Modulus Search for Elliptic Curve Cryptosystems

Kenji Koyama, Yukio Tsuruoka, and Noboru Kunihiro

NTT Communication Science Laboratories
2-4, Hikaridai, Seika-cho, Soraku-gun, Kyoto, 619-0237 Japan
{koyama, tsuru, kunihiro}@cslab.kecl.ntt.co.jp

Abstract. We propose a mathematical problem, and show how to solve it elegantly. This problem is related with elliptic curve cryptosystems (ECC). The solving methods can be applied to a new paradigm of key generations of the ECC.

1 Problem

Celebrating Asiacrypt'99 held in November (11th month) of 1999, we propose a mathematical problem after these numbers.

Let c, x, y be integers such that $0 \leq x < c$ and $0 \leq y < c$.
Define $N(c)$ be the number of points (x, y) satisfying
$y^2 \equiv x^3 + 11x \pmod{c}$ (1)
Obtain all values of c such that $N(c) = 1999$.

2 Solving the Problem

2.1 Observing the Behaviour of $N(c)$

This problem itself is easy to understand for junior highschool students, however, solving it may be a little difficult for them. It would be moderate for modern cryptographers.

First, observe the behaivior of $N(c)$ concerning equation (1) from small numerical examples. When $c = 7$, the integer points (x, y) of equation (1) are $(0, 0), (2, 3), (2, 4), (3, 2), (3, 5), (6, 3), (6, 4)$. Thus, we have $N(7) = 7$. Similarly, we compute the values of $N(c)$ for integers c such that $1 \leq c \leq 18$, and primes below 100. The result is shown in Table 1.

Table 1. Examples of $N(c)$

c	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
$N(c)$	1	2	3	6	3	6	7	12	9	6	11	18	17	14	9	24	9	18

c	19	23	29	31	37	41	43	47	53	59	61	67	71	73	79	83	89	97
$N(c)$	19	23	25	31	39	33	43	47	39	59	49	67	71	57	79	83	79	115

We can find the properties of $N(c)$ if we observe Table 1 carefully.

K. Y. Lam, E. Okamoto and C. Xing (Eds.): ASIACRYPT'99, LNCS 1716, pp. 1–7, 1999.

2.2 Obtaining one Solution

Hereafter, considering equation (1) as general as possible, we can obtain the following theorems for the properties of $N(c)$.

Theorem A: *Define $N_u(c)$ be the number of points for a general congruence:*

$$f(x, y) \equiv 0 \pmod{c} \tag{1}$$

If c is composite (i.e. not prime), then $N_u(c)$ is composite. In particular, when c_1 and c_2 are coprime, we have

$$N_u(c_1 c_2) = N_u(c_1) N_u(c_2). \tag{2}$$

Of course, Theorem A holds for $N(c)$ concerning equation (1). If c is a prime power, we have Theorem B.

Theorem B : *Define $N_s(c)$ be the number of points for congruence:*

$$y^2 \equiv x^3 + ax \pmod{c} \tag{3}$$

Let p be a prime and $c = p^n$ $(n \geq 2)$.

(i) If p $(\neq 2)$ is coprime to a, then $N_s(p^n) = p^{n-1} \cdot N_s(p)$,
(ii) If p $(\neq 2)$ divides a, then $N_s(p^n) = (2p-1) \cdot N_s(p)^{n-1}$.
(iii) $N_s(2) = 2$. When $a = 11$, $N_s(2^n) = 3 \cdot 2^{n-1}$.

Putting $a = 11$ in equation (4), Theorem B holds for $N(c)$ concerning equation (1).

Theorem C: *Define $N_s(c)$ in the same way as Theorem B. If p is a prime such that $p \equiv 3 \pmod{4}$ and a is coprime to p, then $N_s(p) = p$.*

Theorem C holds for $N(c)$ concerning equation (1).

In the problem, we just said on purpose "c is an integer." I did not say "c is restricted to a prime." Theorem A can be rewritten as "If $N(c)$ is a prime, then c is a prime." Note that 1999 is a prime. We can observe that c is a prime because $N(c) = 1999$. Moreover, noticing $1999 \equiv 3 \pmod{4}$, we can find from Theorem C that $N(1999) = 1999$. That is, a prime c satisfying $N(c) = 1999$ and $c \equiv 3 \pmod{4}$ is only 1999.

2.3 Obtaining other Solutions

In the problem, we said "Obtain **all** values of c." Therefore, the remaining candidates of c must be primes with $c \equiv 1 \pmod{4}$. What is the range for searching the remaining prime candidates? We show here a strong theorem, which is called Hasse's Theorem and popular in elliptic curve theory.

Hasse's Theorem: *Let p be a prime and coprime to $4a^3 + 27b^2$. Consider an elliptic curve over prime field $GF(p)$:*

$$y^2 \equiv x^3 + ax + b \pmod{p}. \tag{4}$$

Excluding a point at infinity, the number of points on this curve, denoted by $N_w(p)$*, is given by in the following range:*

$$p - 2\sqrt{p} \leq N_w(p) \leq p + 2\sqrt{p}. \tag{5}$$

If $4a^3 + 27b^2$ is coprime to p, the curve of equation (5) becomes an elliptic curve, which is a cubic curve without singular points. Equation (5) is called Weierstraß form. Putting $a = 11$, $b = 0$, equation (5) becomes equation (1). The number of points on elliptic curves is usually called an order, including one point at infinity. Thus, the order is expressed as $N_w(p) + 1$. In the problem, to avoid difficulty of understanding of a point at infinity, we define $N(c)$ (,$N_u(c)$, $N_s(c)$, and $N_w(c)$) excluding a point at infinity. Even for researchers familiar with elliptic curves and their orders, the proposed problem must be a new application paradigm, in which a modulus is determined from given an order of elliptic curve.

Naive Method: Method 1 First, to restrict the range of the solutions c of the problem, we need to get a lemma of Hasse's theorem. Given $N_w(p)(= N(p))$, a prime modulus p of elliptic curve is restricted between a certain range. This range is obtained from equation (5). By rewriting equation (5), we have

$$p^2 - 2(N_w(p) + 2)p + N_w(p)^2 \leq 0.$$

By solving p for this quadratic form, we have an inequality:

$$N_w(p) + 2 - 2\sqrt{N_w(p) + 1} \leq p \leq N_w(p) + 2 + 2\sqrt{N_w(p) + 1} \tag{6}$$

Putting $N(p) = N_w(p) = 1999$, we can get an explicit range as $1911.6 \leq p \leq 2090.4$. Thus, the values of modulus c should be searched from 1912 to 2090. In this range, there are twelve primes ($\equiv 1 \pmod 4$) as 1913, 1933,1949, 1973, 1993, 1997, 2017, 2029, 2053, 2069, 2081 and 2089. The most naive method is to compute $N(p)$ for all of these twelve values of p, and check whether $N(p) = 1999$. We can find that only $p = 2017$ satisfies $N(p) = 1999$.

Elegant Method: Method 2 Elegant methods can be constructed by decreasing the number of candidates of modulus by a simple analysis. Note that for a prime with $p \equiv 1 \pmod 4$, there are integers U, V (U is odd and V is even)such that

$$p = U^2 + V^2. \tag{7}$$

The values of (U, V) is uniquely determined and easily obtained. In elliptic curve theory, the following theorem D is known,

Theorem D : *Let* p *be a prime satisfying* $p \equiv 1 \pmod 4$ *and* $p = U^2 + V^2$*. If* a $(\neq 0)$ *is coprime to* p*, the number of points of equation (4), denoted by* $N_s(p)$*, is one of the following four candidates:*

$$N_s(p) = p \pm 2U, \quad p \pm 2V \tag{8}$$

Let $U' = |p - 1999|/2$ and $W = p - U'^2$. Observing theorem D, W must be a square to satisfy $N(p) = 1999$ for a prime with $p \equiv 1 \pmod 4$. For each p of twelve candidates, the computed values of U' and W are shown in Table 2. Observing Table 2, only four primes such that $p = 1913, 2017, 2081$ and 2089 imply that W are squares. For these reduced four candidates p, the computed values of $N(p)$ are also shown in Table 2. We can find that only $p = 2017$ satisfies $N(p) = 1999$.

Table 2. Reduction of primes p and reduced $N(p)$

p	1913	1933	1949	1973	1993	1997	2017	2029	2053	2069	2081	2089
U'	43	33	25	13	3	1	9	15	27	35	41	45
W	64	844	1324	1804	1984	1996	1936	1804	1324	844	400	64
$N(p)$	1929	–	–	–	–	–	1999	–	–	–	2121	2105

More Elegant Method: Method 3 We would show more elegant and efficient method. If we apply equation (8) and theorem D extendedly, we do not need to know and use Hasse's Theorem and its lemma directly. Note that for prime p with $p \equiv 1 \pmod 4$, $N_s(p) + 1$ is represented as one of four values:

$$N_s(p) + 1 = (U \pm 1)^2 + V^2, \quad U^2 + (V \pm 1)^2$$

Thus, if given $N_s(p) + 1$ is represented as a sum of two squares as $N_s(p) + 1 = \alpha^2 + \beta^2$ $(\alpha \le \beta)$ then (U, V) is one of $(\alpha \pm 1, \beta)$ and $(\alpha, \beta \pm 1)$. We compute candidates of p from these candidates of (U, V). Then we do primality test for p and check whether $N(p) = 1999$. The passed p become solutions.
We show the above method concretely. Since $N_s(p) + 1 = 1999 + 1 = 2000$, we search (α, β) such that $2000 = \alpha^2 + \beta^2$, noticing $\alpha \le \sqrt{2000/2}$. We obtain two pairs $(\alpha, \beta) = (8, 44), (20, 40)$. ¿From each pair, eight candidates of p_i $(1 \le i \le 8)$ can be computed as

$p_1 = (8 + 1)^2 + 44^2 = 2017$, $p_2 = (8 - 1)^2 + 44^2 = 1985$,
$p_3 = 8^2 + (44 + 1)^2 = 2089$, $p_4 = 8^2 + (44 - 1)^2 = 1913$,
$p_5 = (20 + 1)^2 + 40^2 = 2041$, $p_6 = (20 - 1)^2 + 40^2 = 1981$,
$p_7 = 20^2 + (40 + 1)^2 = 2081$, $p_8 = 20^2 + (40 - 1)^2 = 1921$.

Among these values, only p_1, p_3, p_4 and p_7 are primes. These primes are congruent 1 modulo 4, however, only $p_1 = 2017$ satisfies $N(p_i) = 1999$. This method is more efficient than the method 2 because of less primality tests. It is interesting that four candidates derived by method 3 are the same as four candidates derived by method 2.

Much more Elegant Method: Method 4 Moreover, much more elegant method can be constructed by observing the reduced candidates from another viewpoint. When $p \equiv 1 \pmod 4$, order $S = N(p) + 1$ is expressed by

$$S = 4t + 3 + L(11, p),$$

where t is the number of the cases that $x^3 + 11x$ become quadratic residues modulo p when $1 \leq x \leq (p-1)/2$. Generally, the Legendre symbol $L(d,p)$ means as follows. $L = 1$ if d $(\neq 0)$ is a quadratic residue modulo prime p; $L = -1$ if d $(\neq 0)$ is a quadratic non-residue modulo prime p; $L = 0$ if $d = 0$. To satisfy $S = 2000$, we need that $S \equiv 0 \pmod 4$, and 11 is a quadratic residue modulo p. Among four primes 1913, 2017, 2081, and 2089, only $p = 2017$ satisfies $L(11,p) = 1$. Thus, we compute $N(p)$ for only $p = 2017$, and we verify $N(2017) = 1999$.

Note that method 2 and method 3 require four computations of $N(p)$, however, method 4 requires four computations of Legendre symbols and one computation of $N(p)$. Thus, method 4 is more efficient than methods 2 and 3.

3 Counting Points of the Curves

3.1 General Methods

There are several ways to compute $N(c)$ from c. The most naive method is to count the points (x,y) satisfying equation (1) by varying both x and y from 0 to $c-1$. The computational complexity is $O(c^2(\log c)^2)$. If c is a prime, we can compute $N(c)$ using Legendre symbol L as

$$N(c) = \sum_{x=0}^{c-1} \{1 + L(x^3 + 11x, c)\}.$$

We call this method the Legendre method. Since the Legendre symbol itself can be computed in $O((\log c)^3)$, computation of $N(c)$ by the Legendre method requires $O(c(\log c)^3)$. It is more efficient than the naive method.

When c is about 4 digits, $N(c)$ can be computed in less than one second on a typical personal computer if the Legendre symbol method is used. When c is about 200 digits, the computation of $N(c)$ is intractable even if the Legendre symbol method is used. For large p, counting the points (i.e. order or $N_w(p)$) on an elliptic curve over prime field $GF(p)$ had been a difficult problem historically. However, Schoof discovered an efficient method in 1985. The implementation is rather complicated, but it runs in polynomial time i.e. in $O((\log p)^8)$. Recently, an improved Schoof method, which is also called Schoof-Elkies-Atkin (SEA) method, is used and it runs in $O((\log p)^6)$. This newest counting method is used in the design of elliptic curve method (ECC). Note that ECC is a public-key cryptosystem, which is the most promising scheme in the next generation of the RSA scheme.

3.2 Special Counting Method for the Problem

Return to the problem. Since equation (1) has a restricted parameters a, b and p, we can compute $N(p)$ analytically and efficiently using Theorem E.

Theorem E : $N_s(p)$ *is uniquely determined by*

$$N_s(p) = p - \overline{\left(\frac{-a}{\pi}\right)_4 \pi} - \left(\frac{-a}{\pi}\right)_4 \overline{\pi}, \tag{9}$$

where $p = \pi\overline{\pi}$*, and* π *is Gaussian integer* $Z[i]$ $(i = \sqrt{-1})$*, and* $\pi \equiv 1 \pmod{2+2i}$*.*

Note that $\left(\frac{-a}{\pi}\right)_4 = \{1, -1, i, -i\}$*, and computed as* $\left(\frac{-a}{\pi}\right)_4 = (-a)^{(p-1)/4} \bmod \pi$*.*

Using Theorem E, we can easily compute $N(p)$ for each p. For example, when $p = 2017$, we have $p = 9^2 + 44^2$, and $N(2017) = 2017 - 2 \times 9 = 1999$. The computational time on a typical computer using Theorem E is also less than one second.

4 Solution

The above discussion result in a solution of the problem. There are only c=1999 and 2017 satisfying equation (1).

Note that if one try to search them on a computer without any knowledge or any analysis, it need infinite time. The theorems and discussions in this paper convince us that there are only two values of c satisfying equation (1).

5 Viewpoint of ECC Design

In cryptographic design, there are two typical methods for constructing secure elliptic curves for the ECC: the SEA method (the point-counting method based on the improved Schoof algorithm) and the CM(Complex Multiplication) method.
The SEA Method: The point-counting method computes an order of random curve modulo p until the order satisfies the security. Given parameters (a, b) and prime modulus p of elliptic curve, the improved versions of Schoof algorithm can compute order $\#E(a, b, p)$ $(= S)$ in $O((\log p)^6)$. Considering the time of the primality check of p and the security check of S, including their success probability, the computational time for obtaining a suitable triple $(S, (a, b), p)$ based on the improved Schoof algorithm is $O((\log p)^7)$.
The CM method: The CM method chooses a secure order first from modulus p, then builds a curve with that order. Given the prime modulus p of an elliptic curve, the Atkin-Morain algorithm and its variants compute the j-invariant of the curve, and obtains order S and parameters (a, b) satisfying $S = \#E(a, b, p)$. They run in $O((\log p)^5)$. Considering the time of the primality check of p and the security check of S, including their success probability, the computational time for obtaining a suitable triple $(S, (a, b), p)$ based on the CM method is $O((\log p)^6)$.
That is, the CM method based on the Atkin-Morain algorithm is more efficient than the point-counting method based on the (improved) Schoof algorithm.

Now, we consider a new approach based on problem G and its solution, which follows. This approach, which we call the *modulus-searching method*, is

in another direction among $(S,(a,b),p)$, and is different from SEA method and CM method.

Problem G: *Given order S and parameters (a,b) of an elliptic curve, construct an efficient algorithm for determining a prime modulus p satisfying $S = \#E(a,b,p)$, if such p exists.*

When the values of a, b and S are arbitrary, we can construct a general algorithm for problem G. We can find a prime p satisfying $S = \#E(a,b,p)$ if p exists. The time complexity of this algorithm is $O(\sqrt{S}(\log S)^2)$. This general but simple algorithm is not efficient for large S because there are many candidates for the prime modulus.

Therefore, we focus on the constructions of restricted elliptic curves $E(a,b,p)$ with $\{a \neq 0, b = 0\}$, whose j-invariant is 1728, and $\{a = 0, b \neq 0\}$, whose j-invariant is 0. Note that the Atkin-Morain algorithm excludes these "simple" curves. There are a few studies on the ECC using such curves. If $\{a \neq 0, b = 0$ and $p \equiv 1 \pmod 4\}$ or $\{a = 0, b \neq 0$ and $p \equiv 1 \pmod 3\}$, then orders of such curves can be easily computed in $O((\log p)^3)$ by the point-counting method based on complex multiplications over the imaginary quadratic field $\mathbf{Q}(\sqrt{-1})$ or $\mathbf{Q}(\sqrt{-3})$. This "special point-counting algorithm" is faster than the general (improved) Schoof algorithm. This "special point-counting method" constructs a suitable triple $(S,(a,b),p)$ in $O((\log p)^5)$. ¿From the viewpoint of problem 1, however, there have been no concrete proposals or deep discussions of efficient algorithms.

In [1] we proposed efficient algorithms for determining prime modulus p from given order S and parameters (a,b) of elliptic curve $E(a,b,p): y^2 \equiv x^3 + ax + b \pmod p$, where $\{a \neq 0, b = 0\}$ or $\{a = 0, b \neq 0\}$. First we choose secure order S from its size. Next we search prime modulus p satisfying $S = \#E(a,b,p)$. We can obtain a suitable triple $(S,(a,b),p)$ in polynomial time $O((\log S)^5)$. The proposed approach is faster than the previous approaches based on the Schoof algorithm and the Atkin-Morain algorithm.

References

1. K. Koyama, N. Kunihiro and Y. Tsuruoka: "Modulus Searching Methods for Secure Elliptic Curve Cryptosystems", Proc. of 1999 Symposium on Cryptography and Information Security (SCIS 99), pp. 863–868 (1999). 7