Annals of Mathematics, 126 (1987), 649–673

# Factoring integers with elliptic curves

By H. W. LENSTRA, JR.


## Abstract

This paper is devoted to the description and analysis of a new algorithm to factor positive integers. It depends on the use of elliptic curves. The new method is obtained from Pollard's $(p-1)$-method (Proc. Cambridge Philos. Soc. **76** (1974), 521–528) by replacing the multiplicative group by the group of points on a random elliptic curve. It is conjectured that the algorithm determines a non-trivial divisor of a composite number $n$ in expected time at most $K(p)(\log n)^2$, where $p$ is the least prime dividing $n$ and $K$ is a function for which $\log K(x) = \sqrt{(2+o(1))\log x \log\log x}$ for $x \to \infty$. In the worst case, when $n$ is the product of two primes of the same order of magnitude, this is $\exp((1+o(1))\sqrt{\log n \log\log n})$ (for $n \to \infty$). There are several other factoring algorithms of which the conjectural expected running time is given by the latter formula. However, these algorithms have a running time that is basically independent of the size of the prime factors of $n$, whereas the new elliptic curve method is substantially faster for small $p$.


*Acknowledgements.* This paper was written at the Mathematical Sciences Research Institute in Berkeley (NSF grant 8120790) and at the University of Chicago. I thank both institutions for their hospitality and support.

## Introduction

This paper is devoted to the description and analysis of a new method to factor positive integers. It depends on the use of elliptic curves.

The method is analogous to Pollard's $(p-1)$-method [17, Section 4], which attempts to find a non-trivial divisor of a given integer $n > 1$ in the following way. First, one selects an integer $a \pmod n$ and a positive integer $k$ that is divisible by many small prime powers; for example, $k = \operatorname{lcm}\{1, 2, \ldots, b\}$ for a suitable bound $b$. Next one calculates $a^k \pmod n$, and one hopes to obtain a non-trivial divisor of $n$ by calculating $\gcd(a^k - 1, n)$.

Pollard's $(p-1)$-method is usually successful if $n$ has a prime factor $p < n$ for which $p-1$ is built up from small prime numbers. Suppose, to be specific, that $p-1$ divides $k$, and that $p$ does not divide $a$. Then in the multiplicative group $(\mathbf{Z}/p\mathbf{Z})^*$ of integers modulo $p$ the number $a^k$ becomes equal to the neutral element 1, by Fermat's theorem, so that $p$ divides $\gcd(a^k-1, n)$. In many cases one has $p = \gcd(a^k-1, n)$, and the method finds a non-trivial divisor of $n$.

On the other hand, if for each prime number $p$ dividing $n$ the number $p-1$ has a large prime factor, then Pollard's $(p-1)$-method is not likely to be successful within a reasonable time limit.

The new method is obtained from Pollard's $(p-1)$-method by replacing the multiplicative group by the group of points on a random elliptic curve. To find a non-trivial divisor of an integer $n > 1$, one begins by selecting an elliptic curve $E$ over $\mathbf{Z}/n\mathbf{Z}$, a point $P$ on $E$ with coordinates in $\mathbf{Z}/n\mathbf{Z}$, and an integer $k$ as above. Using the addition law of the curve, one next calculates the multiple $k \cdot P$ of $P$. One now hopes that there is a prime divisor $p$ of $n$ for which $k \cdot P$ and the neutral element $O$ of the curve become the same modulo $p$; if $E$ is given by a homogeneous Weierstrass equation $y^2z = x^3 + axz^2 + bz^3$, with $O = (0:1:0)$, then this is equivalent to the $z$-coordinate of $k \cdot P$ being divisible by $p$. Hence, one hopes to find a non-trivial factor of $n$ by calculating the greatest common divisor of this $z$-coordinate with $n$.

If a single curve $E$ is used, then the properties of this algorithm are exactly the same as those of Pollard's $(p-1)$-method, with the order $p-1$ of $(\mathbf{Z}/p\mathbf{Z})^*$ replaced by the order of the group $E(\mathbf{Z}/p\mathbf{Z})$ of points of $E$ with coordinates in $\mathbf{Z}/p\mathbf{Z}$. By a theorem of Hasse (1934), this order is of the form $p + 1 - t_p$, where $t_p$ is an integer depending on $E$ and $p$ for which $|t_p| \leq 2\sqrt{p}$. If, for some prime factor $p < n$ of $n$, the number $p + 1 - t_p$ is built up from small primes, then the above algorithm is likely to lead to a non-trivial divisor of $n$, and otherwise not.

However, if the algorithm is unsuccessful, then an option is available that has no analogue in Pollard's $(p-1)$-method; namely, to repeat the algorithm with a different elliptic curve. A different curve will give rise to a new value for $t_p$, so that $p + 1 - t_p$ has a new chance of being built up from small primes. This can be repeated until a non-trivial divisor of $n$ is found.

The analysis of the elliptic curve factorization method that I present in this paper shows that the performance of the algorithm is largely determined by the density of numbers built up from small primes in the neighborhood of $p + 1$. If a reasonable conjecture concerning this density is assumed, then the following can be proved (see (2.9) and (2.10)). Let an integer $n > 0$ that is not a prime power and that is not divisible by 2 or 3 be given. Let also a positive integer $g$ be

given. Then, with a suitable choice of parameters, the elliptic curve method determines with probability at least $1 - e^{-g}$ a non-trivial divisor of $n$ in time

$$gK(p)M(n),$$

where the notation is as follows: $p$ denotes the least prime divisor of $n$, the function $K$: $\mathbf{R}_{>0} \to \mathbf{R}_{>0}$ is such that

$$K(x) = e^{\sqrt{(2+o(1))\log x \log\log x}} \quad \text{for } x \to \infty,$$

and $M(n)$ denotes an upper bound for the time needed to perform a single addition on an elliptic curve mod $n$; one can take $M(n) = O((\log n)^2)$ or $O(\log n(\log\log n)^2 \log\log\log n)$, depending on which method is employed.

The algorithm can be repeated until the complete prime factorization of $n$ is obtained. If the same conjecture is true, this takes expected time at most

$$e^{(1+o(1))\sqrt{\log n \log\log n}} \quad \text{for } n \to \infty,$$

the worst case occurring if the second largest prime factor of $n$ is not much smaller than $\sqrt{n}$.

There exist other factoring methods that one conjectures to be successful within the same time limit, such as the class group method [23] and the quadratic sieve [18]. Unlike the elliptic curve method, however, none of these has a running time that depends on the size of the prime factors of $n$. For a further comparison of the elliptic curve method with earlier methods, and a discussion of its practical merits, I refer to the end of Section 2.

The unproved assumption on which the analysis of the elliptic curve method is based *only* concerns the distribution of integers built up from small prime factors. In particular, it does not refer to elliptic curves. This is mainly due to a result of Deuring (1941), which gives a formula for the number of elliptic curves $E$ over a finite field $\mathbf{F}_q$ for which $E(\mathbf{F}_q)$ has a given order. A statement of this result, in the case that $q$ is prime, is given in Section 1. In this section one also finds the other results on elliptic curves over finite fields that are needed.

Section 2 is devoted to the factoring algorithm and its analysis. The most natural way to describe the algorithm would make use of elliptic curves over rings that are not fields, as was done in the outline given above. This theory, which one can find in [13, Chapter 2], is not as easily accessible as the theory over fields. For this reason the details have been arranged in such a way that no reference to the theory over rings is necessary. Accordingly, the description of the algorithm given in Section 2 does not follow the above outline in detail.

The version of the elliptic curve method described in this paper was exclusively designed for simplicity of exposition and ease of analysis. An extensive discussion of practical aspects can be found in [16].

An earlier application of elliptic curves to algorithmic number theory can be found in [24]. For primality testing algorithms that depend on the use of elliptic curves I refer to [4], [7], [10].

By $\mathbf{F}_q$ we denote a finite field of cardinality $q$. The group of units of a ring $A$ with 1 is denoted by $A^*$.

## 1. Counting elliptic curves.

In this section we assemble all facts about elliptic curves over fields that we need. Proofs can be found in the book by Silverman [29], if no other reference is given.

We denote by $K$ a field; we shall mainly be interested in the case that $K = \mathbf{F}_p$ for some prime number $p$. To simplify the exposition we assume throughout this section that the characteristic of $K$ is not equal to 2 or 3.

(1.1) *Elliptic curves.* An *elliptic curve* over $K$ is a pair of elements $a, b \in K$ for which $4a^3 + 27b^2 \neq 0$. These elements are to be thought of as the coefficients in the Weierstrass equation

$$y^2 = x^3 + ax + b. \tag{1.2}$$

We denote the elliptic curve $(a, b)$ by $E_{a,b}$, or simply by $E$. The *set of points* $E(K)$ of such an elliptic curve over $K$ is defined by

$$E(K) = \{(x : y : z) \in \mathbf{P}^2(K) : y^2z = x^3 + axz^2 + bz^3\}.$$

Here $\mathbf{P}^2(K)$ denotes the projective plane over $K$. It consists of equivalence classes of triples $(x, y, z) \in K \times K \times K$, $(x, y, z) \neq (0, 0, 0)$, two triples $(x, y, z)$ and $(x', y', z')$ being equivalent if there exists $c \in K^*$ such that $cx = x'$, $cy = y'$ and $cz = z'$; the equivalence class containing $(x, y, z)$ is denoted by $(x : y : z)$.

Let $E$ be an elliptic curve over $K$. Then $E(K)$ contains exactly one point $(x : y : z)$ for which $z = 0$, namely the point $(0 : 1 : 0)$; this point is called the *zero point* of the curve and denoted by $O$. The other points of $E(K)$ are the points $(x : y : 1)$, where $x, y \in K$ satisfy (1.2). The set $E(K)$ has the structure of an *abelian group*; the group law, which is written additively, is defined as follows. First, $O + P = P + O = P$ for all $P \in E(K)$. Next, let $P = (x_1 : y_1 : 1)$, $Q = (x_2 : y_2 : 1)$ be non-zero points. Then $P + Q = O$ if and only if $x_1 = x_2$ and $y_1 = -y_2$. Otherwise, let $\lambda \in K$ be determined by $\lambda = (y_1 - y_2)/(x_1 - x_2)$ if $P \neq Q$ and $\lambda = (3x_1^2 + a)/(2y_1)$ if $P = Q$, and let $\nu = y_1 - \lambda x_1$. Then $P + Q = R$, where $R = (x_3 : y_3 : 1)$ with $x_3 = \lambda^2 - x_1 - x_2$ and $y_3 = -\lambda x_3 - \nu$. Observe that $O$ is the zero element of the group, and that $-(x : y : z) = (x : -y : z)$.

(1.3) *Isomorphisms and automorphisms.* Let $E = E_{a,b}$ and $E' = E_{a',b'}$ be elliptic curves over $K$. An *isomorphism* $E \to E'$ (over $K$) is defined to be an element $u \in K^*$ for which $a' = u^4 a$ and $b' = u^6 b$. If an isomorphism $E \to E'$ exists then $E$ and $E'$ are said to be *isomorphic*; this is clearly an equivalence relation. Any isomorphism $u\colon E \to E'$ induces an isomorphism $E(K) \to E'(K)$ of abelian groups that sends $(x : y : z)$ to $(u^2 x : u^3 y : z)$; this isomorphism will also be denoted by $u$. We shall only be interested in elliptic curves up to isomorphism.

Let $E$ be an elliptic curve over $K$. An *automorphism* of $E$ is an isomorphism $E \to E$. The set of automorphisms of $E$ is a subgroup of $K^*$, which is denoted by $\mathrm{Aut}\, E$ or $\mathrm{Aut}_K E$. An easy calculation shows that it can be explicitly described as follows:

(i) If $a = 0$ and $K^*$ has an element $\rho$ of order 6, then $\rho$ generates $\mathrm{Aut}\, E$ and $\#\mathrm{Aut}\, E = 6$;

(ii) If $b = 0$ and $K^*$ has an element $i$ of order 4, then $i$ generates $\mathrm{Aut}\, E$ and $\#\mathrm{Aut}\, E = 4$;

(iii) In all other cases $\mathrm{Aut}\, E = \{1, -1\}$ and $\#\mathrm{Aut}\, E = 2$.

(1.4) *The number of elliptic curves.* Let $p$ denote a prime number $> 3$. In the remainder of this section we restrict to the case $K = \mathbf{F}_p$.

The number of elliptic curves over $\mathbf{F}_p$, as defined in (1.1), is the number of pairs $(a, b) \in \mathbf{F}_p \times \mathbf{F}_p$ with $4a^3 + 27b^2 \neq 0$. The number of all pairs $(a, b)$ equals $p^2$, and $4a^3 + 27b^2 = 0$ if and only if $a = -3c^2$, $b = 2c^3$ for some $c \in \mathbf{F}_p$; this element $c$ is uniquely determined by $a$, $b$ by $c = -3b/(2a)$ (if $a \neq 0$). Hence $4a^3 + 27b^2 = 0$ for exactly $p$ pairs $(a, b)$. We conclude that the number of elliptic curves over $\mathbf{F}_p$ equals $p^2 - p$.

We use this result to count the set

$$\{E\colon E \text{ elliptic curve over } \mathbf{F}_p\}/\cong_{\mathbf{F}_p}$$

of isomorphism classes of elliptic curves over $\mathbf{F}_p$. The number of elliptic curves isomorphic to a given elliptic curve $E$ is easily seen to be $\#\mathbf{F}_p^*/\#\mathrm{Aut}\, E = (p-1)/\#\mathrm{Aut}\, E$. Summing this over a set of representatives of the isomorphism classes and dividing by $p - 1$ we obtain

$$\sum_E \frac{1}{\#\mathrm{Aut}\, E} = p.$$

We express this by writing

$$\#'\{E\colon E \text{ elliptic curve over } \mathbf{F}_p\}/\cong_{\mathbf{F}_p} = p.$$

Here, and in similar expressions below, $\#'$ denotes the *weighted cardinality*, the isomorphism class of $E$ being counted with weight $(\#\mathrm{Aut}\, E)^{-1}$.

Since $\#\operatorname{Aut} E = 2$ for most $E$ it follows from the above formula that the ordinary cardinality of the set of isomorphism classes of elliptic curves over $\mathbf{F}_p$ is approximately $2p$. The precise number can be derived from (1.3). Using that the existence of $\rho \in \mathbf{F}_p^*$ as in (1.3)(i) is equivalent to $p \equiv 1 \bmod 6$, and the existence of $i \in \mathbf{F}_p^*$ as in (1.3)(ii) to $p \equiv 1 \bmod 4$, one finds that

$$\#\{E\colon E \text{ elliptic curve over } \mathbf{F}_p\}/\cong_{\mathbf{F}_p} = 2p + 6, 2p + 2, 2p + 4, 2p$$

for $p \equiv 1, 5, 7, 11 \bmod 12$, respectively. We shall have no use for this result in the sequel.

(1.5) *The order of* $E(\mathbf{F}_p)$. For any elliptic curve $E$ over $\mathbf{F}_p$ we have by a theorem of Hasse

$$\#E(\mathbf{F}_p) = p + 1 - t, \quad \text{with } t \in \mathbf{Z}, \quad |t| \leq 2\sqrt{p}\,.$$

Let, conversely, $p$ be a prime $> 3$ and $t$ an integer satisfying $|t| \leq 2\sqrt{p}$. Then the weighted number of elliptic curves $E$ over $\mathbf{F}_p$ with $\#E(\mathbf{F}_p) = p + 1 - t$, up to isomorphism, is given by a formula that is basically due to Deuring [9]; see also [1], [30], [25]:

$$\#'\{E\colon E \text{ elliptic curve over } \mathbf{F}_p, \#E(\mathbf{F}_p) = p + 1 - t\}/\cong_{\mathbf{F}_p} = H(t^2 - 4p),$$

where $H(t^2 - 4p)$ denotes the *Kronecker class number* of $t^2 - 4p$, which we now proceed to define.

(1.6) *Kronecker class numbers.* We begin by recalling the properties of binary quadratic forms that we need. See [3] for more details and for proofs.

Let $\Delta$ be a *negative* integer, $\Delta \equiv 0$ or $1 \bmod 4$. A *positive definite integral binary quadratic form of discriminant* $\Delta$, briefly a *form*, is a polynomial $F = aX^2 + bXY + cY^2$ with $a, b, c \in \mathbf{Z}$, $a > 0$, $b^2 - 4ac = \Delta$. An *isomorphism* from a form $F = aX^2 + bXY + cY^2$ to a form $F' = a'X^2 + b'XY + c'Y^2$ is a matrix $\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ with $\alpha, \beta, \gamma, \delta \in \mathbf{Z}$, $\alpha\delta - \beta\gamma = 1$ for which

$$aX^2 + bXY + cY^2 = a'X'^2 + b'X'Y' + c'Y'^2,$$

where $X' = \alpha X + \beta Y$ and $Y' = \gamma X + \delta Y$. If such an isomorphism exists, the forms $F$ and $F'$ are said to be *equivalent*; this is indeed an equivalence relation. An *automorphism* of a form $F$ is an isomorphism from $F$ to $F$. The set of automorphisms of a form $F$ is a subgroup of the group $\mathrm{SL}_2\mathbf{Z}$ of $2 \times 2$-matrices with integral entries and determinant 1; this subgroup is denoted by $\operatorname{Aut} F$. We have:

(i) $\operatorname{Aut} F$ is cyclic of order 6 if $F$ is equivalent to $aX^2 + aXY + aY^2$ for some positive integer $a$; in this case $\Delta = -3a^2$;

(ii) $\operatorname{Aut} F$ is cyclic of order 4 if $F$ is equivalent to $aX^2 + aY^2$ for some positive integer $a$; in this case $\Delta = -4a^2$;

(iii) In all other cases, the group Aut $F$ is of order 2, and equals $\left\{\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}, \begin{pmatrix}-1 & 0\\ 0 & -1\end{pmatrix}\right\}$.

For fixed $\Delta$, the set of equivalence classes of forms of discriminant $\Delta$ is *finite*. The *Kronecker class number* $H(\Delta)$ of $\Delta$ is defined to be the weighted cardinality of this set, the equivalence class containing $F$ being counted with weight $(\#\,\mathrm{Aut}\,F)^{-1}$:

$$H(\Delta) = \#'\{F\colon F \text{ is a form of discriminant } \Delta\}/\sim$$

with $\sim$ denoting equivalence and the meaning of $\#'$ being as in (1.4). For example, $H(-3) = 1/6$, $H(-4) = 1/4$, $H(-7) = 1/2$. (*Warning*: one often finds the Kronecker class number defined twice as large.) The existence of the form $X^2 + bXY - ((\Delta - b^2)/4)Y^2$, where $\Delta \equiv b^2 \bmod 4$, shows that $H(\Delta) > 0$.

A form $F = aX^2 + bXY + cY^2$ is called *primitive* if $\gcd(a, b, c) = 1$. We denote by $h(\Delta)$ the weighted cardinality of the set of equivalence classes of primitive forms of discriminant $\Delta$, counted with the same weights as above. It is easy to see that

$$H(\Delta) = \sum_d h(\Delta/d^2), \tag{1.7}$$

the summation ranging over those positive integers $d$ for which $\Delta/d^2$ is an integer satisfying $\Delta/d^2 \equiv 0$ or $1 \bmod 4$. The largest such $d$ is called the *conductor* $f$ of $\Delta$, and $\Delta_0 = \Delta/f^2$ is the *fundamental discriminant* associated to $\Delta$; the $d$'s in the above summation are exactly the positive divisors of $f$.

The *quadratic character* $\chi\colon \mathbf{Z}_{>0} \to \{0, 1, -1\}$ associated to $\Delta$ is defined by

$$\chi(l) \equiv \Delta^{(l-1)/2} \bmod l,\ \chi(l) \in \{0, 1, -1\} \quad \text{if } l \text{ is an odd prime,}$$

$$\chi(2) = 0, 1, -1 \quad \text{for } \Delta \equiv 0 \bmod 4,\ 1 \bmod 8,\ 5 \bmod 8, \text{ respectively,}$$

$$\chi(nm) = \chi(n)\chi(m) \quad \text{for all } n, m \in \mathbf{Z}_{>0}.$$

The *analytic class number formula* for $h(\Delta)$ is

$$h(\Delta) = \frac{\sqrt{-\Delta}}{2\pi} \cdot L(1, \chi), \quad \text{where } L(s, \chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s} \text{ for } s \in \mathbf{C},\ \mathrm{Re}\, s > 0.$$

If $\chi_0$ denotes the quadratic character associated to $\Delta_0$, one has

$$L(1, \chi) = L(1, \chi_0) \cdot \prod_{l \mid f} \left(1 - \frac{\chi_0(l)}{l}\right)$$

where $l$ ranges over the primes dividing $f$. Combining the last two formulae with (1.7) one finds that

$$H(\Delta) = \frac{\sqrt{-\Delta}}{2\pi} \cdot L(1, \chi_0) \cdot \psi(f)$$

where $\psi\colon \mathbf{Z}_{>0} \to \mathbf{R}$ is defined by

$$\psi(l^k) = \frac{l - l^{-k}}{l - 1}, 1, \frac{l + 1 - 2l^{-k}}{l - 1}$$

if $l$ is prime, $k \geq 1$ and $\chi_0(l) = 0, 1, -1$, respectively,

$$\psi(nm) = \psi(n)\psi(m) \text{ if } n, m \in \mathbf{Z}_{>0}, \gcd(n, m) = 1.$$

We are interested in obtaining upper and lower bounds for $H(\Delta)$. It is easily seen that

$$1 \leq \psi(f) \leq (f/\phi(f))^2 = O\big((\log\log f)^2\big)$$

(see [11, Theorem 328]), where $\phi$ denotes the Euler $\phi$-function. Further we have

$$L(1, \chi_0) = O(\log|\Delta_0|);$$

see [20, Kapitel IV, Lemma 8.1]. To obtain a satisfactory lower bound for $L(1, \chi_0)$ we must sacrifice one value for $\Delta_0$. Applying [20, Kapitel IV, Section 6, Satz 6.6 and the argument following Section 8, eq. (8.26)] one finds that there exists a positive effectively computable constant $c_1$ such that for all $z \in \mathbf{Z}_{>1}$ there exists $\Delta^* < -4$ with the property that

$$L(1, \chi_0) \geq \frac{c_1}{\log z} \text{ if } |\Delta_0| \leq z, \ \Delta_0 \neq \Delta^*.$$

(If the generalized Riemann hypothesis is assumed we can replace $\log z$ by $\log\log z$, and there is no need to exclude an exceptional value $\Delta^*$ for $\Delta_0$.)

(1.8) PROPOSITION. *There exist effectively computable positive constants $c_2, c_3$ such that for each $z \in \mathbf{Z}_{>1}$ there exists $\Delta^* = \Delta^*(z) < -4$ such that*

$$\frac{c_2\sqrt{-\Delta}}{\log z} \leq H(\Delta) \leq c_3 \cdot \sqrt{-\Delta} \cdot \log|\Delta| \cdot (\log\log|\Delta|)^2$$

*for all $\Delta \in \mathbf{Z}$ with $-z \leq \Delta < 0$, $\Delta \equiv 0$ or $1 \bmod 4$, except that the left inequality may be invalid if $\Delta_0 = \Delta^*$.*

*Proof.* This follows from the inequalities in (1.6).

(1.9) PROPOSITION. *There exist effectively computable positive constants* $c_4, c_5$ *such that for each prime number* $p > 3$ *the following two assertions are valid; for the notation* #′, *see* (1.4).

(a) *If* $S$ *is a set of integers* $s$ *with* $|s - (p+1)| \leq 2\sqrt{p}$ *then*

$$\#'\{E\text{: } E \text{ elliptic curve over } \mathbf{F}_p, \#E(\mathbf{F}_p) \in S\}/\cong_{\mathbf{F}_p}$$

$$\leq c_4 \cdot \#S \cdot \sqrt{p} \cdot (\log p) \cdot (\log\log p)^2.$$

(b) *If* $S$ *is a set of integers* $s$ *with* $|s - (p+1)| \leq \sqrt{p}$ *then*

$$\#'\{E\text{: } E \text{ elliptic curve over } \mathbf{F}_p, \#E(\mathbf{F}_p) \in S\}/\cong_{\mathbf{F}_p}$$

$$\geq c_5 \cdot (\#S - 2) \cdot \sqrt{p}/(\log p).$$

*Proof.* In both (a) and (b), the left hand side of the inequality equals

$$\sum_{t,\, p+1-t \in S} H(t^2 - 4p)$$

by the formula in (1.5). We apply (1.8) with $z = 4p$. Then (a) follows immediately, with a suitable constant $c_4$. For (b), we note that $|t^2 - 4p| \geq 3p$ if $p + 1 - t \in S$. To prove (b), it thus suffices to show that there are at most two integers $t$, $|t| \leq \sqrt{p}$, for which the fundamental discriminant associated to $t^2 - 4p$ equals $\Delta^*$. Let $L = \mathbf{Q}(\sqrt{\Delta^*})$, and let $t$ be such an integer. Then the zeros $\alpha, \bar{\alpha}$ of $X^2 - tX + p$ belong to the ring of integers $A$ of $L$. Also, $\alpha\bar{\alpha} = p$, and by unique prime ideal factorization in $A$ and the fact that $A^* = \{1, -1\}$ (because $\Delta^* < -4$) this determines $\alpha$ up to conjugation and sign. Hence $t = \alpha + \bar{\alpha}$ is determined up to sign, as required. This proves (1.9).

(1.10) *Modular curves.* We are interested in estimating the weighted number of elliptic curves $E$ over $\mathbf{F}_p$ for which $\#E(\mathbf{F}_p)$ is divisible by a given prime number $l$. For this purpose we need some facts about the modular curves $X(l)$ and $X_1(l)$. For proofs we refer to [28], [12], [13].

Let $p$ be a prime number, $p > 3$, and $l$ a prime number different from $p$. We consider pairs $(E, P)$ consisting of an elliptic curve $E$ over $\mathbf{F}_p$ and a point $P \in E(\mathbf{F}_p)$ of order $l$. Two such pairs $(E, P)$ and $(E', P')$ are said to be *equivalent over* $\mathbf{F}_p$ if there exists an isomorphism $u\colon E \to E'$ over $\mathbf{F}_p$ that maps $P$ to $P'$ (see (1.3)). We denote the set of equivalence classes by $Z_1(l)(\mathbf{F}_p)$. If, in the definition just given, $u$ is allowed to be in the algebraic closure $\bar{\mathbf{F}}_p$ of $\mathbf{F}_p$ rather than in $\mathbf{F}_p$ (so that a map $E(\bar{\mathbf{F}}_p) \to E'(\bar{\mathbf{F}}_p)$ rather than $E(\mathbf{F}_p) \to E'(\mathbf{F}_p)$ is induced), we obtain the definition of *equivalence over* $\bar{\mathbf{F}}_p$. The set of classes of

this equivalence relation is denoted by $Y_1(l)(\mathbf{F}_p)$. There is an obvious surjective map $Z_1(l)(\mathbf{F}_p) \to Y_1(l)(\mathbf{F}_p)$.

We can estimate the cardinality of $Y_1(l)(\mathbf{F}_p)$ by using the following properties of the *modular curve* $X_1(l)$:

(i) $X_1(l)$ is a complete non-singular irreducible curve defined over $\mathbf{F}_p$;

(ii) The *genus* of $X_1(l)$ equals 0 for $l = 2$ or 3, and $1 + \frac{1}{24}(l-1)(l-11)$ for $l \geq 5$;

(iii) The set $Y_1(l)(\mathbf{F}_p)$ can in a natural way be considered as a subset of the set $X_1(l)(\mathbf{F}_p)$ of points of $X_1(l)$ defined over $\mathbf{F}_p$;

(iv) The cardinality of the complement of $Y_1(l)(\mathbf{F}_p)$ in $X_1(l)(\mathbf{F}_p)$ is bounded from above by the number of *cusps* of $X_1(l)$, which equals 2 for $l = 2$ and $l - 1$ for $l > 2$.

If $C$ is a complete non-singular irreducible curve of genus $g$ over $\mathbf{F}_p$ then by Weil's inequality [2] the cardinality of the set $C(\mathbf{F}_p)$ of points of $C$ over $\mathbf{F}_p$ satisfies

$$\left|\#C(\mathbf{F}_p) - (p+1)\right| \leq 2g\sqrt{p}\,.$$

Applying this to $C = X_1(l)$ we find, using the above properties:

$$\#Y_1(l)(\mathbf{F}_p) = p + O\left(l^2\sqrt{p}\right), \tag{1.11}$$

the constant implied by the $O$-symbol being absolute and effectively computable.

With $p$ and $l$ as above, suppose now in addition that $p \equiv 1 \bmod l$, and let a primitive $l$-th root of unity $\zeta \in \mathbf{F}_p$ be chosen. We consider triples $(E, P, Q)$ consisting of an elliptic curve $E$ over $\mathbf{F}_p$ and two points $P, Q \in E(\mathbf{F}_p)$ of order $l$ satisfying $e_l(P, Q) = \zeta$, where $e_l$ denotes the Weil pairing [29, Chapter III, Section 8]. Equivalence of two such triples $(E, P, Q)$ and $(E', P', Q')$ over $\mathbf{F}_p$ (or over $\bar{\mathbf{F}}_p$) is defined as before; the only difference is that $u$ should not only map $P$ to $P'$ but $Q$ to $Q'$ as well. The sets of equivalence classes over $\mathbf{F}_p$ and $\bar{\mathbf{F}}_p$ are denoted by $Z(l)(\mathbf{F}_p)$ and $Y(l)(\mathbf{F}_p)$, respectively. There is an obvious surjective map $Z(l)(\mathbf{F}_p) \to Y(l)(\mathbf{F}_p)$.

The modular curve $X(l)$ has the following properties:

(i) $X(l)$ is a complete non-singular irreducible curve defined over $\mathbf{F}_p$;

(ii) The genus of $X(l)$ equals 0 for $l = 2$, and $1 + \frac{1}{24}(l^2-1)(l-6)$ for $l \geq 3$;

(iii) The set $Y(l)(\mathbf{F}_p)$ can in a natural way be considered as a subset of the set $X(l)(\mathbf{F}_p)$ of points of $X(l)$ defined over $\mathbf{F}_p$;

(iv) The cardinality of the complement of $Y(l)(\mathbf{F}_p)$ in $X(l)(\mathbf{F}_p)$ is bounded from above by the number of cusps of $X(l)$, which is 3 for $l = 2$ and $(l^2-1)/2$ for $l > 2$.

Applying Weil's inequality cited above to $C = X(l)$ we find from these properties that

$$\#Y(l)(\mathbf{F}_p) = p + O\left(l^3\sqrt{p}\right), \tag{1.12}$$

the $O$-constant again being absolute and effectively computable.

(1.13) LEMMA. *Let $p$, $l$ be primes, $p > 3$, $l \neq p$.*

(a) *Let $E$ be an elliptic curve over $\mathbf{F}_p$ and $P \in E(\mathbf{F}_p)$ a point of order $l$. Denote by $A_{E,P}$ the subgroup of all $u \in \mathrm{Aut}_{\mathbf{F}_p}E$ that send $P$ to $P$. Then the number of elements of $Z_1(l)(\mathbf{F}_p)$ that map to the class of $(E, P)$ in $Y_1(l)(\mathbf{F}_p)$ equals $\#A_{E,P}$.*

(b) *Suppose that $p \equiv 1 \bmod l$, and let a primitive $l$-th root of unity $\zeta \in \mathbf{F}_p$ be chosen. Let $E$ be an elliptic curve over $\mathbf{F}_p$ and $P, Q \in E(\mathbf{F}_p)$ points of order $l$ satisfying $e_l(P, Q) = \zeta$. Denote by $A_{E,P,Q}$ the subgroup $A_{E,P} \cap A_{E,Q}$ of $\mathrm{Aut}_{\mathbf{F}_p}E$. Then the number of elements of $Z(l)(\mathbf{F}_p)$ that map to the class of $(E, P, Q)$ in $Y(l)(\mathbf{F}_p)$ equals $\#A_{E,P,Q}$.*

*Remark.* The numbers $\#A_{E,P}$ and $\#A_{E,P,Q}$ in the lemma equal 2 for $l = 2$ and 1 for $l > 2$, provided that $\#\mathrm{Aut}_{\mathbf{F}_p}E = 2$, which for given $p$ is true in all but $O(1)$ cases.

*Proof of* (1.13). (a) Let $E$ be given by $a$, $b$, and let $P = (x : y : 1)$. If $E'$, $P'$ is another such pair, given by $a'$, $b'$, $x'$, $y'$, then $(E, P)$ and $(E', P')$ give rise to the same element of $Y_1(l)(\mathbf{F}_p)$ if and only if we have $(a', b', x', y') = (u^4a, u^6b, u^2x, u^3y)$ for some $u \in \bar{\mathbf{F}}_p^*$, and to the same element of $Z_1(l)(\mathbf{F}_p)$ if and only if $u$ can be taken in $\mathbf{F}_p^*$. It follows that the number of elements of $Z_1(l)(\mathbf{F}_p)$ mapping to the class of $(E, P)$ equals index $[B_{E,P} : C_{E,P}]$, where the subgroups $B_{E,P}$, $C_{E,P}$ of $\bar{\mathbf{F}}_p^*$ are defined by

$$B_{E,P} = \left\{u \in \bar{\mathbf{F}}_p^* : \left\{u^4a, u^6b, u^2x, u^3y\right\} \subset \mathbf{F}_p\right\},$$

$$C_{E,P} = \left\{u \in \bar{\mathbf{F}}_p^* : \left(u^4a, u^6b, u^2x, u^3y\right) = \left(v^4a, v^6b, v^2x, v^3y\right) \text{ for some } v \in \mathbf{F}_p^*\right\}.$$

To count $B_{l,P}$, we notice that for $u \in \bar{\mathbf{F}}_p^*$ we have $u^4a \in \mathbf{F}_p$ if and only if $(u^4a)^p = u^4a$, so if and only if $(u^{p-1})^4a = a$; and similarly with $u^6b$, $u^2x$, $u^3y$; hence the map sending $u$ to $u^{p-1}$ maps $B_{E,P}$ onto the group $\bar{A}_{E,P}$ of all $u \in \mathrm{Aut}_{\bar{\mathbf{F}}_p}E$ sending $P$ to itself. The kernel is $\mathbf{F}_p^*$, so that

$$\#B_{E,P} = \#\bar{A}_{E,P} \cdot \#\mathbf{F}_p^*.$$

From the definition of $C_{E,P}$ it is easy to see that $C_{E,P}$ is generated by $\mathbf{F}_p^*$ and

$\bar{A}_{E,P}$, so that

$$\#C_{E,P} = \#\mathbf{F}_p^* \cdot \#\bar{A}_{E,P}/\#\left(\bar{A}_{E,P} \cap \mathbf{F}_p^*\right)$$

and

$$\operatorname{index}\left[B_{E,P}: C_{E,P}\right] = \#\left(\bar{A}_{E,P} \cap \mathbf{F}_p^*\right) = \#A_{E,P},$$

as required.

This proves (a). The proof of (b) is similar, and left to the reader. This proves (1.13).

(1.14) PROPOSITION. *Let $p$, $l$ be primes, $p > 3$, $l \neq p$. Then the number*

$$\#'\left\{E: E \text{ elliptic curve over } \mathbf{F}_p, \#E(\mathbf{F}_p) \equiv 0 \bmod l\right\}/\cong_{\mathbf{F}_p}$$

*equals*

$$\frac{1}{l-1}p + O\left(l\sqrt{p}\right) \quad \text{if } p \not\equiv 1 \bmod l,$$

$$\frac{l}{l^2-1}p + O\left(l\sqrt{p}\right) \quad \text{if } p \equiv 1 \bmod l.$$

*Here $\#'$ is as in* (1.4), *and the O-constants are absolute and effectively computable.*

*Remark.* Comparing (1.14) with the result of (1.4) we see that, for fixed $l$, the probability that a "random" elliptic curve $E$ over $\mathbf{F}_p$ satisfies $\#E(\mathbf{F}_p) \equiv 0 \bmod l$ tends to $1/(l-1)$ and $l/(l^2-1)$ if $p$ tends to infinity over the primes with $p \not\equiv 1 \bmod l$ and $p \equiv 1 \bmod l$, respectively. In particular, $\#E(\mathbf{F}_p)$ is even with probability approximately $2/3$; this can also be deduced from the observation that $\#E(\mathbf{F}_p)$ is even if and only if $X^3 + aX + b$ has a zero in $\mathbf{F}_p$, where $E$ is given by $a, b$. A proposition similar to the above one, but with different constants, can be proved for the case in which $l$ is not prime.

*Proof of* (1.14). Write $Y_1$, $Z_1$ for $Y_1(l)(\mathbf{F}_p)$, $Z_1(l)(\mathbf{F}_p)$. If $p \equiv 1 \bmod l$ let an element $\zeta \in \mathbf{F}_p^*$ of order $l$ be chosen, and write $Y$, $Z$ for $Y(l)(\mathbf{F}_p)$, $Z(l)(\mathbf{F}_p)$.

Let $W$ be the set of isomorphism classes of elliptic curves $E$ over $\mathbf{F}_p$ with $\#E(\mathbf{F}_p) \equiv 0 \bmod l$. For each such $E$, the group $E(\mathbf{F}_p)[l] = \{P \in E(\mathbf{F}_p): lP = O\}$ has order $l$ or $l^2$ (see [29, Chapter III, Corollary 6.4]) and if the order is $l^2$ then $p \equiv 1 \bmod l$ (*ibidem*, Corollary 8.1.1). We write $W = W_1 \cup W_2$ (disjoint), with $W_i$ consisting of the classes of those $E$ for which $\#E(\mathbf{F}_p)[l] = l^i$; so $W_2 = \varnothing$ unless $p \equiv 1 \bmod l$.

The map $Z_1 \to W$ mapping the class of $(E, P)$ to the class of $E$ is clearly surjective. Two pairs $(E, P)$, $(E, P')$ with the same $E$ represent the same element of $Z_1$ if and only if $P$ and $P'$ belong to the same orbit of $\operatorname{Aut}_{\mathbf{F}_p} E$; also,

the size of the orbit is exactly index$[\mathrm{Aut}_{\mathbf{F}_p}E\colon A_{E,P}] = \#\mathrm{Aut}_{\mathbf{F}_p}E/\#A_{E,P}$ with $A_{E,P}$ denoting the stabilizer of $P$ in $\mathrm{Aut}_{\mathbf{F}_p}E$ (as in (1.13)(a)). Fixing $E$ with $\#E(\mathbf{F}_p)[l] = l^t$ and summing over the orbits of $P$ we obtain

$$\sum_P \frac{\#\mathrm{Aut}_{\mathbf{F}_p}E}{\#A_{E,P}} = l^t - 1.$$

Dividing by $\#\mathrm{Aut}_{\mathbf{F}_p}E$ and summing over isomorphism classes of $E$ we obtain

$$\sum \frac{1}{\#A_{E,P}} = (l-1)\cdot \#'W_1 + (l^2-1)\cdot \#'W_2$$

with $\#'$ as in (1.4) and the summation ranging over $Z_1$. By Lemma (1.13)(a) the left-hand sum equals exactly $\#Y_1$, and with (1.11) we now find

$$(l-1)\cdot \#'W_1 + (l^2-1)\cdot \#'W_2 = p + O\left(l^2\sqrt{p}\right).$$

If $p \not\equiv 1 \bmod l$, then this simply means that

$$(l-1)\cdot \#'W = p + O\left(l^2\sqrt{p}\right),$$

and the required result follows upon division by $l-1$.

Let, for the rest of the proof, the hypotheses be as in (1.13)(b). Then we study in a similar way the map $Z \to W_2$ that sends the class of $(E, P, Q)$ to the class of $E$. For each $E$ with $\#E(\mathbf{F}_p)[l] = l^2$ there are $l(l^2-1)$ pairs of points $P, Q \in E(\mathbf{F}_p)[l]$ with $e_l(P,Q) = \zeta$. Hence we have, for such an $E$:

$$\sum_{(P,Q)} \frac{\#\mathrm{Aut}_{\mathbf{F}_p}E}{\#A_{E,P,Q}} = l(l^2-1)$$

where the sum is over $\mathrm{Aut}_{\mathbf{F}_p}E$-orbits of pairs of points $P, Q$ as above and $A_{E,P,Q}$ is as in (1.13)(b). In the same way as before this leads to

$$\sum_Z \frac{1}{\#A_{E,P,Q}} = l(l^2-1)\cdot \#'W_2$$

and (1.13)(b) and (1.12) now imply that

$$l(l^2-1)\cdot \#'W_2 = p + O\left(l^3\sqrt{p}\right).$$

Hence

$$\begin{aligned}
\#'W &= \#'W_1 + \#'W_2 \\
&= \frac{1}{l-1}\left((l-1)\cdot \#'W_1 + (l^2-1)\cdot \#'W_2\right) \\
&\quad - \frac{1}{l^2-1}\left(l(l^2-1)\cdot \#'W_2\right) \\
&= \left(\frac{1}{l-1} - \frac{1}{l^2-1}\right)p + O\left(l\sqrt{p}\right),
\end{aligned}$$

which is the required result. This proves (1.14).

(1.15) PROPOSITION. *There exists a positive effectively computable constant* $c_6$ *such that for all pairs of primes* $p$, $l$ *with* $p > 3$ *we have*

$$\#'\{E\text{: } E \text{ elliptic curve over } \mathbf{F}_p, \#E(\mathbf{F}_p) \not\equiv 0 \bmod l\}/\cong_{\mathbf{F}_p} \geq c_6 p.$$

*Proof.* By (1.14) and (1.4), the left-hand side is $((l-2)/(l-1))p + O(l\sqrt{p})$ if $p \not\equiv 0, 1 \bmod l$ and $((l^2-l-1)/(l^2-1))p + O(l\sqrt{p})$ if $p \equiv 1 \bmod l$. The coefficient at $p$ is at least $1/3$, so if $l \leq c_7\sqrt{p}$ for a suitable positive constant $c_7$ then the proposition is correct.

Applying (1.9)(a) to the set $S = \{s \in \mathbf{Z}: |s-(p+1)| \leq 2\sqrt{p}, s \equiv 0 \bmod l\}$, which has cardinality $O(1 + \sqrt{p} \cdot l^{-1})$, we find that the proposition is also valid if $p \geq c_8$ and $l \geq c_9(\log p)(\log\log p)^2$ for suitable positive constants $c_8, c_9$.

In the remaining cases we have $p < c_8$ or $c_9(\log p)(\log\log p)^2 > c_7\sqrt{p}$, i.e. $p$ is bounded. But for fixed $p$ the proposition is obvious, since by Deuring's formula (see (1.5)) and $H(\Delta) > 0$ (see (1.6)) there are elliptic curves $E_1$, $E_2$ over $\mathbf{F}_p$ with

$$\#E_1(\mathbf{F}_p) = p, \#E_2(\mathbf{F}_p) = p+1,$$

and $l$ is not a divisor of at least one of $p$, $p+1$.

This proves (1.15).

(1.16) PROPOSITION. *There is a positive effectively computable constant* $c_{10}$ *such that for every prime number* $p > 3$ *the following two assertions are valid.*

(a) *If* S *is a set of integers* $s$ *with* $|s-(p+1)| \leq \sqrt{p}$, *then the number of triples* $(a, x, y) \in \mathbf{F}_p^3$ *for which*

$$4a^3 + 27b^2 \neq 0, \#E_{a,b}(\mathbf{F}_p) \in S,$$

*where* $b = y^2 - x^3 - ax$, *is at least* $c_{10}(\#S - 2)p^{5/2}/\log p$.

(b) *If* $l$ *is any prime number, then the number of triples* $(a, x, y) \in \mathbf{F}_p^3$ *for which*

$$4a^3 + 27b^2 \neq 0, \#E_{a,b}(\mathbf{F}_p) \not\equiv 0 \bmod l,$$

*where* $b = y^2 - x^3 - ax$, *is at least* $c_{10}p^3$.

*Proof.* (a) The number to be estimated equals the number of quadruples $(a, b, x, y) \in \mathbf{F}_p^4$ for which $E_{a,b}$ is an elliptic curve over $\mathbf{F}_p$ with $(x : y : 1) \in E_{a,b}(\mathbf{F}_p)$ and $\#E_{a,b}(\mathbf{F}_p) \in S$. Each elliptic curve $E$ over $\mathbf{F}_p$ is isomorphic to $E_{a,b}$ for exactly $(p-1)/\#\mathrm{Aut}\, E$ pairs $(a, b) \in \mathbf{F}_p^2$ (see (1.4)), and each $E_{a,b}$ gives rise to exactly $\#E_{a,b}(\mathbf{F}_p) - 1$ points $(x : y : 1)$. Therefore the number to be

estimated equals

$$\sum \frac{(p-1)\big(\#E(\mathbf{F}_p)-1\big)}{\#\operatorname{Aut} E},$$

the sum ranging over the elliptic curves $E$ over $\mathbf{F}_p$, up to isomorphism, for which $\#E(\mathbf{F}_p) \in S$. Applying Hasse's theorem (see (1.5)) and (1.9)(b) we find that this is at least

$$c_5(p-1)\big(p-2\sqrt{p}\big)(\#S-2)\sqrt{p}/\log p,$$

as required.

(b) This is proved in the same way, with (1.15) instead of (1.9)(b).

This proves (1.16).

## 2. The factoring algorithm

We call a divisor $d$ of a positive integer $n$ *non-trivial* if $1 < d < n$. In this section we describe and analyze an algorithm to find a non-trivial divisor of a positive integer.

(2.1) *Elliptic curves modulo n.* Let $n$ be a positive integer. Consider the set of all triples $(x, y, z) \in (\mathbf{Z}/n\mathbf{Z})^3$ for which $x, y, z$ generate the unit ideal of $\mathbf{Z}/n\mathbf{Z}$. The group of units $(\mathbf{Z}/n\mathbf{Z})^*$ acts on this set by $u(x, y, z) = (ux, uy, uz)$. The orbits under this action are the *points of the projective plane over* $\mathbf{Z}/n\mathbf{Z}$. The orbit of $(x, y, z)$ is denoted by $(x : y : z)$, and the set of all orbits by $\mathbf{P}^2(\mathbf{Z}/n\mathbf{Z})$.

For $a, b \in \mathbf{Z}/n\mathbf{Z}$ we consider the cubic curve $E = E_{a,b}$ defined over $\mathbf{Z}/n\mathbf{Z}$ by the equation

$$y^2 = x^3 + ax + b.$$

The *set of points* $E(\mathbf{Z}/n\mathbf{Z})$ of such a curve over $\mathbf{Z}/n\mathbf{Z}$ is defined by

$$E(\mathbf{Z}/n\mathbf{Z}) = \big\{(x : y : z) \in \mathbf{P}^2(\mathbf{Z}/n\mathbf{Z}) : y^2z = x^3 + axz^2 + bz^3\big\}.$$

If $6(4a^3 + 27b^2) \in (\mathbf{Z}/n\mathbf{Z})^*$ then $E$ is called an *elliptic curve* over $\mathbf{Z}/n\mathbf{Z}$, and in this case the set $E(\mathbf{Z}/n\mathbf{Z})$ has a natural abelian group law; it is defined by formulae that are more general than those in (1.1), cf. [4].

The most convenient way to formulate the factoring algorithm to be presented in this section would make use of the group structure just mentioned. We shall avoid this, because the literature on elliptic curves over rings is not easily accessible. We shall only need the group structure in the case that $n$ is prime (see (1.1)). For general $n$ we shall work with a partially defined "pseudo-addition" on a subset of $E(\mathbf{Z}/n\mathbf{Z})$; cf. [10].

We denote the point $(0:1:0)$ of $\mathbf{P}^2(\mathbf{Z}/n\mathbf{Z})$ by $O$, and we let the subset $V_n$ of $\mathbf{P}^2(\mathbf{Z}/n\mathbf{Z})$ consist of the "finite" points together with $O$:

$$V_n = \{(x:y:1): x, y \in (\mathbf{Z}/n\mathbf{Z})\} \cup \{O\}.$$

For $P \in V_n$ and a prime $p$ dividing $n$ we denote by $P_p$ the point of $\mathbf{P}^2(\mathbf{F}_p)$ obtained by reducing the coordinates of $P$ modulo $p$. Observe that $P_p = O_p$ if and only if $P = O$.

(2.2) *Addition.* We describe an algorithm that given $n \in \mathbf{Z}_{>1}$, $a \in \mathbf{Z}/n\mathbf{Z}$ and $P, Q \in V_n$, *either* calculates a non-trivial divisor $d$ of $n$, *or* determines a point $R \in V_n$ with the following property: if $p$ is any prime dividing $n$ for which there exists $b \in \mathbf{F}_p$ such that

$$6(4\bar{a}^3 + 27b^2) \neq 0 \qquad \text{for } \bar{a} = (a \bmod p),$$
$$P_p \in E_{\bar{a},b}(\mathbf{F}_p), \qquad Q_p \in E_{\bar{a},b}(\mathbf{F}_p),$$

then $R_p = P_p + Q_p$ in the group $E_{\bar{a},b}(\mathbf{F}_p)$.

If $P = O$ put $R = Q$ and stop. If $P \neq O$, $Q = O$ put $R = P$ and stop. In the remaining case $P \neq O$, $Q \neq O$, let $P = (x_1 : y_1 : 1)$ and $Q = (x_2 : y_2 : 1)$. Use the Euclidean algorithm to calculate $\gcd(x_1 - x_2, n)$. If this gcd is not 1 or $n$, call it $d$ and stop. If $\gcd(x_1 - x_2, n) = 1$ then the Euclidean algorithm also gives $(x_1 - x_2)^{-1}$; in this case put

$$\lambda = (y_1 - y_2)(x_1 - x_2)^{-1},$$
$$x_3 = \lambda^2 - x_1 - x_2, \quad y_3 = \lambda(x_1 - x_3) - y_1,$$
$$R = (x_3 : y_3 : 1)$$

and stop. Finally assume that $\gcd(x_1 - x_2, n) = n$, so that $x_1 = x_2$. Calculate $\gcd(y_1 + y_2, n)$. If it is not 1 or $n$, call it $d$ and stop. If it is $n$ (so that $y_1 = -y_2$), put $R = O$ and stop. If $\gcd(y_1 + y_2, n) = 1$, put

$$\lambda = (3x_1^2 + a)(y_1 + y_2)^{-1},$$
$$x_3 = \lambda^2 - x_1 - x_2, \quad y_3 = \lambda(x_1 - x_3) - y_1,$$
$$R = (x_3 : y_3 : 1)$$

and stop. (Notice that in this last case one actually has $y_1 = y_2$ and $P = Q$.) This finishes the description of the algorithm.

The correctness of the algorithm is an immediate consequence of the formulae given in (1.1).

If the algorithm determines a point $R$ with the stated property we shall denote it by $P + Q$, and the partial binary operation on $V_n$ defined in this way

shall be called *addition*. If there exists $b \in \mathbf{Z}/n\mathbf{Z}$ such that

$$6(4a^3 + 27b^2) \in (\mathbf{Z}/n\mathbf{Z})^*,$$
$$P \in E_{a,b}(\mathbf{Z}/n\mathbf{Z}), \quad Q \in E_{a,b}(\mathbf{Z}/n\mathbf{Z}),$$

then $P + Q$, if defined, actually equals the sum of $P$ and $Q$ in the group $E_{a,b}(\mathbf{Z}/n\mathbf{Z})$, but we shall not need this. The only property of addition that we do need is formulated at the beginning of (2.2).

(2.3) *Multiplication.* By repeated addition one readily derives from (2.2) an algorithm that accomplishes the following. Given $k \in \mathbf{Z}_{>0}$, $n \in \mathbf{Z}_{>1}$, $a \in \mathbf{Z}/n\mathbf{Z}$ and $P \in V_n$, it *either* calculates a non-trivial divisor $d$ of $n$, *or* determines a point $R \in V_n$ with the following property: if $p$ is any prime dividing $n$ for which there exists $b \in \mathbf{F}_p$ such that

$$6(4\bar{a}^3 + 27b^2) \neq 0 \quad \text{for } \bar{a} = (a \bmod p),$$
$$P_p \in E_{\bar{a},b}(\mathbf{F}_p),$$

then $R_p = k \cdot P_p$ in the group $E_{\bar{a},b}(\mathbf{F}_p)$.

If this algorithm determines a point $R$ with the stated property we shall denote it by $kP$. We call the partial operation defined in this way *multiplication*.

The number of additions that one has to perform in this algorithm is at most the length of the *addition chain* that is used, see [14, Section 4.6.3]. One can, for example, use an addition chain that is derived from the binary representation of $k$, which has length $O(\log k)$. Whether or not $kP$ is defined may depend on the addition chain that is used (if $n$ is composite). It can be proved that if $kP$ is defined for each of two addition chains, then the two outcomes are the same. Since we do not need this fact we omit the proof.

If $k$ is given as $k = k_1k_2$ for certain positive integers $k_1, k_2$, one can calculate $kP$ by $kP = k_1(k_2P)$.

Suppose now that $k$ is given as a product

$$k = \prod r^{e(r)},$$

where $r$ ranges over a certain finite set of positive integers and each $e(r)$ is a positive integer. Applying the above repeatedly we see that in order to multiply a point $P$ by $k$ it suffices to perform $e(r)$ multiplications by $r$ for each $r$. We shall assume in the sequel that the multiplications by $r$ are performed with $r$ in *increasing* order.

(2.4) *Factoring with one curve.* Let $n, v, w \in \mathbf{Z}_{>1}$ and $a, x, y \in \mathbf{Z}/n\mathbf{Z}$ be given. We describe an algorithm that attempts to find a non-trivial divisor $d$ of $n$.

For each integer $r \geq 2$, denote by $e(r)$ the largest integer $m$ with $r^m \leq v + 2\sqrt{v} + 1$, and put

$$k = \prod_{r=2}^{w} r^{e(r)}.$$

Let $P = (x : y : 1) \in V_n$. Attempt to calculate $kP$ by the method just explained. If this attempt fails then a non-trivial divisor of $n$ is found, and the algorithm halts, with $d$ equal to this divisor. If $kP$ is calculated successfully then the algorithm halts as well, with the message that it has failed to find a non-trivial divisor of $n$. This finishes the description of the algorithm.

In (2.6) below we give a sufficient condition for the algorithm to be successful. The choice of $a, x, y$ determines the elliptic curve that one uses. The number $v$ may be thought of as an upper bound for the divisor $d$ that one is trying to find, although it is by no means guaranteed that indeed $d \leq v$. The parameter $w$ essentially measures the time that is spent on the algorithm (see (2.9)); the probability of success increases with $w$.

(2.5) *Factoring with several curves.* Let $n, v, w, h \in \mathbf{Z}_{>1}$ be given. We describe a probabilistic algorithm that attempts to find a non-trivial divisor $d$ of $n$.

(*) Draw three elements $a, x, y \in \mathbf{Z}/n\mathbf{Z}$ at random, and apply algorithm (2.4) to $n, v, w, a, x, y$. If this results in a non-trivial divisor of $n$, halt, with $d$ equal to this divisor. In the other case, go back to (*), except if algorithm (2.4) has already been applied $h$ times; in this case, report failure and halt.

The number $v$ should again be thought of as an upper bound for the divisor that one is trying to find. The parameter $w$ is basically the time that one is willing to spend on a single curve, and $h$ is the number of curves that one tries. For the success probability of the algorithm, as a function of $w$ and $h$, see (2.8). The optimal choice of $w$ and $h$ is discussed in (2.9).

(2.6) PROPOSITION. *Let $n, v, w \in \mathbf{Z}_{>1}$ and $a, x, y \in \mathbf{Z}/n\mathbf{Z}$ be as in* (2.4), *put $b = y^2 - x^3 - ax \in \mathbf{Z}/n\mathbf{Z}$ and $P = (x : y : 1) \in V_n$ (see* (2.1)). *Suppose that $n$ has prime divisors $p$ and $q$ satisfying the following conditions.*

(i) $p \leq v$;

(ii) $6(4\bar{a}^3 + 27\bar{b}^2) \neq 0$ *for* $\bar{a} = (a \bmod p)$, $\bar{b} = (b \bmod p)$;

(iii) *each prime number $r$ dividing $\#E_{\bar{a},\bar{b}}(\mathbf{F}_p)$ satisfies $r \leq w$;*

(iv) $6(4\hat{a}^3 + 27\hat{b}^2) \neq 0$ *for* $\hat{a} = (a \bmod q)$, $\hat{b} = (b \bmod q)$;

(v) $\#E_{\hat{a},\hat{b}}(\mathbf{F}_q)$ *is not divisible by the largest prime number dividing the order of $P_p$* (*see* (2.1)).

*Then algorithm* (2.4) *is successful in finding a non-trivial divisor of $n$.*

*Remark.* Note that conditions (ii) and (iv) imply that $E_{\bar{a},\bar{b}}(\mathbf{F}_p)$ and $E_{\hat{a},\hat{b}}(\mathbf{F}_q)$ have a group structure. Also, $P_p \neq O_p$ in $E_{\bar{a},\bar{b}}(\mathbf{F}_p)$, so the largest prime number referred to in (v) does exist. Clearly (v) implies that $q \neq p$.

*Proof.* From $p \leq v$ and Hasse's inequality (see (1.5)) it follows that $\#E_{\bar{a},\bar{b}}(\mathbf{F}_p) \leq v + 2\sqrt{v} + 1$; so for each prime number $r$ the exponent of $r$ in $\#E_{\bar{a},\bar{b}}(\mathbf{F}_p)$ is at most the number $e(r)$ defined in (2.4). The same is then true for the exponent of $r$ in the order $\omega$ of $P_p$. Denote by $l$ the largest prime number dividing $\omega$, and by $m$ the exponent of $l$ in $\omega$; so $1 \leq m \leq e(l)$. Put

$$k_0 = \left( \prod_{r=2}^{l-1} r^{e(r)} \right) \cdot l^{m-1};$$

then $k_0 \not\equiv 0 \bmod \omega$ and $k_0 l \equiv 0 \bmod \omega$, so that

$$k_0 P_p \neq O_p, \quad k_0 l P_p = O_p \quad \text{in the group } E_{\bar{a},\bar{b}}(\mathbf{F}_p).$$

From (iii) we see that $l \leq w$; so $k_0$ and $k_0 l$ are divisors of the number $k$ appearing in (2.4). Moreover, if $kP$ is successfully calculated by the algorithm, then $k_0 P$ and $k_0 lP$ are calculated along the way. Hence to prove (2.6) it suffices to show that $k_0 P$ and $k_0 lP$ cannot both be defined. To do this, we use the observation made at the end of (2.1), as follows.

If $k_0 lP \in V_n$ exists, then $(k_0 lP)_p = k_0 l \cdot P_p = O_p$ in the group $E_{\bar{a},\bar{b}}(\mathbf{F}_p)$ and therefore $k_0 lP = O$ in $V_n$; but then $k_0 l \cdot P_q = (k_0 lP)_q = O_q$ in the group $E_{\hat{a},\hat{b}}(\mathbf{F}_q)$; so by (v) we have $k_0 P_q = O_q$ as well. Therefore, if $k_0 P \in V_n$ is also defined, we must have $k_0 P = O$ and hence $k_0 P_p = O_p$, contradicting what we proved above.

This proves (2.6).

(2.7) PROPOSITION. *There exists a positive, effectively computable constant $c_{11}$ with the following property. Let $n, v, w \in \mathbf{Z}_{>1}$ be such that $n$ has at least two distinct prime divisors $> 3$, and such that the smallest prime divisor $p$ of $n$ for which $p > 3$ satisfies $p \leq v$. Put*

$$u = \#\{ s \in \mathbf{Z} : |s - (p+1)| < \sqrt{p}, \text{ and each prime dividing } s \text{ is } \leq w \}.$$

*Then the number $N$ of triples $(a, x, y) \in (\mathbf{Z}/n\mathbf{Z})^3$ for which algorithm (2.4) succeeds in finding a non-trivial divisor of $n$ satisfies*

$$\frac{N}{n^3} > \frac{c_{11}}{\log p} \cdot \frac{u-2}{2\lceil \sqrt{p} \rceil + 1}.$$

*Remark.* The proposition asserts that the probability that a random triple $(a, x, y)$ is successful, which is $N/n^3$, is not much less than the probability that a random integer in the interval $(p + 1 - \sqrt{p}, p + 1 + \sqrt{p})$ has all its prime

divisors $\leq w$; the latter probability is $u/(2[\sqrt{p}\,]+1)$. From the proof and the remark made just before (1.8) it will be clear that under the assumption of the generalized Riemann hypothesis the proposition is also valid with the stronger inequality

$$\frac{N}{n^3} > \frac{c_{11}}{\log\log p} \cdot \frac{u}{2[\sqrt{p}\,]+1}.$$

*Proof.* Let $q$ be a prime divisor $> 3$ of $n$ that is different from $p$. For each positive integer $s$, let $T_s$ be the set of triples $(\alpha, \xi, \eta) \in \mathbf{F}_p^3$ with the property that

$$4\alpha^3 + 27\beta^2 \neq 0, \qquad \#E_{\alpha,\beta}(\mathbf{F}_p) = s,$$

where $\beta = \eta^2 - \xi^3 - \alpha\xi$. For $(\alpha, \xi, \eta) \in T_s$, let the largest prime divisor of the order of the point $(\xi : \eta : 1)$ in the group $E_{\alpha,\beta}(\mathbf{F}_p)$ be denoted by $l_{\alpha\xi\eta}$, and let $U_{\alpha\xi\eta}$ be the set of triples $(\alpha', \xi', \eta') \in \mathbf{F}_q^3$ for which

$$4\alpha'^3 + 27\beta'^2 \neq 0, \quad \#E_{\alpha',\beta'}(\mathbf{F}_q) \text{ is not divisible by } l_{\alpha\xi\eta},$$

where $\beta' = \eta'^2 - \xi'^3 - \alpha'\xi'$. With this notation, Proposition (2.6) implies that

$$N \geq \sum_s \sum_{(\alpha,\xi,\eta)\in T_s} \sum_{(\alpha',\xi',\eta')\in U_{\alpha\xi\eta}} \#V_{\alpha\xi\eta\alpha'\xi'\eta'}$$

where $s$ ranges over the set of positive integers built up from primes $\leq w$ and

$$V_{\alpha\xi\eta\alpha'\xi'\eta'} = \big\{(a, x, y) \in (\mathbf{Z}/n\mathbf{Z})^3 : (a \bmod p, x \bmod p, y \bmod p) = (\alpha, \xi, \eta),$$
$$(a \bmod q, x \bmod q, y \bmod q) = (\alpha', \xi', \eta')\big\}.$$

Clearly each $V_{\alpha\xi\eta\alpha'\xi'\eta'}$ has cardinality $n^3/(pq)^3$, and by (1.16)(b) we have $\#U_{\alpha\xi\eta} \geq c_{10}q^3$. Hence we obtain

$$\frac{N}{n^3} \geq c_{10}\sum_s \frac{\#T_s}{p^3},$$

the sum ranging over the positive integers $s$ built up from primes $\leq w$. Restricting the sum to the integers $s$ that also satisfy $|s - (p+1)| \leq \sqrt{p}$, and applying (1.16)(a), one finds that

$$\frac{N}{n^3} \geq c_{10}^2(u-2)p^{-1/2}/\log p,$$

and the proposition follows.

This proves (2.7).

We now suppose that the random number generator that is used in algorithm (2.5) to draw the triple $(a, x, y) \in (\mathbf{Z}/n\mathbf{Z})^3$ gives each triple with

equal probability, and that the successive calls to the random number generator are independent.

(2.8) COROLLARY. *There exists an effectively computable constant* $c_{12} > 1$ *with the following property. Let* $n, v \in \mathbf{Z}_{>1}$ *be such that* $n$ *has at least two distinct prime divisors* $> 3$, *and such that the smallest prime divisor* $p$ *of* $n$ *for which* $p > 3$ *satisfies* $p \leq v$. *Let further* $w \in \mathbf{Z}_{>1}$ *be such that the number* $u$ *defined by*

$$u = \#\{ s \in \mathbf{Z} : |s - (p+1)| < \sqrt{p}, \text{ and each prime dividing } s \text{ is } \leq w \}$$

*satisfies* $u \geq 3$, *and let* $f(w) = u/(2[\sqrt{p}] + 1)$ *denote the probability that a random integer in the interval* $(p + 1 - \sqrt{p}, p + 1 + \sqrt{p})$ *has all its prime factors* $\leq w$. *Then for any* $h \in \mathbf{Z}_{>1}$ *the success probability of algorithm* (2.5) *on input* $n, v, w, h$ *is at least* $1 - c_{12}^{-hf(w)/\log v}$.

*Proof.* By Proposition (2.7) and the assumptions made just before the corollary, the failure probability of the algorithm equals $(1 - N/n^3)^h$, where

$$\frac{N}{n^3} > \frac{c_{11}}{\log p} \cdot \frac{u-2}{2[\sqrt{p}]+1} \geq \frac{c_{11} f(w)}{3 \log v}.$$

It follows that

$$\left(1 - \frac{N}{n^3}\right)^h \leq e^{-hc_{11}f(w)/(3\log v)}.$$

This proves (2.8).

(2.9) *Efficiency.* Let $M(n)$ denote an upper bound for the time, measured in bit operations, that is needed to perform a single addition as in algorithm (2.2). One can take $M(n) = O((\log n)^2)$ if one uses the ordinary Euclidean algorithm [14, Exercise 4.5.2.30], and a faster version leads to $M(n) = O((\log n)(\log\log n)^2(\log\log\log n))$; see [26].

With this notation, the time required by algorithm (2.4) is $O(w(\log v)M(n))$; this follows from the fact that the number $k$ appearing in (2.4) satisfies $\log k = O(w \log v)$.

The time spent on the factoring algorithm (2.5) is at most $h$ times as large, so is $O(hw(\log v)M(n))$. (This does not count the time that the random number generator may need; it is called at most $h$ times.) Corollary (2.8) shows that in order to have a reasonable chance of success, one should choose the number $h$ of the same order of magnitude as $(\log v)/f(w)$. Hence, to minimize the estimated running time, the number $w$ should be chosen such that $w/f(w)$ is minimal.

At this point we need an unproved conjecture. For a real number $x > e$, define

$$L(x) = e^{\sqrt{\log x \log\log x}}.$$

A theorem of Canfield, Erdös and Pomerance [6, Corollary to Theorem 3.1] implies the following. Let $\alpha$ be a positive real number. Then the probability that a random positive integer $s \leq x$ has all its prime factors $\leq L(x)^{\alpha}$ is $L(x)^{-1/(2\alpha)+o(1)}$, for $x \to \infty$. The conjecture we need is that the same result is valid if $s$ is a random integer in the interval $(x + 1 - \sqrt{x}, x + 1 + \sqrt{x})$. Putting $x = p$ we see that the conjecture implies that

$$f(L(p)^{\alpha}) = L(p)^{-1/(2\alpha)+o(1)} \quad \text{for } p \to \infty,$$

for any fixed positive $\alpha$, with $f$ as in (2.8).

With $w = L(p)^{\alpha}$, the conjecture would imply that

$$w/f(w) = L(p)^{1/(2\alpha)+\alpha+o(1)} \quad \text{for } p \to \infty,$$

which suggests that for the optimal choice of $w$ we have

$$w = L(p)^{1/\sqrt{2}+o(1)}, \quad w/f(w) = L(p)^{\sqrt{2}+o(1)}, \quad \text{for } p \to \infty.$$

A slight practical problem with this choice of $w$ is that $p$, the least prime factor $> 3$ of $n$, is not known beforehand. One can solve this problem by replacing $p$ by $v$ in the above formula for $w$, and performing algorithm (2.5) for a suitable increasing sequence of values for $v$. Notice that the factors $\log v$ in the running time estimate are $L(v)^{o(1)}$.

These arguments lead to the following conjectural running time estimate for the elliptic curve factoring algorithm.

(2.10) CONJECTURE. *There is a function* $K\colon \mathbf{R}_{>0} \to \mathbf{R}_{>0}$ *with*

$$K(x) = e^{\sqrt{(2+o(1))\log x \log\log x}} \quad \textit{for } x \to \infty$$

*such that the following assertion is true. Let* $n \in \mathbf{Z}_{>1}$ *be an integer that is not a prime power and that is not divisible by* 2 *or* 3, *and let* $g$ *be any positive integer. Then algorithm* (2.5), *when applied with suitable values for* $v, w, h$, *can be used to find, with probability at least* $1 - e^{-g}$, *a non-trivial divisor of* $n$ *within time*

$$gK(p)M(n),$$

*where* $p$ *denotes the least prime divisor of* $n$ *and where* $M(n) = O((\log n)^2)$ *or* $O((\log n)(\log\log n)^2(\log\log\log n))$ *is as in* (2.9).

It may be possible to replace the conditions on $n$ in this conjecture by the simpler condition that $n$ be composite; but in any case integers that are divisible by 2 or 3, or that are perfect powers, are easy to recognize directly.

It is not guaranteed that the divisor found by algorithm (2.5) is the smallest prime divisor of $n$, although in practical circumstances this will often be the case.

The algorithm may be repeated on the divisors that are found, until the complete prime factorization of $n$ is obtained. The estimate for the running time will then also contain terms $gK(p')M(n)$ corresponding to the other prime divisors $p'$ of $n$, with the exception of the largest one. In all cases one may expect the total factoring time to be at most $L(n)^{1+o(1)}$ for $n \to \infty$, with $L$ as in (2.9). The worst case occurs if the second largest prime divisor of $n$ is not much smaller than $\sqrt{n}$, so that $n$ is the product of some small primes and two large primes that are of the same order of magnitude.

(2.11) *Comparison to other methods.* We just mentioned that the elliptic curve factoring method may be expected to factor any integer completely in time at most $L(n)^{1+o(1)}$. Several other factoring methods have been proposed for which, conjecturally, the running time is given by the same formula, such as the class group method [23] and the quadratic sieve [18]; see also the discussion in [8]. For these other methods the running time is basically independent of the size of the prime factors of $n$, whereas the elliptic curve method is substantially faster if the second largest prime factor of $n$ is much smaller than $\sqrt{n}$.

The storage requirement of the elliptic curve factoring method is only $O(\log n)$. This is also true for the class group method [23], but all other known factoring algorithms of conjectured speed $L(n)^{1+o(1)}$ have a storage requirement that is a positive power of $L(n)$.

(2.12) *Numbers built up from small prime factors.* The elliptic curve method is particularly efficient in discovering small prime divisors of a number $n$. This means that it can be used for a purpose different from factoring, namely for recognizing numbers that are built up from prime factors below a certain bound. Several factoring methods, such as the continued fraction method, the random squares method of Dixon and the class group method of Seysen (see [18], [27]), need an efficient subroutine for performing this task. The analysis of these methods such as given in [18] assumes that the Pollard $\rho$-method or the Pollard–Strassen method is used for this purpose. Using the elliptic curve method instead improves the theoretical performance of these factoring algorithms. It should be noted that for a rigorous analysis of the elliptic curve method, when applied in this way, much less is needed than the conjecture stated in (2.9). Namely, it suffices to have an average form of a weaker statement,

and this appears to be within reach of the present techniques of analytic number theory; these ideas are developed in [19].

Several practical primality tests depend on large completely factored divisors of certain integers related to the number being tested, see [21], [31]. The elliptic curve method can be used to search for such divisors. It is likely that this will improve the performance of these primality testing algorithms.

(2.13) *Practical performance.* The version of the elliptic curve method described in this paper was designed for simplicity of exposition and ease of analysis. In an actual implementation one might prefer to make several modifications, such as using a different model for elliptic curves, selecting the parameters in a different way, or adding a routine, as in Pollard's original $(p-1)$-method, that enables one to use curves $E_{a,b}$ for which $\#E_{\bar{a}\,\bar{b}}(\mathbf{F}_p)$ is allowed to have one prime factor that is somewhat larger (cf. (2.6)(iii)). For a discussion of these and other points, see [16], [5], [7].

It turns out that, with these modifications, the elliptic curve method is one of the fastest integer factorization methods that is currently used in practice. The quadratic sieve algorithm still seems to perform better on integers that are built up from two prime numbers of the same order of magnitude; such integers are of interest in cryptography [22].

UNIVERSITEIT VAN AMSTERDAM, THE NETHERLANDS
UNIVERSITY OF CALIFORNIA, BERKELEY

## REFERENCES

[1] B J BIRCH, How the number of points of an elliptic curve over a fixed prime field varies, J London Math Soc **43** (1968), 57–60
[2] E BOMBIERI, Counting points on curves over finite fields (d'après S A Stepanov), Sém Bourbaki **25** (1972/73), exp 430, pp 234–241 in Lecture Notes in Math **383**, Springer Verlag, Berlin 1974
[3] Z I BOREVICH and I R SHAFAREVICH, *Teoriya chisel* (Russian), Nauka, Moscow 1964
[4] W BOSMA, Primality testing using elliptic curves, report 85-12, Mathematisch Instituut, Universiteit van Amsterdam 1985
[5] R P BRENT, Some integer factorization algorithms using elliptic curves, research report CMA R32 85, The Australian National University, Canberra 1985
[6] E R CANFIELD, P ERDOS and C POMERANCE, On a problem of Oppenheim concerning "Factorisatio Numerorum", J Number Theory **17** (1983), 1–28
[7] D V CHUDNOVSKY and G V CHUDNOVSKY, Sequences of numbers generated by addition in formal groups and new primality and factorization tests, Advances in Appl Math **7** (1986), 187–237
[8] D COPPERSMITH, A M ODLYZKO and R SCHROEPPEL, Discrete logarithms in GF($p$), Algorithmica **1** (1986), 1–15
[9] M DEURING, Die Typen der Multiplikatorenringe elliptischer Funktionenkorper, Abh Math Sem Hansischen Univ **14** (1941), 197–272

[10] S GOLDWASSER and J KILIAN, Almost all primes can be quickly certified, Proc 18th Annual ACM Symp on Theory of Computing (STOC), Berkeley, May 28–30, 1986, 316–329
[11] G H HARDY and E M WRIGHT, *An Introduction to the Theory of Numbers*, fourth edition, Oxford University Press, Oxford 1960
[12] J IGUSA, Kroneckerian model of fields of elliptic modular functions, Amer J Math **81** (1959), 561–577
[13] N M KATZ and B MAZUR, *Arithmetic Moduli of Elliptic Curves*, Princeton University Press, Princeton 1985
[14] D E KNUTH, *The Art of Computer Programming*, vol 2, *Seminumerical Algorithms*, second edition, Addison-Wesley, Reading, Mass 1981
[15] H W LENSTRA, JR and R TIJDEMAN (eds), *Computational Methods in Number Theory*, Math Centre Tracts **154/155**, Mathematisch Centrum, Amsterdam 1982
[16] P L MONTGOMERY, Speeding the Pollard and elliptic curve methods of factorization, Math Comp **48** (1987), 243–264
[17] J M POLLARD, Theorems on factorization and primality testing, Proc Cambridge Philos Soc **76** (1974), 521–528
[18] C POMERANCE, Analysis and comparison of some integer factoring algorithms, pp 89–139 in [15]
[19] ———, Fast, rigorous factorization and discrete logarithm algorithms, in T Nishizeki, H Wilf (eds), *Discrete Algorithms and Complexity*, Proc Japan–US joint seminar on discrete algorithms and complexity theory, Academic Press, to appear
[20] K PRACHAR, Primzahlverteilung, Grundlehren Math Wiss **91**, Springer-Verlag, Berlin 1957
[21] H RIESEL, *Prime Numbers and Computer Methods for Factorization*, Progr Math **57**, Birkhauser, Boston 1985
[22] R L RIVEST, A SHAMIR and L ADLEMAN, A method for obtaining digital signatures and public-key cryptosystems, Comm ACM **21** (1978), 120–126
[23] C P SCHNORR and H W LENSTRA, JR, A Monte Carlo factoring algorithm with linear storage, Math Comp **43** (1984), 289–311
[24] R J SCHOOF, Elliptic curves over finite fields and the computation of square roots mod $p$, Math Comp **44** (1985), 483–494
[25] ———, Nonsingular plane cubic curves over finite fields, to appear
[26] A SCHONHAGE, Schnelle Berechnung von Kettenbruchentwicklungen, Acta Inform **1** (1971), 139–144
[27] M SEYSEN, A probabilistic factorisation algorithm with quadratic forms of negative discriminant, Math Comp **48** (1987), 757–780
[28] G SHIMURA, *Introduction to the Arithmetic Theory of Automorphic Functions*, Publ Math Soc Japan **11**, Iwanami Shoten, Publishers Tokyo, Princeton University Press, Princeton 1971
[29] J J SILVERMAN, *The Arithmetic of Elliptic Curves*, Graduate Texts in Math **106**, Springer Verlag, New York 1986
[30] W C WATERHOUSE, Abelian varieties over finite fields, Ann Sci Ecole Norm Sup (4) **2** (1969), 521–560
[31] H C WILLIAMS, Primality testing on a computer, Ars Combin **5** (1978), 127–185

(Received September 25, 1986)