Primality testing with Frobenius symbols

Lenstra, H.W.

PRIMALITY TESTING WITH FROBENIUS SYMBOLS

H.W. Lenstra, Jr.

In this lecture we discuss several primality testing algorithms that are based on the following trivial theorem.

Theorem. Let n be a positive integer. Then n is prime if and only if every divisor of n is a power of n.

In the actual primality tests one does not check that any r dividing n is a power of n, but that this is true for the images of r and n in certain groups: in Galois groups, in $(\mathbb{Z}/s\mathbb{Z})^*$ for certain auxiliary numbers s, or in the group of values of a Dirichlet character. We remark that it suffices to consider prime divisors r of n.

We begin with a few considerations from algebraic number theory. Let K be a finite abelian extension of the rational number field $\mathbb{Q}$, and suppose that the discriminant of K is relatively prime to n. By the Kronecker-Weber theorem, we have $K \subset \mathbb{Q}(\zeta_s)$ for some integer s with $\gcd(s, n) = 1$; here ζ_s denotes a primitive s-th root of unity. For any integer r that is coprime to s let σ_r be the restriction to K of the automorphism of $\mathbb{Q}(\zeta_s)$ sending ζ_s to ζ_s^r. Then σ_r belongs to the Galois group G of K over $\mathbb{Q}$. If r is prime, then σ_r is the Frobenius symbol of r for the extension $K/\mathbb{Q}$, and the field $K^{\sigma_r} = \{x \in K: \sigma_r(x) = x\}$ is the largest subfield of K in which r splits completely. Let now A be the ring of integers of K^{σ_n}. If n is actually prime, then it is a prime that splits completely in K^{σ_n}, so there is a ring homomorphism $A \to \mathbb{Z}/n\mathbb{Z}$ (mapping 1 to 1). Also, this ring homomorphism is usually not difficult to find. Suppose, for example, that $\alpha \in A$ is such that the index of $\mathbb{Z}[\alpha]$ in A is finite and relatively prime to n, and let f be the irreducible polynomial of α over $\mathbb{Z}$. Then finding a ring homomorphism $A \to \mathbb{Z}/n\mathbb{Z}$ is equivalent to finding a zero of (f mod n) in $\mathbb{Z}/n\mathbb{Z}$. There are good algorithms to find such a zero if n is prime. If conversely a zero is found, it does not follow that n is prime. But it does follow, by composing the map $A \to \mathbb{Z}/n\mathbb{Z}$ with the natural map $\mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/r\mathbb{Z}$, that for every prime divisor r of n there is a ring homomorphism $A \to \mathbb{Z}/r\mathbb{Z}$. This implies that r splits completely in K^{σ_n}, so $K^{\sigma_n} \subset K^{\sigma_r}$, and therefore σ_r <u>is a power of</u> σ_n <u>in the group</u> G, for every divisor r of n. If $K = \mathbb{Q}(\zeta_s)$ this just means that r is congruent to a power of n modulo s. We shall see below how such information can be used to decide whether n is prime or not.

If n is composite then the zero-finding routine that is used may not converge. Therefore it is advisable to apply the primality tests discussed in this lecture only if one is morally certain that n is prime. This certainty can be obtained by subjecting n to several pseudo-prime tests. The question is how to <u>prove</u> that n is prime.

We consider a special case of the test described above. Let s be the largest divisor of $n - 1$ that one is able to factor completely, and let $K = \mathbb{Q}(\zeta_s)$. Then σ_n is the identity on K, and $A = \mathbb{Z}[\zeta_s]$. The irreducible polynomial of ζ_s over $\mathbb{Z}$ is the s-th cyclotomic polynomial Φ_s. If $a \in \mathbb{Z}$ satisfies

$$a^s \equiv 1 \bmod n,$$

$$\gcd(a^{s/q} - 1, n) = 1 \quad \text{for every prime } q \text{ dividing } s,$$

then $(a \bmod n)$ is a zero of $(\Phi_s \bmod n)$ in $\mathbb{Z}/n\mathbb{Z}$. If n is actually prime, then such an a is usually not difficult to find, by manipulating with elements of the form $(b^{(n-1)/s} \bmod n)$. Conversely, if an a as above has been found then by the result proved above we know that any divisor r of n is congruent to a power of n modulo s, i.e. is congruent to 1 mod s. If we have $s > n^{1/2}$ then it follows immediately from this that n is prime. If the weaker inequality $s > n^{1/3}$ is satisfied we can also easily finish the primality test. Namely, if n is not prime then

$$n = (xs + 1)(ys + 1), \quad x > 0, \quad y > 0, \quad xy < s$$

for certain integers x, y. From $(x-1)(y-1) \geq 0$ we obtain $0 < x+y \leq s$, and since $x+y \equiv (n-1)/s \bmod s$ this means that we know the value of $x+y$. We also know that $n = (xs + 1)(ys + 1)$, so x and y can now be solved from a quadratic equation. The result tells us immediately whether n is prime or not.

The test just described is a classical one, and its correctness can easily be proved without Frobenius symbols. There are several refinements and extensions that we do not go into here.

Let now s be a positive integer that is coprime to n. We assume that the complete prime factorization of s is known. Instead of assuming that s divides $n - 1$ we now require that the order t of $(n \bmod s)$ in the unit group $(\mathbb{Z}/s\mathbb{Z})^*$ is relatively small. If n is prime, then the residue class field of any prime ideal of $\mathbb{Z}[\zeta_s]$ containing n is the finite field $\mathbb{F}_{n^t}$. Also, if $a \in \mathbb{F}_{n^t}^*$ is the image of ζ_s then

$$a^s = 1,$$

$$a^{s/q} - 1 \in \mathbb{F}_{n^t}^* \quad \text{for each prime } q \text{ dividing } s,$$

$$\prod_{i=0}^{t-1} (X - a^{n^i}) \text{ has coefficients in } \mathbb{F}_n.$$

The latter property comes from the fact that the polynomial $\prod_{i=0}^{t-1} (X - \zeta_s^{n^i})$ has coefficients in the ring previously denoted by A (for $K = \mathbb{Q}(\zeta_s)$). There are, again, good methods to construct $\mathbb{F}_{n^t}$ and a as above, if n is prime. Suppose, conversely, that one has constructed a ring extension R of $\mathbb{Z}/n\mathbb{Z}$ and an element $a \in R$ having the above properties, with $\mathbb{F}_{n^t}$, $\mathbb{F}_n$ replaced by R, $\mathbb{Z}/n\mathbb{Z}$. Then there is a ring homomorphism $\mathbb{Z}[\zeta_s] \to R$ mapping ζ_s to a, and the subring generated by the coefficients of $g = \prod_{i=0}^{t-1} (X - \zeta_s^{n^i})$ is mapped to $\mathbb{Z}/n\mathbb{Z}$. But from the fact that g is the irreducible polynomial of ζ_s over A it is easy to derive that this subring is equal to A. That gives us the desired ring homomorphism $A \to \mathbb{Z}/n\mathbb{Z}$, which permits us to conclude that every divisor of n is congruent to a power of n modulo s. If $s > n^{1/2}$ then this conclusion immediately leads to the complete factorization of n, by trying the remainders of $1, n, \ldots, n^{t-1}$ modulo s as divisors. The weaker condition $s > n^{1/3}$ is also sufficient to finish the test, by a procedure that is somewhat more complicated than the one described before.

As an example we treat the Lucas-Lehmer test for Mersenne numbers $n = 2^m - 1$, with $m > 2$. Let $e_1 = 4$, $e_{i+1} = e_i^2 - 2$. Then it is asserted that n is prime if and only if $e_{m-1} \equiv 0 \bmod n$. The case that m is <u>even</u> is easy and uninteresting, by looking mod 3. So let m be odd, and define

$$R = (\mathbb{Z}/n\mathbb{Z})[T]/(T^2 - \sqrt{2}\cdot T - 1)$$

where $\sqrt{2} = (2^{(m+1)/2} \bmod n) \in \mathbb{Z}/n\mathbb{Z}$. Denote the image of T in R by a, and let $b = \sqrt{2} - a = -a^{-1}$ be "the" other zero of $X^2 - \sqrt{2}\cdot X - 1$ in R. Then $a^{2^i} + b^{2^i} = (e_i \bmod n)$. If n is prime then one easily checks that R is a field in which a and b are conjugate, so $a^n = b$ by the theory of finite fields. Multiplying by a one gets $a^{2^m} = -1$, so $(e_{m-1} \bmod n) = a^{2^{m-1}} + b^{2^{m-1}} = a^{2^{m-1}} + a^{-2^{m-1}} = 0$. Conversely, assume that $(e_{m-1} \bmod n) = 0$. Then

$$a^{2^m} = -1, \qquad a^{2^{m+1}} = 1$$

and from $a^n = a^{2^m-1} = -a^{-1} = b$ we find

$$(X - a)(X - a^n) = (X - a)(X - b) = X^2 - \sqrt{2}\cdot X - 1,$$

a polynomial with coefficients in $\mathbb{Z}/n\mathbb{Z}$. Applying the preceding theory with $s = 2^{m+1}$, $t = 2$ we conclude that every divisor of n is congruent to 1 or n mod s. From $s > n$ it now follows that n is prime.

To prove that, in the general case, a suitable value for s can always be found we invoke a result of Pomerance and Odlyzko. They proved that for each $n > e^e$ there exists a positive integer t with

$$t < (\log n)^{c \log\log\log n},$$

where c is an absolute effectively computable constant, such that the number

$$s = \prod_{q \text{ prime},\ q-1 \text{ divides } t} q$$

exceeds $n^{1/2}$. If gcd $(s, n) = 1$ then Fermat's theorem implies that $n^t \equiv 1 \bmod s$, so the order of $(n \bmod s)$ in $(\mathbb{Z}/s\mathbb{Z})^*$ is relatively small. This value for s can be used for all n of the same order of magnitude. Given n, one can often make better choices of s by employing known prime factors of $n^i - 1$ for various small values of i.

It is probably possible to treat Adleman's new primality test (see Séminaire Bourbaki, exp. 576) from the same point of view. Let s, t be as in the result of Pomerance and Odlyzko. The $\mathbb{Q}(\zeta_s)$ can be written as the compositum of a collection of cyclic fields, each of which has prime power degree p^k and prime conductor q, with p^k dividing t and q dividing s. These fields have much smaller degrees over $\mathbb{Q}$ than $\mathbb{Q}(\zeta_s)$, and are therefore more attractive from a computational point of view. Employing Gaussian sums as Lagrange resolvents for these fields one can design tests that, as before, permit one to conclude that every divisor of n is congruent to a power of n modulo s. It is, in fact, more efficient to do the actual calculations with Jacobi sums, in the rings $\mathbb{Z}[\zeta_{p^k}]/n\mathbb{Z}[\zeta_{p^k}]$. This version of Adleman's test is being programmed by H. Cohen on the minicomputer in Bordeaux.

Amsterdam, June 1981

H.W. Lenstra, Jr.

Mathematisch Instituut

Universiteit van Amsterdam

Roetersstraat 15

1018 WB Amsterdam