Elliptic Curves: Theory and Applications

Ben Wright and Junze Ye

Phillips Exeter Academy

Dec. 5th, 2018

Why Elliptic Curves Matter

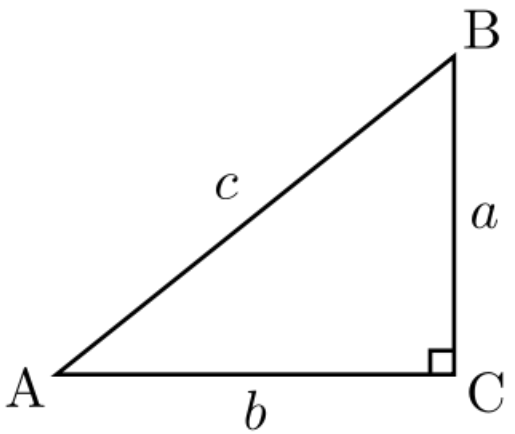
The study of elliptic curves has always been of deep interest, with focus on the points on an elliptic curve with coefficients in certain fields. Applications of elliptic curves include:

- Solving Diophantine equations
- Factorizing large numbers
- Cryptography
- Calculating the perimeter of an ellipse
- Various other well-known problems

Congruent Numbers Open Problem

The *Congruent Numbers Problem* asks which positive integers can be expressed as the area of a right triangle with rational sides. So, a number n is *congruent* if there exist rational numbers a, b, c such that

$$a^2 + b^2 = c^2, \ \frac{ab}{2} = n$$



First few congruent numbers: 5, 6, 7, 13, 14, 15, 20, 21, 22

Because any primitive Pythagorean triple can be expressed as $(p^2 - q^2, 2pq, p^2 + q^2)$, we can set

$$a = \frac{x^2 - n^2}{y}, b = \frac{2xn}{y}, c = \frac{x^2 + n^2}{y},$$

where x, y are rational numbers. Simplifying gives

$$y^2 = x^3 - n^2 x,$$

which is an elliptic curve. So, n is congruent if and only if $y^2 = x^3 - n^2 x$ has a non-trivial rational point.

Definition

A *group* is a pair $(G, *)$ where G is a set and $*$ is a binary operation $G \times G \to G$ that satisfies the following properties:

1. $\forall\ a, b, c \in G,\ a * (b * c) = (a * b) * c.$
2. $\exists\ e \in G$ such that $a * e = e * a = a\ \forall\ a \in G.$
3. $\forall\ a \in G$, there exists $b \in G$ such that $a * b = b * a = e.$

A *group* is *abelian* if $a * b = b * a\ \forall\ a, b \in G.$

Often we write $a * b$ as ab.

Definition

A *ring* is a triple $(R, +, *)$, where R is a set and $*, +$ are binary operations $R \times R \to R$ such that:

1. The pair $(R, +)$ satisfies the properties of an abelian group, where its additive identity is labeled 0,
2. $\forall\ a, b, c \in R,\ a * (b * c) = (a * b) * c.$
3. $\forall\ a, b, c \in R,\ a * (b + c) = a * b + a * c.$
4. $\exists\ 1 \in R$ such that $a * 1 = 1 * a = a.$

R is called *commutative* if in addition we have $a * b = b * a$ for all $a, b \in R$.

Definition

A *field* is a commutative ring such that every nonzero element has a multiplicative inverse.

Definition

The n-dimensional *projective plane* $\mathbb{P}^n_K$ is the set of equivalence classes defined by

$$(K^{n+1} - \{\mathbf{0}\})/(\mathbf{v} \sim \lambda\mathbf{v} \ \forall \ \lambda \in K^*).$$

Denote the equivalence class of $(a_0, a_1, a_2, \ldots, a_n)$ as $[a_0, a_1, a_2, \ldots, a_n]$.

For this presentation, we will only be talking about Elliptic Curves in the Projective plane, or $\mathbb{P}^2_K$.

Definition

A curve is *non-singular* if there is a unique, defined tangent line at every point.

Definition

Let K be a field. An *elliptic curve* over K is a non-singular curve defined by an equation of the form

$$Y^2Z = aX^3 + bX^2Z + cXZ^2 + dZ^3,$$

with coefficients in a field K, living in the projective plane $\mathbb{P}^2_K$.

Alternate form of Elliptic Curves

By mapping $[\frac{X}{Z}, \frac{Y}{Z}, 1]$ to (x, y), we can classify all equivalence classes with $Z \neq 0$:

$$\left(\frac{Y}{Z}\right)^2 = a\left(\frac{X}{Z}\right)^3 + b\left(\frac{X}{Z}\right)^2 + c\left(\frac{X}{Z}\right) + d, \text{ or}$$

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

Plugging in $Z = 0$ gives $X = 0$, so the only point at infinity is $\mathcal{O} = [0, 1, 0]$. Therefore, our elliptic curve is equivalent to the equation $y^2 = ax^3 + bx^2 + cx + d$ in the affine plane, adjoined with the point $\mathcal{O}$.

Definition

An elliptic curve over a field K is in *Weierstrass form* if it is of the form

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

When the characteristic of K is not 2 or 3, the Weierstrass form can be further simplified down to

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

through a series of substitutions. Many of our results will assume this simplified Weierstrass form.

Definition

The *discriminant* D of an elliptic curve $y^2 = x^3 + ax^2 + bx + c$ is

$$D = -4a^3c + a^2b^2 + 18abc - 4b^3 - 27c^2.$$

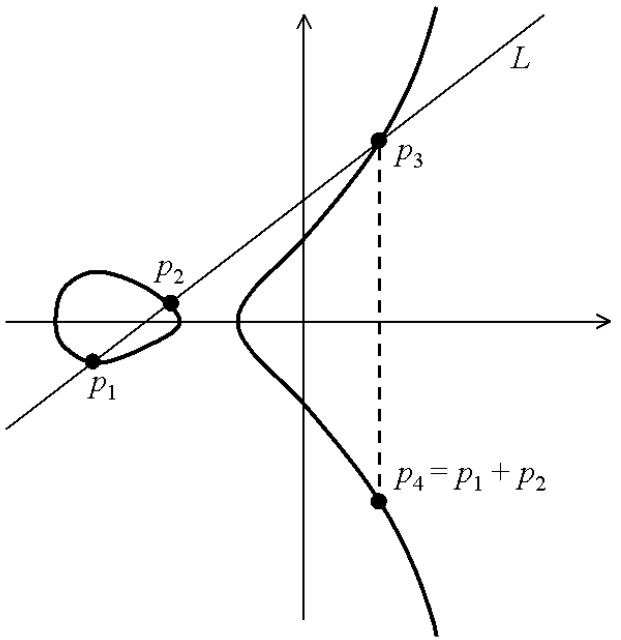
When $a = 0$, or equivalently given simplified Weierstrass form, we have $D = -4b^3 - 27c^2$.

Remark

$D \neq 0$ is equivalent to the curve being non-singular.

Definition

The sum $p_1 + p_2$ is defined to be the reflection of the third intersection of the line p_1p_2 with E over the x-axis.



Elliptic Curve Addition 2

Since connecting $\mathcal{O}$ with a point gives a vertical line, $\mathcal{O} + (x, y) = (x, y)$, so $\mathcal{O}$ is the identity.

Since $(x, y) + (x, -y) = \mathcal{O}$, it is clear that an inverse exists for any point: $(x, -y)$.

In addition, trivially, this addition function is commutative.

Assuming simple Weierstrass form, some algebra gives a complicated formula for addition involving only rational functions. This means that the set of rational points is closed under addition, where the rational points are the set of points with coefficients in K.

This group addition is associative, though we will not prove it. Therefore, this addition function satisfies the conditions:

1. Associative
2. Commutative
3. Closed over $E(K)$
4. Has an identity $\mathcal{O}$
5. Each point has an inverse

which are all the requirements for an abelian group, so the pair $(E(K), +)$ is a group.

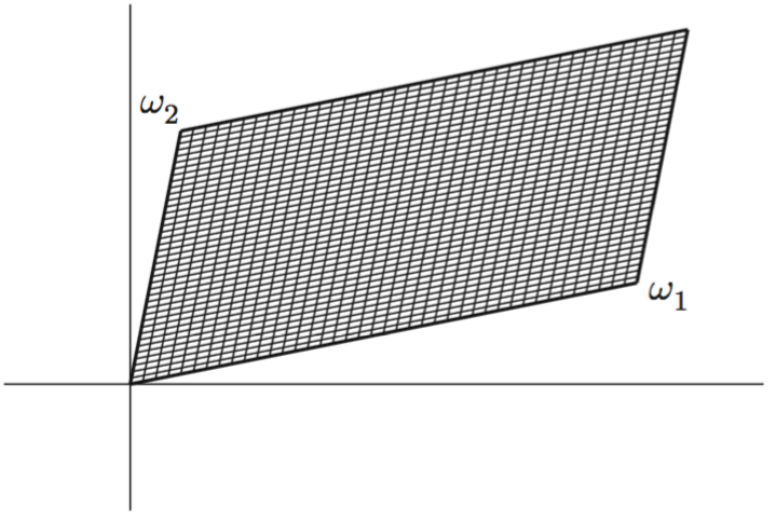
Points of Finite Order

Question

What is the structure of the points of finite order?

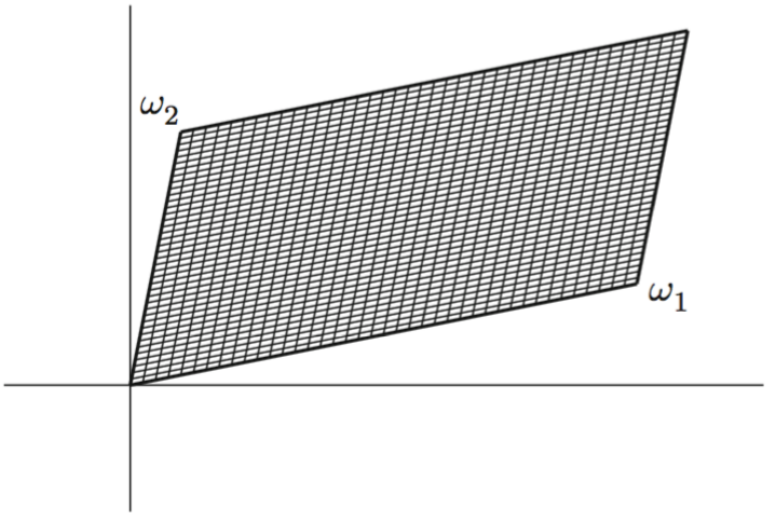
Structure of Complex Points

Let $E(\mathbb{C})$ be all the points with complex coordinates on the elliptic curve. Then, there is an isomorphism between $E(\mathbb{C})$ and a parallelogram in $\mathbb{R}^2$.



Structure of Complex Points

Let $E(\mathbb{C})$ be all the points with complex coordinates on the elliptic curve. Then, there is an isomorphism between $E(\mathbb{C})$ and a parallelogram in $\mathbb{R}^2$.



The elliptic curve addition formula then becomes equivalent to adding the coordinates like vectors, and then subtracting multiples of ω_1 and ω_2 until the point ends back up within the parallelogram. $\mathcal{O}$ is sent to the origin.

From our isomorphism, we see that for nP to equal $\mathcal{O}$, then n times the image of P must be a linear combination of ω_1 and ω_2.

Therefore, the image of P is

$$\frac{a}{n}\omega_1 + \frac{b}{n}\omega_2,$$

for non-negative integers $a, b < n$. Therefore, the set of complex points of order dividing n is isomorphic to $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$.

From our addition formula, all points of finite order are algebraic, so this structure is the same for not only $E(\mathbb{C})$, but also for $E(\overline{\mathbb{Q}})$.

Let the equation $y^2 = x^3 + ax^2 + bx + c$ define a non-singular elliptic curve denoted as E, with $a, b, c \in \mathbb{Z}$. Let D be the discriminant of the curve, as defined earlier.

Theorem

(Nagell-Lutz) If $P = (x, y)$ is a rational point of finite order on E, for the elliptic curve group law, then:

1. *x and y are integers*
2. *If $y = 0$, then P has order two*
3. *If $y \neq 0$, then y divides D, which implies y^2 divides D.*

Mordell's Theorem

Definition

An abelian group G is *finitely generated* if there exists a finite set $S = (a_1, a_2, a_3, \ldots, a_n)$ consisting of elements of G, such that any element e of G can be expressed as an integer combination of elements of S.

Theorem

(Mordell) If a non-singular elliptic curve E has a rational point, then the group of rational points $(E(\mathbb{Q}), +)$ is a finitely generated abelian group.

Elliptic Curves over Finite Fields

An elliptic curve E over a finite field $\mathbb{F}_p$ is the point set $\{(x, y) \in (\mathbb{F}_p)^2 \mid y^2 \equiv x^3 + ax + b \pmod{p}\} \cup \{\mathcal{O}\}$.

Note that $\mathcal{O}$ is the point at infinity, and a and b are two integers in $\mathbb{F}_p$. In particular, the discriminant $4a^3 + 27b^2 \not\equiv 0 \pmod{p}$.

We can use the group structure of elliptic curves to create a number of algorithms.

- Factorization of Large Numbers
- Public Key Cryptography

An Example of an elliptic curve over a finite field

Let E be the curve $y^2 = x^3 + x + 1$ over $\mathbb{F}_5$.

x	$x^3 + x + 1$	y	Points
0	1	± 1	$(0,1), (0,4)$
1	3	-	-
2	1	± 1	$(2,1), (2,4)$
3	1	± 1	$(3,1), (3,4)$
4	4	± 2	$(4,2), (4,3)$
∞		∞	∞

Note that $\#E(\mathbb{F}_5) - p - 1 = 9 - 5 - 1 = 3$

Hasse-Weil Bound

Theorem

If $\mathbf{C}$ *is a non-singular irreducible curve of genus* g *defined over a finite field* $\mathbb{F}_p$*, then the number of points on* $\mathbf{C}$ *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 $\mathbf{C}$ over a finite field $\mathbb{F}_p$, the Hasse-Weil theorem gives the estimate that the number of points of elliptic curve $\mathbf{C}$ is

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

Definition

(**Reduction modulo** p) We write $z \to \tilde{z}$ for the map reduction modulo p, where

$$\mathbb{Z} \longrightarrow \mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p, \qquad z \longmapsto \tilde{z}.$$

Let C be a cubic curve, given by a Weierstrass equation

$$C: \ y^2 = x^3 + ax^2 + bx + c$$

with integer coefficients a, b, c.

Take equation for C, and reduce those coefficients modulo p to get a new curve with coefficients in $\mathbb{F}_p$,

$$\tilde{C}: \ y^2 = x^3 + \tilde{a}x^2 + \tilde{b}x + \tilde{c}.$$

The curve $\tilde{C}$ will be non-singular if $p \geq 3$ and the discriminant

$$\tilde{D} = -4\tilde{a}^3\tilde{c} + \tilde{a}^2\tilde{b}^2 + 18\tilde{a}\tilde{b}\tilde{c} - 4\tilde{b}^3 - 27\tilde{c}^2$$

is non-zero. The reduced curve $\tilde{C} \pmod{p}$ is non-singular provided that $p \geq 3$ and p does not divide the discriminant D.

Let $P = (x, y) \in C(\mathbb{Q})$ be a point with integer coordinates. By reduction modulo p, we have

$$\tilde{y}^2 = \tilde{x}^3 + \tilde{a}\tilde{x}^2 + \tilde{b}\tilde{x} + \tilde{c}.$$

So $\tilde{P} = (\tilde{x}, \tilde{y})$ is a point in $\tilde{C}(\mathbb{F}_p)$. In addition, if $P = \mathcal{O}$, define $\tilde{P} = \tilde{\mathcal{O}}$. We then get a map $P \to \tilde{P}$ from the points in $C(\mathbb{Q})$ with integer coordinates to $\tilde{C}(\mathbb{F}_p)$.

Reduction modulo p Theorem

Theorem

Let C be a non-singular cubic curve

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

with integer coefficients a, b, c, and let D be the discriminant. If p does not divide $2D$, then the group of finite order points in $E(\mathbb{Q})$ under reduction modulo p injects into $\tilde{E}(\mathbb{F}_p)$.

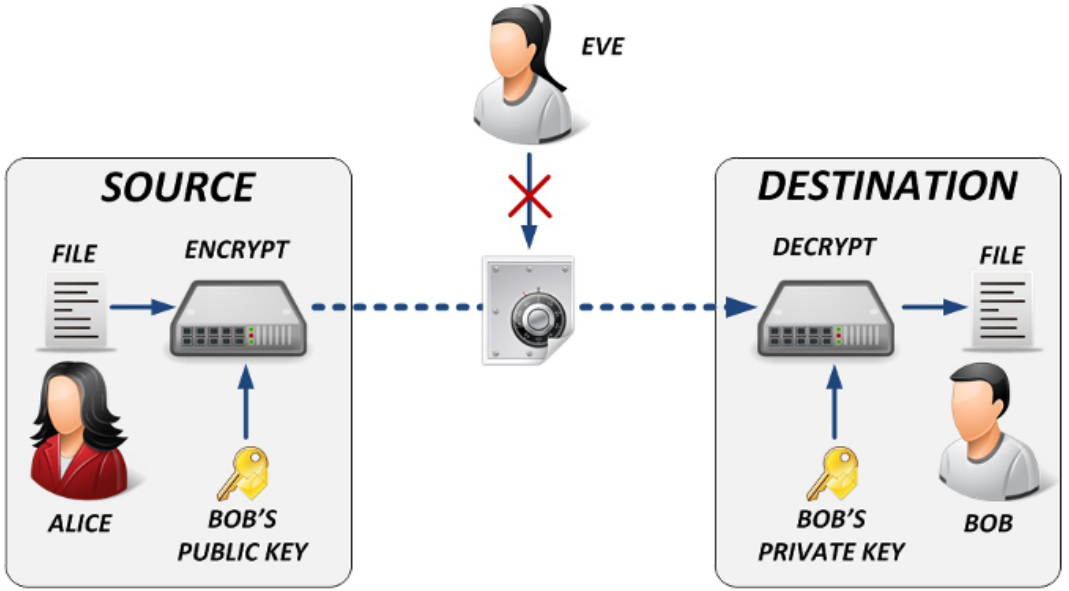
- **Discrete Logarithm Problem**

  Find an integer m that solves the congruence
  $a^m \equiv b (\mathrm{mod}\, p)$

- **Elliptic Curve Discrete Logarithm Problem**

  Given $P, Q \in \mathbf{C}(\mathbb{F}_p)$, find an integer m such that $mP = Q$.

Public-key Cryptography



Diffie-Hellman Key Exchange

1. Alice and Bob agree on an elliptic curve E over a finite field $\mathbb{F}_q$ such that the discrete logarithm problem is hard in $E(\mathbb{F}_q)$. They also agree on a point $P \in E(\mathbb{F}_q)$.

Diffie-Hellman Key Exchange

1. Alice and Bob agree on an elliptic curve E over a finite field $\mathbb{F}_q$ such that the discrete logarithm problem is hard in $E(\mathbb{F}_q)$. They also agree on a point $P \in E(\mathbb{F}_q)$.
2. Alice chooses a secret integer a, computes $P_a = aP$, and sends P_a to Bob.

Diffie-Hellman Key Exchange

1. Alice and Bob agree on an elliptic curve E over a finite field $\mathbb{F}_q$ such that the discrete logarithm problem is hard in $E(\mathbb{F}_q)$. They also agree on a point $P \in E(\mathbb{F}_q)$.
2. Alice chooses a secret integer a, computes $P_a = aP$, and sends P_a to Bob.
3. Bob chooses a secret integer b, computes $P_b = bP$, and sends P_b to Alice.

Diffie-Hellman Key Exchange

1. Alice and Bob agree on an elliptic curve E over a finite field $\mathbb{F}_q$ such that the discrete logarithm problem is hard in $E(\mathbb{F}_q)$. They also agree on a point $P \in E(\mathbb{F}_q)$.
2. Alice chooses a secret integer a, computes $P_a = aP$, and sends P_a to Bob.
3. Bob chooses a secret integer b, computes $P_b = bP$, and sends P_b to Alice.
4. Alice computes $aP_b = abP$.

Diffie-Hellman Key Exchange

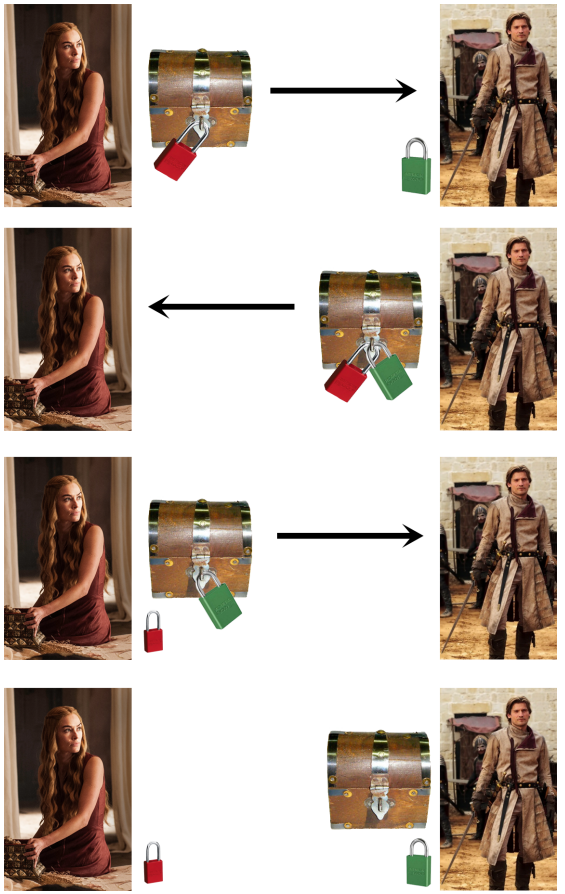
1. Alice and Bob agree on an elliptic curve E over a finite field $\mathbb{F}_q$ such that the discrete logarithm problem is hard in $E(\mathbb{F}_q)$. They also agree on a point $P \in E(\mathbb{F}_q)$.
2. Alice chooses a secret integer a, computes $P_a = aP$, and sends P_a to Bob.
3. Bob chooses a secret integer b, computes $P_b = bP$, and sends P_b to Alice.
4. Alice computes $aP_b = abP$.
5. Bob computes $bP_a = baP$.

Diffie-Hellman Key Exchange (Cont.)

6. Alice and Bob use some publicly agreed on method to extract a key from abP.

The only information that the eavesdropper Eve sees is the curve E, the finite field $\mathbb{F}_q$, and the points P, aP, and bP. She therefore needs to compute abP from the points P, aP, and bP.

Massey-Omura Key Exchange



Mathematical Implementation of Massey-Omura

1. Alice and Bob agree on an elliptic curve E over a finite field $\mathbb{F}_q$. Let $\mathrm{N} = \#E(\mathbb{F}_q)$.

Mathematical Implementation of Massey-Omura

1. Alice and Bob agree on an elliptic curve E over a finite field $\mathbb{F}_q$. Let $\mathrm{N} = \#E(\mathbb{F}_q)$.
2. Alice represents her message as a point $M \in E(\mathbb{F}_q)$.

Mathematical Implementation of Massey-Omura

1. Alice and Bob agree on an elliptic curve E over a finite field $\mathbb{F}_q$. Let N $= \#E(\mathbb{F}_q)$.
2. Alice represents her message as a point $M \in E(\mathbb{F}_q)$.
3. Alice chooses a secret integer A with gcd(A,N)= 1, computes $M_1 = AM$, and sends M_1 to Bob.

Mathematical Implementation of Massey-Omura

1. Alice and Bob agree on an elliptic curve E over a finite field $\mathbb{F}_q$. Let N $= \#E(\mathbb{F}_q)$.
2. Alice represents her message as a point $M \in E(\mathbb{F}_q)$.
3. Alice chooses a secret integer A with gcd(A,N)= 1, computes $M_1 = AM$, and sends M_1 to Bob.
4. Bob chooses a secret integer B with gcd(B,N)= 1, computes $M_2 = BM_1$, and sends M_2 to Alice.

Mathematical Implementation of Massey-Omura

1. Alice and Bob agree on an elliptic curve E over a finite field $\mathbb{F}_q$. Let N $= \#E(\mathbb{F}_q)$.
2. Alice represents her message as a point $M \in E(\mathbb{F}_q)$.
3. Alice chooses a secret integer A with gcd(A,N)= 1, computes $M_1 = AM$, and sends M_1 to Bob.
4. Bob chooses a secret integer B with gcd(B,N)= 1, computes $M_2 = BM_1$, and sends M_2 to Alice.
5. Alice computes $A^{-1} \in \mathbb{Z}_N$. She computes $M_3 = A^{-1}M_2$ and sends M_3 to Bob.

Mathematical Implementation of Massey-Omura

1. Alice and Bob agree on an elliptic curve E over a finite field $\mathbb{F}_q$. Let N $= \#E(\mathbb{F}_q)$.
2. Alice represents her message as a point $M \in E(\mathbb{F}_q)$.
3. Alice chooses a secret integer A with gcd(A,N)$= 1$, computes $M_1 = AM$, and sends M_1 to Bob.
4. Bob chooses a secret integer B with gcd(B,N)$= 1$, computes $M_2 = BM_1$, and sends M_2 to Alice.
5. Alice computes $A^{-1} \in \mathbb{Z}_N$. She computes $M_3 = A^{-1}M_2$ and sends M_3 to Bob.
6. Bob computes $B^{-1} \in \mathbb{Z}_N$. He computes $M_4 = B^{-1}M_3$. Then $M_4 = M$ is the message.

Mathematical implementation of Massey-Omura (cont.)

The eavesdropper Eve knows $E(\mathbb{F}_q)$ and the points AM, BAM, and BM. Let $a = A$, $b = B$, $P = ABM$. Then we see that Eve knows P, bP, aP and wants to find abP. This is exactly the discrete log problem, which is hard to crack!

Massey-Omura vs. Diffie-Hellman

- **Diffie-Hellman Key Exchange**

  The secret keys of Alice and Bob together determine the private key they will use.

- **Massey-Omura Key Exchange**

  One party determines what the shared private key would be.

Acknowledgements

We would like to thank:

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