

Algorithms for Finite Fields Lecture Notes

October 24/26, 2006

1 Primality Testing

A primality testing algorithm takes an integer n as input, and decides whether n is prime or not. (Note: It does not necessarily give factors - this is a different (and harder) problem.)

We will eventually present the AKS algorithm, which is a deterministic, polynomial time primality test.

Many primality tests (including AKS) are based on the following principle: If \mathbf{R} is a ring of prime characteristic n , then $(x+y)^n = x^n + y^n \forall x, y \in \mathbf{R}$.

An example of this is in Fermat's Little Theorem: If n is prime, then $a^n \equiv a \pmod{n} \forall a \in \mathbb{Z}$. This follows from the principle because $(1+1+\dots+1)^n = 1^n + 1^n + \dots + 1^n = a$ in \mathbb{Z}/n .

1.1 A pseudoprimerality test

For random a : test if $a^n \equiv a \pmod{n}$.

If not, then n is composite.

If yes, then we don't know.

By repeating this test, we can usually know if n is probably a prime, but there are cases where it will never work: A Carmichael number is a composite integer n for which $a^n \equiv a \pmod{n} \forall a, (a, n) = 1$. For example, $561 = 3 * 11 * 17$ is a Carmichael number, and there are infinitely many such numbers.

1.2 Legendre and Jacobi symbols

The Legendre symbol is defined for p an odd prime as follows:

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } a \text{ is a square mod } p, a \neq 0 \\ -1 & \text{if } a \text{ is not a square mod } p, a \neq 0 \\ 0 & \text{if } a = 0 \end{cases}$$

The Jacobi symbol is defined for $a, n \in \mathbb{Z}$, n odd, $n = p_1^{\alpha_1} \dots p_r^{\alpha_r}$ by

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right)^{\alpha_1} \cdots \left(\frac{a}{p_r}\right)^{\alpha_r}$$

where $\left(\frac{a}{p_i}\right)$ is the Legendre symbol.

Note: $\left(\frac{ab}{n}\right) = \left(\frac{a}{n}\right) \left(\frac{b}{n}\right)$, and if $a \equiv b \pmod n$ then $\left(\frac{a}{n}\right) = \left(\frac{b}{n}\right)$.

The definition is not useful for computing, because it requires factoring. Instead we use Quadratic Reciprocity: If a, n are odd and $(a, n) = 1$, then

$$\left(\frac{a}{n}\right) \left(\frac{n}{a}\right) = (-1)^{\frac{a-1}{2} \frac{n-1}{2}}$$

We can use this to compute Jacobi symbols by repeatedly factoring out powers of 2 and reducing:

$$\left(\frac{a}{n}\right) = \left(\frac{n}{a}\right) (-1)^{\frac{a-1}{2} \frac{n-1}{2}} = \pm \left(\frac{n \% a}{a}\right)$$

If we iterate, the convergence is polynomial: It will take $O(\log n)$ steps because after two steps, the numbers will get halved.

1.3 Solovay-Strassen Primality Test

If n is an odd prime and $(d, n) = 1$, then let $\mathbf{R} = (\mathbb{Z}/n[x])/(x^2 - d)$.

Then by the earlier principle,

$$(a + b\sqrt{d})^n = a^n + b^n \sqrt{d}^n = a + bd^{\frac{n-1}{2}} \sqrt{d} = a \pm b\sqrt{d}$$

(Note that $d^{\frac{n-1}{2}} = \left(\frac{d}{n}\right) \pmod n$ since n is prime.)

So the test is as follows: Test for a random d whether $d^{\frac{n-1}{2}} \equiv \left(\frac{d}{n}\right)$. We can simply compute each side. If they are not equal, then n is composite. If they are equal, we don't know, but we don't have any Carmichael-like problems.

Theorem 1.1 *If n is odd and composite, then $G = \{d \in (\mathbb{Z}/n)^* : \left(\frac{d}{n}\right) \equiv d^{\frac{n-1}{2}} \pmod n\} \neq (\mathbb{Z}/n)^*$*

Remark: G is a subgroup of $(\mathbb{Z}/n)^*$, because both sides are multiplicative. So if $G \neq (\mathbb{Z}/n)^*$, then $|G| \leq \frac{1}{2}|(\mathbb{Z}/n)^*|$. Thus at least half of the d 's will show that n is composite in the Solovay-Strassen test. So it follows from the theorem that this test is a probabilistic polynomial time primality test.

In fact, if GRH is true and n is composite, then $\exists d \notin G, 1 \leq d \leq 4(\log n)^2$, so this would be a polynomial time deterministic test by testing those d 's.

Proof Suppose by contradiction that n is composite and $G = (\mathbb{Z}/n)^*$. $\forall a \in (\mathbb{Z}/n)^*, a^{n-1} = (a^{\frac{n-1}{2}})^2 \equiv \left(\frac{a}{n}\right)^2 = 1 \pmod n$. Thus n is Carmichael, so n is squarefree.

Then we can write $n = pr$, p prime, $p \nmid r, r > 1$. Let c be a quadratic nonresidue mod p . Find a s.t.

$$a \equiv c \pmod p$$

$$a \equiv 1 \pmod r$$

We know this exists by CRT. Now

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p}\right) \left(\frac{a}{r}\right) = \left(\frac{c}{p}\right) \left(\frac{1}{r}\right) = (-1)(1) = -1$$

Thus if $a \in G$, then $a^{\frac{n-1}{2}} \equiv -1 \pmod n$, so $a^{\frac{n-1}{2}} \equiv -1 \pmod r$, so $1 \equiv -1 \pmod r$, contradiction. Thus $a \notin G$, but this contradicts our original assumption.

Note: The Miller-Rabin test is similar - it uses $d^{\frac{n-1}{2^r}}$, and is stronger although not as mathematically pretty.

Suppose $\left(\frac{d}{n}\right) = -1$. If n is prime, then

$$(a + b\sqrt{d})^n = a - b\sqrt{d}$$

$$(a + b\sqrt{d})^{n+1} = (a - b\sqrt{d})(a + b\sqrt{d}) = a^2 - db^2 \in \mathbb{Z}/n$$

Thus $(a + b\sqrt{d})^{n+1} - (a - b\sqrt{d})^{n+1} = 0$. This is the Lucas-Lehmer Test (which is usually phrased in terms of linear recurrences). A version of this test can be set up by taking say $a = b = 1$ and d minimal with $\left(\frac{d}{n}\right) = -1$. No composite number has been observed to pass this test, although such a number should exist.

Consider the case of Mersenne primes: If $n = 2^l - 1, l$ prime, then $\left(\frac{3}{n}\right) = -1$. So we can use the Lucas-Lehmer test with $a = 2, b = 1$:

Define $S_k = (2 + \sqrt{3})^{2^k} + (2 - \sqrt{3})^{2^k}, S_0 = 4$. (Note that $S_{k+1} = S_k^2 - 2$, so it's easy to compute these mod n .) Then $n = 2^l - 1$ is prime $\iff S_{l-2} \equiv 0 \pmod n$.

To prove this: Proving \Rightarrow comes from the identity above. The idea behind proving \Leftarrow is that $\left(\frac{2+\sqrt{3}}{2-\sqrt{3}}\right)^{2^{l-2}} \equiv -1 \pmod n$ so the order of $\frac{2+\sqrt{3}}{2-\sqrt{3}}$ in \mathbf{R}^* is 2^{l-1} , so \mathbf{R} must be a field, so n is prime.

1.4 AKS Preliminaries

If \mathbf{R} is a ring of prime characteristic n , then $(x + y)^n = x^n + y^n$, for $x, y \in \mathbf{R}$.

Proposition 1.2 *If, for some $a \in (\mathbb{Z}/n)^*$, $(x + a)^n = x^n + a^n$ in $\mathbb{Z}/n[x]$ then n is prime.*

Remark: Computing $(x + a)^n$ is hard (order n), so this is not a useful algorithm.

To prove this proposition, we will use the following lemma:

Lemma 1.3 (Lucas Lemma) *Let $n = a_0 + a_1p + \dots + a_sp^s$, and $m = b_0 + b_1p + \dots + b_sp^s$, where $0 \leq a_i, b_i \leq p$. Then*

$$\binom{n}{m} \equiv \binom{a_0}{b_0} \cdots \binom{a_s}{b_s} \pmod p$$

In particular, $\binom{n}{m} \not\equiv 0 \pmod p \iff b_i \leq a_i \forall i$.

Proof (Lucas Lemma) $\binom{n}{m}$ is the coefficient of x^m in $(x + 1)^n$. OTOH,

$$\begin{aligned} (x + 1)^n &= (x + 1)^{a_0 + a_1p + \dots + a_sp^s} \\ &= \prod_{i=0}^s (x + 1)^{a_i p^i} \\ &= \prod_{i=0}^s (x^{p^i} + 1)^{a_i} \text{ in } \mathbb{F}_p[x] \\ &= \prod_{i=0}^s \left(\sum_{j=0}^{a_i} \binom{a_i}{j} x^{p^i j} \right) \\ &= \sum_{j_0, \dots, j_s} \binom{a_0}{j_0} \cdots \binom{a_s}{j_s} x^{j_0 + p j_1 + \dots + p^s j_s} \end{aligned}$$

Since $0 \leq j_i \leq a_i < p, j_0 + j_1p + \dots + j_s p^s = m \iff j_i = b_i \forall i$. Thus $\binom{n}{m} = \binom{a_0}{b_0} \dots \binom{a_s}{b_s}$ in \mathbf{F}_p .

Proof (Proposition) Suppose n is composite. Assume first that n is not a prime power. Let p be a prime, $p^r | n, p^{r+1} \nmid n$. Then $n/p^r \neq 1$. We'll show that $\binom{n}{p^r} \not\equiv 0 \pmod p$, so $\binom{n}{p^r} \not\equiv 0 \pmod n$, so $(x+a)^n$ has a nonzero coefficient in x^{n-p^r} and thus cannot be $x^n + a^n$.

Now $n = a_r p^r + a_{r+1} p^{r+1} + \dots, a_r \neq 0$ and $p^r = 1 * p^r + 0$. Thus by Lucas Lemma, $\binom{n}{p^r} \equiv \binom{a_r}{1} \equiv a_r \neq 0 \pmod p$.

Suppose instead that $n = p^r$ for some prime $p, r \geq 2$. Then

$$(x+a)^{p^r} = \sum \binom{p^r}{j} a^j x^{p^r-j}$$

$$\binom{p^r}{p} = \frac{p^r(p^r-1)\dots(p^r-p+1)}{p \dots 1}$$

The only terms not prime to p in this are p^r in the numerator and p in the denominator, so $\binom{p^r}{p} = p^{r-1} * u$, where $p \nmid u$, so it cannot be $0 \pmod p^r$.

Theorem 1.4 *Suppose n is not a prime power and $r < n$ is a prime, $r \nmid n$, such that the order of n in $(\mathbb{Z}/r)^*$ is at least $4(\log n)^2$. Then $\exists a, 1 \leq a \leq 2\sqrt{r} \log n$ such that $(x+a)^n \neq x^n + a$ in $(\mathbb{Z}/n[x])/(x^r - 1)$.*

1.5 AKS Primality Test

Input n odd.

1. If $n = a^b, b \geq 2$, then output that n is composite.

To do this, simply take the b th root of n numerically as a real number and check if it's an integer. We only need to check for values of b up to $\log n$.

2. Find the smallest r prime, $r < n, r \nmid n$, such that the order of n in $(\mathbb{Z}/r)^*$ is at least $4(\log n)^2$.
3. Test for $a = 1, \dots, \lfloor 2\sqrt{r} \log n \rfloor$ whether $(x+a)^n = x^n + a$ in $(\mathbb{Z}/n[x])/(x^r - 1) = \mathbf{R}$.

- (a) If yes for all a , then n is prime.

- (b) If no for some a , then n is composite.
- (c) If no such r exists, then n is prime.

For step 3, we have a ring with n^r elements. Computing $(x + a)^n$ in \mathbf{R} takes $O((r \log n)^c)$ steps. So for the algorithm to be polynomial time in $\log n$, we must have $r = O((\log n)^c)$ for some c . Note that $r > 4(\log n)^2$ from step 2.

Lemma 1.5 *If $n \in \mathbb{Z}, \exists$ prime $r, r \nmid n$, such that the order of n in $(\mathbb{Z}/r)^*$ is at least $4(\log n)^2$ and $r = O((\log n)^6)$.*

Proof Let $M = n \prod_{j=1}^{\lfloor 4(\log n)^2 \rfloor} (n^j - 1)$

If r is prime, $r|n$, then $r|M$. If $r \nmid n$ and the order of n in $(\mathbb{Z}/r)^*$ is less than $4(\log n)^2$ then $r|M$.

What we want is a prime $r, r \nmid M$. Claim: at most $\log_2 M$ primes divide M . This is clear. (Note that $M = p_1^{\alpha_1} \cdots p_k^{\alpha_k} \geq 2^k$.)

Then

$$\begin{aligned} \log M &\leq \log n + \sum_j j \log n \\ &\leq \log n \left(1 + \sum_{j=1}^{4(\log n)^2} 4(\log n)^2 \right) \\ &\leq 5(\log n)^2 * 4(\log n)^2 * \log n = O((\log n)^5) \end{aligned}$$

Thus step 2 is ok, and the algorithm is polynomial in $\log n$.