Elliptic Curves, Factorization, and Cryptography

Brian Rhee
MIT PRIMES

May 19, 2017

RATIONAL POINTS ON CONICS

The following procedure yields the set of rational points on a conic **C** given an initial rational point: Take the initial point **O**, and from that point project the conic **C** onto a rational line **L**. Then, all points mapped to a rational point were originally rational points, and vice versa.

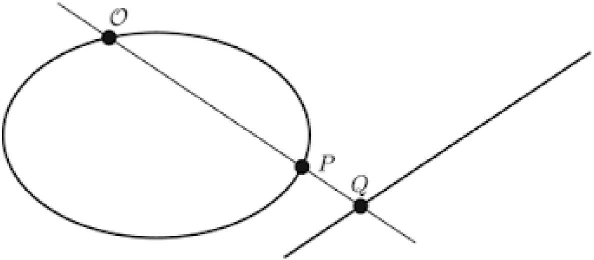


Figure: Projecting a conic onto a line

Rational Points on Conics

If **O** and **P** are both rational points, then **Q** is also a rational point, since two rational lines always intersect at a rational point. If **O** and **Q** are rational points, then **O** and **P** are the roots of the intersection of a conic and a line:

$$ax^2 + bxy + cy^2 + dx + ey + f = 0$$

Simplifies to a quadratic by substituting $y = mx + g$, which is our line **L**. Since the coefficients of the conic and the line are rational, the coefficients of the quadratic are also rational. This implies the sum of the roots are rational, but one root (**O**) is already rational, so **P** must be as well. This shows the bijection between rational points on **C** and rational points on **L**.

Elliptic Curves

Our reading group mainly focused on the study of polynomials of degree 3 and genus 1. One such example is Bachet's equation. By fixing an integer $c \in \mathbb{Z}$, we look for rational solutions to the Diophantine equation

$$y^2 - x^3 = c$$

The solutions to these equations using real numbers are called *cubic curves* or *elliptic curves*, each of which is of the form

$$y^2 = ax^3 + bx^2 + cx + d$$

but can be simplified into the Weierstrass form by substituting $x = x - \frac{b}{3a}$:

$$y^2 = ax^3 + bx + c$$

Projective Plane

We can transform these elliptic curves into the projective plane by substituting $y = \frac{\mathbf{Y}}{\mathbf{Z}}$ and $x = \frac{\mathbf{X}}{\mathbf{Z}}$. Now, the curves become

$$\mathbf{Y}^2 \cdot \mathbf{Z} = a \cdot \mathbf{X}^3 + b \cdot \mathbf{X} \cdot \mathbf{Z}^2 + c \cdot \mathbf{Z}^3$$

Now, each point is expressed as $[\mathbf{X}, \mathbf{Y}, \mathbf{Z}]$. If $\mathbf{Z} = 0$, then the point at infinity must be on the line $y = \frac{\mathbf{Y}}{\mathbf{X}} \cdot x$. Otherwise, the point is $(\frac{\mathbf{X}}{\mathbf{Z}}, \frac{\mathbf{Y}}{\mathbf{Z}})$. This also means that the point $[\mathbf{X}, \mathbf{Y}, \mathbf{Z}]$ is the same as the point $[k\mathbf{X}, k\mathbf{Y}, k\mathbf{Z}]$

Plugging in $\mathbf{Z} = 0$ yields $\mathbf{x} = 0$, so $[0, 1, 0]$ is the only point at infinity on each elliptic curve, denoted as **O**.

Bezout's Law

Bezout's law for general curves states that for a curve of degree m and a curve of degree n, including overlapping points such as tangency, they intersect at exactly mn points in the projective plane.

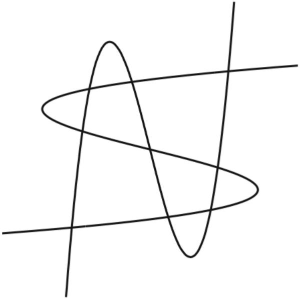


Figure: The two cubics intersect at nine points

ADDITION OF POINTS ON ELLIPTIC CURVES

To define the addition of points on elliptic curves, we need to first define the $*$ operation.

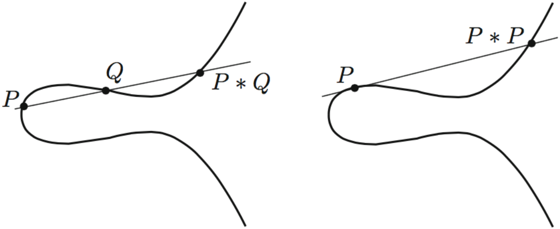


Figure: The $*$ operation

Addition of points on elliptic curves, cont.

To add P and Q, take the third intersection point $P * Q$, join it to $\mathcal{O}$ by a line, and then take the third intersection point to be $P + Q$. In other words, set $P + Q = \mathcal{O} * (P * Q)$.

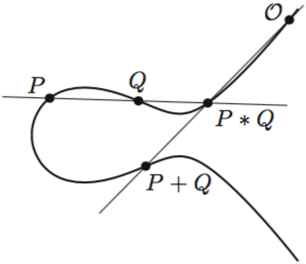


Figure: Addition of P and Q

Groups

- A **group** is a set of elements with an operation that satisfies the condition of closure, associativity, identity and inverse.
- An **abelian group** is a group that satisfies the commutativity property.

Identity Element

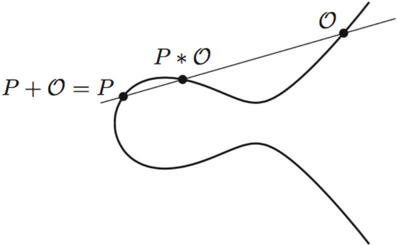


Figure: $\mathcal{O}$ acts as an Identity Element

Because $\mathcal{O}$ acts as the Identity Element, with the operation being $+$, which is obviously commutative, we see that the points on the elliptic curve becomes a group, an abelian one at that.

Mordell's Theorem

For a non-singular cubic curve **C** given by the equation

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

for any $a, b \in \mathbb{Z}$, we know that the group of rational points on curve **C** is an abelian group.

Mordell's Theorem states that

Theorem

The group of rational points of an elliptic curve has a finite number of generators.

Hasse-Weil Theorem

Theorem

If **C** *is a non-singular irreducible curve of genus g defined over a finite field $\mathbb{F}_p$, then the number of points on* **C** *with coordinates in F_p is equal to $p+1-\epsilon$, where the "error term" ϵ satisfies $|\epsilon| \leq 2g\sqrt{p}$.*

For an elliptic curve **C** over a finite field $\mathbb{F}_p$, the Hasse-Weil theorem gives the estimate that the number of points of elliptic curve **C** is

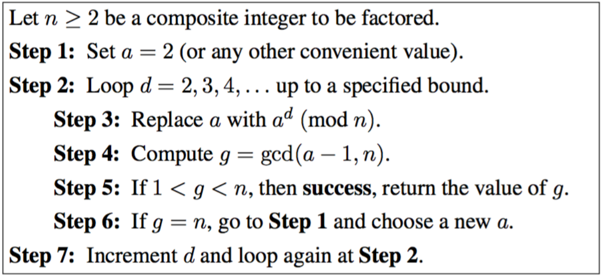
$$-2\sqrt{p} \leq \#\mathbf{C}(\mathbb{F}_p) - p - 1 \leq 2\sqrt{p}$$

Applications

Elliptic curves over finite fields are easy to implement on any computer, since the group law is a simple algebraic equation in the coefficients. We can use the group structure to create a number of algorithms.

- Factorization of Large Numbers
- Public Key Cryptography

Pollard's Method

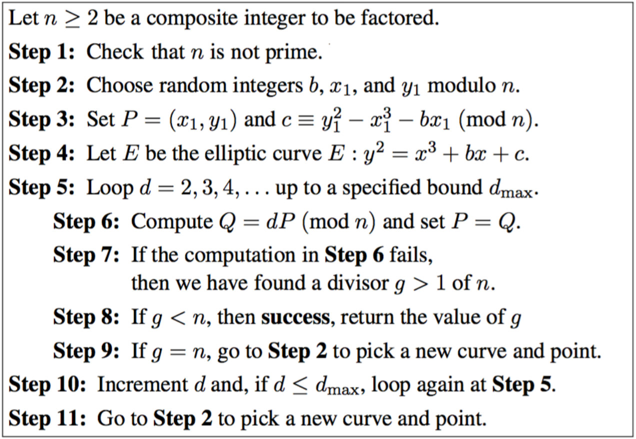


```
Let $n \geq 2$ be a composite integer to be factored.
Step 1: Set $a = 2$ (or any other convenient value).
Step 2: Loop $d = 2, 3, 4, \ldots$ up to a specified bound.
    Step 3: Replace $a$ with $a^d \pmod{n}$.
    Step 4: Compute $g = \gcd(a - 1, n)$.
    Step 5: If $1 < g < n$, then success, return the value of $g$.
    Step 6: If $g = n$, go to Step 1 and choose a new $a$.
Step 7: Increment $d$ and loop again at Step 2.
```

However, we see that Pollard's method quickly grows inefficient, as *d* should be a product of small primes to make the calculations take up a smaller number of steps.

Lenstra's Factorization Method

Although Pollard's factorization method yields around $\log N$ steps, Lenstra's elliptic curve factorization method allows us to keep factorizing.



```
Let $n \geq 2$ be a composite integer to be factored.
Step 1: Check that $n$ is not prime.
Step 2: Choose random integers $b$, $x_1$, and $y_1$ modulo $n$.
Step 3: Set $P = (x_1, y_1)$ and $c \equiv y_1^2 - x_1^3 - bx_1 \pmod{n}$.
Step 4: Let $E$ be the elliptic curve $E : y^2 = x^3 + bx + c$.
Step 5: Loop $d = 2, 3, 4, \ldots$ up to a specified bound $d_{\max}$.
    Step 6: Compute $Q = dP \pmod{n}$ and set $P = Q$.
    Step 7: If the computation in Step 6 fails,
            then we have found a divisor $g > 1$ of $n$.
    Step 8: If $g < n$, then success, return the value of $g$
    Step 9: If $g = n$, go to Step 2 to pick a new curve and point.
Step 10: Increment $d$ and, if $d \leq d_{\max}$, loop again at Step 5.
Step 11: Go to Step 2 to pick a new curve and point.
```

AN EXAMPLE OF LENSTRA'S

We can attempt to factor $n = 1715761513$.

1. Let $x_1 = 2, y_1 = 3$, so $P = (2, 3)$. WLOG, for a given b let $c = 1 - 2b$. First, let $b = 1$ and $c = -1$.
2. As we cycle through steps 6 - 10, observe that for some d

   $$P_d = dP_{d-1} = ...d!P_1$$

   Thus, let $d_{max} = 20$ and calculate up to $20!P$ in modulo n. For example,

   $$P_{20} = 20!P = 20!(2, 3) = (693588502, 858100579)$$

   However, the whole point of Lenstra's algorithm is that the addition law has to break down when we obtain a $\gcd(v, n)$ less than n for some $v \pmod n$ so that the algorithm terminates.
3. We can either keep going or pick different b and c's for the same $d_{max} = 20$.

An Example of Lenstra's (Cont.)

For $b = 5$ and $c = -11$, we hit the jackpot. Everything goes smoothly up until

$$Q = 16!P = (962228801, 946564039) \pmod{1715761513}$$

on the curve $y^2 = x^3 + 5x - 9$. To compute $17!P = 17Q$, we must add $16Q + Q$. We first calculate that $16Q = (505708443, 718251590)$.

Next, we must find the inverse modulo n of the difference of x-coordinates of Q and $16Q$, so we need to invert

$$x(16Q) - x(Q) = 505708443 - 962228801 = -456520358 \pmod{n}$$

An Example of Lenstra's (Cont.)

But when we use the Euclidean algorithm to compute the gcd of this quantity and n, we find that

$$\gcd(x(16Q) - x(Q), n) = \gcd(-456520358, 1715761513) = 26927$$

This gives a non-trivial factor of n and also the complete prime factorization of n, so we are done.

$$n = 1715761513 = 26927 \cdot 63719$$

Cryptography

- **Discrete Logarithm Problem**
  Find an integer m that solves the congruence
  $a^n \equiv b (\bmod p)$
- **Elliptic Curve Discrete Logarithm Problem**
  Given $P, Q \in \mathbf{C}(\mathbb{F}_p)$, find an integer m such that $mP = Q$.

Elliptic Curve Discrete Logarithm Problem

Consider the elliptic curve

$$\mathbf{C} : y^2 = x^3 + x^2 + x + 1 \qquad \text{over the field} \quad \mathbb{F}_{97}$$

Points P = (7,20) and Q = (17,46) are in $C(\mathbb{F}_{97})$. We can use the "collision algorithm" to quickly solve for m.

Make two lists of $P, 2P, 3P, ...,$ and $Q - 10P, Q - 20P, Q - 30P, ...$ until finding a common point $aP = Q - 10P$, so $m = a + 10b$. We pick 10 because its close to $\sqrt{97}$.

Comparing the lists, one can quickly find the collision $7P = (8, 87) = Q - 40P$, so $47P = Q$.

BENEFITS OF ELLIPTIC CURVE CRYPTOGRAPHY

The ECDLP is much more preferred over the DLP

- Much harder to decrypt
- Takes up much less bits
- Much more efficient overall

ACKNOWLEDGEMENTS

We would like to thank:

- Yongyi Chen
- Our Parents
- Dr. Khovanova and Dr. Gerovitch
- MIT PRIMES