Primality testing

- Now we move to factoring, or irreducibility testing, of integers.

- Motivation: • natural qn. (first raised by Gauss formally).
  • Commercially, appears in RSA used in browsers, file transfer applications (eg. SSH), smartcards, etc.

- The first question: Is input n prime?

Historical attempts

1) Antiquity (Eratosthenes Sieve, 300 B.C.)

Divide n by $2, 3, \ldots, \lfloor \sqrt{n} \rfloor$.

• It's doable for small n, eg. 127. But for large n, eg. $2^{127}-1$, $\sqrt{n}$ steps is way too long.

- Ideally, we want a $(\lg n)^{O(1)}$ time algorithm.

2) Fermat test (1660s).

For several a, test $a^n \equiv a \pmod n$.

- It is fast for a single $a \in \mathbb{Z}/n\mathbb{Z}$.
- But how many a's should we try till we can deduce "n is prime" ?

- Carmichael (1910) showed the existence of composite n's s.t. $\forall a \in (\mathbb{Z}/n\mathbb{Z})^*$, $a^n \equiv a \pmod n$.

  Eg. $n = 561 = 3 \times 11 \times 17$.

- Alford, Granville & Pomerance (1994) showed that there are ∞ly many Carmichael numbers.

  In fact, at least $n^{2/7}$ in the set $[n]$.

3) Solovay-Strassen (1974).

- This was the first correct, "practical" primality test.

- It is based on quadratic residuosity and is a randomized poly-time primality test.

Lemma 1 (Legendre symbol): For a prime p & $a \in \mathbb{Z}$, define $\left(\frac{a}{p}\right) := a^{\frac{p(p-1)}{2}} \bmod p$. Then, a is a square in $\mathbb{F}_p^*$ iff $\left(\frac{a}{p}\right) = 1$.

Pf:

- Seen before. □

Lemma 2 (Jacobi symbol): For numbers $a, n \in \mathbb{Z}$, define $\left(\frac{a}{n}\right) := \prod_{\text{prime } p \mid n} \left(\frac{a}{p}\right)$ (with repetition).

Then,

totally multiplicative

(i) $\left(\frac{ab}{n}\right) = \left(\frac{a}{n}\right) \cdot \left(\frac{b}{n}\right)$, $\forall a, b \in \mathbb{Z}$.

(ii) $\left(\frac{2}{n}\right) = (-1)^{\frac{n^2-1}{8}}$ & $\left(\frac{-1}{n}\right) = (-1)^{\frac{n-1}{2}}$, for odd $n \in \mathbb{N}$.

Gauss' (1796) quadratic reciprocity law.

(iii) $\left(\frac{a}{n}\right) \cdot \left(\frac{n}{a}\right) = (-1)^{\frac{a-1}{2} \cdot \frac{n-1}{2}}$, for odd coprime $a, n \in \mathbb{N}$.

Proof:

- (ii) & (iii) are elementary but nontrivial.
- (iii) has more than 200 proofs known! □

- Lemma 2 gives an algorithm to compute $\left(\frac{a}{n}\right)$, in a way similar to Euclid's gcd.

Algo:

1) If $(a,n) \neq 1$ then OUTPUT 0.

2.1) Replace a by $(a \bmod n) \in \left(-\frac{n}{2}, \frac{n}{2}\right]$.

2.2) If $a<0$ then reduce it to a positive case using the properties: $\left(\frac{-1}{2}\right)=1$ & $\left(\frac{a}{n}\right) = (-1)^{\frac{n-1}{2}} \cdot \left(\frac{-a}{n}\right)$.

2.3) If $2|a$ then make it odd using $\left(\frac{2}{n}\right) = (-1)^{\frac{n^2-1}{8}}$.

2.4) If $2|n$ " " " " " $\left(\frac{a}{2n'}\right) = \left(\frac{a}{n'}\right)$.

2.5) If $a=1$ then OUTPUT 1.

3) OUTPUT $(-1)^{\frac{a-1}{2}\cdot\frac{n-1}{2}} \cdot \left(\frac{n}{a}\right)$.

[In each recursive step n gets at least halved. The time complexity is $\tilde{O}(\lg a \cdot \lg n)$.]

- Note that if n is prime $\left(\frac{a}{n}\right) \equiv a^{\frac{n-1}{2}} \pmod n$, which may not be true in the composite n case.

- Solovay-Strassen used this idea to design a test:

Algo.: (Input: $n \in \mathbb{N}$.)

1) If $2 | n$ or $n = a^b$ for $b \in \mathbb{N}_{>1}$, then OUTPUT composite.

2) Pick a random $a \in [n]$.
   If $(a,n) \neq 1$ then OUTPUT composite.

3) If $\left(\frac{a}{n}\right) \equiv a^{\frac{n-1}{2}} \pmod n$ then OUTPUT prime, else OUTPUT composite.

- We easily deduce that it runs in $\tilde{O}(\log^2 n)$ time and that:

Claim 1: If n is prime then it outputs "prime".

Claim 2: If n is composite then $\Pr_{a \in (\mathbb{Z}/n\mathbb{Z})^*}[\text{outputs "prime"}] \leq 1/2$.

Proof:

- Consider the set $B := \{a \in (\mathbb{Z}/n\mathbb{Z})^* \mid \left(\frac{a}{n}\right) \equiv_n a^{\frac{n-1}{2}}\}$.
- It is a subgroup of $(\mathbb{Z}/n\mathbb{Z})^*$. How big is it?