prime.
The test might not return No!, in which case n is a pseudo-prime to base a.
If n passes this for many values of a, then it is likely that n is prime.
However, some composite integers n can pass this test for all integers a.
These are called Carmichael numbers.

Theorem
There are infinitely many Carmichael numbers.

Lucas' test

Input: an integer n
Output: Possible answer to whether n is prime.

- Let $a \in \mathbb{N}$.
- If $\gcd(a,n) \neq 1$, then n is composite; return No!
  - If $a^{n-1} \not\equiv 1 \pmod{n}$, then n is composite; return No!
    - If $a^{\frac{n-1}{p}} \not\equiv 1 \pmod{n}$ for all primes $p \mid n-1$, then return Yes!

This test is only useful when $n-1$ factors easily.

Example

Is 257 prime?

Let $a = 3$; then $\gcd(3, 257) = 1$ and $3^{256} \equiv 1 \pmod{257}$.
The only prime factor of $257 - 1 = 256 = 2^8$ is 2,
and $3^{\frac{256}{2}} = 3^{128} \equiv -1 \not\equiv 1 \pmod{257}$, so 257 is prime.
Note that this test does not in this example work for $a = 2$:

$$2^{\frac{256}{2}} = 2^{128} \equiv 1 \pmod{257}$$

Miller-Rabin probabilistic primality test

Input: an integer n

Output: No! if n is composite; otherwise probably prime!

- Write $n = 2^s t + 1$ with t odd.
- Choose $a \in \{1, \ldots, n-1\}$ randomly.
- If $a^t \equiv 1 \pmod{n}$, then return probably prime!
- For $r = 0, \ldots, s-1$:

  If $a^{2^r t} \equiv -1 \pmod{n}$, then return probably prime!
- Return No!

Suppose that $\gcd(a, n) = 1$.

If n is prime, then $a^{2^s t} = a^{n-1} \equiv 1 \pmod{n}$. Then either

- $a^t \equiv 1 \pmod{n}$ or
- some $r \in \{0, \ldots, s-1\}$ satisfies $a^{2^r t} \equiv -1 \pmod{n}$.

Numbers satisfying one of these conditions are strong pseudo-primes base a.

Miller-Rabin probabilistic primality test

Input: an integer n
Output: No! if n is composite; otherwise probably prime!

- Write $n = 2^s t + 1$ with t odd.
- Choose $a \in \{1, \ldots, n-1\}$ randomly.
- If $a^t \equiv 1 \pmod{n}$, then return probably prime!
- For $r = 0, \ldots, s-1$:
  If $a^{2^r t} \equiv -1 \pmod{n}$, then return probably prime!
- Return No!

It has been proved that at most 25% strong pseudo-primes are composite - but in practice, there seem to be far fewer (0.1%).
Repeated use of the Miller-Rabin test gives very good results.

Theorem
If $n < 3.4 \times 10^{14}$ and n passes this test for all primes $a = 2, 3, \ldots, 17$, then n is prime.