MATHEMATICS OF COMPUTATION
VOLUME 48, NUMBER 177
JANUARY 1987, PAGES 315–322

Very Short Primality Proofs

By Carl Pomerance*

Dedicated to Daniel Shanks on the occasion of his 70th birthday

Abstract. It is shown that every prime p has a proof of its primality of length $O(\log p)$ multiplications modulo p.

1. Introduction. In 1975, Pratt [8] showed that the prime recognition problem is in the complexity class *NP*. That is, for each prime p there is a short (polynomial time) proof that p is prime. *Finding* the short proof may well take exponential time, but at least such a short proof always exists.

Pratt's proofs (or "certificates" as they are often called) are based on the old theorem of Lucas that p is prime if and only if there is some g such that

$$(1.1)\quad g^{p-1} \equiv 1 \bmod p \quad \text{and} \quad g^{(p-1)/q} \not\equiv 1 \bmod p \quad \text{for all primes } q \mid p-1.$$

Thus the proof that p is prime also involves proofs that the various prime factors q of $p-1$ are prime, and so on. There is no combinatorial explosion, for as Pratt showed, the total number of primes involved is $O(\log p)$. Thus verifying a Pratt certificate takes $O(\log^2 p)$ modular multiplications with moduli all at most p. Measured in bit operations, Pratt's proofs thus have length $O(\log^4 p)$ or $O(\log^{3+\varepsilon} p)$ for every $\varepsilon > 0$, depending on whether one uses a naive or a fast multiplication subroutine.

For some primes p, Pratt's certificate is considerably shorter. For example, if $p = 2^{2^k} + 1$ is a Fermat number with $k \geqslant 1$, then p is prime if and only if

$$(1.2)\qquad 3^{(p-1)/2} \equiv -1 \bmod p.$$

This theorem, known as Pepin's test, gives a Pratt certificate for Fermat primes. The work in verifying (1.2) is just $2^k - 1 = [\log_2 p] - 1$ multiplications (in fact, squarings) modulo p.

However, it is not known if there are infinitely many Fermat primes—the conjecture is that there are not. Although there are probably infinitely many primes p with a Pratt certificate involving just $O(\log p)$ modular multiplications, this is also not known.

Another class of primes with very short primality proofs is the class of Mersenne primes. For q an odd prime, it is known that $p = 2^q - 1$ is prime if and only if $s_{q-1} \equiv 0 \bmod p$, where $s_1 = 4$ and, in general, $s_{k+1} \equiv s_k^2 - 2 \bmod p$. This result,

Received May 12, 1986; revised May 30, 1986.
1980 *Mathematics Subject Classification* (1985 *Revision*). Primary 11Y11, 11Y16.
* Supported in part by an NSF grant.

0025-5718/87 $1.00 + $.25 per page

known as the Lucas-Lehmer test, takes $q - 2 = [\log_2 p] - 1$ squarings modulo p and a like number of subtractions. Thus the Lucas-Lehmer test provides an $O(\log p)$ certificate for Mersenne primes p. It is conjectured that there are infinitely many Mersenne primes.

In this paper we shall show that every prime p has an $O(\log p)$ certificate. More precisely, we shall show the following result.

THEOREM 1. *For every prime p there is a proof that it is prime which requires for its verification* $(\frac{5}{2} + o(1)) \log_2 p$ *multiplications* mod p.

As with the recent Goldwasser-Kilian [4] primality test, this theorem exploits some deep results on elliptic curves over finite fields. In particular, p is shown to be prime by showing that otherwise, for any prime factor $r \leqslant \sqrt{p}$ of p, there is an elliptic curve defined over $\mathbf{Z}/r$ which has more points than allowed by the Hasse-Weil theorem. This contradiction shows that p has no prime factor $r \leqslant \sqrt{p}$ and so must be prime. This idea is common to the Goldwasser-Kilian test and to the certificate described here. However, the Goldwasser-Kilian test requires an iteration of the basic step $O(\log p)$ times, while the certificate described here need not be iterated.

Although it is conjectured that every prime has a Goldwasser-Kilian certificate, it has only been proved that most primes have such a certificate. In fact, they prove the stronger result that for most primes the certificate can be found in expected polynomial time. If it exists, a Goldwasser-Kilian certificate has length $O(\log^2 p)$ modular multiplications with moduli at most p and is thus comparable with a Pratt certificate.

Miller [6] has shown that on the assumption of the Extended Riemann Hypothesis (ERH), $p > p_0$ is prime if and only if it passes strong pseudoprime tests for each base b with $1 < b < c_0 \log^2 p$. From recent work of Bach [1] (see Review **5** in this issue of Mathematics of Computation) the constant c_0 may be chosen to be 2 and p_0 may be 13. It is not so important for our purposes what a strong pseudoprime test is, except that it takes $O(\log p)$ multiplications mod p to verify. Thus the Miller ERH-conditional certificate takes $O(\log^3 p)$ multiplications mod p to verify.

Finally, a remark should be made about lower bounds for the lengths of the above-mentioned certificates. The Miller ERH-conditional certificate is easy to examine. There is some positive constant c_1 and infinitely many primes p such that the certificate for p involves at least $c_1 \log^3 p$ multiplications mod p. For example, any prime $p \equiv 3 \bmod 4$ will do. It is conceivable that if $p - 1$ is divisible by a high power of 2, then a strong pseudoprime test for p might take as few as $O(\log \log p)$ multiplications mod p, but this is the absolute minimum. Thus for all primes p, the Miller ERH-conditional certificate is at least of length $c_2 \log^2 p \log \log p$ multiplications mod p. It is my guess that the correct universal lower bound is actually of order $\log^3 p$, but this may be difficult to prove.

For the Goldwasser-Kilian certificate, the minimal length depends on the exact protocol followed. The general iteration step involves replacing p with a prime $q \approx p/2$, but there are variations where $q \approx p/m$ and $m = O(\log^{c_3} p)$ for some c_3. If the first version is followed, the certificate is at least of length $c_4 \log^2 p$ modular multiplications with moduli at least $\sqrt{p}$. If the latter version is used, then the number of multiplications is at least $c_5 \log^2 p / \log \log p$.

We have seen that sometimes a Pratt certificate is of length $O(\log p)$ multiplications mod p and that conjecturally there are infinitely many such primes p. This is optimal—that is, for some $c_6 > 0$, a Pratt certificate is always at least of length $c_6 \log p$ multiplications mod p. It is almost certainly true that there are infinitely many primes p whose Pratt certificate is *not* of length $O(\log p)$ multiplications mod p, but I have not been able to prove this.

In view of (1.1), one possible way of showing that sometimes a Pratt certificate is fairly long is to show there are primes p for which $p - 1$ has many distinct prime factors. This is in fact not so hard. It is possible to show via Linnik's theorem in analytic number theory that there is a positive constant c_7 and infinitely many primes p for which $p - 1$ has at least $c_7 \log p/\log\log p$ distinct prime factors q. It would thus seem that verifying (1.1) would take at least order $\log^2 p/\log\log p$ multiplications mod p. However, from Yao [14] it is possible to reduce this to $O((\log p/\log\log p)^2)$, and it is not inconceivable (but unlikely) that it could be reduced to $O(\log p)$.

The basic step (1.1) in Pratt's algorithm needs to be iterated for the various primes q that divide $p - 1$. Thus, another possible way of showing that sometimes a Pratt certificate is fairly long is to show that there exist long chains of primes $p = q_0, q_1, \ldots, q_t$, where

$$q_{i+1} \mid q_i - 1 \quad \text{for } i = 0, \ldots, t - 1 \text{ and } q_t > p^{\delta}.$$

Specifically, if for some fixed $\delta > 0$ there are such chains of primes with t arbitrarily large, then there would be infinitely many primes p whose Pratt certificate was not of length $O(\log p)$ modular multiplications with moduli between p^{δ} and p. It is not known, however, if there are such long chains of primes. I conjecture that there are. Specifically, there is a heuristic argument (note presented here) that there is some $c_9 > 0$ and infinitely many primes $p = q_0$ for which there is a chain of primes of length $t > c_9 \log p/\log\log p$ and $q_t > p^{1/2}$. If this is correct, a Pratt certificate would be of length at least $c_9 \log^2 p/\log\log p$ modular multiplications with moduli at least $p^{1/2}$ for infinitely many primes p.

Because we know of no shorter primality proofs than Pepin's test or the Lucas-Lehmer test, it is tempting to conjecture that but for the constant factor $5/2$, Theorem 1 is optimal. This conjecture could be made in either a weak or strong form. The weak conjecture is that there is some $c_{10} > 0$ and infinitely many primes p such that *any* certificate of primality for p has length at least $c_{10} \log p$ multiplications mod p. The strong conjecture is that this is true for all primes p. (Because the exact complexity of one modular multiplication is uncertain and because all known primality certificates are dominated by modular multiplications, it has been convenient to measure lengths with the nonstandard unit of one modular multiplication.) Although tempting to make such conjectures, I shall resist since I know of no heuristic supporting them, nor of any direct numerical evidence (cf. Shanks [11]).

2. Background Results on Elliptic Curves Over Finite Fields. Until recently, the theory of elliptic curves over finite fields was perhaps not so well known in the computational number theory community. But with H. W. Lenstra, Jr.'s elliptic curve method for factoring [5] and the Goldwasser-Kilian elliptic curve method for primality testing mentioned in Section 1, it is becoming standard fare. Nevertheless, in this section some basic results are briefly presented.

Let $p > 3$ be prime. Although the theory goes through over arbitrary finite fields of characteristic p, it will be simpler if we restrict ourselves to the prime field $\mathbf{Z}/p$. If a, b are integers with

$$b(a^2 - 4b) \not\equiv 0 \bmod p, \tag{2.1}$$

then

$$y^2z = x^3 + ax^2z + bxz^2 \tag{2.2}$$

defines an elliptic curve $E_{a,b}^p$ over $\mathbf{Z}/p$. Thus $E_{a,b}^p$ is the set of triples $(x, y, z) \in (\mathbf{Z}/p)^3 - \{(0,0,0)\}$ with homogeneous coordinates (so that (x, y, z) and (cx, cy, cz) are considered the same point when $c \neq 0$) that satisfy (2.2). The point $(0,1,0) \in E_{a,b}^p$ is denoted 0. Note that if $(x, y, 0) \in E_{a,b}^p$, then $(x, y, 0) = 0$.

There is a natural way we can "add" points on $E_{a,b}^p$ that makes $E_{a,b}^p$ into an Abelian group with identity 0. We shall be particularly interested in the formula for adding a point to itself, i.e., doubling a point. If $P = (x, y, z) \in (\mathbf{Z}/p)^3$ satisfies (2.2) and $y, z \neq 0$, then $2P = (x', y', z')$, where

$$x' = (x^2 - bz^2)^2, \qquad z' = 4xz(x^2 + axz + bz^2). \tag{2.3}$$

The formula for y' is more complicated and not needed here, but note that from (2.2), if we know x and z and if $z \neq 0$, then

$$y^2 = (x^3 + ax^2z + bxz^2)/z.$$

If $y = 0$, then $2P = 0$. If $z = 0$, then as mentioned, $P = 0$, so that also $2P = 0$. Thus the points of order 2 in the group $E_{a,b}^p$ are precisely those points with $y = 0$. Note also that $(0,0,1) \in E_{a,b}^p$, so that $E_{a,b}^p$ always has at least one point of order 2. In fact (2.2) is the general equation for an elliptic curve with a point of order 2.

Although the transformation (2.3) does not apply when P is a point of order 2, it can be applied to recognize points of order 2.

LEMMA 2.1. *If $P = (x, y, z) \in E_{a,b}^p$, then P has order 2 if and only if $z \neq 0$ and $z' = 0$, where z' is given by* (2.3).

Proof. Let $P = (x, y, z) \in E_{a,b}^p$. Recall that $P = 0$ if and only if $z = 0$, so assume $z \neq 0$. As we have seen, P has order 2 if and only if $y = 0$. But from (2.2), $y = 0$ if and only if $x^3 + ax^2 + bxz^2 = 0$ if and only if $z' = 0$. □

Iterating this idea we may use the transformation (2.3) to recognize points of order 2^k.

. LEMMA 2.2. *If $P = (x_0, y_0, z_0) \in E_{a,b}^p$, let $(x_i, z_i) \in (\mathbf{Z}/p)^2$ be the result of applying the transformation* (2.3) *i times to the initial pair (x_0, z_0). Also let $z_{-1} = 1$. Then P has order 2^k if and only if $z_k = 0$ and $z_{k-1} \neq 0$.*

Proof. The result is obvious if $k = 0$ and is Lemma 2.1 if $k = 1$. Suppose $k > 1$, $z_k = 0$, and $z_{k-1} \neq 0$. Then each of $z_0, z_1, \ldots, z_{k-1} \neq 0$. Since $z_1 \neq 0$, it follows that P does not have order 1 or 2 and that there is some $y_1 \in \mathbf{Z}/p$ with $2P = (x_1, y_1, z_1)$. That is, we are saying that since P does not have order 1 or 2, the transformation (2.3) is valid for finding the first and third coordinates of $2P$. Similarly, if $z_2 \neq 0$, then $2P$ does not have order 1 or 2 and there is some $y_2 \in \mathbf{Z}/p$ with $4P = (x_2, y_2, z_2)$. Continuing in this fashion, we deduce that there are $y_i \in \mathbf{Z}/p$

for i up to $k-1$ with $2^iP = (x_i, y_i, z_i)$. Since $z_{k-1} \neq 0$ and $z_k = 0$, Lemma 2.1 implies that $2^{k-1}P$ has order 2. That is, P has order 2^k.

Now suppose P has order 2^k where $k > 1$. Then there is some $y_{k-1} \in \mathbf{Z}/p$ with $2^{k-1}P = (x_{k-1}, y_{k-1}, z_{k-1})$. Since $2^{k-1}P$ has order 2, it follows that $z_{k-1} \neq 0$ and $z_k = 0$. □

Our primality certificate shall make use of the following three results.

THEOREM 2.1. *The order of the group $E^p_{a,b}$ is $p + 1 - t$, where $|t| \leqslant 2\sqrt{p}$.*

THEOREM 2.2. *For each even integer t satisfying $|t| \leqslant 2\sqrt{p}$ there is some elliptic curve $E^p_{a,b}$ of order $p + 1 - t$.*

THEOREM 2.3. *The group $E^p_{a,b}$ is either cyclic or the direct sum of two cyclic groups.*

Of course, Theorem 2.1 is the Hasse-Weil theorem specialized to even-order elliptic curves over fields of prime order. Theorem 2.2 is a special case of a theorem of Waterhouse [13] which itself has roots in work of Deuring [3] (see Schoof [10]). Theorem 2.3 is an elementary result on elliptic curves over finite fields; see, for example, Tate [12].

3. Very Short Primality Proofs. Suppose n is an integer suspected to be prime. In this section we show how the results of Section 2 can be used to prove n prime.

THEOREM 3.1. *Suppse n, a, b, k are positive integers satisfying*

$$(6b(a^2 - 4b), n) = 1, \qquad a \leqslant n,\ b \leqslant n, \tag{3.1}$$

$$n > 34, \qquad 2\sqrt{n} < 2^k < 4\sqrt{n}. \tag{3.2}$$

Also suppose $P = (x_0, y_0, z_0) \in \mathbf{Z}^3$ with $0 \leqslant x_0,\ y_0,\ z_0 < n$ satisfies (2.2) modulo n. Let $\{(x_i, z_i)\}$ be the sequence of integer pairs with $0 \leqslant x_i,\ z_i < n$ obtained by applying the transformation (2.3) modulo n to the initial pair (x_0, z_0) i times. If $(z_{k-1}, n) = 1$ and $z_k = 0$, then n is prime.

Proof. Suppose not, so that n has a prime factor $p \leqslant \sqrt{n}$. From (3.1), $p > 3$ and $E^p_{a,b}$ is an elliptic curve over $\mathbf{Z}/p$. If $u \in \mathbf{Z}$, let $\bar{u}$ denote the residue of u mod p in $\mathbf{Z}/p$. Let $\bar{P} = (\bar{x}_0, \bar{y}_0, \bar{z}_0)$. Since $p \mid n$, applying the transformation (2.3) i times to the initial pair $(\bar{x}_0, \bar{z}_0)$ gives $(\bar{x}_i, \bar{z}_i)$. Thus $\bar{z}_{k-1} \neq 0$ and $\bar{z}_k = 0$, so that by Lemma 2.2, $\bar{P}$ has order 2^k in $E^p_{a,b}$. But (3.2) implies $2^k > p + 1 + 2\sqrt{p}$, contradicting Theorem 2.1. Thus n is prime.

THEOREM 3.2. *Suppose n, a, b, k are positive integers satisfying (3.1) and (3.2) and suppose $k = k_1 + k_2$, where k_1, k_2 are positive integers. Suppose $P = (x_0, y_0, z_0)$, $Q = (u_0, v_0, w_0)$ satisfy (2.2) modulo n, the coordinates of P and Q are in $[0, n-1]$, and $\{(x_i, z_i)\}$, $\{(u_i, w_i)\}$ are the sequences of integer pairs in $[0, n-1]^2$ obtained by repeatedly applying the transformation (2.3) modulo n to the initial pairs (x_0, z_0), (u_0, w_0), respectively. If*

$$(z_{k_1-1}, n) = 1, \quad z_{k_1} = 0, \quad (w_{k_2-1}, n) = 1, \quad w_{k_2} = 0, \tag{3.3}$$

$$(x_{k_1-1}w_{k_2-1} - u_{k_2-1}z_{k_1-1}, n) = 1 \tag{3.4}$$

hold, then n is prime.

Proof. If not, then n has a prime factor $p \leqslant \sqrt{n}$. As in the proof of Theorem 3.1, (3.3) implies the points $\overline{P}, \overline{Q} \in E_{a,b}^{p}$ have orders $2^{k_1}, 2^{k_2}$, respectively. Thus

$$2^{k_1-1}\overline{P} = \left(\bar{x}_{k_1-1}, 0, \bar{z}_{k_1-1}\right), \qquad 2^{k_2-1}\overline{Q} = \left(\bar{u}_{k_2-1}, 0, \bar{w}_{k_2-1}\right),$$

and so (3.4) implies that $2^{k_1-1}\overline{P} \neq 2^{k_2-1}\overline{Q}$. It follows that $E_{a,b}^{p}$ contains a subgroup isomorphic to $\mathbf{Z}/2^{k_1} \times \mathbf{Z}/2^{k_2}$ and thus $\#E_{a,b}^{p} \geqslant 2^{k_1+k_2} = 2^{k}$. Thus, as before, (3.2) contradicts Theorem 2.1. □

If $n > 34$ is prime and a, b, k, P exist satisfying the hypotheses of Theorem 3.1, we shall say that n has a "type 1" certificate of primality. Similarly, if the hypotheses of Theorem 3.2 hold, we shall say that n has a "type 2" certificate of primality. The next theorem establishes our main result, but with the larger constant $7/2$. The reduction to $5/2$ is established in the remarks following the proof.

THEOREM 3.3. *If $n > 34$ is prime, then it has either a type 1 or type 2 certificate of primality. Moreover, such a certificate may be verified in $\frac{7}{2}\log_2 n + O(1)$ multiplications* $\bmod n$, *$\frac{5}{2}\log_2 n + O(1)$ additions* $\bmod n$, *and one greatest common divisor computation with n and a natural number smaller than n^7.*

Proof. To see the length of a type 1 or type 2 certificate, just note that on input of x, z, the transformation (2.3) allows us to compute x', z' with 7 multiplications $\bmod n$ and 5 additions $\bmod n$. Indeed, by first computing the products

$$x^2, z^2, bz^2, xz, \quad \text{and} \quad axz$$

$\bmod n$, the value of x' can be computed with one addition (actually a subtraction) and one more multiplication. The value of z' can be computed with two additions to get $x^2 + axz + bz^2$, a multiplication by xz, and two more additions to simulate multiplying by 4. Moreover, since the transformation (2.3) is repeated $k = \frac{1}{2}\log_2 n + O(1)$ times, the assertion in the theorem about the length of a type 1 or type 2 certificate is now apparent.

To show the existence of a type 1 or type 2 certificate, first note that if n is odd there is always a unique power of 2 satisfying $2\sqrt{n} < 2^k < 4\sqrt{n}$. Moreover, there must be some integer m with

$$n + 1 - 2\sqrt{n} < m < n + 1 + 2\sqrt{n}, \qquad m \equiv 0 \bmod 2^k. \tag{3.5}$$

If n is prime, then by Theorem 2.2, there is some elliptic curve $E_{a,b}^{n}$ of order m. If there is a point $P \in E_{a,b}^{n}$ of order 2^k, then P satisfies the hypotheses of Theorem 3.1 and n has a type 1 certificate. If there are points $P, Q \in E_{a,b}^{n}$ and positive integers k_1, k_2 with $k_1 + k_2 = k$, $o(P) = 2^{k_1}$, $o(Q) = 2^{k_2}$, and $2^{k_1-1}P \neq 2^{k_2-1}Q$, then P, Q satisfy the hypotheses of Theorem 3.2 and n has a type 2 certificate. From Theorem 2.3, one of these two possibilities must exist for the curve $E_{a,b}^{n}$. □

Remarks. 1. The g.c.d. operation in Theorem 3.3 can be accomplished in time comparable to $O(1)$ multiplications $\bmod n$, provided the naive multiplication algorithm is used. If a fast multiplication algorithm is used, the comparison is harder to make. But in any case, the g.c.d. can always be accomplished in $O(\log^2 n)$-bit operations using only naive methods, and in $O(\log n(\log\log n)^2 \log\log\log n)$-bit operations using Schönhage's algorithm [9].

2. Suppose $p > 3$ is prime and $(b/p) = 1$. Then there is some $c \in \mathbf{Z}/p$ with $b = c^2$, $c \neq 0$. For $x \in \mathbf{Z}/p$, let $\tilde{x} = x/c$. Using the homogeneity of the coordinates of the points on $E^p_{a,b}$, we may replace (2.3) with

$$(2.3)' \qquad \begin{aligned} x' &= c^{-3}(x^2 - c^2z^2)^2 = c(\tilde{x}^2 - z^2)^2, \\ z' &= 4c^{-3}xz(x^2 + axz + c^2z^2) = 4\tilde{x}z(\tilde{x}^2 + ac^{-1}\tilde{x}z + z^2). \end{aligned}$$

Consider now the transformation (cf. Montgomery [7] and Chudnovsky and Chudnovsky [2])

$$(3.6) \qquad u' = (u^2 - v^2)^2, \qquad v' = 4uv(u^2 + ac^{-1}uv + v^2).$$

If $(2.3)'$ is applied i times to the initial pair (x, z), getting (x_i, z_i), and (3.6) is applied i times to the initial pair (u, v), getting (u_i, v_i), then

$$u = \tilde{x},\ v = z \quad \text{imply} \quad u_i = \tilde{x}_i,\ v_i = z_i.$$

Thus, in Theorems 3.1 and 3.2 we may use (3.6) instead of (2.3) or $(2.3)'$. Following Montgomery [7], with (3.6), (u', v') can be computed from (u, v) in 5 multiplications modulo p and 4 additions modulo p. Indeed, by computing

$$u - v, \quad (u - v)^2, \quad u + v, \quad (u + v)^2, \quad (u - v)^2(u + v)^2,$$

the value of u' may be computed with 3 multiplications and 2 additions. Moreover, since $4uv = (u + v)^2 - (u - v)^2$ and

$$u^2 + ac^{-1}uv + v^2 = (u + v)^2 + \frac{ac^{-1} - 2}{4} \cdot 4uv,$$

we may compute v' in 2 more multiplications and 2 more additions, provided $(ac^{-1} - 2)/4 \bmod n$ has been precomputed.

We conclude that if $n > 34$ is prime, the hypotheses of either Theorem 3.1 or 3.2 hold, and $(b/n) = 1$, then n has a certificate of primality of length $(\frac{5}{2} + o(1)) \log_2 n$ multiplications mod n.

3. We now show that every prime $n > 34$ has either a type 1 or type 2 certificate with $(b/n) = 1$ and so, by Remark 2, has a certificate of length $(\frac{5}{2} + o(1))\log_2 n$ multiplications mod n. I was originally only able to show this for primes $n \equiv 1 \bmod 4$, but thanks to a suggestion from Hendrik Lenstra, this can now be shown for all primes and by a simpler argument.

If $n > 34$ is prime and m is given by (3.5), then $8 \mid m$. Thus, by Theorem 2.3, if $E^n_{a,b}$ is an elliptic curve of order m, then $E^n_{a,b}$ has a point P of order 4. Say $2P = (\alpha, 0, 1)$. Making the change of variables $x \to x + \alpha$ in (2.2), we may assume $2P = (0, 0, 1)$. But if $(s, t, 1)$ is on $E^n_{a,b}$ and $2(s, t, 1) = (u, v, 1)$, then from (2.3),

$$u = (s^2 - b)^2/4t^2.$$

Applying this to $P = (s, t, 1)$, we deduce that $s^2 - b \equiv 0 \bmod n$, so that $(b/n) = 1$.

4. It finally should be remarked that every prime $n > 34$ has both type 1 and type 2 certificates. Indeed from Proposition 2.2 and Theorems 4.6 and 4.9 of Schoof [10] it follows that Theorem 2.2 above is true with the extra condition that $E^n_{a,b}$ does not contain the subgroup $\mathbf{Z}/2 \times \mathbf{Z}/2$, and it is also true with the extra condition that $E^n_{a,b}$ does contain such a subgroup. (We have applied Schoof's Theorem 4.9 to

2-torsion points, and it is stipulated in this result that it should only apply to u-torsion points with u odd. However, from the proof of this theorem, it holds for all u when working over a prime field.)

Department of Mathematics
University of Georgia
Athens, Georgia 30602

1. E. BACH, *Analytic Methods in the Analysis and Design of Number-Theoretic Algorithms*, MIT Press, Cambridge, Mass., 1985.

2. D. V. CHUDNOVSKY & G. V. CHUDNOVSKY, *Sequences of Numbers Generated by Addition in Formal Groups and New Primality and Factorization Tests*, Research Report RC 11262 (#50739), IBM Thomas J. Watson Research Center, Yorktown Heights, New York, 1985.

3. M. DEURING, "Die Typen der Multiplikatorenringe elliptischer Funktionenkörper," *Abh. Math. Sem. Univ. Hamburg*, v. 14, 1941, pp. 197–272.

4. S. GOLDWASSER & J. KILIAN, *Almost All Primes Can Be Quickly Certified*, Proc. 18th Annual ACM Sympos. on Theory of Computing (STOC), Berkeley, May 28–30, 1986, pp. 316–329.

5. H. W. LENSTRA, JR., "Factoring integers with elliptic curves." (To appear).

6. G. L. MILLER, "Riemann's hypothesis and tests for primality," *J. Comput. System Sci.*, v. 13, 1976, pp. 300–317.

7. P. L. MONTGOMERY, "Speeding the Pollard and elliptic curve methods of factorization," *Math. Comp.*, v. 48, 1987, pp. 243–264.

8. V. R. PRATT, "Every prime has a succinct certificate," *SIAM J. Comput.*, v. 4, 1975, pp. 214–220.

9. A. SCHÖNHAGE, "Schnelle Berechnung von Kettenbruchentwicklungen," *Acta Inform.*, v. 1, 1971, pp. 139–144.

10. R. J. SCHOOF, "Nonsingular plane cubic curves over finite fields," *J. Combin. Theory*. (To appear).

11. D. SHANKS, *Solved and Unsolved Problems in Number Theory*, 3rd ed., Chelsea, New York, 1985.

12. J. T. TATE, "The arithmetic of elliptic curves," *Invent. Math.*, v. 23, 1974, pp. 179–206.

13. W. C. WATERHOUSE, "Abelian varieties over finite fields," *Ann. Sci. École Norm. Sup.*, v. 2, 1969, pp. 521–560.

14. A. C. YAO, "On the evaluation of powers," *SIAM J. Comput.*, v. 5, 1976, pp. 100–103.