Finding Points on Elliptic Curves with Coppersmith's Method

Virgile Dossou-Yovo[1], Abderrahmane Nitaj[2], Alain Togbé[3]

[1]Institut de Mathématiques et de Sciences Physiques. Dangbo, Bénin

[2]Normandie Univ, UNICAEN, CNRS, LMNO, 14000 Caen, France

[3]Department of Mathematics and Statistics, Purdue University Northwest, Westville USA

CAI, October 2022

Contents

Contents

Contents

Contents

Contents

Elliptic curves in cryptography

- In 1985, Koblitz and Miller independently suggested the use of elliptic curves in public key cryptography
- The benefit of using elliptic curves in cryptography is that the keys are much smaller than the keys in other systems
- Several cryptographic systems are based on elliptic curves such as
  - The Elliptic Curve Diffie-Hellman (ECDH)
  - The Elliptic Curve Digital Signature Algorithm (ECDSA)
  - The Edwards-curve Digital Signature Algorithm (EdDSA)
  - The Elliptic Curve Integrated Encryption Scheme (ECIES)
  - KMOV and Demytko cryptosystems

Elliptic curves in cryptography

- Let p be a prime number and $\mathbb{F}_p$ be the finite field with p elements.
- Let $a, b \in \mathbb{F}_p$. An elliptic curve $E_p(a, b)$ is the set of solutions of the modular equation $y^2 \equiv x^3 + ax + b \pmod{p}$ together with a special point $\mathcal{O}$, called the point at infinity.
- In some systems, the prime number is replaced by a composite integer of the form $n = pq$.
- In some situations, it is required to use a solution $P_0 = (x_0, y_0)$ of the modular equation $y^2 \equiv x^3 + ax + b \pmod{p}$ where both $|x_0|$ and $|y_0|$ are small.

The new method

In this paper, we use Coppersmith's method to find the small solutions (x, y) of the modular elliptic curve equation

$$(Y_0 + y)^2 \equiv (X_0 + x)^3 + a(X_0 + x) + b \equiv 0 \pmod{n},$$

where n is a positive integer with unknown factorization, $a, b \in \mathbb{Z}/n\mathbb{Z}$ are fixed, and X_0, Y_0 are known parameters. The method is valid for $X_0 = Y_0 = 0$ with the equation $y^2 \equiv x^3 + ax + b \pmod{n}$.

Coppersmith's method

- Presented in 1996 by Coppersmith's to compute small roots of bivariate polynomials $f(x, y)$ over the integers, and small solutions of univariate modular polynomial equations $f(x) \equiv 0 \pmod{n}$.
- The method is based on lattice reduction techniques.
- Intensively used in cryptanalysis of some cryptographic systems such as RSA.

Lattice basis reduction

Let $u_1, \ldots, u_m \in \mathbb{R}^n$ be m linearly independent vectors where m and n are two positive integers satisfying $m \leq n$. The lattice $\mathcal{L}$ spanned by $\{u_1, \ldots, u_m\}$ is the set of linear combinations of the vectors $u_1, \cdots, u_m$ using integer coefficients

$$\mathcal{L} = \left\{ \sum_{i=1}^{m} a_i u_i \mid a_i \in \mathbb{Z} \right\}.$$

The set $\{u_1, \ldots, u_m\}$ form a basis for $\mathcal{L}$, and $\dim(\mathcal{L}) = m$ is its dimension. When $m = n$, the determinant is equal to the absolute value of the determinant of the matrix whose rows are the basis vectors $u_1, \ldots, u_m$, that is

$$\det(\mathcal{L}) = |\det(u_1, \ldots, u_m)|.$$

Lattice basis reduction

If $u = \sum_{i=1}^{m} a_i u_i$ is a vector of $\mathcal{L}$, then the Euclidean norm of u is

$$\|u\| = \left(\sum_{i=1}^{m} a_i^2 \right)^{\frac{1}{2}}.$$

A lattice has infinitely many bases with the same determinant and it is useful to find a basis with vectors of small Euclidean norms. However, finding the shortest nonzero vector in a lattice is very hard in general.

Lattice basis reduction

In 1982, Lenstra, Lenstra and Lovász invented the so-called LLL algorithm to reduce a basis.

Theorem 1.1 (Lenstra, Lenstra and Lovász)

Let $\mathcal{L}$ be a lattice of dimension m. In polynomial time, the LLL-algorithm outputs a reduced basis $\{b_1, \ldots, b_m\}$ that satisfies, after rearranging the norms

$$\|b_1\| \leq \|b_2\| \leq 2^{\frac{m}{4}} \det(\mathcal{L})^{\frac{1}{m-1}}.$$

Lattice basis reduction

Howgrave-Graham reformulated Coppersmith's technique and proved the following result.

Theorem 1.2 (Howgrave-Graham)

Let $f(x, y) \in \mathbb{Z}[x, y]$ be a polynomial which is a sum of at most ω monomials. Let N, x_0, y_0, X, and Y be integers such that

$$\begin{aligned} & f(x_0, y_0) \equiv 0 \pmod{N}, \\ & |x_0| < X, |y_0| < Y, \\ & \|f(Xx, Yy)\| < \frac{N}{\sqrt{\omega}}. \end{aligned}$$

Then $f(x_0, y_0) = 0$ holds over the integers.

Contents

Main Theorem

Let X_0, Y_0, a, b and n be integers. If the equation

$$(Y_0 + y)^2 \equiv (X_0 + x)^3 + a(X_0 + x) + b \pmod{n},$$

has a solution (x_0, y_0) with $|x_0|^3 y_0^2 < n$, then one can find x_0 and y_0 in polynomial time.

Proof of Main Theorem

Suppose that

$$(Y_0 + y)^2 \equiv (X_0 + x)^3 + a(X_0 + x) + b \pmod{n},$$

has a solution (x_0, y_0). Consider the polynomial

$$\begin{aligned} f(x, y) &= (X_0 + x)^3 + a(X_0 + x) + b - (Y_0 + y)^2 \\ &= x^3 + 3X_0x^2 + (3X_0^2 + a)x - y^2 - 2Y_0y + X_0^3 - Y_0^2 + aX_0 + b. \end{aligned}$$

Then $f(x_0, y_0) \equiv 0 \pmod{n}$.

Proof of Main Theorem

Suppose that

$$|x_0| < X = n^{\delta}, \quad y_0 < Y = n^{\gamma}.$$

We mix Coppersmith's method with the extended strategy of Jochemsz and May. Let m and t be two positive integers to be optimized later. For $0 \leq k \leq m$, define the polynomials

$$G_{k,i,j}(x,y) = y^j f(x,y)^k n^{m-k} \quad \text{with} \quad \begin{cases} i = 3k, \\ j = 0, 1, \ldots, 2(m-k) + t, \end{cases}$$

$$H_{k,i,j}(x,y) = x^{i-3k} y^j f(x,y)^k n^{m-k} \quad \text{with} \quad \begin{cases} i = 3k+1, 3k+2, \\ j = 0, 1, \ldots, 2(m-k) + t - 2. \end{cases}$$

Proof of Main Theorem

Let $\mathcal{L}$ be the lattice spanned by the coefficients of the vectors $G_{k,i,j}(xX, yY)$ and $H_{k,i,j}(xX, yY)$.
Set $t = m\tau$. Then

$$\det(\mathcal{L}) = n^{e_n} X^{e_X} Y^{e_Y},$$

with

$$e_n = \frac{1}{2}(3\tau + 4)m^3 + o(m^3),$$
$$e_X = \frac{3}{2}(3\tau + 2)m^3 + o(m^3),$$
$$e_Y = \frac{1}{2}\left(3\tau^2 + 6\tau + 4\right)m^3 + o(m^3),$$

while the dimension is $\omega = 3(\tau + 1)m^2 + o(m^2)$.

Proof of Main Theorem

Combing the LLL algorithm and Howgrave-Graham Theorem, we set

$$2^{\frac{\omega}{4}} \det(\mathcal{L})^{\frac{1}{\omega-1}} < \frac{n^m}{\sqrt{\omega}},$$

combining with

$$\det(\mathcal{L}) = n^{e_n} X^{e_X} Y^{e_Y},$$

we get

$$-27\delta^2 + (18 - 12\gamma)\delta + 4\gamma^2 + 4\gamma - 3 < -8\gamma\varepsilon_0.$$

and

$$\delta < \frac{1}{3} - \frac{2}{3}\gamma,$$

that is $|x_0|^3 y_0^2 < n$.

Contents

A Numerical Example

We have implemented our method using Maple on a computer with Windows 11 environment, and Intel(R) Core(TM) i5-8250U CPU 1.60 GHZ, 8.0 GO. Let us present the whole details of the method with a numerical example. Consider the following parameters:

$$n = 365017417331341649000673477806282123 3,$$
$$a = 756683154807978295876184055522467706,$$
$$b = 129668645647693842962538722548781675 5,$$
$$X_0 = 462225448948781571791783950 56,$$
$$Y_0 = 328635377133128443983127812039 67.$$

Our goal is to find the small solutions $(x, y) = (x_0, y_0)$ of the elliptic curve equation

$$(Y_0 + y)^2 \equiv (X_0 + x)^3 + a(X_0 + x) + b \pmod{n}.$$

A Numerical Example

We take $m = 4$, and $t = 1$, and form the lattice $\mathcal{L}$, with dimension $\omega = 70$. Also, we take

$$X = Y = \left\lfloor n^{\frac{1}{5}} \right\rfloor = 20533487.$$

A Numerical Example

We take $m = 4$, and $t = 1$, and form the lattice $\mathcal{L}$, with dimension $\omega = 70$. Also, we take

$$X = Y = \left\lfloor n^{\frac{1}{5}} \right\rfloor = 20533487.$$

By applying the LLL algorithm, we get a new basis with ω polynomials. We use the Gröbner basis method and find the solution

A Numerical Example

We take $m = 4$, and $t = 1$, and form the lattice $\mathcal{L}$, with dimension $\omega = 70$. Also, we take

$$X = Y = \left\lfloor n^{\frac{1}{5}} \right\rfloor = 20533487.$$

By applying the LLL algorithm, we get a new basis with ω polynomials. We use the Gröbner basis method and find the solution

$$x = x_0 = 2114853, \ y = y_0 = 329043.$$

Both lattice reduction phase and Gröbner basis technique took less than 283 seconds. We note that $x_0^3 y_0^2 < n$, as required by the method.

Contents

Conclusion

- We have presented a method to find the small solutions (x, y) of the elliptic curve equation

$$(Y_0 + y)^2 = (X_0 + x)^3 + a(X_0 + x) + b$$

in a finite field $\mathbb{Z}/p\mathbb{Z}$ where p is a prime number, or over a finite ring $\mathbb{Z}/n\mathbb{Z}$ with a composite integer n with unknown factorization.

- Our method is based on Coppersmith's method.
- Our method finds the solutions (x, y) if $|x|^3y^2 < p$ or $|x|^3y^2 < n$.
- The new method can be used to find the encrypted message in certain cryptosystems based on elliptic curves such as ElGamal, KMOV, Demytko and others, if the message is suitably small.

Thank you for your attention !