Primality testing algorithms, Séminaire Bourbaki 33 exp. no. 576

Lenstra, H.W.

Lecture Notes in Mathematics 901, 1981, pp. 243-257, Springer-Verlag.
Séminaire BOURBAKI 576-01
33e année, 1980/1981, n° 576 Juin 1981

PRIMALITY TESTING ALGORITHMS

[after ADLEMAN, RUMELY and WILLIAMS]

by H.W. LENSTRA, Jr.

§ 1. Introduction

Most methods that are used to decide whether a given integer $n > 1$ is prime or composite deal much more easily with composite numbers than with prime numbers. This is, in particular, true for the methods that are based on Fermat's theorem, asserting that $a^n \equiv a \bmod n$ for all prime numbers n and all integers a. A single a not satisfying this congruence suffices to prove that n is composite, without, however, yielding a factorization of n. But not every composite n can be proved composite in this way: the composite numbers $n = 561 = 3 \cdot 11 \cdot 17$, $1105 = 5 \cdot 13 \cdot 17$, $1729 = 7 \cdot 13 \cdot 19$, and probably infinitely many others, have the property that $a^n \equiv a \bmod n$ for all integers a. A stronger version of Fermat's theorem, which does not have this defect, states that

$$a^{(n-1)/2} \equiv \left(\frac{a}{n}\right) = \pm 1 \bmod n \tag{1.1}$$

for all odd primes n and all integers $a \not\equiv 0 \bmod n$. Here $\left(\frac{a}{n}\right)$ denotes the Jacobi symbol, for $a \in \mathbb{Z}$ and n an odd positive integer. It can be proved that for odd, composite n at most half, and usually much less, of all $a \in \{1, 2, \ldots, n-1\}$ satisfy (1.1). For any a in this range, $a^{(n-1)/2} \bmod n$ and $\left(\frac{a}{n}\right)$ can be calculated efficiently: the first by repeated squarings and multiplications modulo n, using the binary representation of $(n-1)/2$, and the second by means of the reciprocity law for Jacobi symbols. These calculations can be done in time $O((\log n)^{2+\varepsilon})$, for any $\varepsilon > 0$. This leads to an easy practical method of recognizing composite numbers: draw integers a at random from $\{1, 2, \ldots, n-1\}$ until one is found not satisfying (1.1). If several hundreds of values for a have been tried, and they all satisfy (1.1), one can safely bet that n is prime, or use n as a prime number for commercial purposes; but one is not mathematically certain.

The algorithm just described is due to Solovay and Strassen [12]. It is an example of a *probabilistic compositeness test*, i.e. an algorithm that on input n tells us whether n is prime or composite if it terminates, and that has a high probability of terminating if n is composite; we do not care about termination if n is prime. The notion of a *probabilistic primality test* is defined similarly, interchanging 'prime' and 'composite'. A *deterministic primality* (or *compositeness*) *test* is one that terminates with certainty and tells us whether n is prime or composite.

The main topic of this lecture is the primality testing algorithm of Adleman

and Rumely [1, 2]. In this algorithm, the number n is subjected to a large number of tests similar to (1.1). If n does not pass all these tests, it is composite. If n does pass all these tests, one can determine a small set of numbers containing all divisors $\leq n^{\frac{1}{2}}$ of n. Checking these individually one can decide whether n is prime or composite.

There are two versions of the algorithm: a probabilistic one, discussed in section 4, and a slightly more complicated deterministic one, which is discussed in section 5. Variants and extensions of these tests are described in sections 6 and 7. Section 8 is devoted to the relation of the new test to older primality algorithms. It is hoped that these later sections will contribute to the practical feasibility of the test for numbers of hundreds of decimal digits.

The analysis of the running time leads to a problem in analytic prime number theory, which was resolved by Pomerance and Odlyzko. They proved that there is an effectively computable constant c_1 such that the running time of the deterministic algorithm, and the expected running time of the probabilistic algorithm for prime n, are bounded by $(\log n)^{c_1 \log\log\log n}$, for $n > e^e$. This is much faster than Pollard's deterministic algorithm [9], which runs in time $O(n^{(1/8)+\varepsilon})$ for any $\varepsilon > 0$.

If certain generalized Riemann hypotheses are admitted, there is a still much faster deterministic primality testing algorithm. It consists of testing (1.1) for all positive integers $a < 70(\log n)^2$ not divisible by n. If n passes all these tests one can show, using the Riemann hypotheses, that n is prime. This algorithm has running time $O((\log n)^{4+\varepsilon})$, for any $\varepsilon > 0$.

We refer to Williams' excellent survey paper [13] for more information about primality testing, and in particular for an improvement, due to Miller and Rabin, of the tests based on (1.1). The related but much different problem of decomposing a number into prime factors is discussed in [5, 11]. For efficient algorithms to perform arithmetic operations we refer to [6].

Throughout this *exposé* we fix an integer $n > 1$. One should think of n as an integer that is very likely to be prime, in the sense that a compositeness test like the one described above failed to show that n is composite. The problem is how to *prove* that n is prime.

Further notation: ζ_m is a primitive m-th root of unity, A^* the group of units of a ring A with 1, and $\langle\alpha\rangle$ the subgroup generated by α; by $a|b$ we mean that a divides b and is positive; $v_p(m)$ is the number of factors p in m, for p prime; $\mathbb{Z}_p$ is the ring of p-adic integers, and $\mathbb{F}_q$ the finite field with q elements.

§ 2. Gaussian sums

In this section we fix two prime numbers p and q with $p|q-1$. We assume that $\gcd(pq, n) = 1$. We put $R = \mathbb{Z}[\zeta_p, \zeta_q]$, and we let χ be a character of order p and conductor q, i.e. a group homomorphism $\chi: \mathbb{F}_q^* \to R^*$ with $\chi[\mathbb{F}_q^*] = <\zeta_p>$. The *Gaussian sum* $\tau(\chi)$ is the element of R defined by

$$\tau(\chi) = -\Sigma_{x=1}^{q-1} \chi(x)\zeta_q^x$$

where $\chi(x) = \chi(x \bmod q)$. By a routine calculation, we have

(2.1) $$\tau(\chi)^n \equiv \chi(n)^{-n}\cdot\tau(\chi^n) \mod nR \quad \text{if } n \text{ is } \textit{prime}.$$

We shall investigate what, conversely, can be said about n if the following slightly weaker congruence holds:

(2.2) $$\tau(\chi)^n \equiv \eta(\chi)^{-n}\cdot\tau(\chi^n) \mod nR \quad \text{for some } \eta(\chi) \in <\zeta_p>.$$

We make the following assumption.

(2.3) Condition on p. *For every prime* $r|n$ *we have* $v_p(r^{p-1}-1) \geq v_p(n^{p-1}-1)$.

This inequality can also be formulated as $r^{p-1} \equiv 1 \mod (n^{p-1}-1)\mathbb{Z}_p$; if it holds for all *primes* $r|n$, it clearly holds for *all* $r|n$. If (2.3) is satisfied we write

$$\ell_p(r) = ((r^{p-1}-1)/(n^{p-1}-1) \mod p) \quad \text{for } r|n;$$

this is considered as an element of $\mathbb{Z}_p/p\mathbb{Z}_p = \mathbb{Z}/p\mathbb{Z}$. We have

(2.4) $$\ell_p(rr') = \ell_p(r) + \ell_p(r') \quad \text{if } rr'|n,$$

(2.5) $$\ell_p(n) = 1.$$

(2.6) Proposition. *Suppose that* (2.2) *and* (2.3) *are true. Then* $\eta(\chi) = \chi(n)$, *and* $\chi(r) = \chi(n)^{\ell_p(r)}$ *for each* $r|n$.

The proof is given below. In (2.9) we shall see that condition (2.3) cannot be omitted. In order to be able to apply (2.6) we need a method to verify (2.3). For this purpose we can often apply the following proposition, the proof of which is also given below.

(2.7) Proposition. *If* (2.2) *is satisfied with* $\eta(\chi) \neq 1$, *then* $p = \text{order}(\chi)$ *satisfies* (2.3).

Trivially, we have

(2.8) $$\text{if } n^{p-1} \not\equiv 1 \mod p^2 \text{ then (2.3) is satisfied.}$$

(2.9) Example. Let $p = 2$. Then χ is given by $\chi(x) = \left(\frac{x}{q}\right)$. Put $a = \chi(-1)q = \pm q$, the sign being such that $a \equiv 1 \mod 4$. It is well known that $\tau(\chi)^2 = a$, so (2.1) amounts to

$$a^{(n-1)/2} \equiv \left(\frac{n}{q}\right) \mod n \quad \text{if } n \text{ is prime, } \gcd(2q, n) = 1.$$

This leads to the quadratic reciprocity law: $\left(\frac{a}{n}\right) = \left(\frac{n}{q}\right)$. Similarly, (2.2) is equivalent to

$$a^{(n-1)/2} \equiv \pm 1 \mod n.$$

Let now n be the Ramanujan number $n = 1729 = 7\cdot13\cdot19$. Then $a^{(n-1)/2} \equiv 1 \mod n$

for all $a \in \mathbb{Z}$ with $\gcd(a, n) = 1$, so (2.2) is satisfied for all q, with $\eta(\chi) = 1$. Choosing q such that $\chi(n) = -1$, e.g. $q = 11$, we obtain an example in which $\eta(\chi) \neq \chi(n)$. This shows that condition (2.3) cannot be omitted from (2.6).

Proof of (2.6) and (2.7). Suppose that (2.2) is satisfied. Applying the automorphism of R sending ζ_p to $\zeta_p^{n^i}$ and ζ_q to itself we find that

$$\tau(\chi^{n^i})^n \equiv \eta(\chi)^{-n^{i+1}} \cdot \tau(\chi^{n^{i+1}}) \mod nR$$

for all $i \in \mathbb{Z}_{\geq 0}$, and by induction on i this yields

$$\tau(\chi)^{n^i} \equiv \eta(\chi)^{-i \cdot n^i} \cdot \tau(\chi^{n^i}) \mod nR$$

for all $i \in \mathbb{Z}_{\geq 0}$. With $i = p - 1$ we have $\tau(\chi^{n^i}) = \tau(\chi)$, and this element represents a unit of R/nR because $\tau(\chi) \cdot \overline{\tau(\chi)} = q$. Therefore we obtain

$$\tau(\chi)^{n^{p-1}-1} \equiv \eta(\chi) \mod nR. \tag{2.10}$$

Now let $r|n$ be prime. Then (2.2), with n replaced by r and $\eta(\chi)$ by $\chi(r)$, is satisfied, so for the same reason we have

$$\tau(\chi)^{r^{p-1}-1} \equiv \chi(r) \mod rR. \tag{2.11}$$

Hence if ω denotes the order of $(\tau(\chi) \bmod rR)$ in $(R/rR)^*$, then $\omega | p(r^{p-1} - 1)$.

To prove (2.7), assume that $\eta(\chi) \neq 1$. From (2.10) we see that $\tau(\chi)^{n^{p-1}-1} \equiv \eta(\chi) \not\equiv 1 \bmod rR$, so ω divides $p(n^{p-1} - 1)$ but it does not divide $n^{p-1} - 1$. Therefore $v_p(\omega) = v_p(p(n^{p-1} - 1))$. Since $v_p(\omega) \leq v_p(p(r^{p-1} - 1))$, this proves that (2.3) is satisfied, as required.

To prove (2.6), assume that (2.3) holds. We can write $(r^{p-1} - 1)/(n^{p-1} - 1) = a/b$ with $a, b \in \mathbb{Z}_{>0}$, $b \not\equiv 0 \bmod p$, and we can even achieve that $b \equiv 1 \bmod p$. Then $\ell_p(r) = (a \bmod p)$, and by (2.10) and (2.11) we now have

$$\chi(r) = \chi(r)^b \equiv \tau(\chi)^{b(r^{p-1}-1)} = \tau(\chi)^{a(n^{p-1}-1)} \equiv \eta(\chi)^a = \eta(\chi)^{\ell_p(r)} \mod rR,$$

and therefore

$$\chi(r) = \eta(\chi)^{\ell_p(r)}.$$

This we proved for *prime* $r|n$. Using (2.4) we see that the same equality holds for arbitrary $r|n$. With $r = n$ we find, by (2.5), that $\chi(n) = \eta(\chi)$. This proves (2.6).

§ 3. A result from analytic prime number theory

Pomerance and Odlyzko have shown that there exists an effectively computable constant c_2 such that for every integer $n > e^e$ there exists $t \in \mathbb{Z}_{>0}$ satisfying the following conditions:

$$t \text{ is squarefree,} \tag{3.1}$$

$$t < (\log n)^{c_2 \cdot \log\log\log n}, \tag{3.2}$$

$$s > n^{1/2} \quad \text{for} \quad s = \prod_{q \text{ prime},\ q-1 | t} q. \tag{3.3}$$

The proof employs an idea due to Prachar [10] and is given in [2]. It does not yield an actual construction of t. In particular, Adleman's conjecture that one can take

$t = \Pi_{p \text{ prime},\ p \le x} p$ for some x remains unproved. See [1, 2] for the heuristic argument and the numerical evidence supporting this conjecture. If we take $x = 19$ then (3.3) is true for $n \le 10^{350}$.

The result of Pomerance and Odlyzko is best possible in the sense that there exists a positive constant c_3 such that $t > (\log n)^{c_3 \cdot \mathrm{loglog} \log n}$ for any positive integer t satisfying (3.3), cf. [2].

§ 4. A probabilistic primality test

The test runs as follows. Find a positive integer t satisfying (3.1) and (3.3), e.g. by trying $t = 1, 2, 3, \ldots$ in succession. Let s be as in (3.3). Check that n is not divisible by any prime dividing s or t. For each pair of primes p, q with $p \mid q - 1$ and $q \mid s$ (so $p \mid t$), select a character χ of order p and conductor q, and verify (2.2) for this χ. Next, prove that each prime p dividing t satisfies (2.3). Usually, for each p there will be at least one χ for which $\eta(\chi) \neq 1$, and then (2.7) suffices to prove (2.3). If this is not the case, and (2.8) does not apply either, test (2.2) for characters χ of order p having other conductors, until an example of $\eta(\chi) \neq 1$ is found. If (2.3) is proved for all primes p dividing t, determine $r_i \in \mathbb{Z}$ by

$$n^i \equiv r_i \bmod s, \qquad 0 \le r_i < s$$

for $i = 0, 1, \ldots, t-1$, and check that none of the r_i is a non-trivial divisor of n. If n passes all these tests, declare n to be prime. This finishes the description of the algorithm.

To justify the algorithm, assume that n passes all tests but is not a prime number. Let r be a non-trivial divisor of n satisfying $r \le n^{\frac{1}{2}}$. Define ℓ, using the Chinese remainder theorem, by

$$\ell \in \{0, 1, \ldots, t-1\},$$
$$\ell \equiv \ell_p(r) \bmod p \qquad \text{for any prime } p \mid t,$$

with $\ell_p(r)$ as in section 2. By (2.6), we have $\chi(r) = \chi(n^\ell)$ for all characters χ that have been tested. Since these characters generate the group of all characters of the group $(\mathbb{Z}/s\mathbb{Z})^* \cong \oplus_{q \mid s \text{ prime}} \mathbb{F}_q^*$, it follows that $r \equiv n^\ell \equiv r_\ell \bmod s$. From $0 \le r \le n^{\frac{1}{2}} < s$ and $0 \le r_\ell < s$ it now follows that $r = r_\ell$, so r_ℓ is a non-trivial divisor of n. This is a contradiction.

The only non-deterministic part of the algorithm is the verification of condition (2.3). This verification may, for n prime, in the worst case be very time consuming; and if n is composite this part of the algorithm need not even terminate, since it is conceivable that (2.3) is not satisfied. If certain generalized Riemann hypotheses are admitted, this non-deterministic aspect can be removed in the same way as was done for the Solovay-Strassen test in the introduction. Another solution, not using unproved hypotheses, is given in section 5.

The analysis of the running time is straightforward if we apply the result of section 3. One finds that, for any ε with $0 < \varepsilon < 1$, the algorithm terminates with probability $\geq 1 - \varepsilon$ in time $\leq |\log \varepsilon| \cdot (\log n)^{c_4 \cdot \log\log\log n}$ for all prime $n > e^e$; here c_4 denotes an absolute, effectively computable constant.

We note an improvement of practical interest. Put $h(p) = v_p(n^{p-1} - 1)$ and $s' = s \cdot \prod p^{h(p)}$, the product ranging over all primes p dividing $\gcd(s, t)$. Then condition (3.3) can be weakened to $s' > n^{\frac{1}{2}}$, and s can be replaced by s' in the algorithm. The justification of this employs that by the definition of $\ell_p(r)$ we have $\chi(r) = \chi(n)^{\ell_p(r)}$ for every $r|n$ and every character χ of p-power order and conductor dividing $p^{h(p)+1}$.

§ 5. A deterministic primality test

First, let p, q, R, χ and $\tau(\chi)$ be as in section 2. We replace the test (2.2) by a somewhat more complicated set of conditions.

Write $n^{p-1} - 1 = p^h \cdot u$ with $u \not\equiv 0 \bmod p$. We consider the sequence

$$\tau(\chi)^{pu},\ \tau(\chi)^{p^2 u},\ \ldots,\ \tau(\chi)^{p^h u}$$

modulo nR. Notice that these elements belong to the subring $\mathbb{Z}[\zeta_p]$ of R. Our first condition is just (2.10):

(5.1) $$\tau(\chi)^{p^h u} \equiv \eta(\chi) \bmod nR \quad \text{for some } \eta(\chi) \in \langle\zeta_p\rangle.$$

We know that (5.1) is satisfied if n is prime, with $\eta(\chi) = \chi(n)$.

Assume that (5.1) holds, and let $w(\chi)$ be the smallest integer $i \in \{1, 2, \ldots, h\}$ with the property that $\tau(\chi)^{p^i u}$ is congruent to an element of $\langle\zeta_p\rangle$ modulo nR. Our second condition is:

(5.2) if $w(\chi) \geq 2$ and $\tau(\chi)^{p^{w(\chi)} u} \equiv 1 \bmod nR$, then for each $j \in \{0, 1, \ldots, p-1\}$ the element $\tau(\chi)^{p^{w(\chi)-1} u} - \zeta_p^j$ of $\mathbb{Z}[\zeta_p]$ has, when expressed on the basis $1, \zeta_p, \ldots, \zeta_p^{p-2}$ of $\mathbb{Z}[\zeta_p]$ over $\mathbb{Z}$, a coefficient that is coprime with n.

By definition of $w(\chi)$, each $\tau(\chi)^{p^{w(\chi)-1} u} - \zeta_p^j$ has a coefficient $\not\equiv 0 \bmod n$, so by a gcd-calculation we can check (5.2), or else find a non-trivial divisor of n.

(5.3) Proposition. *If* (5.1) *and* (5.2) *are satisfied, then* $r^{p-1} \equiv 1 \bmod p^{w(\chi)}$ *for every prime* $r|n$.

Proof. This is trivial if $w(\chi) = 1$. If $\tau(\chi)^{p^{w(\chi)} u} \not\equiv 1 \bmod nR$ we can imitate the proof of (2.7), with $n^{p-1} - 1$ replaced by $p^{w(\chi)} u$. So assume that $w(\chi) \geq 2$ and that $\tau(\chi)^{p^{w(\chi)} u} \equiv 1 \bmod nR$. Suppose that $r^{p-1} \not\equiv 1 \bmod p^{w(\chi)}$. Then we can write $p^{w(\chi)-1} u / (r^{p-1} - 1) = a/b$ with $a, b \in \mathbb{Z}_{>0}$, $b \equiv 1 \bmod p$. Combining $\tau(\chi)^{p^{w(\chi)} u} \equiv 1 \bmod rR$ with (2.11) we find that

$$\tau(\chi)^{p^{w(\chi)-1}u} \equiv \tau(\chi)^{p^{w(\chi)-1}ub} = \tau(\chi)^{(r^{p-1}-1)a} \equiv \chi(r)^a = \zeta_p^j \mod rR$$

for some $j \in \{0, 1, \ldots, p-1\}$. Hence all coefficients of $\tau(\chi)^{p^{w(\chi)-1}u} - \zeta_p^j$ are divisible by r, in contradiction with (5.2). This proves (5.3).

Assume (5.1), and let an integer w be fixed for which $w(\chi) \le w \le h$ and $r^{p-1} \equiv 1 \mod p^w$ for each prime $r|n$. Put

$$\ell_p'(r) = ((r^{p-1} - 1)/(p^w u) \mod p) \in \mathbb{Z}_p/p\mathbb{Z}_p = \mathbb{Z}/p\mathbb{Z}$$

for each $r|n$, and let $\eta'(\chi) \in \langle\zeta_p\rangle$ be determined by $\tau(\chi)^{p^w u} \equiv \eta'(\chi) \mod nR$.

(5.4) Proposition. *With these hypotheses and notations, we have*

$$\chi(r) = \eta'(\chi)^{\ell_p'(r)}$$

for each $r|n$, *and* $\chi(n) = \eta(\chi)$.

The proof is almost identical to the proof of (2.6), and it is left to the reader.

After these preparations we present the deterministic primality test. Choose t, s as in section 4, check that $\gcd(st, n) = 1$, and select a character χ of order p and conductor q for each pair of primes p, q with $p|q-1$ and $q|s$. Verify (5.1) and determine $w(\chi)$ for each χ. Next, for each prime $p|t$, do the following. Put $w = \max w(\chi)$, the maximum being taken over all characters χ of order p that have been selected (if there are none, disregard p). Test (5.2) for a single χ of order p with $w = w(\chi)$. This being done for each p, calculate all $\eta'(\chi)$; these are well-defined, since w satisfies the above hypotheses. By a repeated application of the Chinese remainder theorem, determine the unique residue class $(\nu \mod s)$ for which $\chi(\nu) = \eta'(\chi)$ for all χ's. Let $r_i \in \mathbb{Z}$ satisfy

$$\nu^i \equiv r_i \mod s, \qquad 0 \le r_i < s$$

for $i = 0, 1, \ldots, t-1$, and check that none of the r_i is a non-trivial divisor of n. If n passes all these tests, declare n to be prime. This finishes the description of the algorithm.

The correctness of the algorithm is proved as in section 4, with (2.6) replaced by (5.4). The running time is bounded by $(\log n)^{c_5 \cdot \mathrm{loglog} n}$ for all $n > e^e$, with c_5 denoting an absolute, effectively computable constant.

§ 6. Jacobi sums

Let p, q, R, χ and $\tau(\chi)$ be as in section 2. In this section we shall see that condition (2.2) can be replaced by a condition that refers only to elements of the subring $\mathbb{Z}[\zeta_p]$ of R.

Denote by Δ the Galois group of $\mathbb{Q}(\zeta_p)$ over $\mathbb{Q}$ and by $\mathbb{Z}[\Delta]$ its group ring over $\mathbb{Z}$. We have $\mathbb{F}_p^* \cong \Delta$, under an isomorphism sending $(j \mod p)$ to σ_j, where $\sigma_j(\zeta_p) = \zeta_p^j$. We let Δ act on $\mathbb{Q}(\zeta_p, \zeta_q)$ by $\sigma_j(\zeta_q) = \zeta_q$ for all j. The action of Δ induces natural $\mathbb{Z}[\Delta]$-module structures on the multiplicative groups

$\mathbb{Q}(\zeta_p, \zeta_q)^*$, $\mathbb{Q}(\zeta_p)^*$, $(R/nR)^*$, $(\mathbb{Z}[\zeta_p]/n\mathbb{Z}[\zeta_p])^*$; so for x in any of these groups and $\alpha \in \mathbb{Z}[\Delta]$ we can meaningfully speak of x^α.

Define the ring homomorphism $\psi\colon \mathbb{Z}[\Delta] \to \mathbb{F}_p$ by $\psi(\sigma_j) = (j \bmod p)$, and let p be the kernel of ψ. This is a prime ideal of $\mathbb{Z}[\Delta]$ with $p \in p$, and it is generated by $\{\sigma_j - j\colon\ j \in \mathbb{Z} - p\mathbb{Z}\}$. It is the annihilator of the $\mathbb{Z}[\Delta]$-module $<\zeta_p>$.

Fix an element π of p. Checking the action of the Galois group of $\mathbb{Q}(\zeta_p, \zeta_q)$ over $\mathbb{Q}(\zeta_p)$ we find that $\tau(\chi)^\pi \in \mathbb{Q}(\zeta_p)^*$ and, similarly, that

$$\upsilon(\chi) = (\tau(\chi) \bmod nR)^\pi$$

belongs to the subgroup $(\mathbb{Z}[\zeta_p]/n\mathbb{Z}[\zeta_p])^*$ of $(R/nR)^*$. We attempt to replace (2.2) by a condition on $\upsilon(\chi)$ rather than $\tau(\chi)$.

Using the $\mathbb{Z}[\Delta]$-module structure we can formulate (2.2) as

(6.1) $$(\tau(\chi) \bmod nR)^{n-\sigma_n} = (\eta(\chi)^{-n} \bmod nR) \qquad \text{for some } \eta(\chi) \in <\zeta_p>.$$

Suppose now that $\alpha, \beta \in \mathbb{Z}[\Delta]$ satisfy

(6.2) $$\alpha\pi = \beta(n - \sigma_n), \qquad \beta \notin p.$$

Then we find, by raising (6.1) to the power β:

(6.3) $$\upsilon(\chi)^\alpha = (\eta(\chi)^{-n\psi(\beta)} \bmod n\mathbb{Z}[\zeta_p]) \qquad \text{for some } \eta(\chi) \in <\zeta_p>.$$

(6.4) Proposition. *Propositions* (2.6) *and* (2.7) *remain true with* (2.2) *replaced by* (6.3), *where* $\alpha, \beta \in \mathbb{Z}[\Delta]$ *satisfy* (6.2).

The proof employs that (2.2) is at least true when raised to the power β, where $\psi(\beta) \neq (0 \bmod p)$, and is otherwise similar to the proof given in section 2. It is left to the reader.

Elements α, β as in (6.2) exist if and only if $n - \sigma_n$ belongs to the ideal generated by π in the local ring $\mathbb{Z}[\Delta]_p$. Using standard techniques from commutative algebra one shows that this local ring is a discrete valuation ring with completion isomorphic to $\mathbb{Z}_p$, the corresponding map $\mathbb{Z}[\Delta] \to \mathbb{Z}_p$ being given by $\sigma_j \mapsto \lim_{m\to\infty} j^{p^m}$. Hence α, β certainly exist if

(6.5) π maps to a *generator* of the ideal $p\mathbb{Z}_p$.

If the ring homomorphism $\psi'\colon \mathbb{Z}[\Delta] \to \mathbb{Z}/p^2\mathbb{Z}$ is defined by $\psi'(\sigma_j) = (j^p \bmod p^2)$, then (6.5) is equivalent to

(6.6) $$\psi(\pi) = (0 \bmod p), \qquad \psi'(\pi) \neq (0 \bmod p^2).$$

(6.7) Example: $\pi = p$. In this case we can take

$$\beta = \Sigma_{j=1}^{p-1}\ j\sigma_j^{-1} \qquad (\text{with } \psi(\beta) = (-1 \bmod p)),$$

$$\alpha = \Sigma_{j=1}^{p-1} \left[\frac{nj}{p}\right]\sigma_j^{-1}$$

where $[x]$ denotes the greatest integer $\leq x$. If $p = 2$ then $\upsilon(\chi) = (\tau(\chi)^2 \bmod nR)$ is simply given by $\upsilon(\chi) = (\chi(-1)q \bmod nR)$, cf. (2.9).

(6.8) Example: $\pi = \sigma_a + \sigma_b - \sigma_{a+b}$ where $a, b \in \mathbb{Z}$ satisfy $ab(a + b) \not\equiv 0 \bmod p$

(so $p = 2$ is excluded) and $a^p + b^p \not\equiv (a + b)^p \bmod p^2$ (cf. (6.6)); e.g., $a = b = 1$ for $p < 6 \cdot 10^9$, $p \notin \{1093, 3511\}$. In this case we can take

$$\beta = \Sigma_{j=1}^{p-1} \left(\left[\frac{(a+b)j}{p} \right] - \left[\frac{aj}{p} \right] - \left[\frac{bj}{p} \right] \right) \sigma_j^{-1},$$

$$\alpha = \Sigma_{j=1}^{p-1} \left[\frac{nj}{p} \right] \sigma_j^{-1},$$

where $\psi(\beta) \not\equiv (0 \bmod p)$ is a consequence of $\pi \cdot \Sigma_{j=1}^{p-1} j\sigma_j^{-1} = p\beta$. By [7, Ch. I, § 1], the element $\upsilon(\chi)$ is given by the *Jacobi sum*

$$\upsilon(\chi) = (-\Sigma_{x \in \mathbb{F}_q - \{0, 1\}} \chi(x)^a \chi(1 - x)^b \bmod n\mathbb{Z}[\zeta_p]).$$

This element can be calculated within the ring $\mathbb{Z}[\zeta_p]$.

(6.9) Remark. It is an interesting problem to find a method for the calculation of $\upsilon(\chi)$ that is more efficient than directly using its definition or, in a special case, the formula given in (6.8). For $p = 2$ this is trivial. In the general case, it might be possible to use the arithmetical characterization of Gaussian sums for this purpose [7, Ch. I]. This can certainly be done for $p \leq 11$, employing the Euclidean algorithm in $\mathbb{Z}[\zeta_p]$ (cf. [8]); here we assume that an $x \in \mathbb{F}_q^*$ is known with $\chi(x) \neq 1$.

§ 7. Characters of prime power order

In this section we generalize the results of the preceding sections by indicating how characters of prime power order can be used. The proofs are slightly more involved than those given earlier, and they are omitted.

We start with two prime numbers p and q not dividing n, and an integer $k \geq 1$ with $p^k | q - 1$. Put $R = \mathbb{Z}[\zeta_{p^k}, \zeta_q]$, and let $\chi: \mathbb{F}_q^* \to R^*$ be a character of order p^k and conductor q. The Gaussian sum $\tau(\chi) = -\Sigma_{x=1}^{q-1} \chi(x)\zeta_q^x \in R$ again satisfies (2.1). We consider the analogue of (2.2):

(7.1) $\qquad \tau(\chi)^n \equiv \eta(\chi)^{-n} \cdot \tau(\chi^n) \bmod nR \quad$ for some $\eta(\chi) \in \langle \zeta_{p^k} \rangle$.

(7.2) Condition on p. *For every prime* $r | n$ *there exists* $\ell_p(r) \in \mathbb{Z}_p$ *such that* $r^{p-1} = (n^{p-1})^{\ell_p(r)}$ *in the group* $1 + p\mathbb{Z}_p$.

This condition is equivalent to (2.3) for $p > 2$, and if $n \equiv 1 \bmod 4$ also for $p = 2$. Defining $\ell_p(r) \in \mathbb{Z}_p$ for every $r | n$ by $r^{p-1} = (n^{p-1})^{\ell_p(r)}$ we now have the following analogues of (2.6) and (2.7).

(7.3) Proposition. *Suppose that* (7.1) *and* (7.2) *are true. Then* $\eta(\chi) = \chi(n)$, *and* $\chi(r) = \chi(n)^{\ell_p(r)}$ *for every* $r | n$.

(7.4) Proposition. *Suppose that* (7.1) *is satisfied, with* $\eta(\chi)$ *a primitive* p^k*-th root of unity, and that one of* (a), (b), (c) *holds:*

(a) p *is odd;*

(b) $p = 2$, $k = 1$ *and* $n \equiv 1 \bmod 4$;

(c) $p = 2$, $k > 1$ *and* $\tau(\chi^{2^{k-1}})^{n-1} \equiv -1 \bmod nR$.

Then (7.2) *is satisfied.*

If $p = 2$ and $n \equiv 3 \bmod 8$ then (7.2) is satisfied if $2^{(n-1)/2} \equiv -1 \bmod n$. A further way of verifying (7.2) is given in (8.6).

Using (7.1), (7.2), (7.3) and (7.4) instead of (2.2), (2.3), (2.6) and (2.7) in section 4 we obtain a probabilistic primality test in which the restriction (3.1) that t be squarefree can be removed. This is an improvement of practical interest. As far as the running time is concerned, the improvement affects at most the constant in the exponent (cf. the final paragraph of section 3). As in the final paragraph of section 4, we can replace s by $s' = s \cdot \prod_{p \text{ prime},\, p \mid \gcd(s,t)} p^{m(p)}$, where $m(p) = v_p(n^t - 1) - 1$.

The results of section 6, which are important for practical purposes, have been generalized to the present situation by H. Cohen. For $p \neq 2$ he finds formulae similar to those in (6.8), but the case $p = 2$ is rather more delicate. The conclusion is that all calculations can be performed in the ring $\mathbb{Z}[\zeta_{p^k}]/n\mathbb{Z}[\zeta_{p^k}]$.

The generalization of the deterministic test from section 5 takes the following shape. Let p, k, q, R, χ, $\tau(\chi)$ be as above, and denote by G the Galois group of $\mathbb{Q}(\zeta_{p^k})$ over $\mathbb{Q}$. For $j \in \mathbb{Z}_p^*$ let σ_j be the element of G with $\sigma_j(\zeta_{p^k}) = \zeta_{p^k}^j$. We let G act on R by $\sigma_j(\zeta_q) = \zeta_q$ for all j. Choose $u \in \mathbb{Z} - p\mathbb{Z}$ such that $p^m u \in \mathbb{Z}[G] \cdot (n - \sigma_n)$ for some $m \in \mathbb{Z}_{>0}$; e.g., take for u the largest divisor of $n^{(p-1)p^{k-1}} - 1$ that is not divisible by p. Define $\lambda(\chi) = (\tau(\chi) \bmod nR)^u$, and assume that (7.1) is satisfied. Then $\lambda(\chi)$ belongs to the p-primary part of $(R/nR)^*$. This p-primary part may be considered as a module over $\mathbb{Z}_p[G]$. Let H_χ be the set of all $a \in \mathbb{Z}_p^*$ for which there exists $\eta(\chi, a) \in \langle \zeta_{p^k} \rangle$ such that

$$\lambda(\chi)^{1 - (a/\sigma_a)} = (\eta(\chi, a)^u \bmod nR);$$

e.g., $n \in H_\chi$, with $\eta(\chi, n) = \eta(\chi)$. It is easily checked that H_χ is a *subgroup* of $\mathbb{Z}_p^*$, and that the map $\hat{\chi}: H_\chi \to \langle \zeta_{p^k} \rangle$, $\hat{\chi}(a) = \eta(\chi, a)$, is a group homomorphism. Consider, for $a \in \mathbb{Z}_p^* - H_\chi$, the following condition:

(7.5) for each $j \in \{0, 1, \ldots, p^k - 1\}$ the coefficients of the element $\lambda(\chi)^{1 - (a/\sigma_a)} - \zeta_{p^k}^j$ of $\mathbb{Z}[\zeta_{p^k}]/n\mathbb{Z}[\zeta_{p^k}]$, when expressed on a basis over $\mathbb{Z}/n\mathbb{Z}$, generate the unit ideal of $\mathbb{Z}/n\mathbb{Z}$.

Given a it is easy to check this condition or else to find a non-trivial divisor of n, cf. (5.2).

We shall only be interested in the pro-p-primary subgroup $J_\chi = H_\chi \cap (1 + p\mathbb{Z}_p)$ of H_χ.

(7.6) Proposition. *Let* χ *satisfy* (7.1), *and suppose that every subgroup* $J \subset 1 + p\mathbb{Z}_p$ *with* $J_\chi \subset J$ *and* $\text{index}[J : J_\chi] = p$ *contains an element* a *satisfying*

(7.5). *Then for every* $r|n$ *we have*

$$r^{p-1} \in J_\chi, \qquad \chi(r^{p-1}) = \hat{\chi}(r^{p-1}).$$

Note that at most three subgroups J have to be considered, and at most one if $p > 2$.

The deterministic test based on (7.6) runs as follows. Let s, t be as in (3.3) and check that $\gcd(st, n) = 1$. For each pair of primes p, q with $p|q-1$ and $q|s$ select a character χ of order p^k and conductor q, where $k = v_p(q-1)$. Test (7.1) and determine J_χ for each χ. Next, for each prime $p|t$, do the following. Put $J_p = \cap_\chi J_\chi$, the intersection being taken over all characters χ of p-power order that have been selected. Test (7.5) for a few pairs (a, χ), selected in such a way that by (7.6) we know that $r^{p-1} \in J_p$ for each $r|n$. If $-1 \in J_p$ (so $p = 2$), choose $\gamma_p \in J_p$ such that $J_p = \gamma_p^{\mathbb{Z}_p} \cup (-\gamma_p^{\mathbb{Z}_p})$. Otherwise, choose $\gamma_p \in J_p$ such that $J_p = \gamma_p^{\mathbb{Z}_p}$. This being done for each p, determine the unique residue class $(\nu \bmod s)$ with $\chi(\nu) = \hat{\chi}(\gamma_p)$ for all χ's. Let $\nu^i \equiv r_i \bmod s$, with $0 \le r_i < s$, for $i = 0, 1, \ldots, t-1$, and check that none of the r_i is a non-trivial divisor of n. If $-1 \in J_2$, determine $(\mu \bmod s)$ by

$$\chi(\mu) = \hat{\chi}(-1) \quad \text{if } \chi \text{ has 2-power order,}$$
$$\chi(\mu) = 1 \quad \text{for the other } \chi\text{'s,}$$

define r_i' by $\mu\nu^i \equiv r_i' \bmod s$, $0 \le r_i' < s$, for $i = 0, 1, \ldots, t-1$, and check that none of the r_i' is a non-trivial divisor of n. If n passes all these tests, it is a prime number.

§ 8. Galois theory tests

The probabilistic primality tests discussed in sections 4 and 7 attempt to show that n is prime by proving that any divisor r of n is a *power* of n, in various senses: in the group $1 + p\mathbb{Z}_p$, as in (7.2); in the group of values of a character χ, as in (7.3); and in the group $(\mathbb{Z}/s\mathbb{Z})^*$, as in section 4. It turns out that several older primality tests can be formulated in a similar way. This applies in particular to the tests employed by Williams that depend on Lucas functions and generalizations thereof, see [13] for references. In this section we give an account of these methods from the present point of view, and we discuss how they are related to Adleman's tests. We use the language of finite rings rather than that of Lucas functions. By "ring" we shall mean "commutative ring with 1", and subrings are supposed to have the same unit element.

(8.1) Theorem. *Let* $s \in \mathbb{Z}_{>0}$. *Let* A *be a ring containing* $\mathbb{Z}/n\mathbb{Z}$ *as a subring. Suppose that there exists* $\alpha \in A$ *satisfying the following conditions:*

$$\alpha^s = 1,$$
$$\alpha^{s/q} - 1 \in A^* \quad \text{for every prime } q|s,$$

the polynomial $\prod_{i=0}^{t-1} (X - \alpha^{n^i})$ *has coefficients in* $\mathbb{Z}/n\mathbb{Z}$ *for some* $t \in \mathbb{Z}_{>0}$.

Then every divisor r *of* n *is congruent to a power of* n *modulo* s.

Proof. We may assume that r is *prime*. Since r is a zero-divisor (or zero) in A, there exists a maximal ideal $m \subset A$ with $r \in m$. Let $\bar{A}$ be the field A/m, and $\bar{\alpha} = (\alpha \bmod m) \in \bar{A}$. The first two conditions on α imply that $\bar{\alpha}$ has order s in $\bar{A}^*$. The polynomial $\prod_{i=0}^{t-1} (X - \bar{\alpha}^{n^i})$, which has $\bar{\alpha}$ as a zero, has coefficients in the prime field $\mathbb{F}_r$ of $\bar{A}$. Therefore $\bar{\alpha}^r$ is also a zero of this polynomial, so there exists $i \in \{0, 1, \ldots, t-1\}$ with $\bar{\alpha}^r = \bar{\alpha}^{n^i}$, i. e. $r \equiv n^i \bmod s$. This proves (8.1).

(8.2) To obtain a primality test one applies (8.1) to a ring A that, if n were prime, would be the field $\mathbb{F}_{n^t}$, where t is some positive integer. For s one takes the largest divisor of $n^t - 1$ that one is able to decompose into prime factors. One chooses α to be an element of A^* of order s. If n is actually prime, then such an α is in practice easy to construct by manipulating with elements of the form $\beta^{(n^t-1)/s}$, $\beta \in A^*$, and it satisfies the conditions of (8.1). Conversely, these conditions imply that any $r|n$ is modulo s congruent to a power of n, so if $s > n^{\frac{1}{2}}$ we can check whether n is prime as in the algorithm of section 4.

Classical tests are obtained for small values of t. The test with $t = 1$ and $A = \mathbb{Z}/n\mathbb{Z}$ yields the result that every $r|n$ is $1 \bmod s$, where s is the completely factored part of $n - 1$; so n is prime if $s > n^{\frac{1}{2}}$. For $t = 2$ and n odd one can take $A = (\mathbb{Z}/n\mathbb{Z})[X]/(X^2 - uX + v)$, where $u, v \in \mathbb{Z}/n\mathbb{Z}$ are such that $\left(\frac{d}{n}\right) = -1$ for $d = u^2 - 4v$. In the resulting test, which is usually formulated in terms of Lucas sequences, we can use known prime factors of $n + 1$ in addition to those of $n - 1$. If $n = 2^m - 1$ is a Mersenne number then $n + 1$ is easy to factorize, and in this case (8.1) leads to the well-known Lucas-Lehmer test for Mersenne numbers [13, p. 152].

Two important features of the tests described in [13] are not shared by the test described above. The first is the possibility to employ lower bounds for the unknown prime divisors of $n^t - 1$. Further research is required to find out whether these are equally useful for the larger values of t that we shall be interested in. The second is the possibility to combine the information gained by considering several different values of α and even of t. In order to incorporate this feature into our test we endow A with extra structure.

Let A be a ring containing $\mathbb{Z}/n\mathbb{Z}$ as a subring, and let $\langle\sigma\rangle$ be a cyclic group of ring automorphisms of A, with generator σ. We say that A is a *Galois extension of* $\mathbb{Z}/n\mathbb{Z}$ *with group* $\langle\sigma\rangle$ if there exist $t \in \mathbb{Z}_{>0}$ and $z_1, z_2, \ldots, z_t \in A$ such that

$$\sigma^t = \mathrm{id}_A, \qquad \det\bigl(\sigma^i(z_j)\bigr)_{1\le i,j\le t} \in A^*,$$
$$z_1, z_2, \ldots, z_t \text{ is a basis of } A \text{ over } \mathbb{Z}/n\mathbb{Z}$$

(so $\#A = n^t$). We call t the *rank* of the extension. If A is a Galois extension of $\mathbb{Z}/n\mathbb{Z}$ with group $\langle\sigma\rangle$ then $\mathbb{Z}/n\mathbb{Z} = \{x \in A: \sigma(x) = x\}$, by [4, Ch. III, prop. 1.2].

(8.3) Lemma. *Let n be prime, and let A be a Galois extension of $\mathbb{F}_n$ with group $\langle\sigma\rangle$. Then any ring homomorphism $\tau: A \to A$ with $\tau(1) = 1$ and $\tau\sigma = \sigma\tau$ belongs to $\langle\sigma\rangle$.*

Proof. Let t be the rank. By [3, theorem 3.1] (applied to $f = \mathrm{id}_A$, $g = \tau$) there is a unique system $(e_j)_{j=0}^{t-1}$ of pairwise orthogonal idempotents of A such that $\sum_{j=0}^{t-1} e_j = 1$ and $\tau(x) = \sum_{j=0}^{t-1} \sigma^j(x)e_j$ for all $x \in A$. The uniqueness and the fact that $\sigma\tau\sigma^{-1} = \tau$ imply that $\sigma(e_j) = e_j$, so $e_j \in \mathbb{F}_n$, for $0 \le j < t$. Since $\mathbb{F}_n$ has no non-trivial idempotents it follows that $e_i = 1$ for some i and $e_j = 0$ for all $j \ne i$. Hence $\tau = \sigma^i$, as required.

Alternatively, we can use Grothendieck's theory of étale coverings to reduce (8.3) to the following easily proven fact: if G is an abelian transitive permutation group of a set X, then any map $X \to X$ commuting with all elements of G belongs to G.

If $z_1, z_2, \ldots, z_t$ is a basis of A over $\mathbb{Z}/n\mathbb{Z}$ then an element $x = \sum_{i=1}^t a_i z_i$ of A, with $a_i \in \mathbb{Z}/n\mathbb{Z}$, is called *primitive* if $a_1, a_2, \ldots, a_t$ generate the unit ideal in $\mathbb{Z}/n\mathbb{Z}$.

(8.4) Theorem. *Let $s \in \mathbb{Z}_{>0}$, and let A be a Galois extension of rank t of $\mathbb{Z}/n\mathbb{Z}$ with group $\langle\sigma\rangle$. Suppose that for every prime $q|s$ there exists $\alpha \in A$ with the following properties:*

$$\alpha^{q^{m(q)}} = 1 \quad \text{where } m(q) = v_q(s),$$
$$\alpha^{q^{m(q)-1}} - 1 \quad \text{is primitive,}$$
$$\sigma(\alpha) = \alpha^n.$$

Then $n^t \equiv 1 \bmod s$, and for every $r|n$ we have $(r \bmod s) \in \langle n \bmod s\rangle$ in the group $(\mathbb{Z}/s\mathbb{Z})^*$.

Proof. For each prime $q|s$ the corresponding α has order $q^{m(q)}$ in A^*, and $\alpha = \sigma^t(\alpha) = \alpha^{n^t}$, so $n^t \equiv 1 \bmod q^{m(q)}$. Therefore $n^t \equiv 1 \bmod s$. Let now $r|n$ be prime. Then $\bar{A} = A/rA$ is a Galois extension of $\mathbb{F}_r$ with group $\langle\bar{\sigma}\rangle$, where $\bar{\sigma}$ is induced by σ. The map $\tau: \bar{A} \to \bar{A}$, $\tau(x) = x^r$, is a ring homomorphism with $\tau(1) = 1$ and $\tau\bar{\sigma} = \bar{\sigma}\tau$, so (8.3) implies that $\tau = \bar{\sigma}^i$ for some i. We prove that $r \equiv n^i \bmod s$. Let $q|s$ be prime, and α as in the theorem. Then $\bar{\alpha} = (\alpha \bmod rA)$ has order $q^{m(q)}$ in $\bar{A}^*$, and $\bar{\alpha}^r = \tau(\bar{\alpha}) = \bar{\sigma}^i(\bar{\alpha}) = \bar{\alpha}^{n^i}$, so $r \equiv n^i \bmod q^{m(q)}$. This proves (8.4).

(8.5) The following method to construct Galois extensions is useful for primality testing. Take $A = (\mathbb{Z}/n\mathbb{Z})[X]/(f)$, where $f \in (\mathbb{Z}/n\mathbb{Z})[X]$ has a unit discriminant and is such that

$$f(Y) = \prod_{i=0}^{t-1} (Y - \xi^{n^i}) \qquad \text{in } A[Y]$$

where $t = \text{degree}(f)$ and $\xi = (X \bmod (f)) \in A$. This is a Galois extension of $\mathbb{Z}/n\mathbb{Z}$ with group $\langle\sigma\rangle$, where $\sigma(\xi) = \xi^n$. If n is actually prime then such an f is in practice not difficult to find.

Another construction method for Galois extensions consists of taking tensor products, over $\mathbb{Z}/n\mathbb{Z}$, of Galois extensions of coprime ranks. This method makes it possible to combine information coming from different rings A.

The use of (8.4) for primality testing is analogous to the use of (8.1). One of the main difficulties is to find a relatively small $t \in \mathbb{Z}_{>0}$ and a completely factorized divisor s of $n^t - 1$ for which $s > n^{\frac{1}{2}}$. If $s = \prod_{q \text{ prime},\, q-1 \mid t} q$ then by Fermat's theorem s divides $n^t - 1$ (unless $\gcd(n, s) > 1$), so the result of section 3 shows that a suitable t can be found with $t < (\log n)^{c_2 \cdot \log\log\log n}$. This leads to a probabilistic primality test whose speed is comparable to that of the previously discussed probabilistic tests (sections 4 and 7).

It is an advantage of the new test over the previous ones that known primes $q \mid n^t - 1$ for which $q - 1$ does *not* divide t can also be used; but Pomerance writes me that not too much gain should be expected from this. On the other hand, the previous tests have the advantage that the necessary calculations can be performed in rings whose ranks over $\mathbb{Z}/n\mathbb{Z}$ are much smaller than t.

It is a natural question to ask to which extent both types of tests can be combined. Using Adleman's tests together with the special case $A = \mathbb{Z}/n\mathbb{Z}$ of (8.4) one obtains a test in which the number that should exceed $n^{\frac{1}{2}}$ is the least common multiple of $\prod_{q \text{ prime},\, q-1 \mid t} q$ and the completely factored part of $n - 1$. The following theorem is an example of a result that applies more generally.

(8.6) Theorem. *Let all hypotheses of* (8.4) *be satisfied. Let* $p \mid t$ *be prime, and assume that* $v_p(s) = v_p(n^t - 1) > 0$. *Then* p *satisfies condition* (7.2), *and if* $r \mid n$, $r \equiv n^i \bmod s$, *then* $i \equiv \ell_p(r) \bmod t\mathbb{Z}_p$, *where* $\ell_p(r)$ *is as in section* 7.

The proof is an easy exercise in elementary number theory.

(8.7) Remark. All primality tests in this *exposé* use an auxiliary number s that is required to be greater than $n^{\frac{1}{2}}$. At the cost of some extra work in the algorithms it is possible to replace the lower bound $n^{\frac{1}{2}}$ by $n^{1/3}$. This is done by viewing a possible factorization of n modulo s^2 and applying reduction techniques for two-dimensional lattices.

REFERENCES

1. L.M. ADLEMAN, On distinguishing prime numbers from composite numbers (abstract), Proc. 21st Annual IEEE Symposium on Foundations of Computer Science (1980), 387-406.

2. L.M. ADLEMAN, C. POMERANCE, R.S. RUMELY, On distinguishing prime numbers from composite numbers, preprint.

3. S.U. CHASE, D.K. HARRISON, A. ROSENBERG, Galois theory and Galois cohomology of commutative rings, Memoirs Amer. Math. Soc. 52 (1965), 15-33.

4. F. DEMEYER, E. INGRAHAM, Separable algebras over commutative rings, Lecture Notes in Mathematics 181, Springer, Berlin 1971.

5. R.K. GUY, How to factor a number, Proc. Fifth Manitoba Conf. Numer. Math., Utilitas, Winnipeg (1975), 49-89.

6. D.E. KNUTH, The art of computer programming, vol. 2, Seminumerical algorithms, second edition, Addison-Wesley, Reading 1981.

7. S. LANG, Cyclotomic fields, Springer, Berlin 1978.

8. H.W. LENSTRA, Jr., Euclid's algorithm in cyclotomic fields, J. London Math. Soc. (2) 10 (1975), 457-465.

9. J.M. POLLARD, Theorems on factorization and primality testing, Proc. Cambridge Philos. Soc. 76 (1974), 521-528.

10. K. PRACHAR, Über die Anzahl der Teiler einer natürlichen Zahl, welche die Form $p - 1$ haben, Monatsh. Math. 59 (1955), 91-97.

11. C.P. SCHNORR, Refined analysis and improvements on some factoring algorithms, to appear in: Automata, Languages and Programming, Eighth Colloquium, Haifa 1981, Lecture Notes in Computer Science, to appear.

12. R. SOLOVAY, V. STRASSEN, A fast Monte-Carlo test for primality, SIAM J. Comput. 6 (1977), 84-85; erratum, 7 (1978), 118.

13. H.C. WILLIAMS, Primality testing on a computer, Ars Combin. 5 (1978), 127-185.

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