pp. 341-347 in: N. Koblitz (ed.), Number Theory related to Fermat's last theorem, Progress in Math. 26, Birkhäuser, Boston 1982.

PRIMALITY TESTING WITH ARTIN SYMBOLS.

H.W. Lenstra, Jr.

It is a recent discovery that many primality testing algorithms are based on the following trivial theorem.

Theorem. Let n be an integer, $n > 1$. Then n is prime if and only if every divisor of n is a power of n.

This applies to the tests described by Brillhart, Lehmer and Selfridge [2], to the generalizations thereof mentioned by Williams [8, sections 15 and 16], and to the recent algorithm of Adleman, Pomerance and Rumely [1; 5].

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. For the tests described in [2; 8] these groups are of the form $(\mathbb{Z}/s\mathbb{Z})^*$, for certain auxiliary numbers s. Below we consider, more generally, Galois groups of abelian extensions of $\mathbb{Q}$. The group $(\mathbb{Z}/s\mathbb{Z})^*$ arises in this context as the Galois group of $\mathbb{Q}(\zeta_s)$ over $\mathbb{Q}$, where ζ_s denotes a primitive s-th root of unity.

We can usually distinguish three stages in primality testing algorithms that are based on the above theorem. The first stage consists in the selection of a suitable auxiliary group G. It is supposed that there is a natural map σ from the set of divisors of n to G with the property that $\sigma(rr') = \sigma(r)\sigma(r')$ if rr' divides n. For example, if $G = (\mathbb{Z}/s\mathbb{Z})^*$ for some integer s with $\gcd(s, n) = 1$, we can take $\sigma(r) = (r \bmod s)$.

In the second stage of the algorithm one attempts to show that $\sigma(r)$ is a power of $\sigma(n)$ for every r dividing n; it clearly suffices to consider only *prime* divisors r of n. The second stage generally consists in subjecting n to a collection of "pseudoprimality" tests with the following properties (i) if n is prime, it is known to pass the tests; and conversely, (ii) if n passes the tests, then it follows that $\sigma(r)$ is in the subgroup of G generated by $\sigma(n)$ for every divisor r of n. Below we shall see how such tests can be designed. More examples are found in [5]. Usually, most composite numbers n fail to pass one of the tests. If this occurs, we know that n is composite without explicitly knowing a non-trivial factor of n.

If the second stage has been completed successfully, we know that $\sigma(r)$ is a power of $\sigma(n)$ for every r dividing n. In the third stage of the algorithm this information is used to complete the primality test. This is usually only possible when certain conditions are satisfied, which must be taken into account when the group G is selected. In all examples that I know of, these conditions imply that the subgroup generated by $\sigma(n)$ is "fairly small"; see below for more details.

In the tests that we shall describe the group G will always be the Galois group $\mathrm{Gal}(K/\mathbb{Q})$ of a finite abelian extension K of $\mathbb{Q}$ with the property that $\gcd(\Delta_K, n) = 1$; here Δ_K denotes the discriminant of K over $\mathbb{Q}$. In such a field, all prime divisors of n are unramified, and therefore it is meaningful to define $\sigma(r) \in G$ to be the *Artin symbol* of r for the extension $\mathbb{Q} \subset K$, for r dividing n; see [4, Ch.I §5, Ch.X §1]. In our case, we can describe $\sigma(r)$ explicitly as follows. By the Kronecker-Weber theorem, there is an

embedding $K \subset \mathbb{Q}(\zeta_s)$ for some integer s with $\gcd(s,n) = 1$. Now $\sigma(r)$ is the restriction to K of the automorphism of $\mathbb{Q}(\zeta_s)$ sending ζ_s to ζ_s^r. Notice that $\sigma(rr') = \sigma(r)\sigma(r')$ for rr' dividing n.

We put $K^{\sigma(r)} = \{x \in K : \sigma(r)(x) = x\}$ for r dividing n, and by A we denote the ring of integers of the field $K^{\sigma(n)}$. In the tests that we shall describe, the second stage consists in *looking for a ring homomorphism* $A \to \mathbb{Z}/n\mathbb{Z}$ (mapping 1 to 1). To prove that this fits in our general pattern we must show that (i) if n is prime, then such a ring homomorphism can be found, and (ii) if such a ring homomorphism is found, then $\sigma(r)$ belongs to the subgroup of G generated by $\sigma(n)$, for every (prime) divisor r of n.

To prove (i), assume that n is prime. Then $\sigma(n)$ generates the decomposition group of n for the extension $\mathbb{Q} \subset K$, so $K^{\sigma(n)}$ is the largest subfield of K in which n splits completely. Therefore A has a prime ideal $\underline{n}$ for which $A/\underline{n} \simeq \mathbb{Z}/n\mathbb{Z}$. This proves the *existence* of the required ring homomorphism $A \to \mathbb{Z}/n\mathbb{Z}$. For the purposes of the algorithm we should also show that it *can be found* within a reasonable amount of time. For this we suppose that we know an element $\alpha \in A$ such that the index of $\mathbb{Z}[\alpha]$ in A is finite and relatively prime to n, and we denote by f 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 $(f \bmod n)$ in $\mathbb{Z}/n\mathbb{Z}$. If the degree of $(f \bmod n)$ is not too large there are efficient algorithms to find such a zero, see [3, §4.6.2, p.430]. If the degree of f is larger there may be a special technique, or it may be better to use a different description of the ring A; see the examples below. It should be remarked that all these methods to find a ring

homomorphism $A \to \mathbb{Z}/n\mathbb{Z}$ depend heavily on n being prime. If n is composite it *usually* happens that we discover this in the course of the procedure, e.g. by finding an integer a for which $a^n \not\equiv a \bmod n$. However, there is no guarantee of this sort, and if the homomorphism $A \to \mathbb{Z}/n\mathbb{Z}$ has been found we cannot be certain that n is prime. All we *do* know is formulated in (ii).

To prove (ii), assume that we have a ring homomorphism $A \to \mathbb{Z}/n\mathbb{Z}$, and let r be a prime divisor of n. Composing the map $A \to \mathbb{Z}/n\mathbb{Z}$ with the natural map $\mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/r\mathbb{Z}$ we see that there is a ring homomorphism $A \to \mathbb{Z}/r\mathbb{Z}$, so $A/\underline{r} \simeq \mathbb{Z}/r\mathbb{Z}$ for some prime ideal $\underline{r}$ of A. It follows from this that r splits completely in $K^{\sigma(n)}$, and therefore $K^{\sigma(n)}$ is contained in the decomposition field $K^{\sigma(r)}$ of r in $\mathbb{Q} \subset K$. This means precisely that $\sigma(r)$ belongs to the subgroup of G generated by $\sigma(n)$, as required.

In the third stage of the algorithm this information must be used to finish the primality test. Below we shall see how to do this in the case that $K = \mathbb{Q}(\zeta_s)$ for an integer s satisfying certain conditions. It would be of interest to find methods that work for more general fields K.

We consider a special case of the test outlined above. Let s be the largest divisor of $n-1$ that one is able to factorize completely, and let $K = \mathbb{Q}(\zeta_s)$. The group G is then isomorphic to $(\mathbb{Z}/s\mathbb{Z})^*$, with $\sigma(r) \in G$ corresponding to $(r \bmod s) \in (\mathbb{Z}/s\mathbb{Z})^*$. From $n \equiv 1 \bmod s$ we see that $\sigma(n)$ is the identity on K, so $K^{\sigma(n)} = K$ 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 it is usually not difficult to find such an a, by taking a suitable multiplicative combination of elements of the form $(b^{(n-1)/s} \bmod n)$. Conversely, if an a as above has been found, then by (ii) we know that $\sigma(r)$ is a power of $\sigma(n)$ for every r dividing n. This means that $r \equiv 1 \bmod s$ for every r dividing n. If $s > n^{1/2}$ then it follows immediately that n is prime. If the weaker inequality $s > n^{1/3}$ is satisfied we can also easily finish the primality test [2, theorem 5]. Namely, if n is not prime then

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

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 be solved from a quadratic equation. The result tells us immediately whether n is prime or not. I do not know if there is such a technique for significantly smaller values of s.

The test just described is a classical one due to Pocklington [7], and its correctness can easily be proved without the use of Artin symbols. There are several refinements and extensions that we do not go into here; see [2].

We now come to the main application of our general test. Let 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 group $(\mathbb{Z}/s\mathbb{Z})^*$ is relatively small. For K we choose the field

$\mathbb{Q}(\zeta_s)$. As before, G is isomorphic to $(\mathbb{Z}/s\mathbb{Z})^*$. The degree of K over $K^{\sigma(n)}$ equals t, and the irreducible polynomial of ζ_s over $K^{\sigma(n)}$ is given by

$$g = \prod_{i=0}^{t-1} (X - \zeta_s^{n^i}) .$$

From the fact that $\mathbb{Z}[\zeta_s]$ is the ring of integers of K it is easy to derive that the ring of integers A of $K^{\sigma(n)}$ is, as a ring, generated by the coefficients of g. Hence, to find a ring homomorphism $A \to \mathbb{Z}/n\mathbb{Z}$ it suffices to find an extension ring R of $\mathbb{Z}/n\mathbb{Z}$ and a ring homomorphism $\mathbb{Z}[\zeta_s] \to R$ mapping the coefficients of g inside $\mathbb{Z}/n\mathbb{Z}$. The first question to answer is which ring R should be tried. If n is actually prime, then we can take $R = \mathbb{Z}[\zeta_s]/\underline{n}$ for a prime ideal $\underline{n}$ lying over n, and this is the finite field of n^t elements. So for R we should take a ring of order n^t containing $\mathbb{Z}/n\mathbb{Z}$ with the property that R is a field if n is prime. An example of such a ring is $R = (\mathbb{Z}/n\mathbb{Z})[T]/(h)$ where $h \in (\mathbb{Z}/n\mathbb{Z})[T]$ is a monic polynomial of degree t that is irreducible if n is prime. To find such an h, we can try random monic polynomials $h \in (\mathbb{Z}/n\mathbb{Z})[T]$ of degree t until we find one that passes an irreducibility test as described in [3, §4.6.2, pp. 429-430].

Suppose now that R has been constructed. To find the required ring homomorphism $\mathbb{Z}[\zeta_s] \to R$ it suffices to find an element $a \in R$ (the image of ζ_s) satisfying the following conditions:

$$a^s = 1 ,$$

$$a^{s/q} - 1 \in R^* \text{ for each prime } q \text{ dividing } s ,$$

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

If n is actually prime then it is usually easy to find such an a, by taking a suitable multiplicative combination of elements of the form

$b^{(n^t-1)/s}$, $b \in R$. Conversely, if an a as above has been found then it follows that there exists a ring homomorphism $A \to \mathbb{Z}/n\mathbb{Z}$, so by (ii) every divisor r of n is congruent to a power of n modulo s.

To finish the test using this information we must again assume that s is sufficiently large. If $s > n^{1/2}$ then it suffices to try the remainders of $1, n, n^2, \ldots, n^{t-1}$ modulo s as possible divisors of n. The weaker condition $s > n^{1/3}$ is also sufficient to finish the test, by the following result, applied to $d \equiv 1, n, n^2, \ldots, n^{t-1} \bmod s$: if d, s, n are integers satisfying

$$s > n^{1/3} > 0, \qquad \gcd(d,s) = 1,$$

then n has at most 11 divisors that are congruent to d modulo s, and there is an efficient algorithm that determines all these divisors. This is proved in [6]. I do not know whether a similar result holds for $s > n^{1/4}$.

The expected running time of this primality test is strongly affected by the size of t. To find an upper bound for t we invoke a result of Pomerance and Odlyzko [1, section 6]. 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 s is a completely factored divisor of $n^t - 1$. Using this value for s we can conclude that the expected running time of the algorithm is less than $(\log n)^{c' \log\log\log n}$ for some absolute effectively computable constant c'.

Notice that the above 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. To illustrate this, we show that the well-known Lucas-Lehmer test for Mersenne numbers [8, section 13] is a special case of our test.

Let $n = 2^m - 1$, with $m > 2$. Put $e_1 = 4$, $e_{i+1} = e_i^2 - 2$. Then it is asserted that n is prime if and only if $e_{m-1} \equiv 0 \bmod n$.

We derive this from our theory with $s = 2^{m+1}$ and $t = 2$. The case that m is *even* is easy and uninteresting, by looking modulo 3. So let m be odd, and define

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

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 $X^2 - \sqrt{2}X - 1$ in R. Then one proves by induction on i that $a^{2^i} + b^{2^i} = (e_i \bmod n)$, for $i \geq 1$. If n is prime then it is easy to check 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 $a^{2^m} = -1$, and therefore

$$a^s = a^{2^{m+1}} = 1,$$

$$a^{s/2} - 1 = -2 \in R^*,$$

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

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

a polynomial with coefficients in $\mathbb{Z}/n\mathbb{Z}$. So we checked the conditions which guarantee the existence of a ring homomorphism $A \to \mathbb{Z}/n\mathbb{Z}$, in the notation used earlier. From our theory it now follows that every

divisor of n is congruent to 1 or n modulo s. But $s > n$, so this clearly implies that n is prime.

I expect that the primality test described in this paper, as well as the more flexible version formulated in [5, theorem (8.4)], will mainly be of practical value when used in combination with the test of Adleman et al. [1 ; 5], which can also be interpreted in terms of Artin symbols.

References.

1. L.M. Adleman, C. Pomerance, R.S. Rumely, On distinguishing prime numbers from composite numbers, to appear.
2. J. Brillhart, D.H. Lehmer, J.L. Selfridge, New primality criteria and factorizations of $2^m \pm 1$, Math. Comp. 29 (1975), 620-647.
3. D.E. Knuth, The art of computer programming, vol. 2, Seminumerical algorithms, second edition, Addison-Wesley, Reading, Ma. 1981.
4. S. Lang, Algebraic number theory, Addison-Wesley, Reading, Ma. 1970.
5. H.W. Lenstra, Jr., Primality testing algorithms (after Adleman, Rumely and Williams), Séminaire Bourbaki 33 (1980/81), no. 576. Lecture Notes in Mathematics, Springer, Berlin, to appear.
6. H.W. Lenstra, Jr., Divisors in residue classes, in preparation.
7. H.C. Pocklington, The determination of the prime and composite nature of large numbers by Fermat's theorem, Proc. Cambridge Philos. Soc. 18 (1914-16), 29-30.
8. H.C. Williams, Primality testing on a computer, Ars Combinatoria 5 (1978), 127-185.

H.W. Lenstra, Jr.
Mathematisch Instituut
Universiteit van Amsterdam
Roetersstraat 15
1018 WB Amsterdam