ADVANCES IN APPLIED MATHEMATICS 7, 385–434

Sequences of Numbers Generated by Addition in Formal Groups and New Primality and Factorization Tests

D. V. CHUDNOVSKY AND G. V. CHUDNOVSKY

Department of Mathematics, Columbia University, New York, New York 10027

One can associate with an arbitrary algebroid formal group law F, defined over $\mathbb{F}_p$, a sequence $[n]_F(\bar{x})$ $(=[n-1]_F(\bar{x}) \oplus_F \bar{x})$. These sequences for various F (multiplicative group, reduced elliptic curves and Abelian varieties) provide a variety of new primality tests like Lucas' test for Mersenne primes. Implementations and relations with factorization algorithms are presented.

The problem of distinguishing prime numbers from composite numbers and of resolving the latter into prime factors is known to be one of the most important and useful in arithmetic. It has engaged the industry and wisdom of ancient and modern geometers to such an extent that it would be superfluous to discuss the problem at length. Nevertheless we must confess that all methods that have been proposed thus far are either restricted to very special cases or are so laborious and prolix that even for numbers that do not exceed the limits of tables constructed by estimable men, i.e., for the numbers that do not yield to artificial methods, they try the patience of even the practiced calculator. And these methods do not apply at all to larger numbers. C. F. Gauss, "Disquisitiones Arithmeticae" [GA1]

1. INTRODUCTION

This quotation from Gauss [GA1, PO1] is enough of a justification (if any, in addition to various "applied" problems, is necessary) to devote oneself to divising various primality and factorization tests. Our interest in primality arose as a result of out work in formal groups in diophantine geometry [CH1]–[CH3]. While studying the properties of algebraic laws of addition [CH1, CH4] and integral formal groups associated with them, we realized that the properties of Frobenius map on formal groups mod p can serve as a primality test, generalizing various primality tests based on a converse to the Little Fermat theorem. Essentially, one tries to substitute multiplicative properties of integers by the properties of various formal groups mod n or mod p. The key testing sequence in our approach, is a sequence $\tilde{x}_n = [n]_{\bar{F}}(\tilde{x}_1)$ $(\tilde{x}_{n-1} \oplus_{\bar{F}} \tilde{x}_1)$ obtained by applications of endo-

0196-8858/86 $7.50

morphisms $[n]_{\bar{F}}(\cdot)$ of the formal group $\bar{F}$ ("a multiplication by n" endomorphism). In the simplest cases of various formal groups—multiplicative groups mod p—one recovers standard powers x^n or, say, Lucas sequences $U_n \bmod p$. In these notations the Little Fermat theorem becomes "the law of apparition": the order $\tau(p)$ of $\tilde{x}_1 \bmod p$ in the sequence $\tilde{x}_n$ is a divisor of the value $N_p = P(1)$ of the characteristic polynomial $P(x)$ of the Frobenious map F_p: $x_i \to x_i^p$ of $\bar{F}$ at $x = 1$ (i.e., $\tilde{x}_m \equiv \tilde{0} \bmod p$ iff $\tau(p) | m$). We refer to Section 1 for the discussion of this law of apparition for formal groups $\bar{F}$ arising from commutative algebraic groups (Abelian varieties and their extensions). As it turns out in Section 2, this law of apparition provides with a wide variety of primality tests for "suspect" n to be a prime, whenever various expressions $n^{\pm}$ cooked up from n using various algebraic group laws $\bar{F}$ are (completed or partially) factorizable. This method, that we tested for various elliptic curves and Abelian varieties with complex multiplication, is an extension of Lucas–Lehmer primality tests, where the primality of (a prime) n was proved whenever the complete factorization of $n + 1$ or $n - 1$ was known. Such $n \pm 1$ primality tests were developed by Brillhart, Lehmer, and Selfridge [BLS], building on earlier work of Lucas [LU1, LU2], Lehmer [LH1], Pocklington [POCK], and Proth [PRO]. The famous application of $n + 1$ primality test is the Lucas–Lehmer primality test for Mersenne numbers $M_p = 2^p - 1$: M_p is prime iff in the sequence $L_0 = 4$, $L_{n+1} = (L_n^2 - 2) \bmod M_p$, we have $L_{p-2} = 0$. These $n \pm 1$ tests were further extended by Williams, Judd, and Holte [WJ, WH] for tests involving partial factorization of $n^2 + 1$, $n^2 \pm n + 1$ and, in general, $\psi_q(n)$ for a cyclotomic polynomial ψ_q. Our "$n^{\pm}$" tests for primality of n include, for example, the test of primality of n of the form $n^2 = a^2 + D \cdot b^2$, is based on the knowledge of the (partial) factorization of $n^{\pm} = (a - 1)^2 + D \cdot b^2$. Higher dimensional CM-varieties yield primality test for number n, for which the (partial) factorization of $n^a \pm n^b + 1$ is known, for arbitrary integers $a > b$. These tests were applied to the sequences of numbers $s_m = \mathrm{Norm}_{K/\mathbb{Q}}(\alpha_0 \alpha_1^m + 1)$ with α_0, α_1 from an imaginary quadratic field $K = \mathbb{Q}(\sqrt{-D})$, that can be considered as algebraic generalizations of familiar numbers $ab^m \pm 1$ targeted for $n \pm 1$ primality tests. In Tables 1 and 2 (see explanations at the end of Section 2) we present primes of the form s_m for a few small D and α_0, α_1 having norms not exceeding 10.

Perhaps now it is the time to review briefly the existing primality and factorization algorithms [PO1, PO2, LE1, K1]. Among primality test based on the converse to the ordinary Little Fermat theorem, the most powerful test of primality, polynomial in n, is Miller's test [MI1, LE2] based on the assumption of the extended Riemann hypothesis for all Dirichlet L-functions. Another polynomial test is the probabilistic compositeness test [RA1] that "guarantees" primality with the probability $\geq 1 - \varepsilon$ for $\varepsilon > 0$. Finally, there is Adleman, Rumely, Pomerance, and Lenstra primality test

[PO1], [LE1], whose running time is $O((\log n)^{c \log\log\log n})$. Often $n \pm 1$ primality tests are significantly better, especially for particular n. Our $n^{\pm}$ tests are efficient for all n. In particular, one can use them as a sieve for a large list of curves mod n with complex multiplications to prove the primality of a "probable prime" n for large n. Factorization algorithms are considerably slower. The simplest among them is Pollard's ρ-method [POL1] (with the running time $O(\sqrt{p})$ for a divisor p of n). More sophisticated methods consist of Morrison–Brillharts's continued fraction methods [MB1], Dixon's method [DIX1], a linear sieve method (Schroeppel) and the quadratic sieve method (Pomerance). The running time of these methods is estimated in [PO2] and is $O(\exp(c\sqrt{\log n \log\log n}))$ for (various) $c > 1$. Similar to $n \pm 1$ primality tests, there were proposed $p - 1$ (Pollard [POL2]) and then $p + 1$ (Williams [WIL1], Guy and Conway [Guy]) factorization methods based on the (possible) factorization of $p \pm 1$ into a product of primes significantly smaller than the number n, whose prime factor p we want to find. Very recently, Lenstra (see [ML1]) has proposed a probabilistic algorithm generalizing the $p \pm 1$ method and based on the high probability of finding a random elliptic curve mod p with the number of points $N_p = p + 1 - a_p$ having prime factors small compared to p. The running time of Lenstra's algorithm was estimated as $\exp((1 + o(1))\sqrt{\log n \log\log n})$. Meanwhile the record of the most wanted factorizations (up to 71 digits) belongs to Davis and Holdridge [DH1], who used the quadratic sieve on the Cray 1S.

This paper is written in an elementary and expository way, and we do not assume anything but the basic knowledge of number theory and geometry. This particularly concerns all the references to elliptic curves and Abelian varieties, where all explicit formulas are presented. Our main purpose is to present new methods for primality testing and generation of big prime numbers, and to discuss new versions of factorization methods.

In Section 1 we discuss one of the forms of the Little Fermat theorem as applied to the sequences $\tilde{x}_n$ generated by the endomorphisms $[n]_{\bar{F}}(\cdot)$ of the formal group $\bar{F}$ mod p of an algebraic law of addition. In Section 3 we consider a more general sequence $\tilde{x}_\mu = [\mu]_{\bar{F}}(\tilde{x}_1)$ for $\mu \in \mathrm{End}(\bar{F})$. The properties of $\tilde{x}_m$ are applied in Section 2 in the construction of our new primality tests of numbers $n = \mathrm{Norm}_{K/\mathbf{Q}}(\alpha)$, depending on the (partial) factorization of $n^{\pm} = \mathrm{Norm}_{K/\mathbf{Q}}(\alpha \pm 1)$. These tests were in fact applied to various sequences s_m. In Section 3 we discuss arithmetic properties of the sequences $\tilde{x}_m$ themselves, in particular, of the elliptic divisibility sequences introduced by Lucas [B1] and studied by Ward [W1]. We think that these elliptic divisibility sequences ψ_m and their generalizations provide with an interesting method of generating of very large primes, for ψ_m grow as $c^{m^2(1+o(1))}$ with $c > 1$. Some large probable primes among ψ_m are presented in the Table 3.

In Section 4 we present results of our studies of various forms of laws of addition for different models of elliptic curves and of their relative complexities. In Section 5 an implementation of a version of Lensta's elliptic generalization of $p \pm 1$ factorization methods is presented, and recipes for various parameters and expected running time is presented. In Section 6 Abelian varieties and Jacobians of curves of $g > 1$ are discussed. We present some explicit formulas for addition of points on Abelian surfaces and we discuss the importance of curves with $g > 1$ for speeding up the primality and factorization algorithms. An old problem of ours [CH5] on the isogeny of the Jacobian of generic elliptic curves pops up here.[1]

1. Algebraic Group Laws

It is convenient to use the language of commutative formal groups, providing an easy invariant description of various algebraic group structures.

Definition 1.1. Let A be a commutative ring. A commutative g-dimensional group law over A is (given by) a g-tuple $\bar{F}(\bar{x}, \bar{y}) = (F_1(\bar{x}, \bar{y}), \ldots, F_g(\bar{x}, \bar{y}))$ of formal power series in $2g$ variables $\bar{x} = (x_1, \ldots, x_g)$ and $\bar{y} = (y_1, \ldots, y_g)$ such that

(1) $F_i(\bar{x}, 0) \equiv F_i(\bar{0}, \bar{x}) \equiv x_i$;

(2) $\bar{F}(\bar{x}, \bar{y}) \equiv \bar{F}(\bar{y}, \bar{x})$ (commutativity);

(3) $\bar{F}(\bar{x}, \bar{F}(\bar{y}, \bar{z})) \equiv \bar{F}(\bar{F}(\bar{x}, \bar{y}), \bar{z})$ (associativity);

(4) $\bar{F}(\bar{x}, \bar{y}) \in A[[\bar{x}, \bar{y}]]^g$ (group laws are defined over A).

It follows from (1) that $F_i(\bar{x}, \bar{y}) = x_i + y_i$ (mod terms of degree 2 in $(\bar{x}, \bar{y})$).

Two g-dimensional group laws $\bar{F}$ and $\bar{G}$ over A are strongly isomorphic over A, if there exists a g-tuple $\bar{f}(\bar{x}) \in A[[\bar{x}]]^g$ of power series such that

$$\bar{f}(\bar{x}) = \bar{x} \text{ (mod terms of degree 2 in } \bar{x})$$

and

$$\bar{f}(\bar{F}(\bar{x}, \bar{y})) \equiv \bar{G}(\bar{f}(\bar{x}), \bar{f}(\bar{y})).$$

[1] *Note added in proof.* Lenstra presented a detailed description of his algorithm in "Factoring integers with elliptic curves," 1986 (to appear).

All interesting (from the point of view of this paper) examples of formal group law arise from commutative algebraic groups. Here are a few relevant examples in the one-dimensional case:

EXAMPLES 1.2. (1) The additive formal group law

$$F_a(x, y) = x + y;$$

(2) The multiplicative formal group law

$$F_{\sqrt{D}}(x, y) = x + y + \sqrt{D} \cdot x \cdot y.$$

This law arises from the multiplication rule

$$\left(1 + \sqrt{D} \cdot F_{\sqrt{D}}\right) \equiv \left(1 + \sqrt{D} \cdot x\right) \cdot \left(1 + \sqrt{D} \cdot y\right);$$

(3) The circular formal group law:

$$F(x, y) = \frac{x + y}{1 + xy},$$

where $F(x, y) = \tanh(w + v)$ for $x = \tanh(v)$, $y = \tanh(w)$;

(4) The addition law for the lemniscate elliptic curve (an elliptic curve with complex multiplication by $i = \sqrt{-1}$):

$$v^2 = 1 - u^4,$$

$$F(x, y) = \frac{x\sqrt{1 - y^4} + y\sqrt{1 - x^4}}{1 + x^2y^2}.$$

The most interesting examples of commutative group laws with algebraic integral coefficients ($\mathbb{Z}$ for 1.2, (1), (3); $\mathbb{Z}[\frac{1}{2}]$ for 1.2 (4) and $\mathbb{Z}[\sqrt{D}]$ for 1.2 (2)) arise in the cases when

$$F_i(\bar{x}, \bar{y}) \text{ are algebraic functions of } \bar{x} \text{ and } \bar{y}.$$

In these cases the Eisenstein theorem guarantees that only a finite number of primes divide the denominators of coefficients of the expansions of $\bar{F}(\bar{x}, \bar{y})$.

In our works [CH4] and [CH1], we described the algebraic laws of addition, corresponding to algebraic power series $F_i(\bar{x}, \bar{y})$. After a proper normalization, the algebraic law of addition can be represented in the following form:

DEFINITION 1.3 ([CH1, 3.1]). Let K be an algebraic number field. Assume that the formal group law $\bar{F}(\bar{x}, \bar{y})$ is an algebraic function over $K(\bar{x}, \bar{y})$. This means that there exists an algebraic equation defining x_0 as a

function of $\bar{x}$: $q(x_0, \bar{x}) = 0$ and similarly defining y_0 as a function of $\bar{y}$: $q(y_0, \bar{y}) = 0$ such that $q(x_0, \bar{x})$ is a polynomial from $K[x_0, \bar{x}]$ with integral coefficients and the Taylor expansion of the branch $x_0 = x_0(\bar{x})$ of the root x_0 of $q(x_0, \bar{x}) = 0$ with the initial condition $x_0(\bar{0}) = 0$ in powers of $\bar{x}$ (near $\bar{x} = \bar{0}$) has integral coefficients from K. Let us denote $\tilde{x} = (x_0, \bar{x})$ $(= (x_0, x_1, \ldots, x_g))$ and $\tilde{y} = (y_0, \bar{y})$ $(= (y_0, y_1, \ldots, y_g))$. Then near $\tilde{x} = \tilde{0}$ and $\tilde{y} = \tilde{0}$ we have

$$\bar{F}(\bar{x}, \bar{y}) = \frac{\bar{P}(\tilde{x}, \tilde{y})}{Q(\tilde{x}, \tilde{y})},$$

(with $x_0 = x_0(\bar{x})$, $y_0 = y_0(\bar{y})$), where $\bar{P}(\tilde{x}, \tilde{y}) = (P_1(\tilde{x}, \tilde{y}), \ldots, P_g(\tilde{x}, \tilde{y}))$ and $Q(\tilde{x}, \tilde{y})$ are polynomials in $2(g + 1)$ variables $\tilde{x}$ and $\tilde{y}$ from $K[\tilde{x}, \tilde{y}]$ with integral coefficients.

Consequently, we can define a formal group law $\bar{F}$ in the *rational form* as a function of $2(g + 1)$ variables $\tilde{x} = (x_0, x_1, \ldots, x_g)$ and $\tilde{y} = (y_0, y_1, \ldots, y_g)$:

$$\tilde{x} \oplus_F \tilde{y} = \frac{\tilde{P}(\tilde{x}, \tilde{y})}{Q(\tilde{x}, \tilde{y})} \tag{1.1}$$

for polynomials $\tilde{P} = (P_0, P_1, \ldots, P_g)$ and Q in $K[\tilde{x}, \tilde{y}]$ with integral coefficients. Our normalization implies $Q(\tilde{0}, \tilde{0}) = 0$.

Introducing homogeneous coordinates, the law of addition (1.1) can be represented in the homogeneous *polynomial form*. As a function of $2(g + 2)$ variables $X = (x_0, x_1, \ldots, x_g, x_{g+1})$, $Y = (y_0, y_1, \ldots, y_g, y_{g+1})$, the law of addition (1.1) can be written as

$$X \oplus_F Y = \big(P_0(X, Y), \ldots, P_g(X, Y), Q(X, Y)\big). \tag{1.2}$$

According to Weil and Serre (see [SE1, W5]) all algebraic commutative group laws arise from the parametrization of "generalized Abelian varieties" which are, simple enough, Abelian varieties, or extensions of Abelian varieties by linear groups.

For example, 1-dimensional algebraic group laws are strictly isomorphic either to elliptic curve group laws, or their degenerations: multiplicative or additive group laws. Similarly, 2-dimensional algebraic group laws are strictly isomorphic either to group laws of 2-dimensional Abelian varieties (the general case) or to their degenerations: extensions of elliptic curves by multiplicative or additive groups, or products of two elliptic curves, multiplicative or additive groups.

Most of the properties of Abelian varieties mod p are reflected in their group laws structure, and are invariant under (a strict) isomorphism. That is

why it is important to have a simple criterion of a (strict) isomorphism between two Abelian varieties mod p. Such criteria exist in 1-dimensional case (Honda [H2]), and in g-dimensional case one has to be satisfied with the isogeny criterion of Tate [T1, T2]:

THEOREM 1.4 [T1, T2]. *g-dimensional Abelian varieties over $\mathbb{F}_q$ are isogenous (in particular, have the same number of points over $\mathbb{F}_q$) over $\mathbb{F}_q$, if and only if the characteristic polynomials of Frobenius map F_q: $x_i \to x_i^q$ of these Abelian varieties coincide.*

According to Honda–Tate results [T2, H1], a class of characteristic polynomials of the Frobenius F_q for all g-dimensional Abelian varieties over $\mathbb{F}_q$ coincides with the class of polynomials $P_{2g}(x) \in \mathbb{Z}[x]$ with the leading coefficient one, degree $2g$, and the property

$$|\alpha_i| = \sqrt{q}$$

for any root α_i of $P_{2g}(x) = 0$.

Given a characteristic polynomial $P_{2g}(x) = \prod_{i=1}^{2g}(x - \alpha_i)$ of a g-dimensional Abelian variety A_g over $\mathbb{F}_p$, we conclude that the number of points on $A_g/\mathbb{F}_p$ is $P_{2g}(1) = \prod_{i=1}^{2g}(\alpha_i - 1)$. Moreover, since $A_g/\mathbb{F}_p$ is a group, the order of every element of $A_g/\mathbb{F}_p$ divides $P_{2g}(1)$ as well. (We note that if $\mathbb{F}_p$ is substituted by $\mathbb{F}_{p^a}$, then α_i is substituted by α_i^a).

The order (or, at least, the number of elements in the group variety over $\mathbb{F}_q$) of an element of a group variety over $\mathbb{F}_q$ is relevant for primality and factorization algorithms. A key testing sequence associated with a given group law $\bar{F}$ is defined as a sequence of natural endomorphisms of $\bar{F}$:

$$[0]_F(\bar{x}) = \bar{0};$$
$$[n]_F(\bar{x}) = \bar{F}([n-1]_F(\bar{x}), \bar{x}) : n \geq 1.$$

Whenever $\bar{F}$ is an algebraic group law, the sequence of endomorphisms $[n]_F$ defines a sequence of $(g+1)$-tuples

$$\tilde{x}_n \overset{\text{def}}{=} [n]_F(\tilde{x}); \qquad \tilde{x}_1 = \tilde{x}$$

starting from an arbitrary point $\tilde{x}$ on (a model of) algebraic group variety (in the affine form). The sequence $\tilde{x}_n$: $n = 0, 1, 2, \ldots$, is defined recursively by means of rational expressions. If it is preferable to avoid the division (as it is prudent in mod p arithmetic), the homogeneous polynomial form of a group law can be used:

$$X_n = [n]_F(X), \qquad X_1 = X$$

for $(g + 2)$-tuples, generating a sequence of points on a (projective model of an) algebraic group variety.

The sequences $\tilde{x}_n$ or X_n provide the following version of the Fermat's Little theorem which is a basis of primality and factorization algorithms. We use the terminology common in the theory of recurrent sequences, particularly those defined by linear recurrences with constant coefficients. For a sequence W_m, it is common to call the "rank of apparition of p" of W_m an integer $\tau(p)$ (if it exists), such that

$$W_m = 0 \bmod p$$

if and only if $\tau(p)|m$.

We naturally extend this notion to the sequences $\tilde{x}_m$ and X_m. Then the Little Fermat theorem can be reformulated as follows:

FERMAT THEOREM 1.5. *Let an algebraic group A be defined over $\mathbb{F}_q$ (e.g., is a reduction of an algebraic group scheme defined over $\mathbb{Z}[1/N]$ for $(N, p) = 1$) and let $P(x) = x^e + a_1 x^{e-1} + \cdots + a_e$ be the characteristic polynomial of the Frobenious endomorphism F_q of A (e.g., $p|a_e$). Then the rank of apparition of p exists for any sequence $\tilde{x}_m$ and X_m in $A/\mathbb{F}_q$, and this rank, $\tau(p)$, divides $P(1)$. I.e.,*

$$\tilde{x}_m = \tilde{0} \qquad \text{in } A/\mathbb{F}_q$$

or

$$X_m = \bar{\bar{0}} \qquad \text{in } A/\mathbb{F}_g$$

if and only if

$$\tau(p)|m$$

for $\tau(p)|P(1)$.

Here $\tilde{0}$ (or $\bar{\bar{0}}$) is a neutral (zero) element of $A/\mathbb{F}_q$; with a proper normalization of Definition 1.3 it is

$$\underbrace{(0,\ldots,0)}_{g+1} \left(\text{or } \underbrace{(0,\ldots,0,1)}_{g+1}\right).$$

The quantity $P(1)$, usually denoted by N_q $(= N_q(A))$, is the crucial arithmetic invariant of $A/\mathbb{F}_q$. Known as "the number of points on $A/\mathbb{F}_q$," this quantity enters the definition of ζ-function of A. See [W6, Ka1] for detailed references on this subject, with an obvious simplification due to the fact that A is an Abelian variety, not an arbitrary algebraic.

The Fermat theorem 1.5 is a consequence of the following identity, satisfied by the Frobenius $F = F_q$ of A:

$$P(F) = F^e + a_1 F^{e-1} + \cdots + a_e \cdot I. \tag{1.3}$$

In fact, (1.3) is a functorial identity satisfied in a formal group of A (see [Ka1]).

A few examples are in order. They are: (1) a standard multiplicative group G_m: $F_m(x, y) = x + y + xy$; (2) a multiplicative group $F_{\sqrt{D}}$ over $\mathbb{Z}[\sqrt{D}]$, and (3) an arbitrary Abelian variety of CM-type.

EXAMPLES 1.6. (1) $x^{p-1} \equiv 1 \bmod p$ for any $x \bmod p$, $x \not\equiv 0 \bmod p$.

(2) Let P, Q be rational integers, such that $D = p^2 - 4Q$, and let the Lucas sequence U_n be defined as $U_n = (\alpha^n - \beta^n)/(\alpha - \beta)$ for roots α, β of $x^2 - Px + Q = 0$. Then for $(p, 2QD) = 1$, we have

$$U_{p-(D/p)} \equiv 0 \bmod p$$

where (D/p) denotes a Jacobi symbol.

(3) Let K be a CM-field, i.e., an imaginary quadratic extension of a totally real field, $[K : \mathbb{Q}] = 2g$. Let α be an element of K such that $|\alpha^{(i)}| = \sqrt{p}$ for all $\alpha^{(i)}$, conjugate to α.

Then, as we saw above, there exists an Abelian variety A over $\mathbb{F}_p$ such that the characteristic polynomial $P_{2g}(x)$ of F_p on A coincides with $\prod_{i=1}^{2g}(x - \alpha^{(i)})$. Then for an arbitrary sequence $\tilde{x}_m$ (or X_m) on A we have

$$\tilde{x}_{\mathrm{Norm}(\alpha-1)} \equiv \tilde{0} \bmod p$$

or

$$X_{\mathrm{Norm}(\alpha-1)} \equiv \bar{\bar{0}} \bmod p.$$

Here $\mathrm{Norm}(\alpha) = p^g$.

In fact, case (3) covers all elliptic curves over $\mathbb{F}_p$, since elliptic curves over finite fields always have a complex multiplication [H1].

For the sake of completeness and future references, let E be an elliptic curve over $\mathbb{F}_p$ (a 1-dimensional algebraic group variety) and $p \neq 2, 3$. The characteristic polynomial of F_p on E is a quadratic one:

$$P_2(x) = x^2 - a_p x + p,$$

where

$$-2\sqrt{p} < a_p < 2\sqrt{p}.$$

Then, starting from an arbitrary point $\tilde{x}$ on E (an affine model) or X (a projective model) on E, we obtain

$$\tilde{x}_n \equiv \tilde{0} \bmod p$$

or

$$X_n \equiv \bar{\bar{0}} \bmod p$$

whenever

$$(p + 1 - a_p) | n.$$

For example, if E is given in the standard form $y^2 = x^3 + a_2x^2 + a_1x + a_0$ $(= P_3(x))$ or $v^2 = u^4 + b_3u^3 + b_2u^2 + b_1u + b_0$ $(= P_4(u))$, and for $p \neq 2, 3$ this is the most general form of an elliptic curve,

$$N_p \left(= N_p(E)\right) \stackrel{\text{def}}{=} p + 1 - a_p$$

is the number of points E mod p. (This is the same as the number of solutions of the congruences of the homogeneous forms of $y^2 = P_3(x) \bmod p$, or $v^2 = P_4(u) \bmod p$.)

Various models (forms of the equations) of elliptic curves are discussed below. We present now one such model, where the expression for a_p has a familiar form [Cl1].

Let us assume that an equation defining E is reduced to the Legendre form E_λ: $y^2 = x(x - 1)(x - \lambda)$. Then a_p $(\stackrel{\text{def}}{=} a_p(\lambda))$ is $(-1)^{(p-1)/2} \cdot P_{(p-1)/2}(\lambda) \bmod p$, where $P_n(\lambda) = \Sigma_{m=0}^{n} \binom{n}{m}^2 \lambda^m$ is a (normalized) Legendre polynomial.

We remark, that every elliptic curve having 4 points of order two, defined over $\mathbb{F}_p$, can be reduced to the form E_λ for some $\lambda \bmod p$, $\lambda \neq 0, 1$.

The Little Fermat theorem for elliptic curves E_λ can be restated as follows: In the projective form, for a point

$$\tilde{x} = (x, y) = \left(\frac{X}{Z^2}, \frac{Y}{Z^3}\right)$$

on E_λ, let

$$\tilde{x}_m = [m]_{E_\lambda}(\tilde{x}) = \left(\frac{X_m}{Z_m^2}, \frac{Y_m}{Z_m^3}\right).$$

Then

$$Z_m \equiv 0 \bmod p$$

for all m, divisible by $(p + 1 - a_p(\lambda))/4$ (which is an integer).

2. Primality Tests and Their Elliptic Generalizations

Little Fermat's theorem is the most efficient primality test. Say, the congruence

$$3^{n-1} \equiv 1 \bmod n \tag{2.1}$$

is a necessary condition for $n > 3$ to ba a prime. As Knuth [K1] notes, (2.1)

is also an efficient "practically sufficient" condition of primality of n, having no small factors (though there are infinitely many composite n satisfying (2.1)).

It was known for some time that the knowledge of a complete factorization of $n-1$ is sufficient to *prove* the primality of n [BLS, LU1]:

PROPOSITION 2.1 (Selfridge [BS1]). *If, for every prime divisor p of $n-1$ there exist x_p such that $x_p^{n-1} \equiv 1 \bmod n$ but $x_p^{(n-1)/p} \not\equiv 1 \bmod n$, then n is prime.*

In fact, only a partial factorization of $n-1$ is necessary. For example, we have

PROPOSITION 2.2 (Pocklington [POCK, BLS]). *Let $n-1 = F_1 \cdot R_1$, where $F_1 > \sqrt{n}$. If, for every divisor p of F_1 there exists x_p such that $x_p^{n-1} \equiv 1 \bmod N$ and $(x_p^{(n-1)/p} - 1, n) = 1$, then n is prime.*

In practice these tests are excellent, especially when n is of the form $n = a \cdot b^m + 1$. The most famous is

PROPOSITION 2.3 (Proth [PRO], 1878). *Let $n = k \cdot 2^m + 1$, where $k < 2^m$. If $3 \nmid k$, then n is prime if and only if $3^{(n-1)/2} \equiv -1 \bmod n$. If $3|k$, then choose a such that $(a/n) = -1$. n is prime if and only if $a^{(n-1)/2} \equiv -1 \bmod n$.*

Lucas (see [LU2]) was the first to use (Lucasian) sequences U_m to formulate primality criteria of n, whenever the factorization of $n+1$ is known. Of course, in this case to satisfy the requirements of the Little Ferman theorem (Examples 1.6(2)), the discriminant D of the multiplicative group has to satisfy

$$(D/n) = -1.$$

Even the partial factorization of $n+1$ suffices:

PROPOSITION 2.4 (Brillhart, Lehmer, Selfridge [BLS]). *Let $n+1 = F_2 \cdot R_2$ and $F_2 > \sqrt{n}+1$. If, for each prime p, dividing F_2 there exists a Lucas' sequence $\{U_m^{(p)}\}$ with discriminant D, for which $(D/n) = -1$, $n|U_{n+1}^{(p)}$ and $(U_{(n+1)/p}^{(p)}, n) = 1$, then n is prime.*

The most famous example of this approach is the Lucas–Lehmer criterion of primality of Mersenne numbers $M_p = 2^p - 1$:

PROPOSITION 2.5 (Lucas and Lehmer [LU1, LH1]). *Let in the definition of Lucas' sequence $P = 4$, $Q = 1$. Then M_p is prime if and only if $U_{2^{p-1}} \equiv \bmod M_p$.*

The Lucas–Lehmer criterion is attractive particularly because to compute $U_{2^{p-1}} \bmod M_p$ one needs only p multiplications (not 2^{p-1}). This is typical

for *any* algebraic group law because $[2^m]_F(x)$ can be computed in m iterations of $[2]_F(\cdot)$ (see below). Using the duplication formulas (applied to the multiplicative group law $F_{\sqrt{D}}$), the Lucas–Lehmer criterion is usually restated as follows:

COROLLARY 2.6 [LH1, BLSTW]. *Let* $L_0 = 4$, $L_{n+1} = (L_n^2 - 2) \bmod M_p$. *Then* M_p $(= 2^p - 1)$ *is prime if and only if* $L_{p-2} = 0$.

Similar criteria of primality were developed by Lehmer [LH2], Riesel [Ri1], Inkeri [IN1], Williams [WIL2, BLSTW] for numbers $a \cdot b^m - 1$ for $b = 2, 3$, and by Williams [WIL3] for some numbers of the form $a_2 \cdot b^{2m} + a_1 \cdot b^m - 1$.

Since the factorization of $n \pm 1$ is useful in the proof of primality of n, Brillhart, Lehmer, and Selfridge [BLS, BLSTW] proposed a test that uses partial factorization of $n + 1$ and $n - 1$. Later Williams *et al.* [WH, WJ] proposed a series of tests for primality of n, when factorization of

$$n^2 + 1, \qquad n^2 \pm n + 1, \qquad (n^5 \pm 1)/(n \pm 1)$$

is known (see also [BS]).

The corresponding analogs of the Little Fermats's theorem and its converses in these cases correspond to the degenerate Abelian varieties of CM type associated with cyclotomic fields.

Let us now present elliptic versions of "$n \pm 1$" criterion of primality of n, generalizing Lucas–Lehmer criteria. These criteria were the starting point in our investigation of formal group algorithms in November of 1984 [CH1].

The principle of these algorithms is the following. Let n be a norm of an integer from an imaginary quadratic field $K = \mathbb{Q}(\sqrt{-D})$, $D > 0$:

$$n = \mathrm{Norm}_{K/\mathbb{Q}}(\alpha). \tag{2.2}$$

Then the knowledge of the (complete or partial) factorization of the following numbers:

$$n^{\pm} = \mathrm{Norm}_{K/\mathbb{Q}}(\alpha \pm 1) \tag{2.3}$$

determines the primality of n. The tests uses the Little Fermat theorem for the formal completion of the elliptic curve, having complex multiplication in K. Let E be an elliptic curve over $\mathbb{F}_p$, having complex multiplications in K. This means, according to the discussion above, that eigenvalues α of Frobenius F_p of E are algebraic integers from K, i.e., the roots of the characteristic polynomial $P_2(x) = x^2 - a_p x + p = 0$ are lying in K. Hence, for the trace of the Frobenius a_p, $a_p = a_p(E)$, we have

$$4p = a_p^2 + Dx^2 \tag{2.4}$$

for a (rational) integer x. We again repeat that every elliptic curve over $\mathbb{F}_p$ has a complex multiplication (indeed, it is enough to take D as a square free part of $4p - a_p(E)^2$). In the notations above, for $n = p$ (2.4) means that in (2.2)

$$\alpha = \frac{a_p(E) \pm X\sqrt{-D}}{2}. \tag{2.5}$$

It is clear, that in (2.4) a_p can have two signs. The choice of the sign of a_p in (2.4) determines the choice of the sign of $n^{\pm}$ in (2.3) for $n = p$. Of course, the canonical choice of the sign for a_p leads to n^+ in (2.3). We discuss below how all possible values of $n^{\pm}$ can be achieved.

The criterion of primality of n in terms of an elliptic curve mod n with complex multiplication in K is formulated as follows:

PROPOSITION 2.7. *Let us assume that* $(n, 4D) = 1$ *and for* n *of the form* (2.2) *there exist an elliptic curve* $E \bmod n$ (*i.e., defined in the Weierstrass model by nonsingular equations* $\bmod n$), *having complex multiplication in* K (*i.e., the endomorphism* $\tilde{x} \to [\sqrt{-D}]\tilde{x}$ *of* E *is defined by rational expressions* $\bmod n$ *in coordinates of* $\tilde{x}$). *Let for every divisor* q *of* $n^{\pm}$ *there exist a point* $\tilde{x}_1^{(q)}$ *on* $E \bmod n$, *such that for the sequence*

$$\tilde{x}_m^{(q)} = \left(\frac{X_m}{Z_m^2}, \frac{Y_m}{Z_m^3}\right) \bmod n,$$

we have

$$Z_{n^{\pm}} \equiv 0 \bmod n,$$

but

$$\left(Z_{n^{\pm}/q}, n\right) = 1.$$

Then n *is prime.*

Proposition 2.7 leads to the introduction of functions, similar to Euler's ϕ-function. An example of such function exists in the theory of Lucas sequences [BLS, LH2]. These functions are better defined and understood, when E has a torsion point mod p, typically at least one torsion point of order two. A weaker condition is, say $2|D$. The definition of the analog of Euler function is the following:

Let $n = \prod_{i=1}^{k} p_i^{\alpha_i}$, where $p_1, \ldots, p_k$ are (distinct) odd prime divisors of n. Then for every $p_i|n$, there exists $a_{p_i}(E)$ (because there exists a representation $4p_i = a_{p_i}^2(E) + p_i \cdot x_i^2$) and we put

$$\phi_E(n) = \prod_{i=1}^{k} p_i^{\alpha_i - 1} \cdot \left(p_i + 1 - a_{p_i}(E)\right),$$

or, if E has a torsion point of order two mod n, we put

$$\phi_E(n) = 2\prod_{i=1}^{k}\left\{ p_i^{\alpha_i - 1}\left(p_i + 1 - a_{p_i}(E)\right)/2\right\}$$

$$\left(= 2\prod_{i=1}^{k}\left\{ p_i^{\alpha_i - 1} p_i^{+}/2\right\}\right). \tag{2.6}$$

The crucial property of the ϕ function is the following one: for $(n, 4D) = 1$, $n > 5$, $\phi_E(n) = n^{+}$, if and only if n is a *prime* number. In the case (2.6) the proof of this is very similar to the corresponding results in the case of Lucas sequences (cf. [BLS]). Similar to Propositions 2.2 and 2.4, it is enough to require only a partial factorization of $n^{\pm}$. The use of partial factorization of $n^{\pm}$ can be formalized as an algorithm to prove primality of a probable prime n with excellent running time (heuristic arguments suggest polynomiality).

One can generate similar tests for primality, starting from Abelian varieties of CM type mod n, as in Examples 1.6(3), when n is a norm of an element of the CM field K.

An important problem in this "elliptic primality test" (elliptic generalizations of the Lucas–Lehmer tests) is the construction of E and $n^{\pm}$ starting from n and k. First of all, we have already remarked that condition (2.2) is equivalent to the representation of $4n$ by the quadratic form $x^2 + Dy^2$:

$$4n = a^2 + Db^2, \tag{2.7}$$

and then

$$n^{\pm} = n + 1 \mp a,$$

or $\alpha = (a \pm b\sqrt{-D})/2$.

A necessary condition for a prime $n = p$ to have a representation (2.7) is the congruence condition, given by the following character formula

$$\chi_{-D}(n) = 1. \tag{2.8}$$

Here $\chi_{-D}(x)$ is a quadratic character of the quadratic field $K = \mathbf{Q}(\sqrt{-D})$, defined as follows

$$\chi_d(x) = \left(\frac{x}{|d|}\right) \qquad \text{for } d \equiv 1 \bmod 4$$

$$= (-1)^{(x-1)/2} \cdot \left(\frac{x}{|d|}\right) \qquad \text{for } d \equiv 3 \bmod 4$$

$$= (-1)^{(x^2-1)/8 + (x-1)/2 \cdot (d'-1)/2} \cdot \left(\frac{x}{|d'|}\right) \qquad \text{for } d = 2d',$$

for all x relatively prime with the discriminant of the field K.

The condition (2.8) is not sufficient, in general, for a prime $n = p$ to be represented in the form (2.7). However, if K is a one class field (or, weaker, the discriminant $-D$ has one class per genus), then the condition (2.8) is a necessary and sufficient condition for $4n$ to be represented by the form $x^2 + Dy^2$, whenever $n = p$ is a prime. This brings us to the concept of "numeri idonei" of Euler [BSh] (these are integers $D > 0$, for which the discriminant $-D$ has one class per genus). These numbers were discovered by Euler in his studies of primality testing [DI1], who tabulated 65 of "numeri idonei": 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 12, 13, 15, 16, 18, 21, 22, 24, 25, 28, 30, 33, 37, 40, 42, 45, 48, 57, 58, 60, 70, 72, 78, 85, 88, 93, 102, 105, 112, 120, 130, 133, 165, 168, 177, 190, 210, 232, 249, 253, 273, 280, 312, 330, 345, 357, 385, 408, 462, 520, 760, 840, 1320, 1365, 1848.

There are exactly 65 of these numbers, at least assuming the (generalized) Riemann hypothesis. For each of the numeri idonei D, it only takes $O(\log n)$ operations to find a and b in the representation (2.7) of n, whenever $\chi_{-D}(n) = 1$ and n is a suspect to be a prime. The corresponding algorithm requires the knowledge of $\sqrt{-D} \bmod p$, and proceeds similar to the famous Hermite's algorithm of the representation of a prime $p \equiv 1 \bmod 4$ as a sum of two squares [HW]. For an arbitrary D, one can find in $O(\log n)$ operation the representation (2.7) for a prime $n = p$, whenever this representation is possible, starting from the knowledge of $\sqrt{-D} \bmod p$. There are various algorithms to compute square roots mod p [K1, Chap. 4.6.2; Sch1].

We left out the problem of determination of the sign of a in the representation (2.7), that determines n^+ or n^- in (2.3). Apart from the cases $D = 1$ and $D = 3$, a^2 is unique in the representation (2.7) (in the two former cases, there are 4 or 6 possible values of a, as many as there are roots of unity in K).

Apparently, both values $\pm a$ and $n^{\pm}$ are achievable. If $y^2 = P_3(x)$ or $y^2 = P_4(x)$ is a model of $E/\mathbb{F}_p$, then equations $My^2 = P_3(x)$ or $My^2 = P_4(x)$, respectively, define elliptic curves E_M, called twists of E, corresponding to an arbitrary integer M mod p. The trace (or eigenvalues) of a Frobenius F_p of E_M differ by a multiplicative constant (M/p) from those of E, where (x/p) is the Legendre symbol. This way, after checking of some number of M, till we find a quadratic nonresidue, both values $n^{\pm}$ for a prime $n = p$, can be achieved for an elliptic curve of the form E_M, having complex multiplications in $K = \mathbb{Q}(\sqrt{-D})$. In case $D = 1$ or $D = 3$ all possible values of a can be achieved by considering all possible isogenies and twists of two elliptic curves: $y^2 = x(x^2 - 1)$ and $y^2 = x^3 - 1$ having complex multiplications by i and $i\sqrt{3}$, respectively.

To construct an elliptic curve E having a complex multiplications in K one uses modular equations. If K is a one class field, then the curve E, having complex multiplication in K is defined over $\mathbb{Q}$, see Heegner's

equations in [GR1, He1]. Similar simple formulae exist for all numeri idonei (see Weber's [Web1] and Watson's tables and references in [Wat1]). If D is arbitrary, one has to construct a modular equation directly. In examples below we used only numeri idonei D, to simplify the construction of the corresponding elliptic curve E, which is defined globally. The use of arbitrary complex multiplications in $n^{\pm}$ primality tests is one of the best methods to prove primality of fairly large probable primes.

As much as Lucas–Lehmer tests were designed to test the primality of numbers $M_p = 2^p - 1$ or $a \cdot 2^m - 1$, the elliptic primality tests were designed by us to show the primality of elements in the following sequences generated by the three-term linear recurrences:

$$s_m = \mathrm{Norm}_{K/\mathbb{Q}}(\alpha_0 \cdot \alpha_1^m + 1)$$
$$\left(= \mathrm{Norm}(\alpha_0) \cdot \mathrm{Norm}(\alpha_1)^m + \alpha_0\alpha_1^m + \alpha_0^*\alpha_1^{*m} + 1\right) \qquad (2.9)$$

for two integers α_0 and α_1 from $K = \mathbb{Q}(\sqrt{-D})$. For any element s_m of this sequence s_m^- is known explicitly:

$$s_m^- = \mathrm{Norm}(\alpha_0) \cdot \mathrm{Norm}(\alpha_1)^m,$$

and is readily factorizable.

The sequences s_m are cross-between sequences of powers and Lucas' sequences for negative discriminants. If one wants to include Lucas' sequences with positive discriminants, Abelian varieties of CM type have to be used. The use of varieties with Abelian fields of complex multiplications significantly improves on the speed of primality proving, especially for numbers of special nature.

For sequences s_m with various "initial conditions" $\alpha_0, \alpha_1 \in K$, the elliptic primality tests were implemented, and for α_0, α_1 with $\max(\mathrm{Norm}(\alpha_0), \mathrm{Norm}(\alpha_1)) \leq 10$, a search was conducted for primes s_m with m of the order up to 500. Many interesting large primes were found.

The simplest among the sequences s_m corresponds to a Gaussian field $K = \mathbb{Q}(i)$ with initial conditions: -1 and $1 + i$, i.e.,

$$s_m = \mathrm{Norm}\big((1 + i)^m - 1\big).$$

Of course, s_m can be prime only when $m = p$ is a prime. Apparently, numbers s_m in this particular case are not new, but are connected with Aurifeuillian factorization [BLSTW]:

$$2^{4k-2} + 1 = (2^{2k-1} - 2^k + 1) \cdot (2^{2k-1} + 2^k + 1).$$

Indeed,

$$s_p = 2^p - \left(\frac{2}{p}\right) \cdot 2^{(p+1)/2} + 1. \qquad (2.10)$$

Here is the list of primes s_p for p up to 2000:

$$p = 2,3,5,7,11,19,29,47,73,79,113,151,157,163,167,$$
$$239,241,283,353,367,379,457,997,1367.$$

The prime s_{1367} has 825 digits.

In Tables 1 and 2 we present results of the primality testing of elements of various sequences s_m. In Table 1 prime values of s_m are presented for various D and initial conditions α_0, α_1. The representation Primes $[d,[a,b,c,e],l]$ means that we list prime values of s_m for m in list l and

$$d = D, \qquad \alpha_0 = a + b\sqrt{-D}, \qquad \alpha_1 = c + e\sqrt{-D}.$$

The values of s_m in the list Primes [...] are followed by the value of m. In Table 2 we present prime values of the sequence s_p from (2.10).

3. Large Prime Generation and the Elliptic Divisibility Sequences

The sequences X_n (or $\tilde{x}_n$), generated by endomorphisms $[n]_F(\cdot)$ of the algebraic group laws, are, in general, similar in their divisibility properties to Lucas' sequences. We arrive thus to a particularly interesting problem of the factorization and primality of numbers in these sequences. To fix our ideas, let us consider the elliptic curve case. If the curve $E/\mathbb{Q}$ is given in the Weierstrass form $y^2 = 4x^3 - g_2x - g_3$ with rational (integers) g_2, g_3, let us generate, starting from a rational point

$$\tilde{x}_1 = (x, y) \qquad \left(= \left(\frac{X}{Z^2}, \frac{Y}{Z^3}\right)\right)$$

on $E(\mathbb{Q})$, the sequence

$$\tilde{x}_n = [n]_E(\tilde{x}_1), \qquad n \geq 0$$

$$\tilde{x}_n = \left(\frac{X_n}{Z_n^2}, \frac{Y_n}{Z_n^3}\right).$$

Because of the polynomial character of the law of addition on an elliptic curve, X_n, Y_n, and Z_n are polynomials in X, Y, Z, and g_2, g_3. If we consider an elliptic function parametrization of E given by $\tilde{x} = (\mathscr{P}(u), \mathscr{P}'(u))$ with a Weierstrass elliptic function $\mathscr{P}(u)$, $\mathscr{P}(u)'^2 = 4\mathscr{P}(u)^3 - g_2\mathscr{P}(u) - g_3$, and if u_1 is a parameter such that $\tilde{x}_1 = (\mathscr{P}(u_1), \mathscr{P}'(u_1))$, then $\tilde{x}_n = (\mathscr{P}(n \cdot u_1), \mathscr{P}'(n \cdot u_1))$.

Among the sequences X_n, Y_n, and Z_n a true divisibility sequence (an analog of Lucas' sequence) is only Z_n. This sequence Z_n, in a different form, was, in fact, considered by Lucas, who (wrongly) thought that it is related to solutions of linear recurrences, see Bell [B1] for the discussion of Lucas' claims.

Table 1

```
Primes2(1,[1,-1,2,1],[1,3,5,9,21,37,69,301])
VALUE = ((0 0) (1 17) (3 277) (5 6257) (9 3902417) (21 953674261440497) (37 1455
191522836494821988043337) (69 3388131789017201356273293603494110082037857416817)
(301 490909346529772655309577195498627564297521551249944956511154911718710525472
171585646009788403733195227718736671964356090333864685670735521513295989767379433
892940457423686399338983897852226227101375628068913236971))

Primes2(1,[-1,1,2,1],[1,2,4,6,10,12,16,46,84,90,184,346])
VALUE = ((0 0) (1 5) (2 37) (4 1217) (6 31397) (10 19537957) (12 488278337) (16
305174743297) (46 284217094304040078453110772088997) (84 10339757656912845935892
608650816963688375419432161917282041 7) (90 161558713389263217748320101699226167
792551344496818863790085157) (184 815663058499815565838786763657068444462645532 2
586208184698295569883302582448292279460534920289980439625685875898728427777920444
17) (346 139524828037387082790012640173991816339344481789892414699112041409623 1
245003342524017880886059780309630350408146208530557106856302369041679645866106597
751675278889613917852533694627074153298196867617166282344714315899306508723156805
038334120997))

Primes2(1,[1,1,2,1],[1,3,8,10,12,14,20,26,39,81,82,120,156,192,279,369])
VALUE = ((0 0) (1 13) (3 233) (8 780869) (10 19537009) (12 488325349) (14 122071
51889) (20 190734841020709) (26 2980322242093529329) (39 3637978807091833563222 3
15113) (81 827180612553027674871408692116040668356174773328481762573) (82 413590
306276513837435704346040753797277062075221607072324 9) (120 150463276905252801019
998276764447446760789434662591908126622979813166836809897632709) (156 218952885
050752667331832747389049395512540928418205589275827390366511337315627274945881 79
977645114011552131429) (192 3186183822264904554057760795535426111822091103852 37
572147771706772230460603023751077791243279297389698849559567398679240189603977 14
949) (279 .2059023035787211567255580869388675587443351832493849130874563090841434
431830031170361401439540931734720538231664931934390381572183583901777262504175 50
302937788751942810423416632058596615532655831 3) (369 166326556250318387496486473
290910501884632684934011000036134769212750344872873130323634253270599878982347 29
863956076271020291334734135058092811420903982606361233389392947247427535636770 12
329758766803216884743037065809720033252478989835732243052189049454432013))

Primes2(1,[-1,-1,2,1],[2,3,6,7,8,14,38,48,50,230,252])
VALUE = ((0 0) (2 53) (3 269) (6 31573) (7 156749) (8 781633) (14 12206910613) (
38 72759576141829390906992853 3) (48 710542735760100194269270405700083 3) (50 1776
356839400250461350022881697606 93) (230 11591269220898191830411672692336373479273
639933618096882665747059117441687798841691062929375972450605197471838299803767 23
905593201450191319723171386277426111790 93) (252 2763573937630222280123632596096 1
278627571201166196100432075851104539493770119766585508824623117953509187790680 32
612446077887932826350222263372787222481955496906392731372446243 53))

Primes2(1,[0,2,2,1],[1,3,7,219,349,483])
VALUE = ((0 0) (1 17) (3 457) (7 312617) (219 474778387287989937373662113478097 8
577110482916809972483139889995414504115322289036046212739035448523973147603505 04
170932669111212650487364409747453451 4697) (349 348812070093467706975031600434979
540848361204474731036747780103524057811250835631004470221514945077407587602036 55
213263923119461164617239685798544098152350384087182880418333776070794288450932 45
808444865805535038917477241777831014567617770246897) (483 160166647614648073954
366817210918119658718638404918400195945504926926982428739263932759132608031108 79
923405600554171588439272867379566524339244934701781708385187132449930071842244 10
392381658201261536194021769738731860811050940786992221038653558696669599086284 60
631922577764230205886198183918684287150742921839976045188296513586219032147657))

Primes2(1,[2,0,2,1],[1,2,3,4,10,11,51,68,106,156,273])
VALUE = ((0 0) (1 29) (2 113) (3 509) (4 2473) (10 39061553) (11 195323069) (51
177635683940025046490167878744342386 9) (68 135525271560688054250931831477711745 0
620912993193) (106 493038065763132378382330353301741393565148727995291342221779 9
501776688100 33) (156 437905770101505334663665494778098791025081856836411178542 08
162122970018262886115632139300005513922525225309033) (273 263554948580763080608 7
143512817504751927490345592126887519440756277036072742439898062593842612398931 94
807613137961778588997051416640110022020910787228783127054512389752513789283051 70
4290378909))
```

Table 1—*Continued*

```
Primes2(1,[-2,0,2,1],[1,2,5,6,7,9,23,53,55,89,102,233,263])
VALUE = ((0 0) (1 13) (2 89) (5 12653) (6 62969) (7 313613) (9 7815373) (23 4768
3715962526093) (53 4440892098500626160564892864l124992493) (55 1110223024625l565
4036145034255822617665З) (89 646234853557052870993288040679704821000060875158271
080911261773) (102 78886090522101180541172856528278623142450480726933125281546б7
08143959289) (233 28978173052245479576029181730840933698184099834045242206664367
647793604219497104363423705341340102663698459143527972165340224144993728287813S9
2695787150073274770893) (263 26988026734670139454332349571251248659737501138863З
7932819907334427684938488258455616096094862522557394347815652524374784172691126Z
6247806440527334819465262837165874521170500138248972Э3))

Primes2(1,[1,1,3,2],[1,9,13,61,173])
VALUE = ((0 0) (1 29) (9 21209283869) (13 605750186396189) (61 17847380649136192
3833099463289545771635365155543386674294676632524829) (173 103093182069870963360
3720189715704312188837037259979429913148160856124396210713408227590807978434832Z
549043183928212569274318471725914197028554175929954498656900898279208436060611Т4
6307169000989))

Primes2(1,[1,-1,3,2],[1,2,6,11,13,19,27,58,174])
VALUE = ((0 0) (1 37) (2 373) (6 9647893) (11 3584323911989) (13 605750254480837
) (19 ,2923840580689034917109) (27 238506658502498151441356188382Э) (58 812352328
1354661986030926867981126536745080375399659854334245765З) (174 13402113669083225
2368483624663041560584548814843797325888709260911296171507392743069586805037l965
7390896919460887086727453287382534182114461117084213207864156521873978051830l932
5166424805319З1733))

Primes2(2,[0,-1,1,1],[1,3,5,9,13,15,47,63,73,297,319,397])
VALUE = ((0 0) (1 11) (3 59) (5 443) (9 39659) (13 3188123) (15 28708331) (47 53
1776287182812662733871 (63 2289122546861673553175489857451) (73 1351703972696350
4690012023305704497l) (297 101401095598954352586167427690435789604787922685435l3
8127022363021014073662286555204990026565689557881002771934946214335568670155907З
3999324779) (319 3182073825408694096576523357207762712774832353594923425667237З8
763847991253677461540966171751596981276273505251141104678306783069409366767577ч6
5281067947) (397 522598452492987597870105715377294786788947774909535672317564616
364904337419132845604291100218137989257539169935220462570260826907006753128505Ol
1890902068330741406889086635953187188472241756З))

Primes2(1,[1,2,3,1],[1,3,6,15,23,74,93,237,308,350])
VALUE = ((0 0) (1 53) (3 4933) (6 4995553) (15 500000013285811З) (23 49999999999
9140280799233) (74 50000000000000000000000000000000000043681656025247129294139S
01300492009473) (93 5000000000000000000000000000000000000000000001310171776957Ο
155775523000513748453704454058803З) (237 4999999999999999999999999999999999999
99999999999999999999999999999999999999999999999999999999999999999999999999999999
45839756515939352631974027456629501644129617108834919366568207400403435543058475
370707266479205546250532508484493115393) (308 5000000000000000000000000000000
000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000004238528924778228906601508223587179432756
11780040851623352635463159355872795626427892293097607056750058560474714273905072
689199538100823625574170956734136З3) (350 5000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000
000000000000000000000000000000000000000000000000000036332487249992443982416
16754799973574964519853697189921279172926599102177538195415237092052344521389049
32273310752176166169323041246241306282521303877515215857067831592086405l3))

Primes2(6,[3,0,2,1],[1,4,5,6,7,10,12,16,31,232,414])
VALUE = ((0 0) (1 103) (4 89449) (5 899473) (6 9003409) (7 90018913) (10 8999949
2929) (12 8999997871489) (16 89999999975966209) (31 899999999999999868620426328l
4593) (232 89999999999999999999999999999999999999999999999999999999999999999999
99999999999999999999999999999999999999998781968597432549623932515381307B0
27936592682189828443633320341232240888141927787738949966015686205841815866650184
3089) (414 8999999999999999999999999999999999999999999999999999999999999999999
99999999999999999999999999999999999999999999999999999999999999999999999999999999
39999999999999999999999999999999999999999999999999999553059934415795582131Ο
01217601945736790316215622037517820051246373414273280159982586765341688959820439
1012566852276430544657259300135908918938954232322894697150232362472239384424254З
3801757757275697750789324Э))
```

Table 1—*Continued*

```
Primes2(1,[-3,0,3,1],[1,2,3,4,6,7,10,11,30,53,55,81,90,99,119,180,267,310,324,36
0])
VALUE = ((0 0) (1 73) (2 853) (3 8893) (4 89833) (6 9002113) (7 90011953) (10 90
000598273) (11 900001749313) (30 9000000000000005845076623491073) (53 9000000000
00000000000000000425127297762254652432187393) (55 899999999999999999999999999923
06262679284879840690307073) (81 899999999999999999999999999999999999999988642509
5477592968838291566705822622810113) (90 9000000000000000000000000000000000000000
000004653278966031777658070654668572329474336489473) (99 89999999999999999999999
99999999999999999999999999828124159630153662505022193305276397916190389829633) (
119 8999999999999999999999999999999999999999999999999999999999984225612747259561
34351128106913464248342912572758668903186433) (180 89999999999999999999999999999
99999999999999999999999999999999999999999999999999999999999998782331621428743409
407051719404300190367790572178424298319029150982135682284726459744387073) (267 9
00000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000886917189997721949020923529
84597109751807787877330215790457182283016376666813550682610019150107137866376363
133944000784402141363044353) (310 8999999999999999999999999999999999999999999999
99999999999999999999999999999999999999999999999999999999999999999999999999999999
99999999999999999999999999999576965904498956753397911203166005430833496201514474
68726785358672878022289429941273530924604122772851342377883124818352662122563817
6320574937817633649590273) (324 900000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000005036386689297020057652078068235732728973232821
31341428633122948596139056586475383892711000169204531726495717712241720984096172
8204978398169464942918408705652293633) (360 900000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000005505761239942548
98116513837518747045068998819721556690155436049641166190188102339843400441896750
94168388313021618780044155591386076904690632806275892116526200072400580039303464
22273))
```

```
Primes2(6,[-3,0,2,1],[1,15,16,25,44,130,230,321,350,456])
VALUE = ((0 0) (1 79) (15 8999999857955329) (16 90000000024033793) (25 900000000
00018728958640129) (44 899999999999999999999983273706375007386468353) (130 90000
00000000000000000000000000000000000000000000000000000000000029911386038092326219
8497266410018418653556105671546560280864489473) (230 900000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000551275919800376498740013414195505358091455172512097683087274868917649047
44227839899094869333913286779003647108841473) (321 90000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000002207726694679351129447890859
25214605056143817237818765287141572411570665709660461864314933121485663793404168
23112869078272298905235554665797583445062239396036609) (350 90000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000037733
03735581803337290405530094454505643914736538649586709617029177974578741233864680
73031065306118603200679795810921631134545348679075048065562904988067490433580975
27508303873) (456 90000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000
00000020940487373208801265210231745880264759379354166265953838790658136137743897
08809309088209787864418920041469581923902980717134070429398699961200238768719274
290466695394541571182759597932328412643191097089094918192150188753359470593))
```

```
Primes2(6,[0,-1,2,1],[1,3,4,9,11,17,23,45,65,71,179,309,387,496])
VALUE = ((0 0) (1 73) (3 6073) (4 59809) (9 6000153793) (11 599999509633) (17 60
0000000930941953) (23 600000000001547918057473) (45 6000000000000000000000127548
015428978513805313) (65 60000000000000000000000000000000134098013436510181748288
8674803713) (71 600000000000000000000000000000000000001232206885295045470819596447
85016833) (179 60000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000015477862702147979470266461685575253651816927915379062233
81506166298162807334481900121096193) (309 59999999999999999999999999999999999999
99999999999999999999999999999999999999999999999999999999999999999999999999999999
99999999999999999999999999999999999992856175447922571496114698779721973079050021
19417137574488224246577439522287456883684183041886313482825159425493787165416751
```

Table 1—*Continued*

```
900013415176047214343523055697 93) (387 5999999999999999999999999999999999999999999
999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999
999999999999999999999999999999999999999999999999999999999999999999999999999999992870238
027078638394815681257798843757946020102177038365178587640836757969665539045326732
233640328668949997178839429689858465790615864288568933292321149769899841088438309
302790383859960454337003531) (496 5999999999999999999999999999999999999999999999999999999999
999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999
999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999
999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999
999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999
550171746328256680996967489048867255559386900646381522710961561733982449930758805
310644631193598736909480203885063705314785227277503693380234151839059500063503 1
587682046114085942633966017852672169091626768007169))
```

Note. Primes2(d,[a, b, c, e], l) lists pairs (p, s_p) for values of s_p when p is in list l. Here $s_m = \mathrm{Norm}_{K/\mathbf{Q}}(\alpha_0\alpha_1^m + 1)$, where $K = \mathbf{Q}(\sqrt{-d})$, $\alpha_0 = a + b\sqrt{-d}$, $\alpha_1 = c + e\sqrt{-d}$. The list Primes2(..., l) contains all primes s_m with $m < \sup(l)$.

The sequence Z_n plays a particularly important role in the classical theory of elliptic functions, where it is known in different notations as

$$\psi_n = (-1)^{n-1} \cdot Z_n. \tag{3.1}$$

Here, in the classical notations [T-M]:

$$\psi_n = \frac{\sigma(nu)}{\sigma(u)^{n^2}}, \tag{3.2}$$

Table 2

```
Prime([2,3,5,7,11,19,29,47,73,79,113,151,157,163,167,239,241,283,353,367,379,457
,997,1367])
VALUE = ((2 5) (3 13) (5 41) (7 113) (11 2113) (19 525313) (29 536903681) (47 14
0737471578113) (73 9444732965601851473921) (79 6044629098062150757253 13) (113 10
3845937170696551129458045825843 21) (151 2854495385411919762116496381035264358442
074113) (157 1826877046663628647754612085524518477157892096 1) (163 116920130986
4722334562948349743354261576415916851 3) (167 1870722095783555735300716392448711 1
2681892570202113) (239 8834235323891921647916487503714592565845139526528936061 5E
996040365965313) (241 3533694129556768659166595001485837028996511802181406170435
598282024550401) (283 1554135113780583256735569525458851253139260287603415802 67
0284661840802443732044805 13) (353 1834798892792057209288656716241669552632 5195
1334624879833876810685927571391450007077150047253861521948672 1) (367 3006134505 9
5050653169853516389035139504087366260264943426013315702268533480936328328948524E
5535056803315004211 3) (379 1231312693637327475383720003129487931408741852202045 2
0837495344431652547555024677896249773706917920263632313332531 3) (457 3721414268 3
9350727961253789638658321589064376671906846864122981980486452795766387922536388 6
2096416093892885467378676180365032071832272896 1) (997 1339385758982834151185531 3
1132500226320175601463191700930468798546293881390617015311649797351961982265949 3
3411469414335314839316071153925544980721968389585457957690427880354680260481252 0
8904713757765805163872455056995809556627183222337328039422584942896842901774597 8
0646216235722952074488131497230336 1) (1367 3221098997485605085558716927989721778
9935175791251931715455317553883203115618344044164938531942154869005779656774829 2
5107223623731345073354101813186594829537663733801016403611747568817990605160202 8
0988342499035862290122218104360711147686936015002817824695427538204649048962100 7
1125567363765494016189142051250907560189778942332727075195112641822702867994025 5
0842569867251588415896633690920263550194773479089242113))
```

Note. Prime(l) lists pairs (p, s_p) for all prime values of $s_p = 2^p - (2/p)2^{(p+1)/2} + 1$ for $p < 2500$.

where $\sigma(u)$ is the Weierstrass σ-function, and u $(= u_1)$ is a parameter in the parametrizations of $\tilde{x}_1$: $\tilde{x}_1 = (\mathscr{P}(u), \mathscr{P}'(u))$. The sequence ψ_n satisfies the famous three-term nonlinear recurrence [CA1]:

$$\psi_{m+n}\psi_{m-n} = \psi_{m+1}\psi_{m-1}\psi_n^2 - \psi_{n+1}\psi_{n-1}\psi_m^2, \tag{3.3}$$

with $\psi_0 = 0, \psi_1 = 1$. The recurrence (3.3) follows from the three-term law of addition for σ-functions:

$$\sum_{a,b,c} \sigma(z+a)\sigma(z-a)\sigma(b+c)\sigma(b-c) = 0. \tag{3.4}$$

Another way to see (3.3) (or (3.4)) is to use the identity

$$\frac{\sigma(z+y)\sigma(z-y)}{\sigma(z)^2\sigma(y)^2} = \mathscr{P}(y) - \mathscr{P}(z). \tag{3.5}$$

Ward [W1] was the first to study in detail the divisibility properties of the sequence ψ_n. Ward [W1] called a solution ψ_n of the recurrence (3.3) an "elliptic divisibility sequence" whenever initial conditions ψ_2, ψ_3, ψ_4 are integers and $\psi_2 | \psi_4$. If ψ_n is an "elliptic divisibility sequence," then

$$\psi_m | \psi_n \qquad \text{whenever } m|n \tag{3.6}$$

—the divisibility property. Among the elliptic divisibility sequences there are singular elliptic divisibility sequences corresponding to degenerate elliptic curves, and they have the form: (a) $\psi_n = U_n$ for Lucas sequence from Example 1.6(2) with integers P and $Q = 1$; (b) $\psi_n = (n/3)$ or $(-8/n)$ for Jacobi symbols (m/n); (c) $\psi_n = n$. The general elliptic divisibility sequence ψ_n has, according to Ward [W1], the form (3.2) for some elliptic curve E defined over $\mathbf{Q}$ (i.e., having rational g_2 and g_3) and a rational point $\tilde{x}_1 = (\mathscr{P}(u), \mathscr{P}'(u))$ on $E(\mathbf{Q})$.

The laws of apparition of primes p in the elliptic divisibility sequence ψ_n in (3.2) follow from the properties of the Frobenius F_p of E. For example, the rank of apparition $\tau(p)$ of p in ψ_n always exists. The rank $\tau(p)$ is equal to the order of the point $\tilde{x}_1 \bmod p$ in $E \pmod p$, and divides $N_p = p + 1 - a_p$, whenever p is a prime of good reduction (i.e., $E \pmod p$ is an elliptic curve). Unfortunately, these simple rules for the law of apparition escaped Ward's attention in [W1–W3].

According to the divisibility property (3.6) and the definition (3.2), the number ψ_n may be a prime only when $n = p$ is a prime (at least when n is relatively large) and $\tilde{x}_1$ is one of the *generators* of the Mordell–Weil group

of $E(\mathbb{Q})$ (i.e., $\tilde{x}_1$ is not divisible in $E(\mathbb{Q})$). Thus we are led to an interesting way of generating large numbers ψ_p suspect of being prime. The numbers ψ_p are indeed large for a small p, because the absolute values of the integers ψ_n grow as

$$c^{n^2} \cdot (1 + o(1)),$$

where the constant $c > 1$ is related to the Neron–Tate height of $\tilde{x}_1$ on $E(\mathbb{Q})$.

It was always the most challenging problem to generate the "largest" prime by means of some simple arithmetic expression. That is why, after all, Fermat numbers $F_n = 2^{2^n} + 1$ were invented. Unfortunately, large Fermat numbers are either composite or too big to be checked for primality. Mersenne numbers [K1, Tu1, Slo1] require too much sieving to produce a good candidate. The growth of elements in the elliptic divisibility sequence is less impressive than for Fermat numbers, but much faster than for Mersenne, so it takes only a hundred or so iterations to generate a truly gigantic number, and so there are only a few candidates for primality to be checked. Perhaps, these numbers can be used to generate extremely big primes.

In dealing with the elliptic divisibility sequences, one often finds ψ_n divisible by small primes, particularly by $p = 2$ or $p = 3$. This is usually a consequence of nonminimality of the Weierstrass model for $E/\mathbb{Q}$. In order to dismiss apparent divisors of ψ_n, it is preferable to deal with the minimal model of $E/\mathbb{Q}$. It should be noted that the minimal model of $E/\mathbb{Q}$ does not always have the Weierstrass form, and the most general expression for the equation, defining the minimal model for $E/\mathbb{Q}$, particularly a suitable one for $p = 2, 3$ is

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \tag{3.7}$$

for (rational) integers a_1, a_2, a_3, a_4, a_6, see Tate [T3]. In the case of an elliptic curve equation (3.7), it is better to use the form Z_n of an elliptic divisibility sequence (3.1) rather than ψ_n. Moreover, to rid ourselves from spurious divisors of Z_n, that correspond to the common factors of X_n and Z_n, it is more convenient to introduce the following new sequences. For a rational point $\tilde{x}_1 = (X_1'/Z_1'^2, Y_1'/Z_1'^3)$ on (3.7), written in the irreducible form (i.e., in a form such that for no $l > 1$, $l|Z_1'$, $l_1^2|X_1'$, and $l_1^3|Y_1'$), we multiply $\tilde{x}_1$ by n in the group law of E:

$$\tilde{x}_n = [n]_E(\tilde{x}_1) = \left(\frac{X_n'}{Z_n'^2}, \frac{Y_n'}{Z_n'^3} \right), \tag{3.8}$$

where $(X_n'/Z_n'^2, Y_n'/Z_n'^3)$ is written in the irreducible form. To obtain the

irreducible form of $\tilde{x}_n$, it is enough to look an the g.c.d. of X_n, Y_n, and Z_n. The sequence Z'_n is the most appropriate normalized version of the elliptic divisibility sequence (3.2). It is particularly advisable to start with an integral point $\tilde{x}_1$ on $E(\mathbb{Q})$.

Similar to the general Weierstrass equation (3.7) of E, it is possible to consider other versions of the elliptic divisibility sequences generated by different models of elliptic curves. For example, Ward [W2] considers the elliptic divisibility sequences arising from the Jacobi form of an elliptic curve (see Sect. 4). His sequences A_n, B_n, C_n, and D_n are associated with multiplication law for Jacobi's elliptic functions *sn*, *cn*, and *dn* (e.g., *sn nu/sn u* $= B_n/A_n$, *cn nu/cn u* $= C_n/A_n$, *dn nu/dnu* $= D_n/A_n$).

There exist various generalizations of elliptic divisibility sequences for arbitrary algebraic group laws. Moreover, if a ring of endomorphisms of a formal group law $\bar{F}$, corresponding to a given algebraic law of addition, is larger than $\mathbb{Z}$, then one can introduce a sequence $X_\alpha = [\alpha]_{\bar{F}}(X)$ for $\alpha \in \mathrm{End}_{\mathbb{Z}}(\bar{F})$. In particular, Abelian varieties of CM type with complex multiplications in the order $\mathcal{O}$ of a CM-field K generate a sequence X_α for $\alpha \in \mathcal{O}$. These sequences give rise to divisibility sequences corresponding to the division in $\mathcal{O}$.

The case of elliptic curves with complex multiplications was considered in [W3, D1] for lemniscate and equianharmonic elliptic curves (these are curves with complex multiplication by i and $i\sqrt{3}$, respectively). One can introduce the elliptic divisibility sequences ψ_μ: $\mu \in \mathcal{O}$ for an arbitrary elliptic curve E with complex multiplications in the imaginary quadratic field K, and the ring of integers $\mathcal{O}$ of K. To do so we have to change the σ-function $\sigma(u)$ in (3.2) to a θ-function more appropriate in the complex multiplication case [L1]. Let E be an elliptic curve with complex multiplication in the imaginary quadratic field K, and defined over $\mathbb{Q}$.[1] Let L be the lattice of periods of E, i.e., $L = \Omega \cdot \mathcal{O}$, where $\mathcal{O}$ is an order in K. Following Eisenstein and Weil [W4], one introduces a value of a nonholomorphic Eisenstein series:

$$G_2(L)\,(= s_2(L)) = \lim_{\substack{s \to 0 \\ s>0}} \sum_{\substack{\omega \in L \\ \omega \neq 0}} \omega^{-2} |\omega|^{-2s}.$$

Then we define a normalized σ-function of E [L1]:

$$\theta(u) = \sigma(u) \cdot e^{-(1/2)s_2(L) \cdot u^2}. \tag{3.9}$$

Only in cases $g_2 = 0$ or $g_3 = 0$ (the lemniscate and equianharmonic cases above), $s_2(L) = 0$, and $\theta(u) = \sigma(u)$. For an arbitrary E the laws of

[1] This effectively leaves us with 9 one-class fields. However, these arguments can be generalized for arbitrary E and K.

complex multiplication imply that, for an arbitrary integer μ ($\mu \in \mathcal{O}$), the expression

$$\psi_\mu \stackrel{\text{def}}{=} \frac{\theta(\mu u)}{\theta(u)^{\text{Norm}(\mu)}} \tag{3.10}$$

(for a norm $\text{Norm}(\mu)$ of μ in $K/\mathbb{Q}$) is a polynomial in $\mathcal{P}(u)$, $\mathcal{P}'(u)$ with integral coefficients from K. According to the identity (3.4) the new sequence ψ_μ satisfies the same three term nonlinear recurrence (3.3):

$$\psi_{\mu+\eta}\psi_{\mu-\eta} = \psi_{\mu+1}\psi_{\mu-1}\psi_\eta^2 - \psi_{\eta+1}\psi_{\eta-1}\psi_\mu^2$$

(or its variations [D1], where "1" is replaced by a root ε of unity in K). The sequence ψ_μ is now an elliptic divisibility sequence in $\mathcal{O}$, i.e., ψ_μ divides ψ_η, if $\mu|\eta$ is in $\mathcal{O}$.

The sequence ψ_m contains as a subsequence ψ_n from (3.2). This implies additional divisibility properties for the original elliptic divisibility sequence ψ_n, whenever E has complex multiplication in K. For example, ψ_n can be prime for a prime $n = p$ only when p stays prime in K. If p splits in K: $p = \pi \cdot \pi^*$ for primes π and π^* in K, then $\psi_\pi \cdot \psi_{\pi^*}$ is a rational integer that divides ψ_p. Hence together with possible suspect for primality ψ_p for nonsplit unramified p, we obtain a new divisibility sequence and new suspects for primality

$$\phi_p = \psi_\pi \cdot \psi_{\pi^*}$$

for primes, π, π^* in K. The numbers ϕ_p are extremely interesting (they have no counterparts in the degenerate case), their only deficiency being small growth in p: the absolute value of ϕ_p growth as $c^{p \cdot (1+o(1))}$.

In the relation to the Little Fermat theorem 1.5 one notices that sequences $X_\mu = [\mu]_E(X_1)$ for $\mu \in \mathcal{O}$ can be also used to test the primality of μ or $n = \text{Norm}(\mu)$. Moreover there are additional relations connecting eigenvalues of the Frobenius with the Frobenius map. The fundamental relation, that belongs to Eisenstein [E1] is the following: If $p = \pi \cdot \pi^*$ splits in K, the $a_p = \text{Tr}(\pi)$ and $N_p = p + 1 - a_p = \text{Norm}(\pi - 1)$ (with a proper normalization of π). Then

$$[\pi]_E(X) \equiv X^p \bmod \pi \tag{3.11}$$

(the Lubin–Tate multiplication formula, see [HA1]). The statement (3.11) can be used together with an ordinary Little Fermat theorem and has to be considered as a part of $n^{\pm}$ primality tests of Sec. 2 (Proposition 2.7).

As much as a sequence ψ_p is similar to the Mersenne sequence M_p or Lucas' numbers U_p, one can introduce elliptic analogs of more general binomial numbers $ab^m \pm 1$. These numbers can arise for an elliptic curve $E/\mathbb{Q}$ having rank of the Mordell–Weil group $E(\mathbb{Q})$ at least two. Namely, let

Table 3

```
EllDivSeq4([1,2,7],69,[11,17,73],[2])
VALUE = ((0 0) (11 7000351) (17 -14984370728756449) (73 209196750952413269548441
138000941020917918876780203832700329383431149072313114298766144480557171197594 8
061057720991954838398575570686900731170502455209595453874590783078183385016330 6
908643896007189999876352936926787881606773134439502256827160909985116914084679 0
418274765046021379709995299891473064480 1))

EllDivSeq4([1,5,2],39,[7,43],[2])
VALUE = ((0 0) (7 -15383) (43 145495402062640239822692263631948014096885053962246
005697189549192804720709696919925226707810665209435320392389373176193445320662 7
489321806578596571969750918368 43))

EllDivSeq4([1,1,6],43,[13,23,43,47],[2])
VALUE = ((0 0) (13 56979431) (23 26861829566699646344634101) (43 617244596677482
241312212170172527047460930232865513176610862985485421645925165570685181 1) (47 1
729671144113805335010885800849044954706608863764184826184224390739992834768044 23
296146584878936492611377 99))

EllDivSeq4([1,1,10],57,[13,41,61],[2])
VALUE = ((0 0) (13 10055322559) (41 -241865576106011624699126432409343260902817 3
592165831486623757973883915709179729863503252933426626201520 49) (61 -10155350880
831525025709944716165236865710501038648395450636045899653733662980776256613170 97
315189863736505361954095457488349900801211674427871651755587536613939890073466 88
899625417031107201787065053655126523617655666921498250521280 1))

EllDivSeq4([1,1,-2],67,[13,23,61,71],[2])
VALUE = ((0 0) (13 -10601) (23 70187570532 13) (61 -121226614130047233419050197 29
642262449151310195819386072782387561500829336250894476228864 33) (71 311629949833
858300455722644943151976910982061289921941221647145387464527370298013423184580 35
069970783987329090790197291850 1))

EllDivSeq4([1,1,-9],75,[47,79],[2])
VALUE = ((0 0) (47 304075853353150774978065790453558575296402045027565381519375 3
257955546512643740515179015341722088490784425126786385938553012400816399) (79 40
811871799892425330092797485388635673836907815702068765160456297343665976808890 35
763291359657375622808619141752731951247136356376991771616696247675792560046031 95
065119753944488224480338150366201885018128919596651354243094629043659243026365 74
805201558166781442772910897259411043691909432420685039056501122303141009144720 99
145629472231224061138192072928670026584789275837265 59))

EllDivSeq4([1,4,1],75,[71,79],[2])
VALUE = ((0 0) (71 -28146692511423537150974775809634478301493141456732582506653 8
675399448621606636984466314392860054269442492300432449513648019497639608261139 34
430061438634582965722879865326902771944405349868891265560013808181817003665713 57
665054380766802486729659887441628576970409494518079608760370066406899779220568 84
954424436208958569938495573263281090214657030884198209424474977972092467566899 3)
(79 -402139486480542229300397012154644873022709876885703784415238743641635814 76
180655560487611109085436470221644290933462149510930996985014098518080692051154 77
788827860732169766176955668620669609766702106556848489947966493376093012824714 17
775895360339439072485992494721055233300731562822672172060836521485166028841830 16
309368538915631405114362025533245779677600363579623775528476498258029626195031 08
514442985769126370614788662397636263500718623217660668249441593957173478849))

EllDivSeq4([1,4,3],67,[13,53,71],[2])
VALUE = ((0 0) (13 -3165347956951) (53 623355753869898576806448900892987459734 63
894141188258134940144714098792415475619293957998317314285308517867013192851365 54
369544181144060599086894167715716825006825065685981264862109402590846654064909 62
90235998819) (71 -515414042951934768200007984096737865486894068894066994245939 2
929305153099025949681248573025002232439397340667478120744585351668712363374312 68
116491860218857257670989746006684746026555281682738154352281401030082886442795 32
470457529903197440876433477716901525135614269596594324557737737199438154023648 43
180687549871627461452455911165974195590889162913625230383612804501088434159761))

EllDivSeq4([2,1,4],67,[71],[2])
VALUE = ((0 0) (71 10597810243878468625579173244055908266225023411874930372332 99
580816032293084905691818923797009890935143896598759086515297088536641484995144 05
363322424628530134852957431719570830102805426428256291824676560652507031738251 71
777262891862511354982806781207614192089765541233184948479))
```

Table 3—*Continued*

```
:llDivSeq4(f(-15,1,4),37,[41],[2])
/ALUE = ((0 0) (41 -868555885929119048950561724811766644082389681716394213842383
591231169677653155376770706977166050806337864663003181033875069633279044179145 20
462866334056841726262611680364893255546995862195374577549437007527006266282077 98
560205715573922806935930036777944560695551638429877637252573614838025411077388 24
060071826711253729412974914811149352090231196064407236898431346219562742288708 784
716446465947378652953600915045498644342773279717566928410341658095195473619506 53
446601195055289540871171519455702216646231253111 9))

:llDivSeq4(f(-26,-1,5),25,[29],[2])
/ALUE = ((0 0) (29 790638452743511848761158818744178087635788099338541064436254 1
273648808040827148147995427993584085177311432442790489182422974171101961306377 30
311971208715504684793436661997077692235235983911752702720188830971041186586860 82
496552944443717533650241829664954975772602039248257242809768654 9))
```

Note. EllDivSeq4($[\psi_2, \psi_3, \psi_4]$, N, l,[2]) lists pairs (m, ψ_m) for primes and "probable primes" ψ_m in the elliptic divisibility sequence with initial terms $\psi_0 = 0$, $\psi_1 = 1$, ψ_2, ψ_3, ψ_4 and $m < N + 4$ for m from l. Similarly EllDivSeq4($f(d, x, y)$, N, l,[2]) lists as (m, ψ_m) "probable primes" ψ_m with m in l for a point (x, y) on $y^2 = x^3 - d$. Typically we checked the range $m < 100$.

$\tilde{x}_1$ and $\tilde{x}_2$ be two points from $E(\mathbb{Q})$ that are linearly independent over $\mathbb{Z}$. Let us consider

$$\tilde{X}_{n,12} \stackrel{\text{def}}{=} [n]_E \tilde{x}_1 \oplus_E \tilde{x}_2, \quad \tilde{X}_{n,12} = \left(\frac{X_{n,12}}{Z_{n,12}^2}, \frac{Y_{n,12}}{Z_{n,12}^3} \right),$$

where $\tilde{X}_{n,12}$ is written in an irreducible form. Then the numbers $Z_{n,12}$ are the analogs of $ab^m \pm 1$. The divisibility of numbers $Z_{n,12}$ by various (small) primes p follows from the relations between $\tilde{x}_1 \bmod p$ and $\tilde{x}_2 \bmod p$ in $E \pmod p$. Again the number $Z_{n,12}$ has an absolute value that grows as $c_{12}^{n^2 + O(1)}$, and is suitable to check for possible primality.

In Table 3, we present primes and "very probable primes" among elements of the elliptic divisibility sequences ψ_p, Z'_n, and $Z'_{n,12}$ and also ϕ_p (for E with complex multiplication in the last case). Primality of numbers was checked here using Rabin's probabilistic algorithm [RA1]. We did not try (till the moment the paper was completed, June 12, 1985) our primality test from Section 2 to check the primality of large numbers from Table 3.

For the fast computation of ψ_n one can use methods of Section 4 of efficient computation of nth multiple $\tilde{x}_n = (X_n/Z_n^2, Y_n/Z_n^3)$ of $\tilde{x}_1 = (X, Y)$. An alternative approach is to use the recurrence (3.3) directly to obtain the following formulas:

$$\psi_{2n+1} = \psi_{n+2}\psi_n^3 - \psi_{n-1}\psi_{n+1}^3,$$

$$\psi_{2n}\psi_2 = \psi_n\left(\psi_{n+2}\psi_{n-1}^2 - \psi_{n-2}\psi_{n+1}^2\right). \tag{3.12}$$

These formulas allow us to compute $(\psi_{2n+1}, \psi_{2n+2}, \ldots, \psi_{2n+9})$ starting from $(\psi_{n-1}, \psi_n, \ldots, \psi_{n+6})$. This method is similar to the binary method of multiplication applied to $[n]_{\tilde{F}}(\tilde{x})$ in Section 4.

The total number of multiplications to compute ψ_n do not exceed 20 $[\log_2 n]$, starting from ψ_2, ψ_3, ψ_4. In fact, the recurrent formulas (3.12) can be used mod p, instead of conventional addition formulas of Section 4.

4. Explicit Forms of Laws of Addition on Elliptic Curves and Their Computer Implementation

The key problem in the computer implementations, is to generates $\tilde{x}_n$ from $\tilde{x}_1$ as cost efficiently as possible. This problem is an obvious counterpart to the classical problem of evaluation of powers x^n (or exponentiations). As it is well known, that problem is polynomial in n. The same is true for the problem of generating nth multiple $\tilde{x}_n$ of $\tilde{x}_1$ using only algebraic operation of $\tilde{x} \oplus_F \tilde{y}$ (a general addition) and of $\tilde{x} \oplus_F \tilde{x}$ (a duplication).

Methods of fast evaluations of powers can be used here (see the discussion in [K1, Ch. 4.6.2]). For example, the simplest binary methods (right-to-left or left-to-right) require $[\log_2 n]$ additions and $\nu(n)$ duplications, where $\nu(n)$ is the number of "1" in the binary expansion of n, to compute $\tilde{x}_n$ from $\tilde{x}_1$. More sophisticated addition chains methods guarantee that $[\log_2 n] + o(n)$ additions are sufficient.

The crucial problem becomes the choice of the model of an algebraic group variety, where computations mod p are the least time consuming. We discuss various models for elliptic curve case. We remind the main quantity: $N_p = P_2(1)$ $(= p + 1 - a_p)$—the order of the group E (mod p)—is invariant under birational transformations and isogenies of the elliptic curve over the minimal ground field.

It is preferable to use models of elliptic curves lying in low-dimensional spaces, for otherwise the number of coordinates and operations is increasing. This limits us (up to obvious transformations) to 4 basic models of elliptic curves. These are:

4.1. (a) The Weierstrass model

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

(This form is sufficient instead of a more general equation (3.7)).

(b) The Jacobi model

$$v^2 = u^4 + au^2 + b.$$

(c) The Jacobi form representing the curve as an intersection of two quadrics in the 3-space:

$$x^2 + y^2 = 1,$$

$$k^2 \cdot x^2 + z^2 = 1,$$

parametrized by the Jacobi elliptic function $(sn(u, k) : cn(u, k) : dn(u, k) : 1)$.

(d) The cubic form, that can be reduced, after fractional transformations, to the canonical homogeneous (Hessian) form [Cleb]:

$$x^3 + y^3 + z^3 = Dxyz.$$

If one uses an affine model, then, perhaps, the Weierstrass model (a) is the most attractive. The *rational* expression for the laws of addition and duplication on (a) is the following:

If (x_1, y_1) and (x_2, y_2) are two points on the elliptic curve E in the form 4.1(a), then the expression for addition on the curve (a) $(x_1, y_1) \oplus_{E_a} (x_2, y_2) = (x_3, y_3)$ is

$$\begin{aligned} x_3 &= -(x_1 + x_2) + m^2 \\ y_3 &= -y_1 + m(x_1 - x_3) \end{aligned} \tag{4.1}$$

with m defined as

(i) $m = (y_2 - y_1)/(x_2 - x_1)$ when $(x_1, y_1) \neq (x_2, y_2)$;

(ii) $m = (3x_1^2 + a)/(2y)$ when $(x_1, y_1) = (x_2, y_2)$

(the formula (ii) defines the duplication case).

These formulae (4.1) (Euler and Abel) require an inversion mod p, if you treat these expressions mod p. We found that inversion is very costly—an obvious implementation of inversion mod p requires $O(\log^2 p)$ operations [K1]. There are, though some arguments for using the rational form of the law of addition. For example, Montgomery [MO1] proposes a different implementation of mod n arithmetic and notes that the inversion of k numbers mod n can be reduced to the inversion mod n of their product only and to several mutiplications mod n.

Nevertheless, we found it preferable to use a projective (homogeneous) form of elliptic curve equations, where the addition laws are *polynomial*.

4.2. (a) For the Weierstrass equation (a), the traditional choice of the homogeneous coordinates is $x = X/Z^2$, $y = Y/Z^3$, i.e., $(E^1_{a,b})$: $Y^2 = X^3 + aXZ^4 + bZ^6$. In these notations, the expression for the sum of two points $\tilde{x}_1 = (X_1/Z_1^2, Y_1/Z_1^3)$ and $\tilde{x}_2 = (X_2/Z_2^2, Y_2/Z_2^3)$ on the elliptic curve $(E^1_{a,b})$ is the following: $\tilde{x}_1 \oplus_{E^1_{a,b}} \tilde{x}_2 = \tilde{x}_{1,2}$, where $\tilde{x}_{1,2} = (X_{1,2}/Z_{1,2}^2, Y_{1,2}/Z_{1,2}^3)$ and

$$\begin{aligned} X_{1,2} &= -2Y_1Y_2W + (U_1 + U_2)\big(X_1X_2 + aW^2\big) + 2bW^4, \\ Y_{1,2} &= Z_2(U_1 + 3U_2)\big(aS_1Z_1 - X_1^2Y_2\big) \\ &\quad + Z_1(3U_1 + U_2)\big(X_2^2Y_1 - aS_2Z_2\big) + 4bW^3(S_1 - S_2), \\ Z_{1,2} &= U_2 - U_1, \end{aligned} \tag{4.2i}$$

with $U_1 = X_1 Z_2^2$, $U_2 = X_2 Z_1^2$, $S_1 = Y_1 Z_2^3$, $S_2 = Y_2 Z_1^3$, $W = Z_1 Z_2$, provided that $U_1 \neq U_2$ or $S_1 \neq S_2$. If $U_1 = U_2$ and $S_1 = S_2$ (i.e., in the duplication case) we put

$$\begin{aligned} X_{1,2} &= T, \\ Y_{1,2} &= -8Y_1^4 + M(S - T), \\ Z_{1,2} &= 2Y_1 Z_1 \end{aligned} \tag{4.2ii}$$

with $S = 4X_1 Y_1^2$, $M = 3X_1^2 + aZ_1^4$, $T = -2S + M^2$.

Expressions (4.2i)–(4.2ii) are symmetric and very convenient to use in the global case (say, over $\mathbf{Z}$), because we remove common factors between $X_{1,2}$, $Y_{1,2}$, and $Z_{1,2}$. However, the number of operations in (4.2i) is excessive and the law (4.2i) for addition depends on a and b. The duplication formula (4.2ii) is, on the other hand, quite efficient. It requires *9 multiplications* (to generate Y_1^2, Y_1^4, S, $Z_{1,2}$, Z_1^2, Z_1^4, M, T, $Y_{1,2}$) and one multiplication by a. The last multiplication can be disregarded, whenever in the general form of the Weierstrass equation $(E^1_{a,b})$ one puts $a \equiv 1$. It is even smarter to put $a \equiv -3$ in (4.2ii), though it might impair the generality of the Weierstrass equation $(E^1_{a,b})$ (it does not impare the generality for the purposes of Sect. 5). If $a \equiv -3$, then to compute (4.2ii) one needs only *8 multiplications* to generate Y_1^2, Y_1^4, S (through $X_1 Y_1^2$), Z_1^2, $M = 3 \cdot (X_1 - Z_1^2) \cdot (X_1 + Z_1^2)$, $Y_1 Z_1$ (and thus $Z_{1,2}$), M^2 (and thus T), $M \cdot (S - T)$ (and thus $X_{1,2}$). To repair the situation with (4.2i) we can refer directly to (4.1) and not remove common factors $Z_1 \cdot Z_2$ in the numerators and denominators of (4.1). Then instead of (4.2i) we obtain the following expressions:

$$\begin{aligned} \tilde{x}_{1,2} &= \left(X_3/Z_3^2, Y_3/Z_3^3 \right), \\ X_3 &= -(U_1 + U_2) \cdot P^2 + R^2, \\ Y_3 &= -S_1 \cdot P^3 + R \cdot \left(U_1 \cdot P^2 - X_3 \right), \\ Z_3 &= Z_1 \cdot Z_2 \cdot P \end{aligned} \tag{4.3i}$$

with $U_1 = X_1 Z_2^2$, $U_2 = X_2 Z_1^2$, $S_1 = Y_1 Z_2^3$, $S_2 = Y_2 Z_1^3$, when

$$P \overset{\text{def}}{=} U_2 - U_1 \neq 0 \quad \text{or} \quad R \overset{\text{def}}{=} S_2 - S_1 \neq 0.$$

The form (4.3i) of the general addition formula does not depend on the form of the Weierstrass equation $(E^1_{a,b})$. It requires *17 multiplications*. There is a way to reduce the number of multiplications, if to notice that (4.3i) is *not* symmetric in the definition of Y_3 (as the expression of y_3 is not in (4.1)). An obvious symmetrization of (4.3i) gives the following different expression

for Y_3 in (4.3i), leaving X_3 and Z_3 without changes,

$$2Y_3 = R \cdot \left(-2R^2 + 3P^2(U_1 + U_2)\right) - P^3(S_1 + S_2). \qquad (4.3i')$$

This reduces the number of multiplications only to *16* in the general addition formula (4.3i)–(4.3i'). We do not know, whether this number is the best possible in the representation $x = X/Z^2$, $y = Y/Z^3$ of (a). On the other hand, we can use a simple homogeneous model of (a): $x = X'/Z'$, $y = Y'/Z'$, i.e. $(E^{1'}_{a,b})$: $Y'^2Z' = X'^3 + aX'Z'^2 + bZ'^3$. In these notations the sum of two points $\tilde{x}_1 = (X_1'/Z_1', Y_1'/Z_1')$ and $\tilde{x}_2 = (X_2'/Z_2', Y_2'/Z_2')$ on $(E^{1'}_{a,b})$ is $\tilde{x}_1 \oplus_{E^{1'}_{a,b}} \tilde{x}_2 = \tilde{x}'_{1,2}$, where $\tilde{x}_{1,2} = (X'_{1,2}/Z'_{1,2}, Y'_{1,2}/Z'_{1,2})$ and

$$\begin{aligned} X'_{1,2} &= P' \cdot \left(-(U_1' + U_2') \cdot P'^2 + W'R'^2\right), \\ 2Y'_{1,2} &= R' \cdot \left(-2W' \cdot R'^2 + 3(U_1' + U_2') \cdot P'^2\right) - P'^3(S_1' + S_2'), \\ Z'_{1,2} &= W' \cdot P'^3 \end{aligned} \qquad (4.4i)$$

with $U_1' = X_1'Z_2'$, $U_2' = X_2'Z_1'$, $S_1' = Y_1'Z_2'$, $S_2' = Y_2'Z_1'$, $W' = Z_1' \cdot Z_2'$ when $P' \overset{\text{def}}{=} U_2' - U_1' \neq 0$ or when

$$R' \overset{\text{def}}{=} S_2' - S_1' \neq 0.$$

The duplication formula (when $P' = 0$ and $R' = 0$) is

$$\begin{aligned} X'_{1,2} &= (2Z_1'Y_1') \cdot \left[\left(3X_1'^2 + aZ_1'^2\right)^2 - 4(2Z_1'Y_1') \cdot X_1'Y_1'\right], \\ Y'_{1,2} &= -Y_1'^2 \cdot (2Z_1'Y_1')^2 + \left(3X_1'^2 + aZ_1'^2\right) \\ &\quad \times \left(6(2Z_1'Y_1') \cdot X_1'Y_1' - \left(3X_1'^2 + aZ_1'^2\right)^2\right), \\ Z'_{1,2} &= (2Z_1'Y_1')^3. \end{aligned} \qquad (4.4ii)$$

It takes *14 multiplications* in formulas (4.4i), and it takes *12 multiplications* in duplication formulas (4.4ii) including one multiplication by a. If, as above, one puts $a \equiv -3$, then the number of multiplications in (4.4ii) decreases to *10* (one computes $Z_1'Y_1'$, $(Z_1'Y_1')^2$, $(Z_1'Y_1')^3$, $Z_1'Y_1'^2$, $Z_1'Y_1'^2X_1'$, $(X_1' - Z_1') \cdot (X_1' + Z_1')$, $(Z_1'Y_1'^2X_1')^2$, $Y'_{1,2}$, $(X_1'^2 - Z_1'^2)^2$, $X'_{1,2}$).

There is a discrepancy between the number of operations in the addition formulas (4.3i), (4.2ii) and (4.4i)–(4.4ii) for two representations of points $\tilde{x}$: of $(x, y) = (X/Z^2, Y/Z^3)$ and of $(x, y) = (X'/Z', Y'/Z')$ from equations of the elliptic curve in the Weierstrass form (a): 16–17 multiplications versus 14 multiplications in the general addition formula and 8–10 multiplications versus 10–12 multiplications in the duplication formula. Since

duplication occurs as often as general addition (at least in the binary method of exponentiation), the laws of addition (4.3i), (4.2ii) are preferable. However, to achieve better results (on average) we propose to mix both representations of (x, y). Namely, in the form $(x, y) = (X/Z^2, Y/Z^3)$, we suggest to write addition formulas involving (X, Y, Z, Z^2, Z^3) as 5 variables. This obviously corresponds to a particular parametrization of the Jacobian of the elliptic curve by means of θ-functions of the third order (see below for cubic curves). Expressions for the law of addition are again based on (4.2ii) and (4.3i). Let the data $v_1 = (X_1, Y_1, Z_1, Z_1^2, Z_1^3)$, $v_2 = (X_2, Y_2, Z_2, Z_2^2, Z_2^3)$ correspond to $\tilde{x}_1 = (X_1/Z_1^2, Y_1/Z_1^3)$, $\tilde{x}_2 = (X_2/Z_2^2, Y_2/Z_2^3)$. Then the data $v_1 \oplus_E v_2 = (X_3, Y_3, Z_3, Z_3^2, Z_3^3)$ corresponding to $\tilde{x}_1 \oplus_{E_{a,b}^1} \tilde{x}_2 = (X_3/Z_3^2, Y_3/Z_3^3)$ are

$$\begin{aligned} X_3 &= -(U_1 + U_2) \cdot P^2 + R^2, \\ 2Y_3 &= R \cdot \left(-2R^2 + 3P^2(U_1 + U_2)\right) - P^3(S_1 + S_2), \\ Z_3 &= Z_1 \cdot Z_2 \cdot P, \\ Z_3^2 &= Z_3^2,\ Z_3^3 = Z_3^3 \end{aligned} \tag{4.5i}$$

with $U_1 = X_1 \cdot (Z_2^2)$, $U_2 = X_2 \cdot (Z_1^2)$, $S_1 = Y_1 \cdot (Z_2^3)$, $S_2 = Y_2 \cdot (Z_1^3)$, $P = U_2 - U_1 \neq 0$, $R = S_2 - S_1 \neq 0$.

In the case $U_1 = U_2$, $S_1 = S_2$ we put

$$\begin{aligned} X_3 &= -2S + M^2, \\ Y_3 &= -8Y_1^4 + M \cdot (3S - M^2), \\ Z_3 &= 2Y_1Z_1, \\ Z_3^2 &= Z_3^2,\ Z_3^3 = Z_3^3 \end{aligned} \tag{4.5ii}$$

with $S = 4X_1Y_1^2$, $M = 3X_1^2 + a \cdot (Z_1^2)^2$.

The addition formulas (4.5i) require *14 multiplications*, and a storage of quintiplet (X, Y, Z, Z^2, Z^3), instead of a triplet (X, Y, Z). The duplication formulas (4.5ii) require *10 multiplications* and one multiplication by a. If, as above, one puts $a \equiv -3$, then we need only *9 multiplications* in (4.5ii). Of course, there are plenty of additions and one can notice that formulas (4.5i)–(4.5ii) are just another way to represent (4.3i) and (4.2ii). We are not sure that (4.5i)–(4.5ii) give any significant practical improvement over (4.2ii) and (4.3i).

4.2. (b)–(c) Jacobi models (b) or (c) in some respects are preferable to (a). In dealing with Jacobi models one uses a large body of addition formulas for Jacobi θ-functions $\theta_1(z), \theta_2(z), \theta_3(z)$, and $\theta_4(z)$ [Jac1]. Many of these addition formulas can be used directly to derive algebraic

laws of addition, whenever an elliptic curve is represented as an intersection of two (arbitrary) quadrics. In general, projective coordinates for such an imbedding are given by $(\theta_1(z):\theta_2(z):\theta_3(z):\theta_4(z))$. The relation with the Jacobi's elliptic functions is given by

$$\begin{aligned} sn(u,k) &= (\theta_3(0)\cdot\theta_1(z))/(\theta_2(0)\cdot\theta_4(z)),\\ cn(u,k) &= (\theta_4(0)\cdot\theta_2(z))/(\theta_2(0)\cdot\theta_4(z)),\\ dn(u,k) &= (\theta_4(0)\cdot\theta_3(z))/(\theta_3(0)\cdot\theta_4(z)), \end{aligned} \tag{4.6}$$

for $z = u/\theta_3(0)^2$ and for

$$k^2 = \theta_2(0)^4/\theta_3(0)^4.$$

To represent the laws of addition for the Jacobi model (c), parametrized by $(sn(u,k):cn(u,k):dn(u,k):1)$, in the *polynomial* form we introduce homogeneous coordinates:

$$\begin{aligned} sn(u,k) &= S/T,\\ cn(u,k) &= C/T,\\ dn(u,k) &= D/T. \end{aligned} \tag{4.7}$$

In these notations, the Jacobi form (c) of the elliptic curve E $(= E_{k^2})$ is described by the equations:

$$(E_{k^2})\colon S^2 + C^2 = T^2,\ k^2S^2 + D^2 = T^2. \tag{4.8}$$

In the notations (4.7), the rational form of the laws of addition for *sn*, *cn*, *dn* [Jac1; T-M] are represented in the following polynomial form.

Let $\overline{\overline{X}}_1 = (S_1, C_1, D_1, T_1)$ and $\overline{\overline{X}}_2 = (S_2, C_2, D_2, T_2)$ be two points on the elliptic curve (E_{k^2}) (4.8). Then the sum $\overline{\overline{X}}_3 = \overline{\overline{X}}_1 \oplus_{E_{k^2}} \overline{\overline{X}}_2$ of $\overline{\overline{X}}_1$ and $\overline{\overline{X}}_2$ is defined as

$$\overline{\overline{X}}_3 = (S_3, C_3, D_3, T_3),$$

where

$$\begin{aligned} S_3 &= T_1C_2\cdot S_1D_2 + D_1S_2\cdot C_1T_2,\\ C_3 &= T_1C_2\cdot C_1T_2 - D_1S_2\cdot S_1D_2,\\ D_3 &= T_1D_1T_2D_2 - k^2\cdot S_1C_1S_2C_2,\\ T_3 &= (T_1C_2)^2 + (D_1S_2)^2. \end{aligned} \tag{4.9i}$$

The formulas (4.9i) have a tremendous advantage of being universally valid as general addition formulas, and simultaneously as duplication formulas, when $\overline{\overline{X}}_1 = \overline{\overline{X}}_2$ (i.e., no limit analysis as $\overline{\overline{X}}_2 \to \overline{\overline{X}}_1$ is necessary, as it is necessary for the Weierstrass model (a)). Nevertheless, since a duplication

formula plays a special role in the fast schemes of multiplication, we present it separately:

The duplication $\overline{\overline{X}}_3 = \overline{\overline{X}}_1 \oplus_{E_{k^2}} \overline{\overline{X}}_1$ of $\overline{\overline{X}}_1 = (S_1, C_1, D_1, T_1)$ on (E_{k^2}) is defined as:

$$\overline{\overline{X}}_3 = (S_3, C_3, D_3, T_3),$$

where

$$\begin{aligned} S_3 &= 2 \cdot C_1T_1 \cdot D_1S_1, \\ C_3 &= (C_1T_1)^2 - (D_1T_1)^2 + (C_1D_1)^2, \\ D_3 &= (D_1T_1)^2 - (C_1T_1)^2 + (C_1D_1)^2, \\ T_3 &= (D_1T_1)^2 + (C_1T_1)^2 - (C_1D_1)^2. \end{aligned} \tag{4.9ii}$$

The number of multiplications in the duplication formula (4.9ii) is *8 only* $(C_1T_1,\ D_1S_1,\ C_1T_1 \cdot D_1S_1, (C_1T_1)^2,\ D_1T_1,\ C_1D_1, (D_1T_1)^2, (C_1D_1)^2)$, 3 of which are squaring. Perhaps (?), this is the most efficient duplication formulas which do not depend on the coefficients of an elliptic curve.

The general addition formula (4.9i) on the other hand require *17 multiplications*, including one multiplication by a constant k^2 $(T_1C_2,\ S_1D_2,\ D_1S_2,\ C_1T_2,\ T_1C_2 \cdot S_1D_2,\ D_1S_2 \cdot S_1D_2,\ T_1C_2 \cdot C_1T_2,\ D_1S_2 \cdot S_1D_2, (T_1C_2)^2, (D_1S_2)^2,\ T_1D_1,\ T_2D_2,\ T_1D_1 \cdot T_2D_2,\ S_1C_1,\ S_2C_2,\ S_1C_1 \cdot S_2C_2,\ k^2 \cdot S_1C_1 \cdot S_2C_2)$. The number of operations in the addition formula (4.9i) can be slightly decreased, if to increase the number of variables involved by considering θ-functions of order higher than two (similar to formulas (4.5i)–(4.5ii)). Instead, we start with the Weierstrass model (b), which itself is parametrized by θ-functions of orders 2 and 4.

For the Weierstrass model (b), we introduce the homogeneous coordinates by $u = U/W$, $v = V/W^2$ and obtain the equation $(E^2_{a,b})$: $V^2 = U^4 + aU^2W^2 + bW^4$. Then the "proper" form of the law of addition on $(E^2_{a,b})$, that removes common factors, has the following form:

The sum, $\tilde{z}_3$, of two points $\tilde{z}_1 = (U_1/W_1, V_1/W_1^2)$ and $\tilde{z}_2 = (U_2/W_2, V_2/W_2^2)$ on $(E^2_{a,b})$ is

$$\tilde{z}_3 = \left(U_3/W_3, V_3/W_3^2\right),$$

where

$$\begin{aligned} U_3 &= U_1W_1V_2 - U_2W_2V_1, \\ W_3 &= U_2^2W_1^2 - U_1^2W_2^2, \\ V_3 &= V_1V_2\left(U_2^2W_1^2 + U_1^2W_2^2\right) \\ &\quad - U_1U_2W_1W_2\left(2U_1^2U_2^2 + a\left(U_2^2W_1^2 + U_1^2W_2^2\right)\right. \\ &\qquad \left. + 2b \cdot W_1^2W_2^2\right). \end{aligned} \tag{4.10i}$$

The duplication formula cannot be considered as a part of (4.10i). Instead the double $\tilde{z}_3$ of the point $\tilde{z}_1 = (U_1/W_1, V_1/W_1^2)$ has the form

$$\tilde{z}_3 = \left(U_3/W_3, V_3/W_3^2\right),$$

where

$$\begin{aligned} U_3 &= U_1^4 - bW_1^4, \\ W_3 &= 2U_1V_1W_1 \\ V_3 &= V_1^4 - (a^2 - 4b)U_1^4W_1^4 \cdot \end{aligned} \tag{4.10ii}$$

The duplication formula (4.10ii) requires slightly more operations than in (4.9ii), though less storage. First of all, if a and b are arbitrary, the number of operations is *11 multiplications* (U_1^2, W_1^2, V_1^2, U_1^4, W_1^4, V_1^4, bW_1^4, $U_1^4W_1^4$, $(a^2 - 4b)U_1^4W_1^4$, U_1V_1, $U_1V_1W_1$), two of which are multiplications by fixed numbers: b and $a^2 - 4b$, and 6 of the multiplications are squarings. However, if parameters of the $(E^2_{a,b})$ are chosen in the form: $b = \xi^2$, $a^2 - 4b = \zeta^2$, then the number of operations in the law of addition becomes *10 multiplications* (U_1^2, W_1^2, ξW_1^2, V_1^2, $U_1^2W_1^2$, $\zeta U_1^2W_1^2$, U_1V_1, $U_1V_1W_1$ and 2 more multiplications to generate U_3, V_3). The number of operations in the general addition formula (4.10i) is *16 multiplications* and *2* multiplications by fixed integers a and b.

One can try to use, as for model (a), another form for the law of addition for $(E^2_{a,b})$, when U_3, W_3, and V_3 are not in the reduced form, i.e., have a common factor. An advantage of such approach is the independence of the addition formula from the parameters a and b. The new expression for the sum $\tilde{z}_3 = (U_3/W_3, V_3/W_3^2)$ of $\tilde{z}_1 = (U_1/W_1, V_1/W_1^2)$ and $\tilde{z}_2 = (U_2/W_2, V_2/W_2^2)$ is the following

$$\begin{aligned} U_3 &= W_1W_2(U_1W_1V_2 - U_2W_2V_1), \\ W_3 &= W_1W_2\left(U_2^2W_1^2 - U_1^2W_2^2\right), \\ V_3 &= W_1W_2U_1U_2\left(U_2^2W_1^2 - U_1^2W_2^2\right) \\ &\quad + W_1W_2U_1U_2\left(V_1^2W_2^4 + V_2^2W_1^4\right) \\ &\quad + (W_1W_2)^2V_1V_2\left(U_1^2W_2^2 + U_2^2W_1^2\right). \end{aligned} \tag{4.11}$$

Still another possibility is to use the "common sense" projective coordinates on $(E^2_{a,b})$: $(UW : V : W^2)$. Indeed, in these notations the double of the point $\tilde{z}_1' = (U_1'/W_1', V_1'/W_1')$ on $(E'^2_{a,b})$: $V'^2W'^2 = U'^4 + aU'^2W'^2 +$

bW'^4 has the form

$$\begin{aligned} \tilde{z}_3' &= (U_3'/W_3', V_3'/W_3'); \\ U_3' &= 2U_1'V_1'\left(V_1'^4 - aU_1'^2 - 2bW_1'^2\right), \\ W_3' &= 4U_1'^2V_1'^2, \\ V_3' &= V_1'^4 - (a^2 - 4b)U_1'^4. \end{aligned} \tag{4.12i}$$

Similarly, the sum of two points $\tilde{z}_1' = (U_1'/W_1', V_1'/W_1')$ and $\tilde{z}_2' = (U_2'/W_2', V_2'/W_2')$ on $(E'^2_{a,b})$ as defined as

$$\tilde{z}_3' = (U_3'/W_3', V_3'/W_3'),$$

where

$$\begin{aligned} U_3' &= (U_1'V_2' - U_2'V_1') \cdot \left(U_2'^2 \cdot W_1'^2 - U_1'^2W_2'^2\right)W_1'W_2', \\ W_3' &= \left(W_1'^2U_2'^2 - W_2'^2U_1'^2\right)^2, \\ V_3' &= U_1'U_2' \cdot \left(W_1'U_2'^2 - W_2'U_1'^2\right) \\ &\quad + W_1'W_2'U_1'U_2'\left(V_1'^2W_2'^2 + V_2'^2W_1'^2\right) \\ &\quad + W_1'W_2'V_1'V_2'\left(U_1'^2W_2'^2 + U_2'^2W_1'^2\right). \end{aligned} \tag{4.12ii}$$

Let us present a comparison of the computational cost of the addition formulas (4.11) and addition and duplication formulas (4.12i)–(4.12ii). The general addition formula (4.11) on $(E^2_{a,b})$ takes *18 multiplications* (W_1W_2, U_2W_1, U_1W_2, $U_1^2W_2^2$, $U_2^2W_1^2$, W_1^2, W_2^2, $V_1W_2^2$, $V_2W_1^2$, $V_1^2W_2^4$, $V_2^2W_1^4$, $V_1V_2 \cdot W_1^2W_2^2$, $U_1U_2W_1W_2$, $U_1W_2 \cdot V_2W_1^2$, $U_2W_1 \cdot V_1W_2^2$ and 3 more multiplications to obtain W_3 and V_3), though the law (4.11) is independent of a and b.

The total number of multiplications in the duplication formula (4.12i) is *8 plus 3* multiplications by fixed integers a, b, $a^2 - 4b$. (The number can be further reduced, if b and $a^2 - 4b$ are squares.) The number of operations to compute the addition formula (4.12ii) is 22 multiplications, but the addition formula (4.12ii) does not depend on the form of the equation $(E'^2_{a,b})$.

If one uses an addition chain or addition–subtraction chain methods of multiplication, it might be useful to have simple laws of multiplication $[n]_E(\tilde{x})$ for small n, that are simpler than those following from general addition and duplication formulas. The case in question is a simple triplication formula for the Jacobi model (c) in the notations (4.8). Let $\tilde{\tilde{X}}_1 = (S, C, D, T)$ be the point on (E_{k^2}). Then its triple, $\tilde{\tilde{X}}_3 = [3]_{E_{k^2}}(\tilde{\tilde{X}}_1)$ has the form

$$\tilde{\tilde{X}}_3 = (S_3, C_3, D_3, T_3),$$

where

$$S_3 = S\big(3T^8 - 4(1+k^2)S^2T^6 + 6k^2S^4T^4 - k^4S^8\big),$$
$$C_3 = C\cdot\big(T^8 - 4S^2T^6 + 6k^2S^4T^4 - 4k^4S^6T^2 + k^4S^8\big),$$
$$D_3 = D\cdot\big(T^8 - 4k^2S^2T^6 + 6k^2S^4T^4 - 4k^2S^6T^2 + k^4S^8\big),$$
$$T_3 = T\cdot\big(T^8 - 6k^2S^4T^4 + 4k^2(1+k^7)S^6T^2 - 3k^4S^8\big).$$

The number of operations in the computations $\overline{\overline{X}}_3 = 3 * \overline{\overline{X}}_1$ is at most 19 multiplications (T^2, T^4, T^8, S^2, S^4, k^2S^4, k^4S^8, S^2T^4, S^2T^6, k^2S^6, k^2T^2, $k^2S^2T^6$, $k^2S^6T^2$, $k^4S^6T^2$, $k^2S^4T^4$ and four multiplications by S, C, D, and T in S_3, C_3, D_3, T_3).

Sometimes it is preferable to set your mind on the use of simplest binary (left-to-right) method of multiplication. An example of an application of such method was given in Section 3, where a fast method of evaluation of elliptic divisibility sequences by means of recurrences (3.12) was presented. As we remarked, this binary method requires $20[\log_2 n]$-multiplications to compute ψ_n from the initial conditions ψ_2, ψ_3, ψ_4. Taking into account the identification (3.1), one realizes that it gives a method of computation Z_n in $\tilde{x}_n\ (= [n]_{E^1_{a,b}}(\tilde{x}_1)) = (X_n/Z_n^2, Y_n/Z_n^3)$ from $\tilde{x}_1 = (X_1/Z_1^2, Y_1/Z_1^3)$ and a, b on the curve $(E^1_{a,b})$.

The binary method, that we are using, has the following pattern: you use the duplication formula to find $\tilde{x}_{2n}$ from $\tilde{x}_n$, and you find $\tilde{x}_{2n+1}$ from $\tilde{x}_n$ and $\tilde{x}_{n+1}$. Thus we need: (a) the duplication formula, and (b) the law of addition in the form familiar from Jacobi [Jac1]:

$$\theta_\alpha(\bar{u}+\bar{v})\theta_\alpha(\bar{u}-\bar{v}) = \text{"polynomial in } \theta_\beta(\bar{u}), \theta_\beta(\bar{v})\text{."} \qquad (4.13)$$

It turns out that the original Jacobi computations [Jac1] for the one dimensional law of addition in the form (4.13) provide a perfect setting for the binary method of multiplications. We start with a Jacobi model (b) of the form $(E^2_{a,b})$: $V^2 = U^4 + aU^2W^2 + bW^4$. Then from the original formulas for the law of addition (4.10i)–(4.10ii) on $(E^2_{a,b})$ we deduce the following "binary laws of addition": let $\tilde{z}_r = (U_r/W_r, V_r/W_r^2)$ and $\tilde{z}_s = (U_s/W_s, V_s/W_s^2)$ be two points on $(E^2_{a,b})$. Then for *the sum* $\tilde{z}_{r+s}$ and for *the difference* $\tilde{z}_{r-s}$ of points $\tilde{z}_r$ and $\tilde{z}_s$ we obtain the expressions

$$\tilde{z}_{r+s} = \big(U_{r+s}/W_{r+s}, V_{r+s}/W_{r+s}^2\big),$$
$$\tilde{z}_{r-s} = \big(U_{r-s}/W_{r-s}, V_{r-s}/W_{r-s}^2\big)$$

where

$$U_{r+s}U_{r-s} = U_r^2U_s^2 - bW_r^2W_s^2,$$
$$W_{r+s}W_{r-s} = U_s^2W_r^2 - U_r^2W_s^2,$$
$$V_{r+s}V_{r-s} = V_r^2V_s^2 - (a^2-4b)U_r^2U_s^2W_r^2W_s^2. \qquad (4.14)$$

The binary law (4.14) is used to compute $\tilde{z}_{2m}$ and $\tilde{z}_{2m+1}$ from $\tilde{z}_m$ and $\tilde{z}_{m+1}$ (and $\tilde{z}_1$). In obvious notations $\tilde{z}_i = (U_i/W_i, V_i/W_i^2)$, we deduce from (4.14):

$$\begin{aligned} U_{2m} &= U_m^4 - bW_m^4, \qquad V_{2m} = V_m^4 - (a^2 - 4b)U_m^2W_m^2, \\ W_{2m} &= 2U_mV_mW_m, \\ U_{2m+1}U_1 &= U_m^2U_{m+1}^2 - bW_m^2W_{m+1}^2, \\ W_{2m+1}W_1 &= U_m^2W_{m+1}^2 - U_{m+1}^2W_m^2, \\ V_{2m+1}V_1 &= V_m^2V_{m+1}^2 - (a^2 - 4b)U_m^2U_{m+1}^2W_m^2W_{m+1}^2. \end{aligned} \tag{4.15}$$

The total number of multiplications in (4.15) is

(a) *18 multiplications* (U_m^2, U_m^4, V_m^2, V_m^4, W_m^2, W_m^4, $U_m^4W_m^4$, U_mW_m, $U_mW_mV_m$, U_{m+1}^2, $U_m^2U_{m+1}^2$, W_{m+1}^2, $W_m^2W_{m+1}^2$, $U_m^2W_{m+1}^2$, $U_{m+1}^2W_m^2$, V_{m+1}^2, $V_m^2V_{m+1}^2$, $U_m^2W_{m+1}^2W_m^2U_{m+1}^2$);

(b) *4 multiplications* by fixed numbers b, $(a^2 - 4b)$; and

(c) at most *2* multiplications by U_1^{-1} and V_1^{-1} (say, considered mod n as in Section 5). Here $\tilde{x}_1 = (U_1, V_1)$ is an (arbitrary) initial point on $(E_{a,b}^2)$. The number of operations can be reduced to *21* total in (a)–(b), if, as we suggested earlier, b and $a^2 - 4b$ are squares.

The most spectacular version of the binary method of multiplication can be achieved in the Jacobi model (c) in the form (E_{k^2})—(4.8). If one uses Jacobi's law of addition (4.13) for $\theta_1(u)$ and $\theta_4(u)$ [Jac1], then it turns out that the laws of addition for $\theta_1^2(u)$ and $\theta_4^2(u)$ involve *only* θ_1^2 and θ_4^2! This enables us to write a binary rule of multiplication involving only two variables. In the notations of the Jacobi curve (E_{k^2}) these variables are S^2 and T^2. To see these binary laws of addition we reproduce from [T-M; Jac1] the binary laws of addition for the function $sn^2(u) = sn^2(u, k)$:

$$\begin{aligned} sn^2(u+v)\cdot sn^2(u-v) &= \frac{\left(sn^2(u) - sn^2(v)\right)^2}{\left(1 - k^2sn^2(u)sn^2(v)\right)^2} \\ sn^2(2u) &= \frac{4sn^2(u)\cdot\left(1 - sn^2(u)\right)\cdot\left(1 - k^2sn^2(u)\right)}{\left(1 - k^2sn^4(u)\right)^2}. \end{aligned} \tag{4.16}$$

Introducing the natural homogeneous variables X and Y such that $sn^2(u, k) = X/(kY)$, we obtain the following version of the addition law. Let $\overline{\overline{X}}_r = (S_r, C_r, D_r, T_r)$ and $\overline{\overline{X}}_t = (S_t, C_t, D_t, T_t)$ be two points on (E_{k^2}), and let $\overline{\overline{X}}_{r+t} = (S_{r+t}, C_{r+t}, D_{r+t}, T_{r+t})$ be the *sum*, and $\overline{\overline{X}}_{r-t} =$

$(S_{r-t}, C_{r-t}, D_{r-t}, T_{r-t})$ be the *difference* of $\overline{\overline{X}}_r$ and $\overline{\overline{X}}_s$ on (E_{k^2}). Let us put, as above,

$$\begin{aligned} S_r^2 : T_r^2 &= X_r : kY_r \\ S_t^2 : T_t^2 &= X_t : kY_t \\ S_{r+t}^2 : T_{r+t}^2 &= X_{r+t} : kY_{r+t} \\ S_{r-t}^2 : T_{r-t}^2 &= X_{r-t} : kY_{r-t}. \end{aligned} \tag{4.17}$$

Then the binary form of the law of addition for $(X_{r\pm t} : Y_{r\pm t})$ from $(X_r : Y_r)$, $(X_t : Y_t)$ is

$$\begin{aligned} X_{r+t}X_{r-t} &= (X_rY_t - X_tY_r)^2, \\ Y_{r+t}Y_{r-t} &= (X_rX_t - Y_rY_t)^2. \end{aligned} \tag{4.18i}$$

The duplication formulas for $(X_{2r} : Y_{2r})$ from $(X_r : Y_r)$ are

$$\begin{aligned} X_{2r} &= 4X_rY_r\left(Y_r - \frac{1}{k}X_r\right)(Y_r - kX_r) \\ &= 4X_rY_r(X_r^2 + Y_r^2 - \xi X_rY_r), \\ Y_{2r} &= (X_r^2 - Y_r^2)^2, \end{aligned} \tag{4.18ii}$$

with $\xi = k + 1/k$.

The total number of operations in (4.18i) is *6 multiplications* (two of which are squarings). The number of operations in (4.18ii) is *6 multiplications*, 3 of which are squarings and one is a multiplication by a fixed number $\xi = k + 1/k$. Thus we arrive from (4.18ii) to the following scheme of computation of $(X_{2n+1} : Y_{2n+1})$ and $(X_{2n} : Y_{2n})$ from $(X_n : Y_n)$ and $(X_{n+1} : Y_{n+1})$ (the binary method):

$$\begin{aligned} X_{2n+1} \cdot X_1 &= (X_{n+1}Y_n - X_nY_{n+1})^2, \\ Y_{2n+1} \cdot Y_1 &= (X_{n+1}X_n - Y_{n+1}Y_n)^2, \\ X_{2n} &= 4X_nY_n(X_n^2 + Y_n^2 - \xi X_nY_n), \\ Y_{2n} &= (X_n^2 - Y_n^2)^2. \end{aligned} \tag{4.19}$$

If X_1 and Y_1 are properly chosen from (4.17) and (4.8) (say, X_1^{-1} or Y_1^{-1} is a smaller number), then the binary scheme (4.19) produces, starting from $(X_1 : Y_1)$ and ξ the nth multiple $(X_n : Y_n)$ of $(X_1 : Y_1)$ in $13[\log_2(n)]$ *multiplications*. If X_1 and Y_1 are arbitrary, one needs $11[\log_2(n)]$ multiplications and $3[\log_2(n)]$ multiplications by fixed numbers: ξ, X_1^{-1}, Y_1^{-1}.

We recommend the scheme (4.19) as a better law of addition. It should be noted, that the point on infinity on (E_{k^2}) in variables X, Y (4.18) corresponds to $X = 0$. Thus in the algorithms of Section 5 one should look for $\gcd(X_N, n)$, and in algorithms of Sections 2–3 one should study the divisibility properties of X_m.

4.2. (d) Our experience shows that the expression of the law of addition on the cubic Hessian form (d) of an elliptic curve is by far the best and the prettiest. First of all, it is because of the obvious homogeneous and symmetric character of the equation

$$\left(E_D^3\right): x^3 + y^3 + z^3 = Dxyz.$$

The original form for the law of addition on the general cubic, and, in particular, on the cubic (E_D^3), belong to Cauchy (see [Des]). For the sake of completeness we present the Cauchy formulas for $\overline{\overline{X}}_3$—the minus of the sum of two points $\overline{\overline{X}}_1 = (x_1, y_1, z_1)$ and $\overline{\overline{X}}_2 = (x_2, y_2, z_2)$ on (E_D^3)—

$$\overline{\overline{X}}_3 = -\left(\overline{\overline{X}}_1 + \overline{\overline{X}}_2\right),$$

$$\overline{\overline{X}}_3 = (x_3, y_3, z_3),$$

where

$$\begin{aligned} x_3 &= 3y_1y_2(x_1y_2 - y_1x_2) + 3z_1z_2(x_1z_2 - z_1x_2) \\ &\quad - D\left(x_1^2y_2x_2 - x_2^2y_1z_1\right), \\ y_3 &= 3x_1x_2(y_1x_2 - x_1y_2) + 3z_1z_2(y_1z_2 - z_1y_2) \\ &\quad - D\left(y_1^2x_2z_2 - y_2^2x_1z_1\right), \\ z_3 &= 3x_1x_2(z_1x_2 - x_1z_2) + 3y_1y_2(z_1y_2 - z_2y_1) \\ &\quad - D\left(z_1^2x_2y_2 - z_2^2x_1y_1\right). \end{aligned} \tag{4.20}$$

These formulas are inconvenient to use, though they were chosen in [De-F]. Sylvester was the first to note (see the derivation in [Des]), that the general formula of Cauchy, as applied to the canonical Hessian form (E_D^3) takes much simpler form.

First of all we remark that the *inverse*, $-\overline{\overline{X}}$, of the $\overline{\overline{X}} = (x, y, z)$ on (E_D^3) is

$$-\overline{\overline{X}} = (y, x, z).$$

Similarly, the neutral point on (E_D^3) corresponding to the point of infinity on the Weierstrass model of (E_D^3) is $\overline{O} = (1, -1, 0)$.

Taking these remarks into consideration, let $\overline{\overline{X}}_1 = (x_1, y_1, z_1)$ and $\overline{\overline{X}}_2 = (x_2, y_2, z_2)$ be two points on (E_D^3). Then the inverse of the sum of $\overline{\overline{X}}_1$ and

$\overline{\overline{X}}_2$ on (E_D^3): $\overline{\overline{X}}_3 = -(\overline{\overline{X}}_1 \oplus_{E_D^3} \overline{\overline{X}}_2)$ of two points $\overline{\overline{X}}_1 = (x_1, y_1, z_1)$ and $\overline{\overline{X}}_2 = (x_2, y_2, z_2)$ on (E_D^3) – $\overline{\overline{X}}_3 = \overline{\overline{X}}_1 \oplus_{E_D^3} \overline{\overline{X}}_2$ is $\overline{\overline{X}}_3 = (x_3, y_3, z_3)$, where

$$\begin{aligned} x_3 &= x_1^2 y_2 z_2 - x_2^2 y_1 z_1 \\ y_3 &= y_1^2 x_2 z_2 - y_2^2 x_1 z_1, \\ z_3 &= z_1^2 y_2 x_2 - z_2^2 y_1 x_1. \end{aligned} \tag{4.21i}$$

Here we assume that $\overline{\overline{X}}_1 \neq \overline{\overline{X}}_2$, i.e. $(x_1 : y_1 : z_1) \neq (x_2 : y_2 : z_2)$. If, however, $\overline{\overline{X}}_1 = \overline{\overline{X}}_2$, i.e. $(x_1 : y_1 : z_1) = (x_2 : y_2 : z_2)$, then we have the duplication formula for $\overline{\overline{X}}_1$. The inverse of the double of $\overline{\overline{X}}_1$ is: $\overline{\overline{X}}_3 = -(\overline{\overline{X}}_1 \oplus_{E_D^3} \overline{\overline{X}}_1)$,

$$\overline{\overline{X}}_3 = (x_3, y_3, z_3),$$

where

$$\begin{aligned} x_3 &= x_1(y_1^3 - z_1^3), \\ y_3 &= y_1(z_1^3 - x_1^3), \\ z_3 &= z_1(x_1^3 - y_1^3). \end{aligned} \tag{4.21ii}$$

The addition of two points on (E_D^3) according to (4.21i) thus requires only *12 multiplications* and *3 substitutions*. The duplication of the curve of the form (E_D^3) requires *9 multiplications* and *3 substitutions*.

In particular, one can obtain $\overline{\overline{X}}_n$ from $\overline{\overline{X}}_1$ in the model (d): (E_D^3) in $12 \log_2 n + o(n)$ multiplications.

It is important to note that the addition laws on elliptic curves of the form (d), *do not depend* on the equation of a curve. Thus, if one starts, say with a triple

$$X = (x_1, y_1, z_1) \bmod n$$

of (non-zero) mod n numbers, then the equation (E_D^3) of the form (d), of an elliptic curve, on which X is lying, is uniquely determined as

$$x^3 + y^3 + z^3 = Dxyz$$

for $D = (x_1^3 + y_1^3 + z_1^3)/(x_1 y_1 z_1) \bmod n$. Of course, one *does* not have to compute D at all.

5. Implementations of Elliptic Curve Factorization Algorithms

Let us describe the implementation of Lenstra's probabilistic factorization algorithm that uses elliptic curves, and its relations to other factorization algorithms.

It is useful to return to "$n \pm 1$" primality testing of Section 2. We saw that the factorization (complete or partial) of $n \pm 1$ can be used to prove the primality of n. Similarly, Pollard [POL1] suggested in 1974 the "$p - 1$" factorization method that used the factorization of $p - 1$ for a prime p of n, to find p itself. This method, apparently, was known for years to Lehmer and Lehmer, see [WIL1].

The idea here is the following. If you "know" that n has a factor p such that $(p - 1)|B$ say, then all powers q^a of primes that divide $p - 1$ are bounded by M: $q^a \leq M$, or $B = \text{lcm}\{1, \ldots, M\}$. Then by Fermat's little theorem:

$$a^B \equiv 1 \bmod p \qquad \text{for } (a, n) = 1$$

or

$$p | \gcd(n, a^B - 1).$$

Thus $\gcd(n, a^B - 1)$ gives a factor n. It was natural then to Williams *et al.* [WIL1] to propose a "$p + 1$" method of factorization, that uses Lucas functions and the Little Fermat Theorem for Lucas's sequence, to check the factorization of n, when for its suspect factor p there is a (partial) factorization of $p + 1$.

Lenstra proposed recently (see [ML1]) an elliptic generalization of "$p \pm 1$" factorization method. His method starts with the key quantity—

$$N_p = p + 1 - a_p—$$

the number of points on an elliptic curve $E(\bmod p)$—and may give a factorization of n if its prime factor p has a controllable factorization of N_p (i.e., when all prime factors of N_p are bounded by a quantity significantly smaller than p).

Here $|a_p| < 2\sqrt{p}$, so $N_p \in (p + 1 - 2\sqrt{p}, p + 1 + 2\sqrt{p})$. Thus Lenstra proposes to vary $E(\bmod n)$ randomly, so a_p is random and N_p is random in the interval $(p + 1 - 2\sqrt{p}, p + 1 + 2\sqrt{p})$. Then there are "high" chances that N_p will have only "small" factors for some $E(\bmod n)$, and thus $\tilde{x}_M \equiv \tilde{0} \bmod p$ for an appropriate computable M, and thus the gcd of n and the (denominator) of $\tilde{x}_M$, gives a nontrival factor of n.

We propose the following implementation of Lenstra algorithm of factorization of a composite n. Two parameters, M_n and K_n (the running time) are described at the end of algorithm.

One starts with a composite number n and precomputes a "seed number" $N = \prod_{p \leq M_n} p^{[\log M_n / \log p]} = \text{lcm}\{1, \ldots, M_n\}$. Then the following operations are repeated:

(1) Start with a "random" $\overline{\overline{X}}_1 = (x_1 : y_1 : z_1) \bmod n$—say, $\overline{\overline{X}}_1 = (x_1 : y_1 : 1)$ for two "random" numbers $x_1 \bmod n$ and $y_1 \bmod n$;

(2) compute $\overline{\overline{X}}_N = [N]_{E_D}(\overline{\overline{X}}_1) = (x_N : y_N : z_N)$ for a seed number N, starting from $\overline{\overline{X}}_1$ on the elliptic curve (E_D^3) in the cubic Hessian form (d) of Section 4.

(3) Check for $\lambda = \gcd(z_N, n)$. If $1 < \lambda < n$, then λ is a factor of n; if $\lambda = n$ then one looks for $\overline{\overline{X}}_m$ as in (2) for $m|N$, say $m = \operatorname{lcm}\{1, \ldots, M'\}$ and $M' < M_n$.

If $\lambda = 1$ repeat.

The number of trials for which (1)–(3) are to be repeated to "guarantee" the factorization of n with a probability $\geq 1 - \varepsilon$ is about K_n.

The numbers M_n and K_n are defined as follows. If P $(< \sqrt{n})$ is the "expected" bound for a divisor of n and y is a solution of

$$y^2 = \frac{\log P}{\log y + 1}, \tag{5.1}$$

then

$$M_n = P^{1/y};$$

$$K_n = -\log \varepsilon \cdot y^y. \tag{5.2}$$

The number of multiplications is about $12 \cdot (1 + o(1)) \cdot K_n M_n / \log 2$, the number of additions is $3(1 + o(1))K_n M_n / \log 2$ and there are $3(1 + o(1))K_n M_n / \log 2$ reductions mod n.

Step (2) of the algorithm—the multiplication on the elliptic curve—takes practically the entire running time. It is here, where all the exercises of Section 4 appear. Depending on the model and on the scheme of multiplication, and also due to the randomness in the choice of curve, the time in part (2) can vary significantly. We implemented parts (1)–(2) of the algorithm for nearly all schemes of addition laws from Section 4. Our preferences clearly lies with the cubic model (d). However, the Weierstrass model (a) performed fairly. Sometimes, it is advantageous to use the binary method of multiplication in Jacobi model (c) in the form (4.19) because of its simplicity. Another point, connected with comments of Section 6, is the choice of "random" elliptic curve and a point on it. This is done naturally for the cubic curves (d) in step (1) above, because a point $\overline{\overline{X}}_1$ determines a curve (E_D^3). It is not obvious, though, how to find a point on an elliptic curve in models (a)–(c). We propose the following simplest recipes. For the Weierstrass model (a), one can choose randomly $x \bmod n$, $y \bmod n$, and $a \bmod n$ (either randomly or as $a \equiv 1$ or $a \equiv -3$ as recommended in Section 4) and then put $b = y^2 - x^3 - ax \bmod n$. If, in the Weierstrass model (a) one wants to have all possible values of the invariant j, the most known form of the curve $(E_{a,b}^1)$, having the invariant j is $(E_{a,-a}^1)$: $y^2 = x^3 + a(x - 1)$ for $a = 27j/(4(1 - j))$. The nontrivial point on this curve is $(x, y) = (1, 1)$. If one wants a point on a Jacobi curve in the form (b), similar arguments can be

applied. This is not the case, however, with the Jacobi model (c). The difference can be explained by looking on the corresponding elliptic surfaces. The elliptic curve $(E^1_{a,-a})$ above, considered over the function field $\mathbb{C}(j)$, has rank of its Mordell–Weil group one. On the other hand, the elliptic curve of the form (c)—(4.8)—considered over $\mathbb{C}(k)$, has only torsion points. One can use the following alternative: choose randomly $x, y, z \bmod n$ and put $k^2 = ((x^2 + y^2)^2 - z^2)/(4x^2y^2) \bmod n$, and get a nontrivial point $\overline{\overline{X}}_1 = (2xy, x^2 - y^2, z, x^2 + y^2) \bmod n$ on the curve $(E^2_{k^2})$.

Our personal experience with the implementation of Lenstra's algorithm is, generally speaking, positive. We are not going to compare it with other factorization algorithms (see Introduction). It seems that the general algorithm (1)–(3), together with various modifications of Sections 4 and 6, is powerful enough to factorize numbers accessible to other methods only on very big machines with highly customized software. We, on the contrary, use LISP(!) as a programming language and standard IBM hardware.

We will describe successes of various implementations of factorization algorithms in our next report.

6. More on Elliptic Curves and Abelian Varieties

We want to comment on some ways of reducing the number of operations in computations with elliptic curves.

One of the bottlenecks in implementation of the factorization algorithm of Section 5 is the computation of $\overline{\overline{X}}_N$ in step (2) for a large $N \sim e^{M_n}$, where M_n is determined by (5.1), (5.2). Clearly, N is enormous, when P (the bound on the factor of n) is large. One of the ways to decrease N, and thus the number of operations in step (2), is to be sure that the order N_p of $E \bmod p$ is a priori divisible by some number m. In this case P in (5.1)–(5.2) can be substituted by P/m. To achieve such a situation one should start with an elliptic curve E having a torsion point of order m. In fact, it is enough to examine the cases, when the Galois group of the Tate module E_l for $l|m$ is smaller than a generic one. Unfortunately, such elliptic curves exist in characteristic zero over $\mathbb{Q}$ only for a few m or a few curves (due to Mazur [Maz1] and the Mordell conjecture). Moreover, even in the cases, when the torsion is parametrizable over $\mathbb{Q}$ (15 exceptional torsion subgroups), it is not easy to construct rationally an elliptic curve E_{ex} with a given torsion subgroup (genus zero case for an appropriate modular curve) and a point of infinite order on this curve. Without such a point of infinite order in characteristic zero, it would be hard to find nontrivial points on $E_{ex} \bmod n$ for a composite n. Still it is possible to obtain a model of an elliptic curve $E_{ex} = E_{ex}(t)$, having over $\mathbb{Q}(t)$ exceptional torsion subgroups,

and having over $\mathbb{Q}(t)$ a point of infinite order. If $f\colon X \to \mathbb{C}(t)$ is the Neron model of $E(t)/\mathbb{C}(t)$, and p_g be the arithmetic genus of X, then $p_g = 0$ can happen only when the order m of the torsion subgroup is bounded by 4. For $p_g = 1$ the only new torsion subgroups are $\mathbb{Z}/5\mathbb{Z}$, $\mathbb{Z}/6\mathbb{Z}$, $\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$ (the last case is over $\mathbb{Q}(\sqrt{-3}, t)$), cf. [Cox].

Nevertheless, the construction of elliptic curves $E/\mathbb{F}_p$ with an arbitrary torsion m is definitely possible, however large m is. One simply looks on mod p solutions to the modular equations, or, in other words, on points on modular curves, like $X_1(m)$ over finite fields. In our implementations with various m, this and other methods were often useful, when, say, the number n is of a particular form (so that roots of unity mod n are easy to find: e.g., n is of the form $a^k - 1$), or when one searches for a curve E mod n with a large torsion and finds it "half of the time." It is possible that the method of choosing large m can lead to a significant reduction of part (2) of the algorithm of Section 5. In this method one takes a special representation of E, say with $j = P(x)$, and a model of $X_1(m)$ as a covering of x-plane of the smallest degree.

A large field for future studies is open by the possibility of considering other algebraic laws of addition related to the Frobenius operator (say, cubic surfaces or intermediate Jacobians). These methods are, actually, useful in various primality tests similar to those described in Section 2. We already remarked in this relation that the use of Abelian varieties with complex multiplications [T1, H1] allows us to obtain the tests of primality of n depending on (complete or partial) factorization of $n^a \pm n^b + 1$ with integers $a > b$. The use of CM-curves and varieties is by far the best method of primality proving. Little Fermat theorem 1.5 and its natural generalizations provide us with a variety of such primality tests involving ζ-functions of algebraic varieties over function fields. Implementation of these tests is a serious problem because explicit expression for addition laws are hard to come by.

In the factorization algorithm of Section 4 the immediate use of higher dimensional Abelian varieties does not seem to be helpful, because whenever $g > 1$, N_p grows as $p^g + O(p^{g/2})$ and "it is less likely" that N_p will be divisible by small primes only. Nevertheless, several possibilities arise. First of all we can try to decrease the number of computations. For this we propose to consider g "arbitrary" elliptic curves simultaneously as a single Jacobian of a curve of genus $g > 1$, isogeneous to the product of these g elliptic curves. For $g > 3$ we do not know whether such a Jacobian always exists (and whether the coefficients of the corresponding curve are algebraic functions in invariants of elliptic curves). However, for $g = 2$ and $g = 3$ we have explicit formulas, connected with our work on poles of meromorphic solutions of the Kadomtzev–Petviashvili equation [CH5]. We have studied, in general, various possible forms of laws of addition on Abelian varieties,

Prym varieties, and Abelian surfaces for small genuses and their computer implementations. In particular, we investigated simple forms of laws of addition on hyperelliptic surfaces, isogenous to the product of two elliptic curves. The number of operations for a duplication on such a surface is *14 multiplications* (i.e., 7×2 for 2 curves) and *23 multiplications* for the general addition.

Expressions for laws of addition of Jacobians and other Abelian varieties can be found, e.g., in [BA, IGU, MUM]. The use of θ-functions with characteristics provides a simple form of the addition law, however, a number of variables is growing fast with the genus (dimension) g. Laws of addition on Jacobians and Abelian varieties are nicely presented through their representation (see [MUM]) as intersection of quadrics (cf., with the Jacobi model (c) of Sect. 4). For the 2-dimensional case we have chosen even θ-functions of order two and a Kummer surface parametrized by them.

We present here only the duplication formula on Kummer surfaces. For a point $\overline{\overline{X}}_1 = (x, y, z, w)$ on a Kummer surface ($g = 2$), we put

$$\begin{aligned} x' &= (x + y + z + w)^2, \\ y' &= y_0' \cdot (x + y - z - w)^2, \\ z' &= z_0' \cdot (x - y + z - w)^2, \\ w' &= w_0' \cdot (x - y - z + w)^2. \end{aligned} \tag{6.1}$$

Then the double $\overline{\overline{X}}_2$ of $\overline{\overline{X}}_1$ is defined as

$$\overline{\overline{X}}_2 = (x_2, y_2, z_2, w_2),$$

where

$$\begin{aligned} x_2 &= (x' + y' + z' + w')^2, \\ y_2 &= y_0 \cdot (x' + y' - z' - w')^2, \\ z_2 &= z_0 \cdot (x' - y' + z' - w')^2, \\ w_2 &= w_0 \cdot (x' - y' - z' + w')^2. \end{aligned} \tag{6.2}$$

Here

$$\begin{aligned} y_0' &= (\mu - 1)(\nu - 1)/(\mu + 1)(\nu + 1), \\ z_0' &= (\nu - 1)(\lambda - 1)/(\nu + 1)(\lambda + 1), \\ w_0' &= (\lambda - 1)(\mu - 1)/(\lambda + 1)(\mu + 1), \\ y_0 &= (\lambda\mu\nu - 1)/(\lambda - \mu\nu), \\ z_0 &= (\lambda\mu\nu - 1)/(\mu - \nu\lambda), \\ w_0 &= (\lambda\mu\nu - 1)/(\nu - \lambda\mu), \end{aligned}$$

and λ, μ, ν are the moduli of the hyperelliptic curves—explicit functions of coefficients of the quintic polynomial $P_5(x)$ in the hyperelliptic curve equation $y^2 = P_5(x)$. The values of $y_0', z_0', \ldots, z_0, w_0$ are precomputed mod$n$.

Note a pretty symmetry in the doubling formulas (6.1)–(6.2); also most of the multiplications are squares (and others are multiplications by fixed numbers).

We did not yet address the question of the distribution of the trace of Frobenius a_p, or, of $N_p = p + 1 - a_p$, as an elliptic curve E (mod p) varies and p is fixed. This is not the Sato–Tate distribution problem, though it is related [SAR]. This problem is important in the analysis of Lenstra's probabilistic algorithm of Section 5.

There are at most $[4\sqrt{p}]$ values of a_p, but there are p nonisomorphic curves mod p, if to count only absolute invariants (in general, there are p^2 curves in the Weierstrass form). What is the distribution function of $E \to a_p(E)$ as a curve E (mod p) varies? It is convenient here to use the Legendre form E_λ, introduced in Section 1 with $a_p = a_p(\lambda)$ defined there. Let us denote

$$u_p(\lambda) = a_p(\lambda)^2/p$$

(i.e., $0 \le u_p(\lambda) \le 4$), then the trace formula implies [YAM] that the distribution function of $u_p(\lambda)$ with a fixed (large) p is

$$\rho(u) = \frac{1}{2}\sqrt{\frac{4-u}{u}}\,. \tag{6.3}$$

Thus one is more likely to get a small value of $a_p(\lambda)$. However, the distribution (6.3) has little to do with the speed of Lenstra's algorithm, where the distribution of numbers with small prime factors is more important than that of traces of Frobenius.

ACKNOWLEDGMENTS

We want to thank Computer Algebra Group at IBM Research, particularly Richard Jenks and Barry Trager for their constant support and help. Many of the results presented in this report would never have materialized without their support and the support of their systems—SCRATCHPAD and SCRATCHPAD II. We thank N. Brenner for his advice and V. Miller for many references. Our computations were performed at IBM Research at Yorktown Heights. This work was partially supported by the U.S. Air Force under Grant AFOSR-81-0190 and by the National Science Foundation under grant MCS-82-10292. The text of this paper was presented as IBM Research Report RC 11262 on 7/12/85.

REFERENCES

[BS] E. BACH AND J. SHALLIT, Factoring with cyclotomic polynomials, *in* "IEEE Annu. Found. of Comput. Sci. Symposium," to appear.

[BA] H. F. BAKER, "Abel's Theorem and the Allied Theory Including the Theory of the Theta Function," Cambridge Univ. Press, 1897.

[B1] E. T. BELL, Analogies between the u_n, v_n of Lucas and elliptic functions, *Bull. Amer. Math. Soc.* **29** (1923), 401–406.

[BSh] Z. I. BOREVIČ AND I. R. SHAFAREVICH, "Number Theory," Academic Press, New York, 1966.

[BS1] J. BRILLHART AND J. L. SELFRIDGE, Some factorization of $2^n \pm 1$ and related results, *Math. Comp.* **21** (1967), 87–96; correction ibid., p. 751.

[BLS] J. BRILLHART, D. H. LEHMER, AND J. L. SELFRIDGE, New primality criteria and factorization of $2^m \pm 1$, *Math. Comp.* **29** (1975), 620–647.

[BLSTW] J. BRILLHARD, D. H. LEHMER, L. J. SELFRIDGE, B. TUCKERMAN, AND S. S. WAGSTAFF, JR., Factorization of $b^n \pm 1$, $b = 2, 3, 5, 6, 7, 10, 11, 12$ up to high powers, Contemp. Math. Vol. 22, Amer. Math. Soc., Providence, R.I., 1980.

[CA1] J. W. S. CASSELS, Diophantine equations with special reference to elliptic curves, *J. London Math. Soc.* **41** (1966), 193–291; correction, **42** (1967), 183.

[CH1] D. V. CHUDNOVSKY AND G. V. CHUDNOVSKY, Padé approximations and diophantine geometry, *Proc. Natl. Acad. Sci. U.S.A.* **82** (1985), 2212–2216.

[CH2] D. V. CHUDNOVSKY AND G. V. CHUDNOVSKY, Applications of Padé approximations to the Grothendieck conjecture on linear differential equations, *in* "Number Theory, New York 1984," Lecture Notes in Math. Vol. 1135, Springer-Verlag, New York, 1985, 52–100.

[CH3] D. V. CHUDNOVSKY AND G. V. CHUDNOVSKY, The Grothendieck conjecture and Padé approximations, *Proc. Japan Acad. Ser. A. Math. Sci.* **61** (1985), 87–91.

[CH4] G. V. CHUDNOVSKY, "Contributions to the Theory of Transcendental Numbers," Math. Surveys Monogr. Vol. 19, Chap. 7, Amer. Math. Soc., Providence, R.I., 1984.

[CH5] D. V. CHUDNOVSKY, Meromorphic solutions of nonlinear partial differential equations and many particle completely integrable systems, *J. Math. Phys.* **20** (1979), 2416–2422.

[Cleb] A. CLEBSCH, "Lecons sur la Géométrie," Vol. 2, Gauthier–Villars, Paris, 1880.

[Cox] D. A. COX, Mordell–Weil groups and invariants of elliptic surfaces, Amherst College preprint, in press.

[Cl1] C. H. CLEMENS, "A Scrapbook of Complex Curve Theory," Plenum, New York, 1980.

[DH1] J. A. DAVID AND D. B. HOLDRIDGE, Most wanted factorizations using the quadratic sieve, Sandia report SAND 84–1658, 1984.

[De-F] B. N. DELONE AND D. K. FADDEEV, "The Theory of Irrationalities of the Third Degree," Amer. Math. Soc. Translation Vol. 10, Providence, R.I., 1964.

[Des] M. DESBOVES, Résolution en nombres entiers et sous sa forme la plus générale, de l'equation cubique, homogène, a trois incounues, *Nouvelles Ann. de Math.* **45** (1886), 545–579.

[DI1] L. E. DICKSON, "History of the Theory of Numbers," Vols. 1–3, Chelsea, New York, 1952.

[DIX1] J. D. DIXON, Asymptotically fast factorization of integers, *Math. Comp.* **36** (1981), 255–260.

[D1] L. K. DURST, The apparition problem for equianharmonic divisibility sequences, *Proc. Natl. Acad. Sci. U.S.A.* **38** (1952), 330–333.

[E1] G. EISENSTEIN, "Mathematische Werke," 2 vols., Chelsea, New York, 1957.

[GA1] C. F. GAUSS, "Disquisitiones Arithmeticae" (translated by A. A. Clarke), Yale Univ. Press, New Haven, Conn., 1966.

[Gr1] B. H. GROSS, Arithmetic on elliptic curves with complex multiplication, Lecture Notes in Math. Vol. 776, Springer-Verlag, New York, 1980.

[Guy] R. K. GUY, How to factor a number, *in* "Proc. Fifth Manitoba Conf. Numer. Math., Utilitas," Winnipeg, 1975, pp. 49–89.

[HW] G. H. HARDY AND E. M. WRIGHT, "An Introduction to the Theory of Numbers," 4 ed., (Clarendon), Oxford Univ. Press, London, 1960.

[HA1] M. HAZEWINKEL, "Formal Groups and Applications," Academic Press, New York, 1973.

[He1] K. HEEGNER, Diophantische analysis and modulfunktionen, *Math. Z.* **56** (1952), 227–253.

[H1] T. HONDA, Isogeny classes of Abelian varieties over finite fields, *J. Math. Soc. Japan* **20** (1968), 83–95.

[H2] T. HONDA, On the theory of commutative formal groups, *J. Math. Soc. Japan* **22** (1970), 213–246.

[IGU] J.-I. IGUSA, "Theta Functions," Springer-Verlag, New York, 1972.

[IN1] K. INKERI, Tests for primality, *Ann. Acad. Sci. Fenn. Ser. A I Math.* **279** (1960).

[Jac1] C. L. JACOBI, Fundamenta Nova Theoriae Functionum Ellipticarum, Konigsberg, 1829; Gesammelte Werke, Vol. 1, pp. 49–239; 497–538, 1881.

[Ka1] N. M. KATZ, An overview of Delign's proof of the Riemann hypothesis for varieties over finite field, *in* "Mathematical developments arising from Hilbert problem, Proc. Sympos. Pure Math." Vol. 28, pp. 275–305, Amer. Math. Soc., Providence, R.I., 1976.

[K1] D. E. KNUTH, "The Art of Computer Programming," Vol. 2, 2nd ed. Addison–Wesley, Reading, Mass., 1981.

[LH1] D. H. LEHMER, Computer technology applied to the theory of numbers, MAA Studies in Math. Vol. 6, pp. 117–151, Prentice–Hall, Englewood Cliffs, N.J., 1969.

[LH2] D. H. LEHMER, An extended theory of Lucas' functions, *Ann. of Math.* **31** (1930), 419–448.

[LE1] H. W. LENSTRA, JR., Primality testing algorithms (after Adleman, Rumely and Williams), Séminaire Bourbaki, 33 année, 1980/81, No. 576.

[LE2] H. W. LENSTRA, JR., Miller's primality test, *Inform. Process. Lett.* **8** (1979), 86–88.

[L1] S. LICHTENBAUM, On p-adic L-functions associated to elliptic curves, *Invent. Math.* **56** (1980), 19–55.

[LU1] E. LUCAS, "Théorie des Nombres," Tome 1, Blanchard, Paris, 1961.

[LU2] E. LUCAS, Considerations nouvelles sur la théorie des nombres premiers et sur la division géometrique de la circonference en parties egales, *Assoc. France Adv. Sci. C.R.* **6** (1877), 162.

[Maz1] B. MAZUR, Modular curves and the Eisenstein ideal, *Inst. Hautes Etudes Sci. Publ. Math.* **47** (1978), 33–186.

[MI1] G. L. MILLER, Riemann's hypothesis and tests for primality, *J. Comput System Sci.* **13** (1976), 300–317.

[ML1] V. MILLER, Use of elliptic curves in cryptography, to appear.

[MO1] P. MONTGOMERY, Modular multiplication without trial division, *Math. Comp.* **44** (1985), 519–521.

[MB1] M. A. MORRISON AND J. BRILLHART, A method of factoring and the factorization of F_7, *Math. Comp.* **29** (1975), 183–205.

[MUM] D. MUMFORD, On the equations defining Abelian varieties, I–III, *Invent. Math.* **1** (1966), 287–354; **3** (1967), 75–135, 215–244.

[POCK] H. C. POCKLINGTON, The determination of the prime or composite nature of large numbers by Fermat's theorem, *Proc. Cambridge Philos. Soc.* **18** (1914–16), 29–30.

[POL1] J. M. POLLARD, A Monte Carlo method for factorization, *BIT* **15** (1975), 331–334.

[POL2] J. M. POLLARD, Theorems on factorization and primality testing, *Proc. Cambridge Philos. Soc.* **76** (1974), 521–528.

[PO1] C. POMERANCE, Recent development in primality testing, *Math. Intelligencer* **3** (1980–81), 97–105.

[PO2] C. POMERANCE, Analysis and comparison of some integer factoring algorithms, *in* "Computational Methods in Number Theory (H. W. Lenstra, Jr. and R. Tijdeman, Eds.), Math. Centrum Tracts Vol. 154, Part I, pp. 89–139, Math. Centrum, Amsterdam.

[PRO] E. PROTH, Théoremes sur les nombres premiers, *C.R. Acad. Sci. Paris Ser. I Math.* **87** (1879), 926.

[RA1] M. O. RABIN, Probabilistic algorithm for primality testing, *J. Number Theory* **12** (1980), 128–138.

[Ri1] H. RIESEL, Lucasian criteria for the primality of $N = h \cdot 2^n - 1$, *Math. Comp.* **23** (1969), 869–875.

[SAR] P. SARNAK, Statistical properties of eigenvalues of the Hecke operators, 1985, preprint, to appear.

[Sch1] R. SCHOOF, Elliptic curves over finite fields and the computation of square roots mod p, *Math. Comp.* **44** (1985), 483–494.

[SE1] J. P. SERRE, "Groupes Algébriques et Corps de Classes," Hermann, Paris, 1959.

[Slo1] D. SLOWINSKI, Searching for the 27th Mersenne prime, *J. Recreational Math.* **11** (1978–79), 258–261.

[T-M] J. TANNERY AND J. MOLK, "Éléments de la Théorie des Fonctions Elliptiques," 2 vols., Gauthier–Villars, Paris, 1898; Chelsea, New York, 1956.

[T1] J. TATE, Endomorphisms of Abelian varieties over finite fields, *Invent. Math.* **2** (1966), 134–144.

[T2] J. TATE, Classes d'isogénie des variétés Abéliennes sur un corps fini, Séminaire Bourbaki No. 352, 1968.

[T3] J. TATE, Algorithm for determining the type of a singular fiber in an elliptic pencil, *in* "Modular Functions of One Variable IV," Lecture Notes Math. Vol. 476, pp. 33–52, Springer-Verlag, New York, 1975.

[Tu1] B. TUCKERMAN, The 24th Mersenne prime, *Proc. Natl. Acad. Sci. U.S.A.* **68** (1971), 2319–2320.

[W1] M. WARD, Memoir on elliptic divisibility sequences, *Amer. J. Math.* **70** (1948), 31–74.

[W2] M. WARD, Arithmetical properties of the elliptic polynomials arising from the real multiplication of the Jacobi functions, *Amer. J. Math.* **72** (1950), 284–302.

[W3] M. WARD, Arithmetical properties of polynomials associated with the lemniscate elliptic functions, *Proc. Natl. Acad. Sci. U.S.A.* **36** (1950), 359–362.

[W4] A. WEIL, "Elliptic Functions According to Eisenstein and Kronecker," Springer-Verlag, New York, 1976.

[W5] A. WEIL, "Variétiés Abéliennes et Courbes Algébriques," Hermann, Paris, 1948.

[W6] A. WEIL, Number of solutions of equations in finite fields, *Bull. Amer. Math. Soc.* **55** (1949), 497–508.

[Wat1] G. N. WATSON, Singular moduli (3), *Proc. London Math. Soc.* **40** (1936), 83–142.

[Web1] H. WEBER, "Lehrbuch der Algebra," Vol. 3, Braunschweig, 1908.

[WIL1] H. C. WILLIAMS A $p + 1$ method of factoring, *Math. Comp.* **39** (1982), 225–234.

[WIL2] H. C. WILLIAMS, The primality of $N = 2A3^n - 1$, *Canad. Bull.* **15** (1972), 585–589.

[WIL3] H. C. WILLIAMS, A class of primality tests for trinomials which includes the Lucas–Lehmer test, *Pacific J. Math.* **98** (1962), 477–497.

[WJ] H. C. WILLIAMS AND J. S. JUDD, Some algorithms for prime testing using generalized Lehmer functions, *Math. Comp.* **30** (1976), 867–886.

[WH] H. C. WILLIAMS AND R. HOLTE, Some observations on primality testing, *Math. Comp.* **32** (1978), 905–917.

[YAM] M. YAMAUCHI, Some identities on the character sum containing $x(x-1)(x-\lambda)$, *Nagoya Math. J.* **42** (1971), 109–113.