Data Protection

Jorge L. Villar

MCYBERS, UPC, Fall 2025

Outline

1 Modular Arithmetic

2 Background on Finite Fields

3 Background on Elliptic Curves

Modular Arithmetic

The quotient $\mathbb{Z}/n\mathbb{Z}$, or simply $\mathbb{Z}_n$, represented as $\{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}$, is a ring with the operations:

$\overline{x} + \overline{y} = \overline{x + y \mod n}$

$\overline{x} * \overline{y} = \overline{xy \mod n}$

Modular Arithmetic

The quotient $\mathbb{Z}/n\mathbb{Z}$, or simply $\mathbb{Z}_n$, represented as $\{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}$, is a ring with the operations:

$\overline{x} + \overline{y} = \overline{x + y \mod n}$

$\overline{x} * \overline{y} = \overline{xy \mod n}$

Example ($n = 15$):

$\overline{7} = \{\ldots, -8, \mathbf{7}, 22, 37, \ldots\}$

$\overline{13} = \{\ldots, -2, \mathbf{13}, 28, 43, \ldots\}$

$\overline{7} + \overline{13} = \overline{20 \mod 15} = \overline{5}$

$\overline{7} * \overline{13} = \overline{91 \mod 15} = \overline{1}$ Then, $\overline{7}^{-1} = \overline{13}$ in $\mathbb{Z}_{15}$

Modular Arithmetic

The quotient $\mathbb{Z}/n\mathbb{Z}$, or simply $\mathbb{Z}_n$, represented as $\{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}$, is a ring with the operations:

$\overline{x} + \overline{y} = \overline{x + y \mod n}$

$\overline{x} * \overline{y} = \overline{xy \mod n}$

Example ($n = 15$):

$\overline{7} = \{\ldots, -8, \mathbf{7}, 22, 37, \ldots\}$

$\overline{13} = \{\ldots, -2, \mathbf{13}, 28, 43, \ldots\}$

$\overline{7} + \overline{13} = \overline{20 \mod 15} = \overline{5}$

$\overline{7} * \overline{13} = \overline{91 \mod 15} = \overline{1}$ Then, $\overline{7}^{-1} = \overline{13}$ in $\mathbb{Z}_{15}$

In general, not every $\overline{x}$ han an inverse.

Indeed, there exist zero divisors: $\overline{6} * \overline{5} = \overline{0}$

Modular Arithmetic

The quotient $\mathbb{Z}/n\mathbb{Z}$, or simply $\mathbb{Z}_n$, represented as $\{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}$, is a ring with the operations:

$\overline{x} + \overline{y} = \overline{x + y \mod n}$

$\overline{x} * \overline{y} = \overline{xy \mod n}$

Example ($n = 15$):

$\overline{7} = \{\ldots, -8, \mathbf{7}, 22, 37, \ldots\}$

$\overline{13} = \{\ldots, -2, \mathbf{13}, 28, 43, \ldots\}$

$\overline{7} + \overline{13} = \overline{20 \mod 15} = \overline{5}$

$\overline{7} * \overline{13} = \overline{91 \mod 15} = \overline{1}$ Then, $\overline{7}^{-1} = \overline{13}$ in $\mathbb{Z}_{15}$

In general, not every $\overline{x}$ han an inverse.
Indeed, there exist zero divisors: $\overline{6} * \overline{5} = \overline{0}$

For simplicity, we identify $\overline{x}$ with x.

Computing Modular Inverses

Bezout's Equality

For all $x, y \in \mathbb{Z}$ there exist $a, b \in \mathbb{Z}$ such that $ax + by = \gcd(x, y)$

a and b can be efficiently computed with (extended) Euclid's algorithm.

Computing Modular Inverses

Bezout's Equality

For all $x, y \in \mathbb{Z}$ there exist $a, b \in \mathbb{Z}$ such that $ax + by = \gcd(x, y)$

a and b can be efficiently computed with (extended) Euclid's algorithm.

Taking $y = n$, for all x such that $\gcd(x, n) = 1$, the inverse of x in $\mathbb{Z}_n$ is $x^{-1} = a \mod n$.

Computing Modular Inverses

Bezout's Equality

For all $x, y \in \mathbb{Z}$ there exist $a, b \in \mathbb{Z}$ such that $ax + by = \gcd(x, y)$

a and b can be efficiently computed with (extended) Euclid's algorithm.

Taking $y = n$, for all x such that $\gcd(x, n) = 1$, the inverse of x in $\mathbb{Z}_n$ is $x^{-1} = a \mod n$.

If $\gcd(x, n) \neq 1$, then x has no inverse in $\mathbb{Z}_n$.

Computing Modular Inverses

Bezout's Equality

For all $x, y \in \mathbb{Z}$ there exist $a, b \in \mathbb{Z}$ such that $ax + by = \gcd(x, y)$

a and b can be efficiently computed with (extended) Euclid's algorithm.

Taking $y = n$, for all x such that $\gcd(x, n) = 1$, the inverse of x in $\mathbb{Z}_n$ is $x^{-1} = a \mod n$.

If $\gcd(x, n) \neq 1$, then x has no inverse in $\mathbb{Z}_n$.

The number of invertible elements in $\mathbb{Z}_n$ is given by Euler's totient function $\phi(n)$.

Computing Modular Exponentiations

Squares and multiplications algorithm:

Let $a = 2^m + a_{m-1}2^{m-1} + \ldots + a_1 2 + a_0$, where $a_0, \ldots, a_{m-1} \in \{0, 1\}$.

Then, $x^a = x^{a_0}(x^{a_1}(\cdots(x^{a_{m-1}}x^2)^2\cdots)^2)^2$.

Computing Modular Exponentiations

Squares and multiplications algorithm:

Let $a = 2^m + a_{m-1}2^{m-1} + \ldots + a_1 2 + a_0$, where $a_0, \ldots, a_{m-1} \in \{0, 1\}$.

Then, $x^a = x^{a_0}(x^{a_1}(\cdots(x^{a_{m-1}}x^2)^2\cdots)^2)^2$.

Example: $x^{11} = x^{1+2+2^3} = x(x((x^2)^2)^2$.

Computing Modular Exponentiations

Squares and multiplications algorithm:

Let $a = 2^m + a_{m-1}2^{m-1} + \ldots + a_1 2 + a_0$, where $a_0, \ldots, a_{m-1} \in \{0, 1\}$.

Then, $x^a = x^{a_0}(x^{a_1}(\cdots(x^{a_{m-1}}x^2)^2\cdots)^2)^2$.

Example: $x^{11} = x^{1+2+2^3} = x(x((x^2)^2)^2$.

In $\mathbb{Z}_n$ all multiplications and squares are computed modulo n.

Computing Modular Exponentiations

Squares and multiplications algorithm:

Let $a = 2^m + a_{m-1}2^{m-1} + \ldots + a_1 2 + a_0$, where $a_0, \ldots, a_{m-1} \in \{0, 1\}$.

Then, $x^a = x^{a_0}(x^{a_1}(\cdots(x^{a_{m-1}}x^2)^2\cdots)^2)^2$.

Example: $x^{11} = x^{1+2+2^3} = x(x((x^2)^2)^2$.

In $\mathbb{Z}_n$ all multiplications and squares are computed modulo n.

Theorem (Fermat's Little Theorem)

For all $x \in \mathbb{Z}$, *such that* $\gcd(x, n) = 1$, $x^{\phi(n)} = 1 \pmod{n}$

Computing Modular Exponentiations

Squares and multiplications algorithm:

Let $a = 2^m + a_{m-1}2^{m-1} + \ldots + a_1 2 + a_0$, where $a_0, \ldots, a_{m-1} \in \{0, 1\}$.

Then, $x^a = x^{a_0}(x^{a_1}(\cdots(x^{a_{m-1}}x^2)^2\cdots)^2)^2$.

Example: $x^{11} = x^{1+2+2^3} = x(x((x^2)^2)^2$.

In $\mathbb{Z}_n$ all multiplications and squares are computed modulo n.

Theorem (Fermat's Little Theorem)

For all $x \in \mathbb{Z}$, *such that* $\gcd(x, n) = 1$, $x^{\phi(n)} = 1 \pmod{n}$

The exponents in $\mathbb{Z}_n$ work modulo $\phi(n)$.

Composite Modulus

Theorem (Chineese Remaider Theorem)

If $n = n_1 n_2$ with $\gcd(n_1, n_2) = 1$, then the rings $\mathbb{Z}_n$ and $\mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2}$ are isomorphic, with the map $x \mapsto (x \mod n_1, x \mod n_2)$.

$$x \text{ invertible mod } n \quad \Leftrightarrow \quad \begin{cases} x \text{ invertible mod } n_1, \text{ and} \\ x \text{ invertible mod } n_2. \end{cases}$$

Composite Modulus

Theorem (Chineese Remaider Theorem)

If $n = n_1 n_2$ with $\gcd(n_1, n_2) = 1$, then the rings $\mathbb{Z}_n$ and $\mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2}$ are isomorphic, with the map $x \mapsto (x \mod n_1, x \mod n_2)$.

$$x \text{ invertible mod } n \quad \Leftrightarrow \quad \begin{cases} x \text{ invertible mod } n_1, \text{ and} \\ x \text{ invertible mod } n_2. \end{cases}$$

Then, $\phi(n) = \phi(n_1)\phi(n_2)$.

Composite Modulus

Theorem (Chineese Remaider Theorem)

If $n = n_1 n_2$ with $\gcd(n_1, n_2) = 1$, then the rings $\mathbb{Z}_n$ and $\mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2}$ are isomorphic, with the map $x \mapsto (x \mod n_1, x \mod n_2)$.

$$x \text{ invertible mod } n \quad \Leftrightarrow \quad \begin{cases} x \text{ invertible mod } n_1, \text{ and} \\ x \text{ invertible mod } n_2. \end{cases}$$

Then, $\phi(n) = \phi(n_1)\phi(n_2)$.

x can be recovered from $x_1 = x \mod n_1$ and $x_2 = x \mod n_2$:

$x = \lambda_1 x_1 + \lambda_2 x_2$, where $\lambda_i \mod n_j$ is 1 if $i = j$, and 0 otherwise.

Square Modulus

For every $x \in \mathbb{Z}_{n^2}$, there is a unique representation $x = x_0 + x_1 n$ with $x_0, x_1 \in \{0, \ldots, n-1\}$.

Square Modulus

For every $x \in \mathbb{Z}_{n^2}$, there is a unique representation $x = x_0 + x_1 n$ with $x_0, x_1 \in \{0, \ldots, n-1\}$.

x invertible mod $n^2 \quad \Leftrightarrow \quad x_0$ invertible mod n.

Thus, $\phi(n^2) = n\phi(n)$.

Square Modulus

For every $x \in \mathbb{Z}_{n^2}$, there is a unique representation $x = x_0 + x_1 n$ with $x_0, x_1 \in \{0, \ldots, n-1\}$.

x invertible mod $n^2 \quad \Leftrightarrow \quad x_0$ invertible mod n.

Thus, $\phi(n^2) = n\phi(n)$.

Hensel lifting: The inverse of x mod n^2 is $y = y_0 + y_1 n$, where $y_0 = x_0^{-1} \mod n$ and $y_1 = -y_0 \left(x_1 y_0 + \frac{x0y0-1}{n} \right) \mod n$.

Square Modulus

For every $x \in \mathbb{Z}_{n^2}$, there is a unique representation $x = x_0 + x_1 n$ with $x_0, x_1 \in \{0, \ldots, n-1\}$.

x invertible mod $n^2 \quad \Leftrightarrow \quad x_0$ invertible mod n.

Thus, $\phi(n^2) = n\phi(n)$.

Hensel lifting: The inverse of x mod n^2 is $y = y_0 + y_1 n$, where $y_0 = x_0^{-1} \mod n$ and $y_1 = -y_0 \left(x_1 y_0 + \frac{x0y0-1}{n} \right) \mod n$.

Invertible elements can be written as $x = x_0(1 + \alpha_x n)$, and then:

$$xy = x_0(1 + \alpha_x n) y_0(1 + \alpha_y n) = x_0 y_0 (1 + (\alpha_x + \alpha_y) n) \pmod{n^2}$$

$$x^k = x_0^k (1 + \alpha_x n)^k = x_0^k (1 + k\alpha_x n) \pmod{n^2}$$

Outline

1 Modular Arithmetic

2 Background on Finite Fields

3 Background on Elliptic Curves

Prime Fields

The quotient ring $\mathbb{Z}/n\mathbb{Z}$ is a field if and only n is prime (all nonzero elements have inverses).

We denote it as $GF(n)$ or $\mathbb{F}_n$. It is called a **prime field**.

If n is composite then $\mathbb{Z}/n\mathbb{Z}$ has zero divisors.

If n is prime then Bezout's equality guarantees the existence of all inverses modulo n.

Prime Fields

The quotient ring $\mathbb{Z}/n\mathbb{Z}$ is a field if and only n is prime (all nonzero elements have inverses).

We denote it as $GF(n)$ or $\mathbb{F}_n$. It is called a **prime field**.

If n is composite then $\mathbb{Z}/n\mathbb{Z}$ has zero divisors.

If n is prime then Bezout's equality guarantees the existence of all inverses modulo n.

Then, for a prime n, $\phi(n) = n - 1$.

Prime Fields

The quotient ring $\mathbb{Z}/n\mathbb{Z}$ is a field if and only n is prime (all nonzero elements have inverses).

We denote it as $GF(n)$ or $\mathbb{F}_n$. It is called a **prime field**.

If n is composite then $\mathbb{Z}/n\mathbb{Z}$ has zero divisors.

If n is prime then Bezout's equality guarantees the existence of all inverses modulo n.

Then, for a prime n, $\phi(n) = n - 1$.

Fermat's little theorem implies $x^p = x$ in $\mathbb{F}_p$, i.e., the elements in $\mathbb{F}_p$ are exactly the roots of the polynomial $X^p - X$.

Square Roots

Not every $x \in \mathbb{F}_q$ has a square root (in $\mathbb{F}_q$). Such an x (non-zero) is called a **quadratic residue**.

$QR(q)$ denotes the set of quadratic residues modulo q.

Square Roots

Not every $x \in \mathbb{F}_q$ has a square root (in $\mathbb{F}_q$). Such an x (non-zero) is called a **quadratic residue**.

$QR(q)$ denotes the set of quadratic residues modulo q.

Lemma

$x \in QR(q)$ if and only if $x^{(q-1)/2} = 1$

Square Roots

Not every $x \in \mathbb{F}_q$ has a square root (in $\mathbb{F}_q$). Such an x (non-zero) is called a **quadratic residue**.

$QR(q)$ denotes the set of quadratic residues modulo q.

Lemma

$x \in QR(q)$ if and only if $x^{(q-1)/2} = 1$

If $q = 3 \pmod 4$, then the two square roots of $x \in QR(q)$ can be computed as $\text{SQRT}(x) = \pm x^{(q+1)/4}$

Square Roots

Not every $x \in \mathbb{F}_q$ has a square root (in $\mathbb{F}_q$). Such an x (non-zero) is called a **quadratic residue**.

$QR(q)$ denotes the set of quadratic residues modulo q.

Lemma

$x \in QR(q)$ if and only if $x^{(q-1)/2} = 1$

If $q = 3 \pmod 4$, then the two square roots of $x \in QR(q)$ can be computed as $\text{SQRT}(x) = \pm x^{(q+1)/4}$

If $q = 1 \pmod 4$, there exist some probabilistic algorithms that compute square roots.

Subfields

The **characteristic** of a field $\mathbb{K}$, char($\mathbb{K}$), is the minimum positive integer p such that $p1_{\mathbb{K}} = 0_{\mathbb{K}}$.
char($\mathbb{K}$) $= 0$, if no such p exists.

p is always prime. (Otherwise, $\mathbb{K}$ would have zero divisors.)

Subfields

The **characteristic** of a field $\mathbb{K}$, $\mathrm{char}(\mathbb{K})$, is the minimum positive integer p such that $p1_{\mathbb{K}} = 0_{\mathbb{K}}$.
$\mathrm{char}(\mathbb{K}) = 0$, if no such p exists.

p is always prime. (Otherwise, $\mathbb{K}$ would have zero divisors.)

$\mathbb{F}_p$ is always a subfield of any finite field $\mathbb{K}$ with $\mathrm{char}(\mathbb{K}) = p$. Therefore, $\mathbb{K}$ is a $\mathbb{F}_p$-vector space, and it has cardinality $q = p^e$ for some $e \geq 1$.

Then any finite field is a finite **extension** of a prime field.

Subfields

The **characteristic** of a field $\mathbb{K}$, $\mathrm{char}(\mathbb{K})$, is the minimum positive integer p such that $p1_{\mathbb{K}} = 0_{\mathbb{K}}$.
$\mathrm{char}(\mathbb{K}) = 0$, if no such p exists.

p is always prime. (Otherwise, $\mathbb{K}$ would have zero divisors.)

$\mathbb{F}_p$ is always a subfield of any finite field $\mathbb{K}$ with $\mathrm{char}(\mathbb{K}) = p$. Therefore, $\mathbb{K}$ is a $\mathbb{F}_p$-vector space, and it has cardinality $q = p^e$ for some $e \geq 1$.

Then any finite field is a finite **extension** of a prime field.

If $\mathbb{K}'$ is a subfield of a finite field $\mathbb{K}$, then $\mathbb{K}$ is a $\mathbb{K}'$-vector space. If $\mathbb{K}$ has $q = p^e$ elements, then $\mathbb{K}'$ has $q' = p^d$ elements for some $d \mid e$.

Subfields

The **characteristic** of a field $\mathbb{K}$, $\mathrm{char}(\mathbb{K})$, is the minimum positive integer p such that $p1_{\mathbb{K}} = 0_{\mathbb{K}}$.
$\mathrm{char}(\mathbb{K}) = 0$, if no such p exists.

p is always prime. (Otherwise, $\mathbb{K}$ would have zero divisors.)

$\mathbb{F}_p$ is always a subfield of any finite field $\mathbb{K}$ with $\mathrm{char}(\mathbb{K}) = p$. Therefore, $\mathbb{K}$ is a $\mathbb{F}_p$-vector space, and it has cardinality $q = p^e$ for some $e \geq 1$.

Then any finite field is a finite **extension** of a prime field.

If $\mathbb{K}'$ is a subfield of a finite field $\mathbb{K}$, then $\mathbb{K}$ is a $\mathbb{K}'$-vector space. If $\mathbb{K}$ has $q = p^e$ elements, then $\mathbb{K}'$ has $q' = p^d$ elements for some $d \mid e$.

E.g., a field with 2^{15} elements can only have proper subfields of cardinalities 2, 2^3 and 2^5.

Primitive Elements

Theorem

For any finite field $\mathbb{K}$, the multiplicative group $\mathbb{K}^\times$ is cyclic.

Primitive Elements

Theorem

For any finite field $\mathbb{K}$, the multiplicative group $\mathbb{K}^\times$ is cyclic.

Assume $\mathbb{K}$ has p^e elements. Since $\mathbb{K}^\times$ is an abelian finite group, it is the direct product of r cycles of lengths $l_1, l_2 \ldots, l_r$ fulfilling $l_1 \mid l_2 \mid \cdots \mid l_r$.
But the order of the group is $p^e - 1 = l_1 l_2 \cdots l_r$, and all $x \in \mathbb{K}^\times$ fulfils $x^{l_r} = 1$.
Therefore, the polynomial $X^{l_r} - 1 \in \mathbb{K}[X]$ has at least $p^e - 1$ roots, which is only possible if $l_r \geq p^e - 1$, and then $r = 1$.

Primitive Elements

Theorem

For any finite field $\mathbb{K}$, the multiplicative group $\mathbb{K}^\times$ is cyclic.

Assume $\mathbb{K}$ has p^e elements. Since $\mathbb{K}^\times$ is an abelian finite group, it is the direct product of r cycles of lengths $l_1, l_2 \ldots, l_r$ fulfilling $l_1 \mid l_2 \mid \cdots \mid l_r$.
But the order of the group is $p^e - 1 = l_1 l_2 \cdots l_r$, and all $x \in \mathbb{K}^\times$ fulfils $x^{l_r} = 1$.
Therefore, the polynomial $X^{l_r} - 1 \in \mathbb{K}[X]$ has at least $p^e - 1$ roots, which is only possible if $l_r \geq p^e - 1$, and then $r = 1$.

Every generator α of $\mathbb{K}^\times$ is called a **primitive** element.

Primitive Elements

Theorem

For any finite field $\mathbb{K}$, the multiplicative group $\mathbb{K}^\times$ is cyclic.

Assume $\mathbb{K}$ has p^e elements. Since $\mathbb{K}^\times$ is an abelian finite group, it is the direct product of r cycles of lengths $l_1, l_2 \ldots, l_r$ fulfilling $l_1 \mid l_2 \mid \cdots \mid l_r$.
But the order of the group is $p^e - 1 = l_1 l_2 \cdots l_r$, and all $x \in \mathbb{K}^\times$ fulfils $x^{l_r} = 1$.
Therefore, the polynomial $X^{l_r} - 1 \in \mathbb{K}[X]$ has at least $p^e - 1$ roots, which is only possible if $l_r \geq p^e - 1$, and then $r = 1$.

Every generator α of $\mathbb{K}^\times$ is called a **primitive** element.

In particular, we can write $\mathbb{K} = \{0, 1 = \alpha^0, \alpha^1, \ldots, \alpha^{p^e-2}\}$

Irreducible Polynomials

Lemma

A polynomial $g \in \mathbb{F}_p[X]$ of degree $e > 0$ is irreducible if and only if $g \mid X^{p^e} - X$, but $g \nmid X^{p^d} - X$ for all nontrivial $d \mid e$.

Irreducible Polynomials

Lemma

A polynomial $g \in \mathbb{F}_p[X]$ of degree $e > 0$ is irreducible if and only if $g \mid X^{p^e} - X$, but $g \nmid X^{p^d} - X$ for all nontrivial $d \mid e$.

Corollary

The irreducible factors of $X^{p^e} - X$ in $\mathbb{F}_p[X]$ are exactly the irreducible polynomials in $\mathbb{F}_p[X]$ of degree dividing e

Irreducible Polynomials

Lemma

A polynomial $g \in \mathbb{F}_p[X]$ of degree $e > 0$ is irreducible if and only if $g \mid X^{p^e} - X$, but $g \nmid X^{p^d} - X$ for all nontrivial $d \mid e$.

Corollary

The irreducible factors of $X^{p^e} - X$ in $\mathbb{F}_p[X]$ are exactly the irreducible polynomials in $\mathbb{F}_p[X]$ of degree dividing e

Let $n_e(p)$ be the no. of irred. polynomials of degree e in $\mathbb{F}_p[X]$.

Corollary

$$\sum_{d|e} d n_d(p) = p^e \quad \text{and} \quad 0 \leq \frac{p^e - 2p^{\lfloor e/2 \rfloor}}{e} < n_e(p) \leq \frac{p^e - p}{e}$$

Construction of Finite Fields

The quotient ring $\mathbb{F}_p[X]/g\mathbb{F}_p[X]$ is a field if and only g is an irreducible polynomial in $\mathbb{F}_p[X]$. If g has degree e, then the field has p^e elements.

Construction of Finite Fields

The quotient ring $\mathbb{F}_p[X]/g\mathbb{F}_p[X]$ is a field if and only g is an irreducible polynomial in $\mathbb{F}_p[X]$. If g has degree e, then the field has p^e elements.

Theorem

For every prime p and for every $e \geq 1$ there exists a unique (up to isomorphism) finite field with p^e elements.

The finite field with p^e elements, denoted as $GF(p^e)$ or $\mathbb{F}_{p^e}$, can always be constructed as the quotient ring $\mathbb{F}_p[X]/g\mathbb{F}_p[X]$, for any irreducible polynomial $g \in \mathbb{F}_p[X]$ of degree e.

Example: $\mathbb{F}_{2^8}$

$\mathbb{F}_2 = \{0, 1\}$

$g = X^8 + X^4 + X^3 + X^2 + 1$ is irreducible in $\mathbb{F}_2[X]$

$\mathbb{F}_{2^8} = \mathbb{F}_2[X]/g\mathbb{F}_2[X]$

Addition:
$(X^7 + X^4 + X) + (X^6 + X^5 + X^4 + 1) = X^7 + X^6 + X^5 + X + 1$

$10010010 + 01110001 = 11100011$

Multiplication: $(X^7 + X^4 + X) * (X^6 + X^5 + X^4 + 1) =$
$X^7 + X + 1 + (X^5 + X^4 + X^3 + X^2 + 1)g$

$10010010 * 01110001 = 10000011$

Example: $\mathbb{F}_{2^8}$

Primitive element: $\alpha = X$ or 00000010

$|\mathbb{F}_{2^8}^{\times}| = 2^8 - 1 = 255 = 3 * 5 * 17$

$\alpha^{255/17} = X^5 + X^2 + X$ or 00100110

$\alpha^{255/5} = X^3 + X$ or 00001010

$\alpha^{255/3} = X^7 + X^6 + X^4 + X^2 + X$ or 11010110

$\alpha^{255} = 1$ or 00000001

Outline

1 Modular Arithmetic

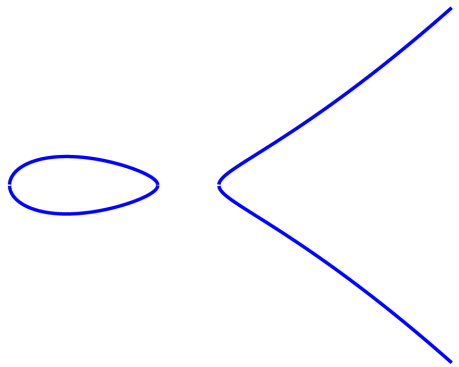
2 Background on Finite Fields

3 Background on Elliptic Curves

Geometric Definition

Elliptic Curve (over a field $\mathbb{K}$ with $\text{char}(\mathbb{K}) \neq 2, 3$)

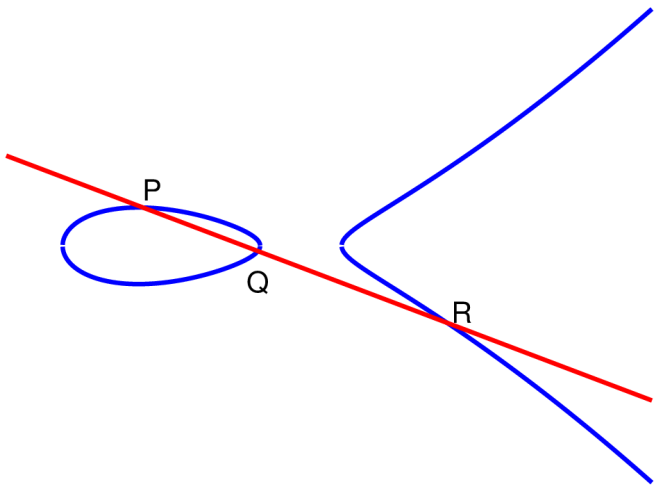
For $a, b \in \mathbb{K}$ such that $\Delta = 27b^2 + 4a^3 \neq 0$,
$E_{a,b}(\mathbb{K}) = \{(x, y) \in \mathbb{K} \times \mathbb{K} \mid y^2 = x^3 + ax + b\} \cup O$
O is the "point at infinity".



Non singularity is given by $\Delta = 27b^2 + 4a^3 \neq 0$.

Group Operation

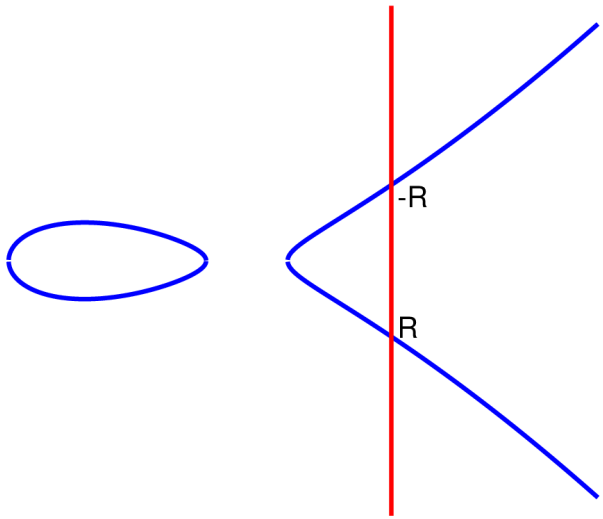
$E_{a,b}(\mathbb{K})$, is a group with the "tangent and chord" geometric operation.



Any line L intersects the elliptic curve at exactly three points (counting multiplicity and the point at the infinity).

Group Operation

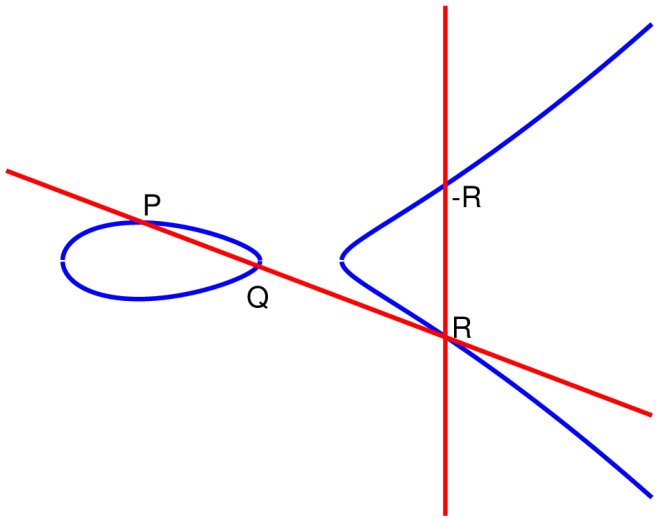
$E_{a,b}(\mathbb{K})$, is a group with the "tangent and chord" geometric operation.



A vertical line intersects the curve at two symmetric points $P = (x, y)$ and $-P = (x, -y)$. The third intersection point is the point at infinity O.

Group Operation

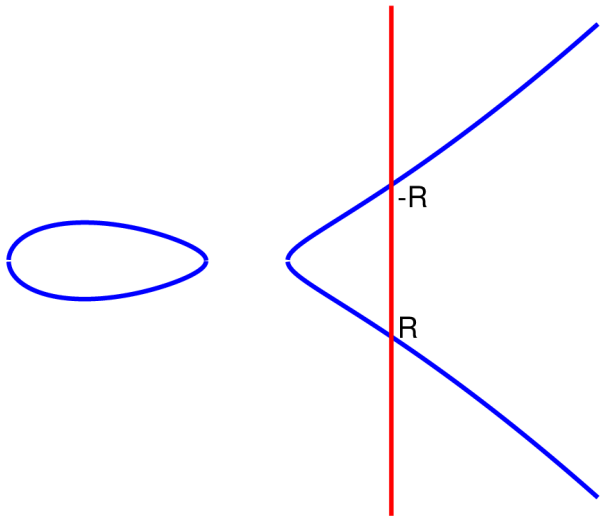
$E_{a,b}(\mathbb{K})$, is a group with the "tangent and chord" geometric operation.



$P + Q = -R$, the symmetric of the third intersection point of the line passing through P and Q.

Group Operation

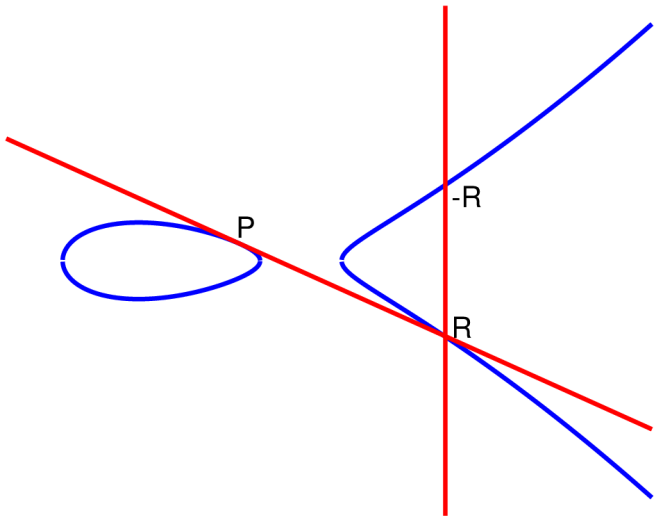
$E_{a,b}(\mathbb{K})$, is a group with the "tangent and chord" geometric operation.



$P + (-P) = O$, the third intersection is the point at infinity.

Group Operation

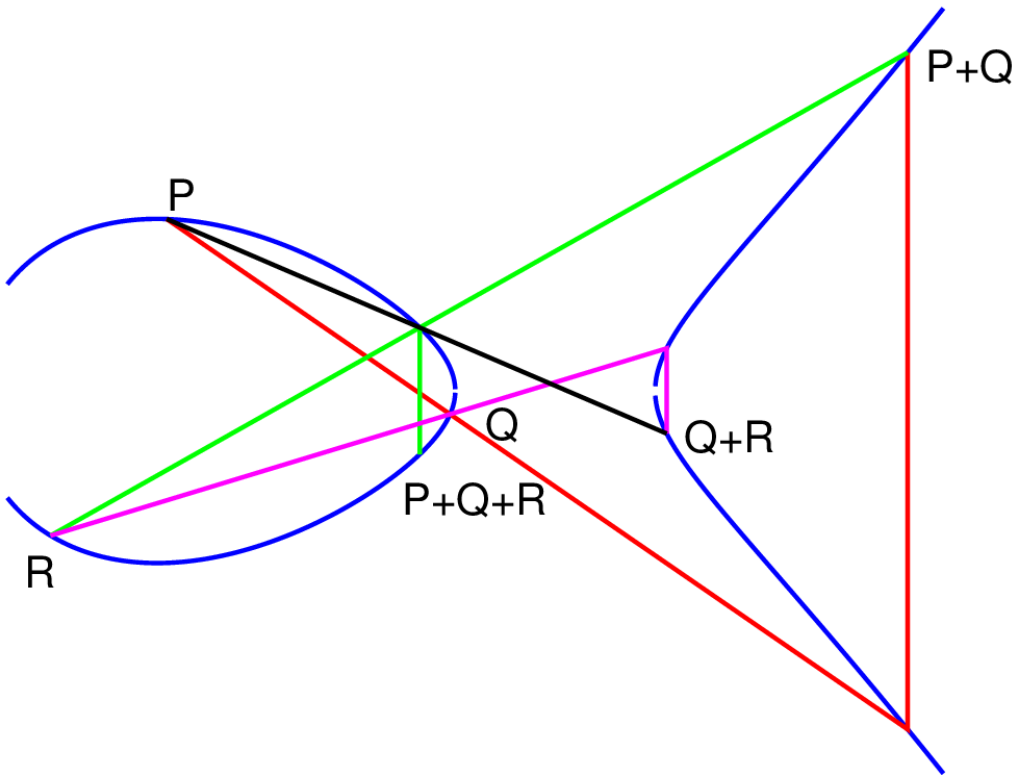
$E_{a,b}(\mathbb{K})$, is a group with the "tangent and chord" geometric operation.



$P + P = 2P = -R$, for the tangent line at P, P counts as a double intersection.

Group Operation

Associativity $(P + Q) + R = P + (Q + R)$ can be proved in different (but not easy) ways.



Group Law Formulas

Case $Q \neq P, -P, O$:

$$x_{P+Q} = \frac{(y_Q - y_P)^2}{(x_Q - x_P)^2} - x_P - x_Q$$

$$y_{P+Q} = -\frac{y_Q - y_P}{x_Q - x_P}(x_{P+Q} - x_P) - y_P$$

Case $Q = P$:

$$x_{2P} = \frac{(3x_P^2 + a)^2}{(2y_P)^2} - 2x_P$$

$$y_{2P} = -\frac{3x_P^2 + a}{2y_P}(x_{2P} - x_P) - y_P$$

$P + (-P) = O$

$P + O = P$

Elliptic Curves in Fields of Characteristic 2 or 3

The curve equation and group law formulas are different that the above when $\text{char}(\mathbb{K}) = 2$ or 3.

For $\text{char}(\mathbb{K}) = 2$: the curve equation is either
$y^2 + xy = x^3 + ax^2 + b$ (with $b \neq 0$) or
$y^2 + ay = x^3 + bx + c$ (with $a \neq 0$).

For $\text{char}(\mathbb{K}) = 3$: the curve equation is either
$y^2 = x^3 + ax^2 + b$ (with $a \neq 0$ and $b \neq 0$) or
$y^2 = x^3 + bx + c$ (with $b \neq 0$).

Scalar Multiples of Points

Similarly to modular exponentiation:

Doubles and additions algorithm:

Let $a = 2^m + a_{m-1}2^{m-1} + \ldots + a_1 2 + a_0$, where $a_0, \ldots, a_{m-1} \in \{0, 1\}$.

Then, $aP = a_0 P + 2(a_1 P + 2(\cdots 2(a_{m-1} P + 2P)\cdots))$.

Example: $11P = (1 + 2 + 2^3)P = P + 2(P + 2(2P))$.

Computing the number of points in $E_{a,b}(\mathbb{F}_q)$ is costly.

Theorem (Hasse)

The number of points of $E_{a,b}(\mathbb{F}_q)$ is an element of the interval $[q+1-2\sqrt{q}, q+1+2\sqrt{q}]$.

Selecting a curve with a suitable number of points is done by:

- Choosing random $a, b \in E_{a,b}(\mathbb{F}_q)$ and running a (costly) point counting algorithm (e.g., Schoof's algorithm).
- Building a curve of a chosen number of points (e.g., complex multiplication method).
- Using a particular subfamily of elliptic curves (e.g., supersingular curves). Less secure, in general!
- **Using a standarized curve**

Example of Standarized Curve

The Certicom secp256k1 Elliptic Curve (used in Bitcoin)

Defined on the prime field of p elements, where
$p = 2^{256} - 2^{32} - 2^9 - 2^8 - 2^7 - 2^4 - 2^4 - 1$.

The elliptic curve is defined by the equation $y^2 = x^3 + 7$

The number of points is a prime
$q = 2^{256} - 432420386565659656852420866394968145599$.

A standarized base point (group generator) is $B = (x_B, y_B)$, where

x_B=55066263022277343669578718895168534326250603453777594175500187 3

y_B=32670510020758816978083085130507043184471273380659243275938904 3

Data Protection

Jorge L. Villar

MCYBERS, UPC, Fall 2025

END