Mathematical Foundations for Modern Cryptography

DAT510: Security and vulnerability in networks

Dept. of Electronic Engineering and Computer Science
University of Stavanger, Norway

The slides is made based on the textbook "*Cryptography and Network Security*", 5th ed
Credits to Lawrie Brown, Steven Gordon and Chunming Rong

Contents

Outline of Mathematical Foundations

- **Symmetric Cryptography**: Finite Fields $GF(2^n)$ for $n = 4, 8, 16, 64, 128$
- **Asymmetric Cryptography**: hard mathematical prob.
  - **RSA**:
    - Enc/Dec: Fermat's and Euler's theorem
    - Security: Integer Factorization
  - **Elgamal Encryption**:
    - Enc/Dec: cyclic group $(\mathbb{Z}_p^*, \cdot)$ for large prime p
    - Security: Discrete Logarithms Prob.
  - **Elliptic Curve Crypto**:
    - Enc/Dec: $(\langle P \rangle, \boxplus)$ for a generating point P on an elliptic curve $y^2 = x^3 + ax + b$ over $GF(p)$ for large prime p
    - Security: Discrete Logarithms Prob.
  - **Diffie-Hellman Key Exchange**:
    - Functionality: a cyclic group (either large prime or EC)
    - Security: Discrete Logarithms Prob.

Contents

Algebra Structure

Algebraic Structure $(S, \circledast)$

A set S with certain arithmetic operations "$\circledast$"

$$\begin{aligned} S \times S &\to S \\ (x_i, x_j) &\mapsto x_i \circledast x_j \end{aligned}$$

satisfying certain laws/conditions.

Algebra Structure - Group

Group $(G, \otimes)$

A set G with an arithmetic operation $\otimes$ on elements in G satisfying the following laws:

- **closure**: $x \otimes y \in G$ for any $x, y \in G$;
- **associative**: $(x \otimes y) \otimes z = x \otimes (y \otimes z)$;
- **identity element**: $\exists\, I \in G$ such that $x \otimes I = I \otimes x = x$;
- **inverse element**: $\exists\, y \in G$ such that $x \otimes y = y \otimes x = I$.

G is a **cyclic group** if $G = < g > = \{I, g, g^2, \cdots, \}$, where g is called a **generator** of G;

Algebra Structure - Group

Group $(G, \otimes)$

A set G with an arithmetic operation $\otimes$ on elements in G satisfying the following laws:

- **closure**: $x \otimes y \in G$ for any $x, y \in G$;
- **associative**: $(x \otimes y) \otimes z = x \otimes (y \otimes z)$;
- **identity element**: $\exists\, I \in G$ such that $x \otimes I = I \otimes x = x$;
- **inverse element**: $\exists\, y \in G$ such that $x \otimes y = y \otimes x = I$.

G is a **cyclic group** if $G =< g >= \{I, g, g^2, \cdots, \}$, where g is called a **generator** of G;

Example (Which is a group?)

- $(\{0, 1, 2, 3\}, +)$, $(\mathbb{N}, +)$, $(\mathbb{Z}, +)$, $(\mathbb{Z}, \times)$;
- $(\mathbb{Q}, +)$, $(\mathbb{Q}, \times)$

Observation: the arithmetic matters!!!

Algebra Structure - Ring

Ring $(R, \otimes, \oplus)$

A set R with two arithmetic operations $\otimes$ and $\oplus$ on elements in G satisfying the following laws:

- $(R, \oplus)$ is a group and $x \oplus y = y \oplus x$ (Abelian Group)
- for multiplication $\otimes$:
  - **closure**: $x \otimes y \in R$;
  - **associative**: $(x \otimes y) \otimes z = x \otimes (y \otimes z)$;
- **distributive**: $x \otimes (y \oplus z) = (x \otimes y) \oplus (x \otimes z)$

Algebra Structure - Ring

Ring $(R, \otimes, \oplus)$

A set R with two arithmetic operations $\otimes$ and $\oplus$ on elements in G satisfying the following laws:

- $(R, \oplus)$ is a group and $x \oplus y = y \oplus x$ (Abelian Group)
- for multiplication $\otimes$:
  - **closure**: $x \otimes y \in R$;
  - **associative**: $(x \otimes y) \otimes z = x \otimes (y \otimes z)$;
- **distributive**: $x \otimes (y \oplus z) = (x \otimes y) \oplus (x \otimes z)$

Example (Rings we have learned)

- Integer Ring $(\mathbb{Z}, +, \times)$;
- $(\mathbb{Z}_n, +, \times)$ where $\mathbb{Z}_n := \{x \mod n : x \in \mathbb{Z}\}$;
- Polynomial Ring $(P, +, \otimes)$ with $P = \{\sum_i a_i x^i : a_i \in \mathbb{Z}\}$;

Algebra Structure - Field

Summary
Finite Fields
Number Theory
Cyclic Group

Ring $(F, \otimes, \oplus)$

A set F with two arithmetic operations $\otimes$ and $\oplus$ on elements in F satisfying the following laws:

- $(R, \oplus)$ is an Abelian group;
- $(R \setminus \{0\}, \otimes)$ is also an Abelian group;
- $x \otimes (y \oplus z) = (x \otimes y) \oplus (x \otimes z)$

Algebra Structure - Field

Ring $(F, \otimes, \oplus)$

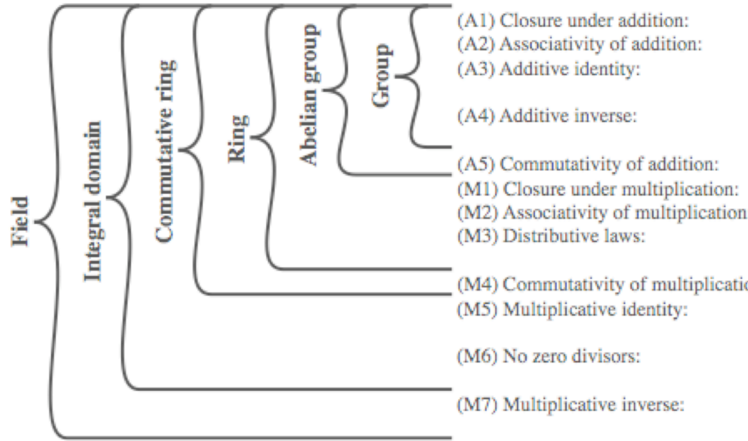
A set F with two arithmetic operations $\otimes$ and $\oplus$ on elements in F satisfying the following laws:

- $(R, \oplus)$ is an Abelian group;
- $(R \setminus \{0\}, \otimes)$ is also an Abelian group;
- $x \otimes (y \oplus z) = (x \otimes y) \oplus (x \otimes z)$

Example

- Is $(\mathbb{Z}, +, \times)$ or $(\mathbb{Z}_n, +, \times)$ a field? No
- Number Fields: $(\mathbb{Q}, +, \times)$, $(\mathbb{R}, +, \times)$, $(\mathbb{C}, +, \times)$; (Infinite number of elements)

Algebra Structure - Group, Ring, Field



Finite Fields $GF(p^n)$

In cryptography, we are only interested in **finite fields**, i.e., fields with finite number of elements.

Existence of Finite Fields

Finite fields exist iff. they contain p^n elements for a prime p.

Construction of Finite Fields

- $n = 1$, $\mathbb{Z}_p = \{0, 1, 2, \cdots, p-1\}$ with $(+, \times)$ is a field;
  - $(\mathbb{Z}_p, +)$ is an abelian group;
  - $(\mathbb{Z}_p, \times)$ is also an abelian group: $\forall\ x \in \mathbb{Z}_p^*$, $\exists\ y \in \mathbb{Z}_p^*$ s.t. $xy \equiv 1 \mod p$ since $(x, p) = 1$
- $GF(p^n)$ is constructed based on $GF(p)$
- The binary case $p = 2$ is of particular interest
  - the addition in $GF(2) = \{0, 1\}$ is the logic XOR

Finite Fields $GF(p^n)$

- Integer Ring $(\mathbb{Z}, +, \times)$
  - prime $p \in \mathbb{Z}$: divisible only by 1 and itself;
  - $a \equiv b \mod p$ iff. $p|(a-b)$
  - The ring $\mathbb{Z}$ modulo a prime p yields $GF(p)$;

Finite Fields $GF(p^n)$

- Integer Ring $(\mathbb{Z}, +, \times)$
  - prime $p \in \mathbb{Z}$: divisible only by 1 and itself;
  - $a \equiv b \mod p$ iff. $p|(a-b)$
  - The ring $\mathbb{Z}$ modulo a prime p yields $GF(p)$;
- Poly. Ring $(\mathbb{Z}_p[x], +, \times)$, $\mathbb{Z}_p[x] = \{\sum_i a_i x^i : a_i \in \mathbb{Z}_p\}$
  - irreducible poly. $f(x)$: "prime" in $\mathbb{Z}_p[x]$;
  - $g_1(x) \equiv g_2(x) \mod f(x)$ iff. $f(x)|(g_1(x) - g_2(x))$
  - The ring $\mathbb{Z}$ modulo an irreducible poly $f(x)$ of degree n yields $GF(p^n)$

Finite Fields $GF(p^n)$

Unique Representation

Let $f(x)$ be an irreducible poly. of degree n in $GF(p)[x]$.

$$GF(p^n) := GF(p)[x] \Big/ f(x) = \left\{ \sum_{i=0}^{n-1} a_i x^i,\ a_i \in GF(p) \right\}$$

- $a(x) \oplus b(x) = \sum_{i=0}^{n-1} (a_i \oplus b_i) x^i = c(x) = \sum_{i=0}^{n-1} c_i x^i$
- $a(x) \otimes b(x) = a(x)b(x) \Big/ f(x) = c(x) = \sum_{i=0}^{n-1} c_i x^i$

$$a(x) = a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \longleftrightarrow a = (a_{n-1}, \cdots, a_1, a_0)$$

- $a \oplus b \leftrightarrow a(x) \oplus b(x) = c(x) \leftrightarrow c = (c_0, \cdots, c_{n-1})$
- $a \otimes b \leftrightarrow a(x) \otimes b(x) = c(x) \leftrightarrow c = (c_0, \cdots, c_{n-1})$

Finite Fields $GF(2^3)$

Table 4.7 Polynomial Arithmetic Modulo $(x^3 + x + 1)$

(a) Addition

		000	001	010	011	100	101	110	111
	$+$	0	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
000	0	0	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
001	1	1	0	$x+1$	x	x^2+1	x^2	x^2+x+1	x^2+x
010	x	x	$x+1$	0	1	x^2+x	x^2+x+1	x^2	x^2+1
011	$x+1$	$x+1$	x	1	0	x^2+x+1	x^2+x	x^2+1	x^2
100	x^2	x^2	x^2+1	x^2+x	x^2+x+1	0	1	x	$x+1$
101	x^2+1	x^2+1	x^2	x^2+x+1	x^2+x	1	0	$x+1$	x
110	x^2+x	x^2+x	x^2+x+1	x^2	x^2+1	x	$x+1$	0	1
111	x^2+x+1	x^2+x+1	x^2+x	x^2+1	x^2	$x+1$	x	1	0

(b) Multiplication

		000	001	010	011	100	101	110	111
	$\times$	0	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
000	0	0	0	0	0	0	0	0	0
001	1	0	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
010	x	0	x	x^2	x^2+x	$x+1$	1	x^2+x+1	x^2+1
011	$x+1$	0	$x+1$	x^2+x	x^2+1	x^2+x+1	x^2	1	x
100	x^2	0	x^2	$x+1$	x^2+x+1	x^2+x	x	x^2+1	1
101	x^2+1	0	x^2+1	1	x^2	x	x^2+x+1	$x+1$	x^2+x
110	x^2+x	0	x^2+x	x^2+x+1	1	x^2+1	$x+1$	x	x^2
111	x^2+x+1	0	x^2+x+1	x^2+1	x	1	x^2+x	x^2	$x+1$

Finite Fields $GF(2^4)$

Let $f(x) = x^4 + x + 1$ be the irreducible polynomial in $GF(2)[x]$ and

$$GF(2^4) = GF(2)[x]\Big/f(x) = \{a_0 + a_1x + a_2x^2 + a_3x^3 \ : \ a_i \in GF(2$$

Calculate the following arithmetic

- $(0, 0, 1, 1) \oplus (1, 1, 0, 1)$; $(1, 0, 1, 0) \oplus (1, 1, 1, 0)$;
- $(1, 0, 0, 1) \otimes (1, 1, 0, 0)$; $(1, 0, 1, 1) \otimes (1, 0, 0, 1)$;

Complete the Addition table and Multiplication table

Contents

Prime Numbers (used everywhere in PKC)

- **Prime Numbers:** only divisible by 1 and itself
- **Prime Factorisation:** $n = p_1^{e_1} p_2^{e_2} \cdots p_t^{e_t}$
- **Greatest Common Divisor (GCD)**: for two integers $n = p_1^{e_1} p_2^{e_2} \cdots p_t^{e_t}$ and $m = p_1^{f_1} p_2^{f_2} \cdots p_t^{f_t}$,

$$\gcd(n, m) = \prod_{i=1}^{t} p_i^{\min(e_i, f_i)}$$

- **Relative Prime:** $\gcd(n, m) = 1$

The Euclidean Algorithm - $\gcd(n, m)$

Calculation of $\gcd(n, m)$ for two integers n, m:

$$
\begin{aligned}
r_0 &= n \\
r_1 &= m \\
&\vdots \\
r_{i+1} &= r_{i-1} - q_i r_i, \ 0 \le r_{i+1} < |r_i| \\
&\vdots \\
r_{k+1} &= r_{k-1} - q_k r_k = 0
\end{aligned}
$$

Fact: $\gcd(r_0, r_1) = \gcd(r_1, r_2) = \cdots = \gcd(r_k, r_{k+1}) = r_k$

E.g.: $\gcd(203, 10) = \gcd(10, 3) = \gcd(3, 1) = \gcd(1, 0) = 1.$

Extended Euclidean Algorithm

Calculation of d, s, t such that $d = \gcd(n, m) = sn + tm$ for two integers n, m,

$$
\begin{array}{rclll}
r_0 & = & n & & s_0 = 1, t_0 = 0 \\
r_1 & = & m & & s_1 = 0, t_1 = 1 \\
 & \vdots & & & \vdots \\
r_{i+1} & = & r_{i-1} - q_i r_i, & & s_{i+1} = s_{i-1} - q_i s_i \\
 & & & & t_{i+1} = t_{i-1} - q_i t_i \\
 & \vdots & & & \vdots \\
r_{k+1} & = & r_{k-1} - q_k r_k = 0 & &
\end{array}
$$

where $0 \leq r_{i+1} < |r_i|$. Then $\boxed{\gcd(n, m) = r_k = s_k n + t_k m}$

E.g.:
$\mathrm{Xgcd}(203, 10) \Rightarrow \gcd(203, 10) = \boxed{1} = \boxed{-3} * 203 + \boxed{61} * 10$

Two Important Theorems (RSA)

Little Fermat's Theorem

For any integer a coprime to a prime p,

$$a^{p-1} \equiv 1 \mod p$$

- $a^{k(p-1)} \equiv 1 \mod p$ for any integer $k \geq 1$
- $a^{k(p-1)+1} \equiv a \mod p$ for any integer a

Two Important Theorems (RSA)

Little Fermat's Theorem

For any integer a coprime to a prime p,

$$a^{p-1} \equiv 1 \mod p$$

- $a^{k(p-1)} \equiv 1 \mod p$ for any integer $k \geq 1$
- $a^{k(p-1)+1} \equiv a \mod p$ for any integer a

Euler's Theorem

For any integer a coprime to an integer n,

$$a^{\phi(n)} \equiv 1 \mod n$$

where $\phi(n) = \#\{x \in \mathbb{Z}_n : \gcd(x, n) = 1\}$.

- $a^{k\phi(n)} \equiv 1 \mod n$ for any integer $k \geq 1$
- If $n = pq$, then $a^{k\phi(n)+1} \equiv a \mod n$ for any integer a

Foundation of RSA Decryption

Theorem

Let $n = pq$. Then for any integers a and $k \geq 1$,

$$a^{k\phi(n)+1} \equiv a \mod n$$

Proof. If $\gcd(a, n) = 1$, it follows from Euler's theorem. If $\gcd(a, n) > 1$, suppose $\gcd(a, n) = p$ and $a = a_1 p$. Then,

$$\begin{aligned} a^{k\phi(n)+1} - a &= a(a^{k\phi(n)} - 1) \\ &= a_1 p(a^{k\phi(n)} - a_1^{k\phi(n)} + a_1^{k\phi(n)} - 1) \\ &= a_1 p[a_1^{k\phi(n)}(p^{k\phi(n)} - 1) + (a_1^{k\phi(n)} - 1)] \end{aligned}$$

By Fermat's Theorem, $q|x^{(q-1)-1}|(x^{\phi(n)} - 1)|(x^{k\phi(n)} - 1)$ for any x coprime to q. Thus $q|(a_1^{k\phi(n)} - 1)$ and $q|(p^{k\phi(n)} - 1)$. Thus, $n = pq|(a^{k\phi(n)+1} - a)$.

Generation of Primes Numbers (in PKC)

Randomly generate a large number and test the primality:

- **Deterministic Test** (Slow)
  - p is a prime $\Leftrightarrow k \not| \, p$ for any $1 \leq k \leq \sqrt{p}$;
  - p is a prime $\Leftrightarrow p|\binom{p}{k}$ for any $1 \leq k < p$
- **Probabilistic Test** (Fast but erroneous)
  - **Fermat's Test:** For any integer $1 \leq a < n$,
    - $a^{n-1} \not\equiv 1 \mod n \Rightarrow n$ is not a prime;
    - $a^{n-1} \equiv 1 \mod n \Rightarrow n$ is probably a prime;
  - **Square-Root test**:
    - $x^2 \equiv 1 \mod n$ while $n \not| \, (x+1)$ and $n \not| \, (x-1)$ $\Rightarrow n$ is not a prime;
    - $x^2 \equiv 1 \mod n$ implies $n|(x \pm 1)$ $\Rightarrow n$ is probably a prime
- **In practice**: multiple probabilistic test (optionally plus a final deterministic test)

Miller-Rabin's Primality Test

- **Conditions**: Let $n-1=2^s d$. For $1 \le a < n$,
  - $a^{n-1} = a^{2^s d} \equiv 1 \mod n$
  - $a^{2^i d} \equiv 1 \mod n$ implies $a^{2^(i-1)d} \equiv \pm 1 \mod n$ for $i = s, s-1, \cdots, 1$
- If n doesn't meet the conditions, n is a composite; Otherwise, n is probably a prime
- **Miller-Rabin's Test**
  1. Randomly choose a with $1 \le a < n$
  2. If $a^{2^s d} \equiv 1 \mod n$ then
     For $i = s-1$ to 0 do,
     If $a^{2^i d} \equiv -1 \mod n$, then
     return " n is probably a prime";
  3. return "n is a composite"
- Error Prob.: $\Pr_e$[a composite n passes test] $< 1/4$
- Repeat Test k times:
  $\Pr_e$[a composite n passes k tests] $< 4^{-k}$

Fast Modular Exponentiation

How to efficiently calculate $x^k \mod n$?

- Example: $3^{65} \mod 31$
  - naive way: compute $3, 3^2, 3^3, \cdots, 3^{65} \mod 31$
  - efficient way: compute $3, 3^2, 3^{2^2}, 3^{2^3}, 3^{2^4}, 3^{2^5}, 3^{2^6}$ mod 31 and then compute $3 \times 3^{2^6} \mod (31)$
  - 64 multiplication vs (6 squares + 1 multiplication)
- **Square-and-Multiply Algorithm**

  $k = k_{t-1}k_{t-2}\cdots k_0$; $f = 1$;
  for $i = t-1$ downto 0 do
  $\quad f = f^2 \mod n$ (Square)
  $\quad$ if $k_i = 1$ then
  $\quad\quad f = x * f \mod n$ (Multiply)
  return f

Fast Modular Exponentiation

Example: compute $3^{65} \mod 21$;
The exponent $65 = 1000001$

k_i	1	0	0	0	0	0	1
square	1	9	18	9	18	9	18
multiply	3	9	18	9	18	9	12

The Chinese Remainder Theorem (CRT)

Chinese Remainder Theroem

Let $n = m_1 m_2 \cdots m_t$. Compute $M_i = n/m_i$ and $c_i = M_i \times (M_i^{-1} \mod m_i)$ for $1 \leq i \leq t$. Then,

$$a \equiv \sum_{i=1}^{t} a_i c_i \mod n \Leftrightarrow \begin{cases} a \equiv a_1 \mod m_1 \\ a \equiv a_2 \mod m_2 \\ \quad \vdots \\ a \equiv a_t \mod m_t \end{cases}$$

How to efficiently calculate $x^k \mod n$ for $n = m_1 m_2 \cdots m_t$?

- direct calculation modular n is slow
- calculations modular m_i is faster

Solution: calculate $x^k \mod m_i$ instead, then apply CRT.

Chinese Remainder Theorem

Example: compute $3^{65} \mod 21$;

- $n = p_1 p_2$ with $(p_1, p_2) = (3, 7)$
- $x_1 : 3^{65} \mod 3 = 0$
- $x_2 : 3^{65} \equiv 3^{65 \mod 6} \equiv 3^5 \equiv 3(3^2)^2 \equiv 3 * 4 \equiv 5 \mod 7$
- $(M_1, M_2) = (7, 3)$
- $(M_1^{-1} \mod 3, M_2^{-1} \mod 7) = (1, 5)$
- $(c_1, c_2) = (7, 15)$
- $3^{65} \equiv a_1 c_1 + a_2 c_2 = 0 + 5 * 15 = 75 \equiv 12 \mod 21$

Chinese Remainder Theorem

Example: compute $3^{65} \mod 21$;

- $n = p_1 p_2$ with $(p_1, p_2) = (3, 7)$
- $x_1 : 3^{65} \mod 3 = 0$
- $x_2 : 3^{65} \equiv 3^{65 \mod 6} \equiv 3^5 \equiv 3(3^2)^2 \equiv 3 * 4 \equiv 5 \mod 7$
- $(M_1, M_2) = (7, 3)$
- $(M_1^{-1} \mod 3, M_2^{-1} \mod 7) = (1, 5)$
- $(c_1, c_2) = (7, 15)$
- $3^{65} \equiv a_1 c_1 + a_2 c_2 = 0 + 5 * 15 = 75 \equiv 12 \mod 21$

Alternatively,

- $M_1^{-1} \mod 3 = 1$ and $h = (x_1 - x_2) * M_1^{-1} \mod 3 = 1$
- $3^{65} \mod p_1 p_2 = x_2 + p_2 * h = 5 + 7 * 1 = 12$

CRT in RSA

RSA algorithm:

- Large primes: (p, q)
- Public key: $n = pq$ and e; Private key (p, q, d)
- Encryption: $c = x^e \mod pq$;
- Decryption: $x = c^d \mod pq$

CRT in RSA decryption: calculate $m \equiv c^d \mod pq$

- $(dP, dQ) := (d \mod p-1, d \mod q-1)$;
- $qInv := q^{-1} \mod p$;
- $x_1 = c^{dP} \mod p$, $x_2 = c^{dQ} \mod q$;
- $h = (x_1 - x_2)qInv \mod p$

Then, $x = x_2 + q * h$ is the desired result since m satisfies

$$\begin{cases} m \equiv m_1 \mod p \\ m \equiv m_2 \mod q \end{cases}$$

Contents

Finite Cyclic Groups in PKC

- A group $(G, \odot)$ with m elements is called *cyclic* if G can be generated by an element, i.e.
  $G = \langle g \rangle = \{1, g, g^2, \cdots, g^{m-1}\}$ with $g^i = \underbrace{g \odot \cdots \odot g}_{i}$.
  g is called a **generator(primitive element)** of G.
- **Basic Fact** If a group G has prime $|G|$, then G is cyclic.
- In PKC we need cyclic groups with such properties:
  - easy to calculate $y = g^x$ for given x and g;
  - it is difficult to compute $x = \mathrm{dlog}_g(y)$ for given y, g;
  - This is so-called *Discrete Logarithms Prob. (DLP)*
- Two cyclic groups used in PKC so far:
  - $\mathbb{Z}_p^* = \{1, 2, \cdots, p-1\}$ for a prime p with $\odot$: multip.;
  - A group of prime number of points (x, y) satisfying

    $$y^2 = x^3 + ax + b \mod p$$

    for a prime p with $\odot$: point addition.

Finite Cyclic Groups in PKC

- A group $(G, \odot)$ with m elements is called *cyclic* if G can be generated by an element, i.e.
  $G = \langle g \rangle = \{1, g, g^2, \cdots, g^{m-1}\}$ with $g^i = \underbrace{g \odot \cdots \odot g}_{i}$.

  g is called a **generator(primitive element)** of G.
- **Basic Fact** If a group G has prime $|G|$, then G is cyclic.
- In PKC we need cyclic groups with such properties:
  - easy to calculate $y = g^x$ for given x and g;
  - it is difficult to compute $x = \mathrm{dlog}_g(y)$ for given y, g;
  - This is so-called *Discrete Logarithms Prob. (DLP)*
- Two cyclic groups used in PKC so far:
  - $\mathbb{Z}_p^* = \{1, 2, \cdots, p-1\}$ for a prime p with $\odot$: multiply;
  - A group of prime number of points (x, y) satisfying

    $$y^2 = x^3 + ax + b \mod p$$

    for a prime p with $\odot$: point addition;

Finite Cyclic Groups in PKC

- A group $(G, \odot)$ with m elements is called *cyclic* if G can be generated by an element, i.e.
  $G = \langle g \rangle = \{1, g, g^2, \cdots, g^{m-1}\}$ with $g^i = \underbrace{g \odot \cdots \odot g}_{i}$.

  g is called a **generator(primitive element)** of G.
- **Basic Fact** If a group G has prime $|G|$, then G is cyclic.
- In PKC we need cyclic groups with such properties:
  - easy to calculate $y = g^x$ for given x and g;
  - it is difficult to compute $x = \mathrm{dlog}_g(y)$ for given y, g;
  - This is so-called *Discrete Logarithms Prob. (DLP)*
- Two cyclic groups used in PKC so far:
  - $\mathbb{Z}_p^* = \{1, 2, \cdots, p-1\}$ for a prime p with $\odot$: multiply;
  - A group of prime number of points (x, y) satisfying

    $$y^2 = x^3 + ax + b \mod p$$

    for a prime p with $\odot$: point addition;

Finite Cyclic Groups in PKC

- A group $(G, \odot)$ with m elements is called *cyclic* if G can be generated by an element, i.e. $G = \langle g \rangle = \{1, g, g^2, \cdots, g^{m-1}\}$ with $g^i = \underbrace{g \odot \cdots \odot g}_{i}$.
  g is called a **generator(primitive element)** of G.
- **Basic Fact** If a group G has prime $|G|$, then G is cyclic.
- In PKC we need cyclic groups with such properties:
  - easy to calculate $y = g^x$ for given x and g;
  - it is difficult to compute $x = \mathrm{dlog}_g(y)$ for given y, g;
  - This is so-called *Discrete Logarithms Prob. (DLP)*
- Two cyclic groups used in PKC so far:
  - $\mathbb{Z}_p^* = \{1, 2, \cdots, p-1\}$ for a prime p with $\odot$: multiply;
  - A group of prime number of points (x, y) satisfying

$$y^2 = x^3 + ax + b \mod p$$

for a prime p with $\odot$: point addition;

The Cyclic Group $\mathbb{Z}_p^*$

Cyclic group $(\mathbb{Z}_p^*, \cdot)$

- $\mathbb{Z}_p^* = \{x \mod p : x \in \mathbb{Z}^*\} = \{1, 2, \cdots, p-1\}$
- $(\mathbb{Z}_p^*, \cdot)$ is cyclic: $\mathbb{Z}_p^* = \langle a \rangle = \{a^i : i = 0, 1, \cdots, p-2\}$

E.g., $\mathbb{Z}_7^* = \{1, 2, 3, 4, 5, 6\}$

$$\begin{array}{rcl}
\langle 2 \rangle & = & \{2^0, 2, 2^2, \mathbf{2^3}, 2^4, 2^5\} = \{1, 2, 4\} \\
\langle 3 \rangle & = & \{3^0, 3, 3^2, 3^3, 3^4, 3^5\} = \{1, 3, 2, 6, 4, 5\} \\
\langle 4 \rangle & = & \{4^0, 4, 4^2, 4^3, 4^4, 4^5\} = \{1, 2, 4\} \\
\langle 5 \rangle & = & \{5^0, 5, 5^2, 5^3, 5^4, 5^5\} = \{1, 5, 4, 6, 2, 3\} \\
\langle 6 \rangle & = & \{6^0, 6, 6^2, 6^3, 6^4, 6^5\} = \{1, 6\}
\end{array}$$

Thus, $\mathbb{Z}_7^*$ is a cyclic group with generators 3 and 5.

- any $b \in \mathbb{Z}_7^*$ can be written as $b \equiv 3^i \mod 7$ for some i;
- denote the integer i as $i = \text{dlog}_{3,7}(b)$

Discrete Logarithm Problem (DLP)

For a prime p with generator a, calculate $\text{dlog}_{a,p}(y)$ for y.

The Cyclic Group from Elliptic Curve

Cyclic group $\langle P, \boxplus \rangle$, where $P = (x, y)$ is a base point on the elliptic curve

$$E_p(a, b) := y^2 = x^3 + ax + b \mod p,$$

where $4a^3 + 27b^2 \not\equiv 0 \mod p$.

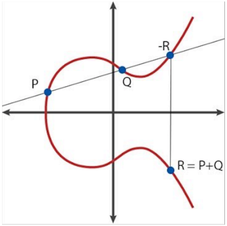
Point Addition $\boxplus$ in EC

For all points P, Q on $E_p(a, b)$,

- $P \boxplus O = P$;
- If $P = (x_p, y_p)$, then $P \boxplus (x_p, -y_p) = O$. Denote $(x_p, -y_p)$ as $-P$;
- For P and Q with $Q \neq -P$, $P + Q = R = (x_r, y_r)$ with
$$\begin{cases} x_r = (k^2 - x_p - x_q) \mod p \\ y_r = (k(x_p - x_r) - y_p) \mod p \end{cases},$$
where $k = \begin{cases} (y_q - y_p)/(x_q - x_p) \mod p, & \text{if } P \neq Q \\ (3x_p^2 + a)/(2y_p) \mod p, & \text{if } P = Q \end{cases}$

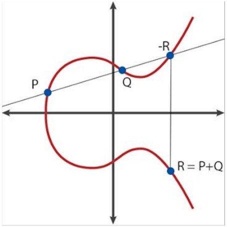
The Cyclic Group from Elliptic Curve

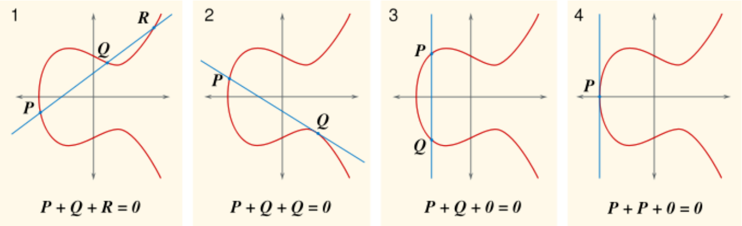
"Strange" Points Addition $\boxplus$ in EC in geometry:



The Cyclic Group from Elliptic Curve

“Strange” Points Addition $\boxplus$ in EC in geometry:



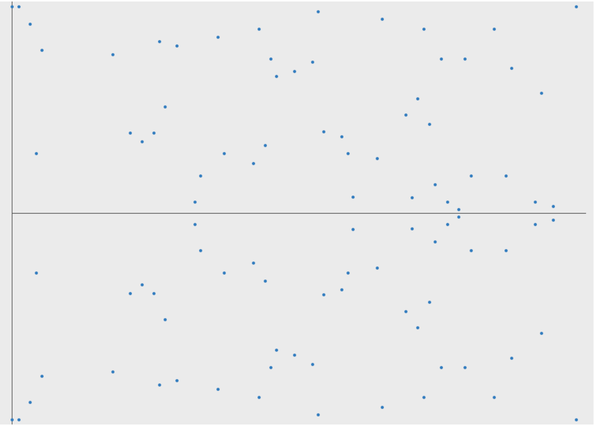


The addition process repeated...

The Cyclic Group from Elliptic Curve

More about the points on $E_p(a, b)$ over $GF(p)$:

- finite number of points (x, y) on $E_p(a, b)$



- point addition modulo p

The Cyclic Group from Elliptic Curve

Generation of a cyclic group $\langle P \rangle$ with point addition $\boxplus$

- Starting from one point P, we get

$$E = \{P, 2P, 3P, \cdots, (m-1)P\} mP = O\}$$

- E is a group with $\boxplus$
- If $|E|$ is a prime, we get a cyclic group

EC-based DLP

Given a cyclic group $E = \langle P \rangle$ with point addition, find x such that

$$xP = Q$$

for a given point Q on $E_p(a, b)$.

Complexity of PKC algorithms

Integer Factorisation

- Given $n = pq$ with unknown primes p, q, find p and q
- Largest RSA number factored into two primes is 768 bits (232 decimal digits)

Euler's Totient

- Given composite n, find $\phi(n)$
- Harder than integer factorisation

Discrete Logarithms

- $\mathbb{Z}_p^*$: calculate $\mathrm{dlog}_{a,p}(b)$;
- EC cyclic group $\langle P \rangle$: find x satisfying $xP = Q$;
- best alg. has complexity in order of $e^{(\ln p)^{1/3}(\ln(\ln p)^{2/3})}$
- Comparable to integer factorisation