Compact elliptic curve representations

Mathieu Ciet, Jean-Jacques Quisquater and Francesco Sica

Communicated by Neal Koblitz

Abstract. Let $y^2 = x^3 + ax + b$ be an elliptic curve over $\mathbb{F}_p$, $p$ being a prime number greater than 3, and consider $a, b \in [1, p]$. In this paper, we study elliptic curve isomorphisms, with a view towards reduction in the size of elliptic curves coefficients. We first consider reducing the ratio $a/b$. We then apply these considerations to determine the number of elliptic curve isomorphism classes. Later we work on both coefficients. We introduce the number $M(p)$ as the lower bound of all $M \in \mathbb{N}$ such that each isomorphism class has a representative with $\max(a, b) < M$. Using results from the theory of uniform distributions, we prove upper and lower bounds of the form $c_1 p^{1/2} < M(p) < c_2 p^{3/4}$ with explicit constants $c_1, c_2 > 0$.

Keywords. Elliptic curves, exponential sums, uniform distribution, cryptography.

2010 Mathematics Subject Classification. 14H52, 14G50.

1 Introduction

It is always an arduous task to classify elliptic curves according to certain properties. Here we are interested in determining isomorphic representatives of elliptic curves with coefficients in a given size range. This is especially important for cryptographic applications and other explicit computations where size matters. In the first part, we give a method to construct, given an elliptic curve over $\mathbb{F}_p$ with equation $y^2 = x^3 + ax + b$, an isomorphic curve where $a \in [1, p]$ is small. We prove that it is possible to determine such an isomorphic curve from a given one and we produce an algorithm for it. Later we construct from a curve another isomorphic one with the particularity that both $a$ and $b$ are equal or equal up to a small multiplicative constant. We also define a function

$$M(p) = \max_i \min_{E \in \text{Cl}_i} \max(a, b),$$

This work was performed when the first two authors were working on the NESSIE project (see www.cryptonessie.org) at the Université catholique de Louvain, Belgium.
where the first maximum is taken over all isomorphism classes of elliptic curves over $\mathbb{F}_p$ and the minimum over all elliptic curves of the $i$-th isomorphism class. We use Weil’s celebrated bound on exponential sums together with an idea of Tietäväinen to get a non-trivial explicit upper bound on $M(p)$.

2 Normalization

We denote $E_{/\mathbb{F}_p}(a, b)$ the curve defined over the finite field $\mathbb{F}_p$ with the equation $y^2 = x^3 + ax + b$.

In choosing one of the two parameters of the curve, it is possible to reduce the cost of operations where these parameters appear, as in formulas of duplication.

**Proposition 2.1.** Let $p > 3$ be a prime number. Let $\tilde{E}_{/\mathbb{F}_p}(\tilde{a}, \tilde{b})$, where $\tilde{a}$ and $\tilde{b}$ are two fixed numbers in the interval $[0, p - 1]$. There exists a curve $E_{/\mathbb{F}_p}(a, b)$ where $a \in [0, p - 1]$ is a “small number” (less than a small bound $B$), isomorphic over $\mathbb{F}_p$ to $\tilde{E}_{/\mathbb{F}_p}(\tilde{a}, \tilde{b})$.

**Proof.** We know that two curves $E_{/\mathbb{F}_p}(a, b)$ and $E_{/\mathbb{F}_p}(\tilde{a}, \tilde{b})$ are isomorphic over $\mathbb{F}_p$ if and only if there exists $u \in \mathbb{F}_p \setminus \{0\}$ such that

$$\begin{cases} \tilde{a} = u^4 a, \\ \tilde{b} = u^6 b. \end{cases}$$

(2.1)

If $\tilde{a} \leq B$, take $a = \tilde{a}$ and $b = \tilde{b}$. Otherwise, it is possible to choose a quadratic residue $v^2 \pmod{p}$ such that $\tilde{a} v^{-2}$ is very small (say $< \sqrt[3]{B}$ if $B$ is chosen carefully). If $v = u^2$, we are done since we can define $a$ and $b$ by (2.1). Otherwise, choose a small $w^{-1} < \sqrt[3]{B}$ quadratic non-residue and set $a = \tilde{a} (vw)^{-2}$. This time $vw = u^2$ is a quadratic residue and we can define $a$ and $b$ by (2.1) again. Note that in all cases $a$ is represented by an integer less than $B$. A nearly optimal choice of $B$ depends conditionally on the extended Riemann hypothesis and would give $B = \log^6 p$.

This proof is constructive. Hence it is possible to choose the classical method to find a “good” curve, in cryptographic sense, and later obtain a curve with one coefficient which is a “small number”.

So with this method, it is possible to reduce the number of multiplications, by replacing some multiplications into multiplication by constant, particularly for point duplication, where the coefficient $a$ is always used.

**Proposition 2.2.** Let $E(db, b)$ and $\tilde{E}(\tilde{d}b, \tilde{b})$ be two curves defined over the finite field $\mathbb{F}_p$. If $d \neq 0$ and $E$ is isomorphic to $\tilde{E}$, then $b = \tilde{b}$. 
Proof. Let \( E(db,b) \) and \( \sim E(d\tilde{b},\tilde{b}) \) be two curves defined over \( \mathbb{F}_p \), and \( d \neq 0 \). Then \( E \) and \( \sim E \) are isomorphic if and only if there exists \( u \in \mathbb{F}_p \) such that \( \tilde{b} = u^4b \) and \( \tilde{b} = u^6b \) which implies \( u^2 = 1 \), and hence \( u = \pm 1 \). \( \square \)

**Proposition 2.3.** Let \( E \) be a curve defined over a finite field \( \mathbb{F}_p \), by the equation \( E : y^2 = x^3 + ax + b \). If \( (\frac{ab}{p}) = 1 \), there exists a curve \( \sim E \) over \( \mathbb{F}_p \)-isomorphic to \( E \), defined by the equation \( \sim E : y^2 = x^3 + \tilde{a}x + \tilde{b} \), where \( \tilde{a} = b \). Furthermore, this curve is unique.

**Proof.** Let \( E \) and \( \sim E \) be two curves defined and isomorphic over \( \mathbb{F}_p \). The first curve \( E \) is given and the second \( \sim E \) is to determine.

The equations of the curves are

\[
E : y^2 = x^3 + ax + b \quad \text{and} \quad \sim E : y^2 = x^3 + \tilde{a}x + \tilde{b}.
\]

We have that \( E \) and \( \sim E \) are isomorphic over \( \mathbb{F}_p \) if and only if there exists an element \( u \in \mathbb{F}_p^* \) such that

\[
\begin{align*}
\tilde{a} &= u^4a, \\
\tilde{b} &= u^6b.
\end{align*}
\]

Let \( (g) = \mathbb{F}_p^* \). We will distinguish two cases.

**Case 1:** \( a \) and \( b \) are quadratic residues in \( \mathbb{F}_p \).

The system of equations (2.2) is equivalent to the fact that there exists \( k, \alpha \) and \( \beta \) such that

\[
\begin{align*}
a &= g^{2\alpha}, \\
b &= g^{2\beta}, \\
u &= g^k, \\
\tilde{a} &= g^{4k}g^{2\alpha} = (g^2)^{2k+\alpha}, \\
\tilde{b} &= g^{6k}g^{2\beta} = (g^2)^{3k+\beta}.
\end{align*}
\]

If we choose \( k \equiv \alpha - \beta \ (\mod \frac{p-1}{2}) \), then we have \( 2k + \alpha \equiv 3k + \beta \ (\mod \frac{p-1}{2}) \) and \( \tilde{a} \equiv \tilde{b} \ (\mod \ p) \), and the curve \( \sim E \) is isomorphic to \( E \) in \( \mathbb{F}_p \).

**Case 2:** \( a \) and \( b \) are quadratic non-residues.

The system of equations (2.2) is now equivalent to the fact that there exist \( k, \alpha \) and \( \beta \) such that:

\[
\begin{align*}
a &= g^{2\alpha+1}, \\
b &= b^{2\beta+1}, \\
u &= g^k, \\
\tilde{a} &= (u^2g^{\alpha})^2g, \\
\tilde{b} &= (u^3g^{\beta})^2g, \quad \text{hence} \quad \tilde{a} = (g^{2k+\alpha})^2g, \\
\tilde{b} &= (g^{3k+\beta})^2g.
\end{align*}
\]

So by choosing \( k \equiv \alpha - \beta \ (\mod \frac{p-1}{2}) \), we get \( \tilde{a} = \tilde{b} \).
It is clear from Proposition 2.2, with $d = 1$, that if such a curve exists, then it is unique.

**Remark 2.4.** We may note that if $\tilde{E}(\tilde{a}, \tilde{b}) \cong \tilde{E}(a, b)$, then

$$\left( \frac{a}{p} \right) = \left( \frac{\tilde{a}}{p} \right) \quad \text{and} \quad \left( \frac{b}{p} \right) = \left( \frac{\tilde{b}}{p} \right).$$

**Proposition 2.5.** With the notation in Proposition 2.3, for $d \in \mathbb{F}_p$ with $\left( \frac{d}{p} \right) = -1$, if $\left( \frac{ab}{p} \right) = -1$, there exists a unique curve $\tilde{E}(\tilde{a}, \tilde{b})$ isomorphic to $E$ with $\tilde{a} = d\tilde{b}$.

**Proof.** We use the same idea of proof as for Proposition 2.3.

**Case 1:** $\left( \frac{a}{p} \right) = -1$ and $\left( \frac{b}{p} \right) = 1$.

Reasoning as before, we have

$$\begin{cases} 
\tilde{a} = (g^{2k+\alpha})^2g, \\
\tilde{b} = (g^{3k+\beta})^2,
\end{cases} \quad \text{and} \quad d = g^{2\gamma+1}.$$ 

So if we choose $k \equiv \alpha - \beta - \gamma \pmod{\frac{p-1}{2}}$, then $\tilde{a} = g^{2\gamma+1}\tilde{b} = d\tilde{b}$.

**Case 2:** $\left( \frac{a}{p} \right) = 1$ and $\left( \frac{b}{p} \right) = -1$.

Reasoning as before, we have

$$\begin{cases} 
\tilde{a} = (g^{2k+\alpha})^2, \\
\tilde{b} = (g^{3k+\beta})^{2g},
\end{cases} \quad \text{and} \quad d = g^{2\gamma+1}.$$ 

So if we choose $k \equiv \alpha - \beta - \gamma - 1 \pmod{\frac{p-1}{2}}$, then $\tilde{a} = g^{2\gamma+1}\tilde{b} = d\tilde{b}$. \hfill $\Box$

Propositions 2.1 and 2.5 are very interesting if it is possible to find small quadratic non-residues. This leads us to the problem of finding an upper bound for the smallest quadratic non-residue $n(p)$ modulo $p$ which is a well-known and difficult problem in number theory.

It is known [3] that $n(p) = O(p^{\frac{1}{\sqrt{p}}} + g)$. If we assume the extended Riemann hypothesis, we have a much better bound, namely $n(p) = O(\log^2 p)$ (cf. [1]).

This discussion applies to the case where $p$ is fixed and we have to choose $d$, particularly for cryptographic application. However, if we have more freedom of choice for $p$, it seems interesting to choose $d$ first (e.g. 2, 3 or 5) and then $p$ subject to specific cryptographic constraints. We state the following results without proof, as they can be routinely shown using quadratic reciprocity.

**Proposition 2.6.** For all primes $p \equiv \pm 3 \pmod{8}$, the value 2 for $d$ is acceptable. For all primes $p \equiv \pm 5 \pmod{12}$, the value 3 for $d$ is acceptable...
Corollary 2.7. If we choose a random $p$ in the set of all primes, after 4 trials, there is 99% chance to get 2 or 3 as quadratic non-residue.

The following theorem can be derived from the preceding material but is also a standard result, appearing for instance in [4, Theorem 3.15 (ii)].

Theorem 2.8. The number of isomorphism classes of elliptic curves over $\mathbb{F}_p$, $p > 3$ prime, is

$$2p - 4 + \gcd(4, p - 1) + 2 \gcd(3, p - 1).$$

3 Isomorphism representatives with small coefficients

It is useful for computations to normalise elliptic curves $E$ over $\mathbb{F}_p$ in such a way as to obtain $E \cong_{\mathbb{F}_p} E(a, b)$ with $\max(|a|, |b|) \leq M < p$. We shall denote $M(p)$ the infimum of such $M$. The problem is:

(i) Can we estimate $M(p)$ in terms of $p$?

(ii) Can we find an algorithm which, given $E$, will produce $a$ and $b$ of absolute value lower than $M$ such that $E \cong_{\mathbb{F}_p} E(a, b)$?

To the first question, we have a partial answer. Indeed, we can prove the following.

Theorem 3.1. We have the following upper and lower bounds:

$$\sqrt{2p} < M(p) < 6\sqrt{15} p^{3/4} (\log p + 4).$$

Proof. The lower bound is easy. We have seen in Theorem 2.8 that there are at least $2p$ isomorphism classes of elliptic curves over $\mathbb{F}_p$. If $M(p) < \sqrt{2p}$, then the number of possible $E(a, b)$ would certainly be less than $M(p)^2 < 2p$, contradicting the definition of $M(p)$.

The upper bound is more delicate since it involves the distribution of certain numbers modulo 1. We start by recalling the definition of discrepancy of a sequence.

Definition 3.2. Let $k$ be a positive integer, $x_1, \ldots, x_N$ be $N$ vectors of $\mathbb{R}^k$. Define the discrepancy $D_N(x_1, \ldots, x_N)$ to be

$$D_N(x_1, \ldots, x_N) = \sup_{I} \left| \frac{\# \{1 \leq i \leq N : x_i \mod \mathbb{Z}^k \in I \} - |I|}{N} \right|,$$

the supremum being taken over all product of intervals $\prod_{1 \leq j \leq k} [\alpha_j, \beta_j)$ contained in the unit cube. Here $|I|$ denotes the volume of $I$, that is, $\prod_{1 \leq j \leq k} (\beta_j - \alpha_j)$.
In other terms, $D_N$ measures the degree of uniformity (modulo the lattice of integers) in the distribution of $x_1, \ldots, x_N$. There is a theorem due independently to Koksma [5] and Szüsz [7] (which when $k = 1$ was proved by Erdős and Turán) which gives an upper bound of $D_N$ in terms of exponential sums on the vectors $x_i$.

**Theorem 3.3.** We have

$$D_N(x_1, \ldots, x_N) \leq 2k^2 3^{k+1} \left( \frac{1}{m} + \sum_{h \in \mathbb{Z}^k \atop 0 < \|h\| \leq m} \frac{1}{r(h)} \left| \frac{1}{N} \sum_{n=1}^{N} \exp(2\pi i \langle h, x_n \rangle) \right| \right),$$

where $m$ is any positive integer, $\|h\| = \max_{1 \leq j \leq k} |h_j|$, $r(h) = \prod_{j=1}^{k} \max(|h_j|, 1)$ and $\langle \cdot, \cdot \rangle$ denotes the usual scalar product in $\mathbb{R}^k$.

We now reduce our problem to a question on uniform distribution modulo 1. Let $E(a, b)$ be an elliptic curve over $\mathbb{F}_p$. Our goal is to find $E(\tilde{a}, \tilde{b}) \approx E(a, b)$ with $\tilde{a}, \tilde{b}$ as small as possible. In other terms we have to find $u \in \mathbb{Z}$ coprime to $p$ such that there exists $(m, n) \in \mathbb{Z}^2$ satisfying the following system of inequalities:

$$\begin{aligned}
\left\{ \begin{array}{l}
|u^4a - mp| < M, \\
|u^6b - np| < M.
\end{array} \right.
\end{aligned} \quad (3.1)$$

Here $M$ is a constant, depending on $p$, to be determined later, such that (3.1) has a solution. Dividing the previous system by $p$, we get

$$\begin{aligned}
\left\{ \begin{array}{l}
\left| \left\{ \frac{u^4a}{p} \right\} - 1 \right| < \frac{M}{p}, \\
\left| \left\{ \frac{u^6b}{p} \right\} - 1 \right| < \frac{M}{p},
\end{array} \right.
\end{aligned} \quad (3.2)$$

where $\{t\} = t - [t]$ denotes the fractional part of $t$. Using Theorem 3.3, we are now in a position to find a precise estimation of the number of solutions of (3.2).

**Theorem 3.4.** The number of solutions of (3.2) with $1 \leq u \leq p-1$ is $4M^2/p + E$, where $|E| \leq 2160\sqrt{p} (\log p + 4)^2$.

**Corollary 3.5.** Equation (3.2) has at least one solution whenever

$$M \geq 6\sqrt{15} p^{3/4} (\log p + 4).$$

In particular, $M(p) \leq 6\sqrt{15} p^{3/4} (\log p + 4)$.
In order to prove Theorem 3.4 we will apply Theorem 3.3 to the $p$ real vectors $(x_1, \ldots, x_p)$, where $x_u = (u^4 a / p, u^6 b / p)$. We then get
\[
D_p(x_1, \ldots, x_p) \leq \frac{216}{m} + 216 \sum_{(h_1, h_2) \in \mathbb{Z}^2 \atop 0 < \max(|h_1|, |h_2|) \leq m} \frac{1}{\max(|h_1|, 1) \max(|h_2|, 1)} \times \left| \frac{1}{p} \sum_{u=1}^{p} \exp \left( 2\pi i \frac{u^4 a h_1 + u^6 b h_2}{p} \right) \right|.
\]

**Lemma 3.6** (Weil’s bound). We have
\[
\left| \sum_{u=1}^{p} \exp \left( 2\pi i \frac{u^4 a h_1 + u^6 b h_2}{p} \right) \right| \leq 5\sqrt{p}.
\]

**Proof.** See [6] □

From Weil’s bound and (3.3) we can infer that
\[
D_p(x_1, \ldots, x_p) \leq 216 \left( \frac{1}{m} + \sum_{(h_1, h_2) \in \mathbb{Z}^2 \atop 0 < \max(|h_1|, |h_2|) \leq m} \frac{5}{\max(|h_1|, 1) \max(|h_2|, 1) \sqrt{p}} \right).
\]

Note that
\[
\sum_{(h_1, h_2) \in \mathbb{Z}^2 \atop 0 < \max(|h_1|, |h_2|) \leq m} \frac{1}{\max(|h_1|, 1) \max(|h_2|, 1)} \leq 4 \sum_{h \leq m} \frac{1}{h} + 4 \left( \sum_{h \leq m} \frac{1}{h} \right)^2 \leq 4(1 + \log m)(2 + \log m).
\]

Hence
\[
D_p(x_1, \ldots, x_p) \leq \frac{216}{m} + \frac{4320(2 + \log m)^2}{\sqrt{p}}, \quad \forall \ m \geq 1.
\]

The quantity on the right side is minimised by taking $m$ around $\left[ \frac{\sqrt{\sqrt{p}}}{5(2 + \log p)^2} \right]$. We thus get
\[
D_p(x_1, \ldots, x_p) \leq \frac{2160(4 + \log p)^2}{\sqrt{p}}.
\]

Consequently, we have proved that
\[
\# \left\{ 1 \leq u \leq p : x_u = (u^4 a / p, u^6 b / p) \in ([0, \mu) \cup (1 - \mu, 1])^2 \right\} = 4\mu^2 p + E,
\]
with $|E| \leq 2160\sqrt{p} (\log p + 4)^2$. Taking $\mu = M / p$ yields Theorem 3.4.

This concludes the proof of Theorem 3.1 □
4 Improving the upper bound

In this section we show how to improve the upper bound to get the following

**Theorem 4.1.** For any \( \varepsilon > 0 \), there exists an effectively computable constant \( c(\varepsilon) \) depending on \( \varepsilon \) alone such that

\[
M(p) < \left( \frac{4\sqrt{5}}{\pi} + \varepsilon \right) p^{3/4} \quad \text{for all } p > c(\varepsilon).
\]

**Proof.** The number \( \mathcal{N}(M) \) of \((u, h_1, h_2, k_1, k_2)\) with \( 1 \leq u \leq p \) and \( 0 \leq h_i, k_i \leq M - 1 \) such that \( u^4 a \equiv h_1 - h_2 \pmod{p} \) and \( u^6 b \equiv k_1 - k_2 \pmod{p} \) is

\[
\frac{1}{p^2} \sum_{h_1, h_2=0}^{p-1} \sum_{k_1, k_2=0}^{p-1} \exp \left( \frac{2\pi i (u^4 a - h_1 + h_2)t + (u^6 b - k_1 + k_2)s}{p} \right).
\]

Our aim is now to find an explicit \( M \) such that \( \mathcal{N}(M) > 1 \). In doing so we will extract the main term and estimate the error term in the previous expression. We single out the contribution corresponding to the terms with \( t = p \) and \( s = p \). We obtain

\[
\mathcal{N}(M) = \frac{M^4}{p} + \frac{M^2}{p^2} \sum_{k_1, k_2=0}^{M-1} \sum_{u=1}^{p} \sum_{s=1}^{p-1} \exp \left( \frac{2\pi i (u^6 b - k_1 + k_2)s}{p} \right) \quad (4.1)
\]

\[
+ \frac{M^2}{p^2} \sum_{h_1, h_2=0}^{M-1} \sum_{u=1}^{p} \sum_{t=1}^{p-1} \exp \left( \frac{2\pi i (u^4 a - h_1 + h_2)t}{p} \right) \quad (4.2)
\]

\[
+ \frac{1}{p^2} \sum_{h_1, h_2=0}^{M-1} \sum_{k_1, k_2=0}^{M-1} \sum_{u=1}^{p} \sum_{t=1}^{p-1} \sum_{s=1}^{p-1} \exp \left( \frac{2\pi i (u^4 a - h_1 + h_2)t + (u^6 b - k_1 + k_2)s}{p} \right). \quad (4.3)
\]

**Lemma 4.2.** We have, for any value of \( 1 \leq N < p/2 \),

\[
\left| \sum_{s=1}^{p-1} \sum_{k=0}^{M-1} \exp \left( \frac{2\pi i k s}{p} \right) \right|^2 < \frac{2M^2 N}{\left(1 - \frac{1}{6} \left( \frac{\pi N}{p} \right)^2 \right)^2} + \frac{2p^2}{N \left( \pi - \frac{\pi^3}{24} \right)^2}.
\]

**Proof.** Start from the trivial equality

\[
\sum_{s=1}^{p-1} \sum_{k=0}^{M-1} \exp \left( \frac{2\pi i k s}{p} \right) = \sum_{s=1}^{p-1} \frac{\sin^2 \pi Ms}{p} = 2 \sum_{s=1}^{(p-1)/2} \frac{\sin^2 \pi s}{p}.
\]
Now we split the sum into two parts, corresponding to $1 \leq s \leq N$ and $N < s < p/2$. Note that for $0 < s < p/2$ we have the following lower bound:

$$\sin \frac{\pi s}{p} \geq \frac{\pi s}{p} - \frac{1}{6} \left( \frac{\pi s}{p} \right)^3 = \frac{\pi s}{p} \left( 1 - \frac{1}{6} \left( \frac{\pi s}{p} \right)^2 \right).$$

Also we have the well-known inequality $\sin^2 x \leq x^2$ valid for all real $x$, hence

$$\sum_{s=1}^{(p-1)/2} \frac{\sin^2 \frac{\pi M s}{p}}{\sin^2 \frac{\pi s}{p}} \leq \frac{M^2 N}{(1 - \frac{1}{6} \left( \frac{\pi N}{p} \right)^2)^2} + \frac{1}{1 - \frac{\pi^2}{24}} \sum_{N < s < p/2} \frac{p^2}{\pi^2 s^2} < \frac{M^2 N}{(1 - \frac{1}{6} \left( \frac{\pi N}{p} \right)^2)^2} + \frac{p^2}{N \left( \pi - \frac{\pi^3}{24} \right)^2}. \tag{4.4}$$

We apply this lemma together with the Weil bound to the triple sum in (4.1). We have

$$\sum_{k_1, k_2=0}^{M-1} \sum_{u=1}^p \sum_{s=1}^{p-1} \exp \left( 2\pi i \frac{(u^6 b - k_1 + k_2)s}{p} \right) \leq \sum_{s=1}^{p-1} \sum_{u=1}^p \exp \left( 2\pi i \frac{u^6 b s}{p} \right) \left| \sum_{k=0}^{M-1} \exp \left( 2\pi i \frac{ks}{p} \right) \right|^2.$$

Therefore

$$\sum_{s=1}^{p-1} \left| \sum_{u=1}^p \exp \left( 2\pi i \frac{u^6 b s}{p} \right) \left| \sum_{k=0}^{M-1} e^{2\pi i \frac{ks}{p}} \right|^2 \right| \leq \frac{10 \sqrt{p}}{N} \frac{M^2 N}{(1 - \frac{1}{6} \left( \frac{\pi N}{p} \right)^2)^2} + \frac{10p^{5/2}}{N \left( \pi - \frac{\pi^3}{24} \right)^2}. \tag{4.5}$$

Similarly we have for (4.2)

$$\left| \sum_{h_1, h_2=0}^{M-1} \sum_{u=1}^p \sum_{t=1}^{p-1} \exp \left( 2\pi i \frac{(u^4 a - h_1 + h_2)t}{p} \right) \right| \leq \frac{10 \sqrt{p}}{N} \frac{M^2 N}{(1 - \frac{1}{6} \left( \frac{\pi N}{p} \right)^2)^2} + \frac{10p^{5/2}}{N \left( \pi - \frac{\pi^3}{24} \right)^2}. \tag{4.5}$$

It remains to bound (4.3).
Again we make use of the Weil bound and of the lemma to get
\[
\left| \sum_{h_1, h_2 = 0}^{M-1} \sum_{k_1, k_2 = 0}^{M-1} \sum_{t=1}^{p-1} \sum_{s=1}^{p-1} \exp \left( 2\pi i \frac{(u^4 a - h_1 + h_2)t + (u^6 b - k_1 + k_2)s}{p} \right) \right|
\]
\[= \sum_{t=1}^{p-1} \left| \sum_{s=1}^{p-1} \exp \left( 2\pi i \frac{u^4 at + u^6 bs}{p} \right) \right| \]
\[\times \left| \sum_{h_1, h_2 = 0}^{M-1} \sum_{k_1, k_2 = 0}^{M-1} \exp \left( 2\pi i \frac{ht}{p} \right) \sum_{k_1, k_2 = 0}^{M-1} \exp \left( 2\pi i \frac{ks}{p} \right) \right|^2
\]
\[\leq \left( \frac{2\sqrt{5}p^{1/4}M^2N}{(1 - \frac{1}{6}(\frac{\pi N}{p})^2)^2} + \frac{2\sqrt{5}p^{9/4}}{N(\pi - \frac{\pi^3}{24})^2} \right)^2.
\]

Finally, from (4.1), (4.2), (4.3), (4.4), (4.5) and (4.6) we get
\[\mathcal{N}(M) = \frac{M^4}{p} + E(M, p)\]

with
\[|E(M, p)| \leq \frac{20M^4N}{p^{3/2}(1 - \frac{1}{6}(\frac{\pi N}{p})^2)^2} + \frac{20\sqrt{p}M^2}{N(\pi - \frac{\pi^3}{24})^2}\]
\[+ \left( \frac{2\sqrt{5}M^2N}{p^{3/4}(1 - \frac{1}{6}(\frac{\pi N}{p})^2)^2} + \frac{2\sqrt{5}p^{5/4}}{N(\pi - \frac{\pi^3}{24})^2} \right)^2.
\]

We minimise the right-hand side of the preceding inequality by taking
\[N = \frac{p}{M(\pi - \frac{\pi^3}{24})}.
\]

We get that
\[|E(M, p)| \leq \frac{20CM^3}{p^{1/2}(\pi - \frac{\pi^3}{24})} + \frac{20C^2M^2p^{1/2}}{(\pi - \frac{\pi^3}{24})^2}\]

with
\[C = 1 + \left( 1 - \frac{1}{6}M^{-2} \left( 1 - \frac{\pi^2}{24} \right)^{-2} \right)^{-2} = 2 + O \left( \frac{1}{p} \right)\]
since we know $M > \sqrt{p}$. For $M < p^\theta$ with $\theta < 1$, the dominant summand in the error term is the second one. We want therefore to ensure that asymptotically

$$\frac{80M^2 p^{1/2}}{(\pi - \frac{\pi^3}{24})^2} < \frac{M^4}{p^3}.$$ 

Hence in taking

$$M = \left(\frac{4\sqrt{5}}{\pi - \frac{\pi^3}{24}} + \varepsilon\right) p^{3/4},$$

we see that $\mathcal{N}(M) > 1$ implying that there exists an effective constant $c(\varepsilon)$ such that

$$M(p) < \left(\frac{4\sqrt{5}}{\pi - \frac{\pi^3}{24}} + \varepsilon\right) p^{3/4}$$

whenever $p > c(\varepsilon)$ and the theorem is proved. □

5 Conclusion

We have considered the problem of normalized representations of elliptic curves by imposing some control on the size of their coefficients. In the first part we proposed an algorithm to transform an elliptic curve with arbitrary coefficients into a curve where the first coefficient is a small number. Then we saw that it is also possible to impose that the ratio $a/b$ of the coefficients be small. In contrast to these one-dimensional problems, it is a much more delicate task to bring $\max(a, b)$ below $p$. Uniform distribution of powers $u^4$ and $u^6$ mod $p$ intervenes and using Weil’s bound, one can manage to get to $O(p^{3/4})$. Also one cannot get below $\sqrt{p}$ so this poses the problem of determining the least exponent $\theta$ such that for any $\varepsilon$, $M(p) < p^{\theta + \varepsilon}$ for all sufficiently large primes $p$.

After working on this problem, we were made aware of a related work [2], which gives an average improvement of an upper bound for $M(p)$. Its authors prove that on average over all the isomorphism classes of elliptic curves one has $M(p) = O(p^{2/3})$. Our work nevertheless remains the best estimate valid for all isomorphism classes.

Acknowledgments. We would like to thank Marc Joye, Igor Shparlinski, Aimo Tietäväinen as well as a reviewer for their help and comments.
Bibliography


Received February 15, 2011; revised May 9, 2011.

Author information

Mathieu Ciet, Université catholique de Louvain, Microelectronics Laboratory, Place du Levant 3, 1348 Louvain-la-neuve, Belgium.
E-mail: mathieu.ciet@gmail.com

Jean-Jacques Quisquater, Université catholique de Louvain, Microelectronics Laboratory, Place du Levant 3, 1348 Louvain-la-neuve, Belgium.
E-mail: jjq@uclouvain.be

Francesco Sica, Via Toscana 50, 58024 Prata (GR), Italy.
E-mail: fracrypto@gmail.com