

Introduction to Number Theory

This slide is made based the online course of Cryptography by Dan Boneh

Notation

From here on:

- N denotes a positive integer.
- p denote a prime.

Notation: $Z_N = \{0, 1, 2, \dots, N - 1\}$

Can do addition and multiplication modulo N

Modular arithmetic

Examples: let $N = 12$

$$9 + 8 = 5 \quad \text{in } \mathbb{Z}_{12}$$

$$5 \times 7 = 11 \quad \text{in } \mathbb{Z}_{12}$$

$$5 - 7 = 10 \quad \text{in } \mathbb{Z}_{12}$$

Arithmetic in \mathbb{Z}_N works as you expect, e.g. $x \cdot (y+z) = x \cdot y + x \cdot z$ in \mathbb{Z}_N

Greatest common divisor

Def: For ints. x, y : $\text{gcd}(x, y)$ is the greatest common divisor of x, y

Example: $\text{gcd}(12, 18) = 6$ $\boxed{2} \times 12 - \boxed{1} \times 18 = 6$

Fact: for all ints. x, y there exist ints. a, b such that

$$a \cdot x + b \cdot y = \text{gcd}(x, y)$$

a, b can be found efficiently using the extended Euclid alg.

If $\text{gcd}(x, y) = 1$ we say that x and y are relatively prime

Modular inversion

Over the rationals, inverse of 2 is $\frac{1}{2}$. What about \mathbb{Z}_N ?

Def: The **inverse** of x in \mathbb{Z}_N is an element y in \mathbb{Z}_N s.t. $x \cdot y = 1$ in \mathbb{Z}_N

y is denoted x^{-1} .

Example: let N be an odd integer. The inverse of 2 in \mathbb{Z}_N is

$$\frac{N+1}{2},$$
$$2 \cdot \left(\frac{N+1}{2} \right) = N+1 = 1$$

Modular inversion

Which elements have an inverse in \mathbb{Z}_N ?

Lemma: x in \mathbb{Z}_N has an inverse if and only if $\gcd(x, N) = 1$

Proof:

$$\begin{aligned}\gcd(x, N) = 1 &\Rightarrow \exists a, b: a \cdot x + b \cdot N = 1 \Rightarrow a \cdot x = 1 \text{ in } \mathbb{Z}_N \\ &\Rightarrow x^{-1} = a \text{ in } \mathbb{Z}_N\end{aligned}$$

x in \mathbb{Z}_N has an inverse \Rightarrow gives us a number y s.t. $xy \equiv 1 \pmod{n}$.

It means that $xy = kn + 1$, or $xy - kn = 1$.

For any common divisor, c , of x and n we have $c \mid (xy - kn)$ which gives $c \mid 1$, that is, $c = 1$.

More notation

Def: $\mathbb{Z}_N^* = (\text{set of invertible elements in } \mathbb{Z}_N) =$
 $= \{ x \in \mathbb{Z}_N : \gcd(x, N) = 1 \}$

Examples:

1. for prime p , $\mathbb{Z}_p^* = \mathbb{Z}_p \setminus \{0\} = \{1, 2, \dots, p-1\}$
2. $\mathbb{Z}_{12}^* = \{1, 5, 7, 11\}$

For x in \mathbb{Z}_N^* , can find x^{-1} using extended Euclid algorithm.

Solving modular linear equations

Solve: $\mathbf{a \cdot x + b = 0}$ in \mathbb{Z}_N

Solution: $\mathbf{x = -b \cdot a^{-1}}$ in \mathbb{Z}_N

Find a^{-1} in \mathbb{Z}_N using extended Euclid. Run time: $O(\log^2 N)$

What about modular quadratic equations?

next segments

End of Segment

Intro. Number Theory

Fermat and Euler

Review

N denotes an n -bit positive integer. p denotes a prime.

- $Z_N = \{ 0, 1, \dots, N-1 \}$
- $(Z_N)^* = (\text{set of invertible elements in } Z_N) =$
 $= \{ x \in Z_N : \gcd(x, N) = 1 \}$

Can find inverses efficiently using Euclid alg.: time = $O(n^2)$

Fermat's theorem (1640)

Thm: Let p be a prime

$$\forall x \in (\mathbb{Z}_p)^* : x^{p-1} = 1 \text{ in } \mathbb{Z}_p$$

Example: $p=5$. $3^4 = 81 = 1 \text{ in } \mathbb{Z}_5$

So: $x \in (\mathbb{Z}_p)^* \Rightarrow x \cdot x^{p-2} = 1 \Rightarrow x^{-1} = x^{p-2} \text{ in } \mathbb{Z}_p$

another way to compute inverses, but less efficient than Euclid

Application: generating random primes

Suppose we want to generate a large random prime

say, prime p of length 1024 bits (i.e. $p \approx 2^{1024}$)

Step 1: choose a random integer $p \in [2^{1024} , 2^{1025}-1]$

Step 2: test if $2^{p-1} = 1$ in Z_p

If so, output p and stop. If not, goto step 1 .

Simple algorithm (not the best). **$\Pr[p \text{ not prime }] < 2^{-60}$**

The structure of $(\mathbb{Z}_p)^*$

Thm (Euler): $(\mathbb{Z}_p)^*$ is a **cyclic group**, that is

$$\exists g \in (\mathbb{Z}_p)^* \text{ such that } \{1, g, g^2, g^3, \dots, g^{p-2}\} = (\mathbb{Z}_p)^*$$

g is called a **generator** of $(\mathbb{Z}_p)^*$

Example: $p=7$, please give a generator

The structure of $(\mathbb{Z}_p)^*$

Thm (Euler): $(\mathbb{Z}_p)^*$ is a **cyclic group**, that is

$$\exists g \in (\mathbb{Z}_p)^* \text{ such that } \{1, g, g^2, g^3, \dots, g^{p-2}\} = (\mathbb{Z}_p)^*$$

g is called a **generator** of $(\mathbb{Z}_p)^*$

Example: $p=7$. $\{1, 3, 3^2, 3^3, 3^4, 3^5\} = \{1, 3, 2, 6, 4, 5\} = (\mathbb{Z}_7)^*$

Not every elem. is a generator: $\{1, 2, 2^2, 2^3, 2^4, 2^5\} = \{1, 2, 4\}$

Order

For $g \in (Z_p)^*$ the set $\{1, g, g^2, g^3, \dots\}$ is called
the **group generated by g** , denoted $\langle g \rangle$

Def: the **order** of $g \in (Z_p)^*$ is the size of $\langle g \rangle$

$$\text{ord}_p(g) = |\langle g \rangle| = (\text{smallest } a > 0 \text{ s.t. } g^a = 1 \text{ in } Z_p)$$

Examples: $\text{ord}_7(3) = ?$; $\text{ord}_7(2) = ?$; $\text{ord}_7(1) = ?$

Thm (Lagrange): $\forall g \in (Z_p)^* : \text{ord}_p(g) \text{ divides } p-1$

Euler's generalization of Fermat (1736)

Def: For an integer N define $\varphi(N) = |(Z_N)^*|$ (Euler's φ func.)

Examples: $\varphi(12) = |\{1,5,7,11\}| = 4$; $\varphi(p) = p-1$

For $N=p \cdot q$: $\varphi(N) = N-p-q+1 = (p-1)(q-1)$

Thm (Euler): $\forall x \in (Z_N)^* : x^{\varphi(N)} = 1 \text{ in } Z_N$

Example: $5^{\varphi(12)} = ? \text{ in } Z_{12}$

Generalization of Fermat. Basis of the RSA cryptosystem

GROUP

A set of elements and a binary operation \cdot on that set, satisfying some properties.

Group $G = \{G, \cdot\}$ where

1. Closure: $(a \cdot b) \in G, \forall a, b \in G$
2. Associativity: $a \cdot (b \cdot c) = (a \cdot b) \cdot c, \forall a, b, c \in G$
3. Identity: $\exists e \in G: a \cdot e = e \cdot a = a, \forall a \in G$
4. Inverses: $\forall a \in G, \exists a^{-1} \in G: a \cdot a^{-1} = a^{-1} \cdot a = e$
5. Commutativity: $\forall a, b \in G, a \cdot b = b \cdot a$ (Abelian Group)

End of Segment

Intro. Number Theory

Modular e 'th roots

Modular e'th roots

We know how to solve modular linear equations:

$$\mathbf{a \cdot x + b = 0} \quad \text{in } \mathbb{Z}_N \qquad \text{Solution: } \mathbf{x = -b \cdot a^{-1}} \quad \text{in } \mathbb{Z}_N$$

What about higher degree polynomials?

Example: let p be a prime and $c \in \mathbb{Z}_p$. Can we solve:

$$x^2 - c = 0 \quad , \quad y^3 - c = 0 \quad , \quad z^{37} - c = 0 \quad \text{in } \mathbb{Z}_p$$

Modular e'th roots

Let p be a prime and $c \in \mathbb{Z}_p$.

Def: $x \in \mathbb{Z}_p$ s.t. $x^e = c$ in \mathbb{Z}_p is called an **e'th root** of c .

Examples: $7^{1/3} = 6$ in \mathbb{Z}_{11}

$$3^{1/2} = 5 \text{ in } \mathbb{Z}_{11}$$

$$1^{1/3} = 1 \text{ in } \mathbb{Z}_{11}$$

$$6^3 = 216 = 7 \text{ in } \mathbb{Z}_{11}$$

$$2^{1/2} \text{ ?}$$

The easy case

When does $c^{1/e}$ in \mathbb{Z}_p exist? Can we compute it efficiently?

The easy case: suppose $\gcd(e, p-1) = 1$

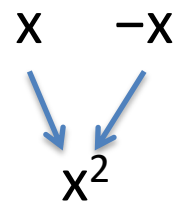
Then for all c in $(\mathbb{Z}_p)^*$: $c^{1/e}$ exists in \mathbb{Z}_p and is easy to find.

Proof: let $d = e^{-1}$ in \mathbb{Z}_{p-1} . Then $c^{1/e} = c^d$ in \mathbb{Z}_p

$$\begin{aligned} d \cdot e = 1 \text{ in } \mathbb{Z}_{p-1} &\Rightarrow \exists k \in \mathbb{Z}: d \cdot e = k \cdot (p-1) + 1 \Rightarrow (c^d)^e = c^{de} = \\ c^{k(p-1)+1} &= (c^{p-1})^k \cdot c = c \text{ in } \mathbb{Z}_p \end{aligned}$$

The case $e=2$: square roots

If p is an odd prime then $\gcd(2, p-1) \neq 1$



Fact: in \mathbb{Z}_p^* , $x \rightarrow x^2$ is a 2-to-1 function

Example: in \mathbb{Z}_{11}^* :

1	10	2	9	3	8	4	7	5	6
↙	↘	↙	↘	↙	↘	↙	↘	↙	↘
1		4		9		5		3	

Def: x in \mathbb{Z}_p is a **quadratic residue** (Q.R.) if it has a square root in \mathbb{Z}_p

p odd prime \Rightarrow the # of Q.R. in \mathbb{Z}_p is $(p-1)/2 + 1$

Euler's theorem

Thm: x in $(\mathbb{Z}_p)^*$ is a Q.R. $\iff x^{(p-1)/2} = 1$ in \mathbb{Z}_p (p odd prime)

Example:

$$\begin{array}{rcccccccccc} \text{in } \mathbb{Z}_{11} : & 1^5 & 2^5 & 3^5 & 4^5 & 5^5 & 6^5 & 7^5 & 8^5 & 9^5 & 10^5 \\ & = & 1 & -1 & 1 & 1 & 1 & -1 & -1 & -1 & 1 & -1 \end{array}$$

Note: $x \neq 0 \Rightarrow x^{(p-1)/2} = (x^{p-1})^{1/2} = 1^{1/2} \in \{1, -1\}$ in \mathbb{Z}_p

Def: $x^{(p-1)/2}$ is called the **Legendre Symbol** of x over p (1798)

Computing square roots mod p

Suppose $p \equiv 3 \pmod{4}$

Lemma: if $c \in (\mathbb{Z}_p)^*$ is Q.R. then $\sqrt{c} = c^{(p+1)/4}$ in \mathbb{Z}_p

Proof: $(c^{(p+1)/4})^2 = c^{(p+1)/2} = c^{(p-1)/2} \cdot c = c$ in \mathbb{Z}_p

When $p \equiv 1 \pmod{4}$, can also be done efficiently, but a bit harder

run time $\approx O(\log^3 p)$

Solving quadratic equations mod p

Solve: $a \cdot x^2 + b \cdot x + c = 0$ in Z_p

Solution: $x = (-b \pm \sqrt{b^2 - 4 \cdot a \cdot c}) / 2a$ in Z_p

- Find $(2a)^{-1}$ in Z_p using extended Euclid.
- Find square root of $b^2 - 4 \cdot a \cdot c$ in Z_p (if one exists)
using a square root algorithm

Computing e 'th roots mod N ??

Let N be a composite number and $e > 1$

When does $c^{1/e}$ in \mathbb{Z}_N exist? Can we compute it efficiently?

Answering these questions requires the factorization of N
(as far as we know)

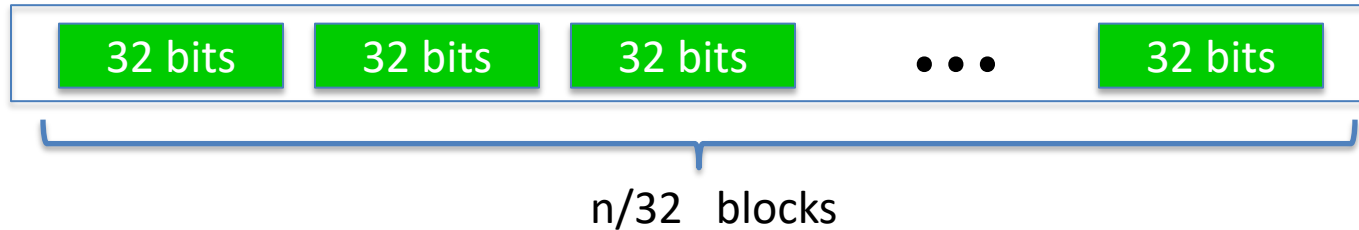
End of Segment

Intro. Number Theory

Arithmetic algorithms

Representing bignums

Representing an n -bit integer (e.g. $n=2048$) on a 64-bit machine



Note: some processors have 128-bit registers (or more) and support multiplication on them

Arithmetic

Given: two n -bit integers

- **Addition and subtraction:** linear time $O(n)$
- **Multiplication:** naively $O(n^2)$. Karatsuba (1960): $O(n^{\log_2^3})$

Basic idea: $(2^b x_2 + x_1) \times (2^b y_2 + y_1)$ with 3 mults.

Best (asymptotic) algorithm: about $O(n \cdot \log n)$.

- **Division with remainder:** $O(n^2)$.

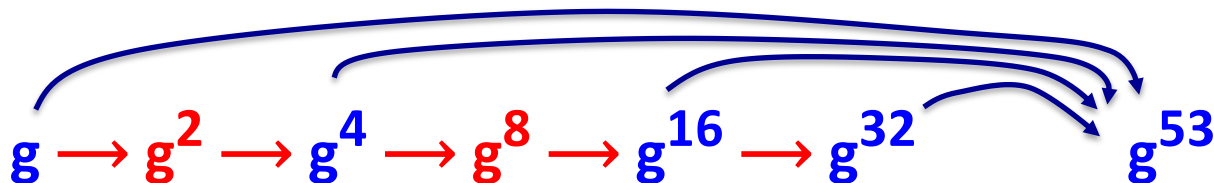
Exponentiation

Finite cyclic group G (for example $G = \mathbb{Z}_p^*$)

Goal: given g in G and x compute g^x

Example: suppose $x = 53 = (110101)_2 = 32+16+4+1$

$$\text{Then: } g^{53} = g^{32+16+4+1} = g^{32} \cdot g^{16} \cdot g^4 \cdot g^1$$



The repeated squaring alg.

Input: g in G and $x > 0$; **Output:** g^x

write $x = (x_n x_{n-1} \dots x_2 x_1 x_0)_2$

$y \leftarrow g$, $z \leftarrow 1$

for $i = 0$ to n do:

if $(x[i] == 1)$: $z \leftarrow z \cdot y$

$y \leftarrow y^2$

output z

example: g^{53}

<u>y</u>	<u>z</u>
g^2	g
g^4	g
g^8	g^5
g^{16}	g^5
g^{32}	g^{21}
g^{64}	g^{53}

Running times

Given n -bit int. N :

- **Addition and subtraction in \mathbb{Z}_N :** linear time $T_+ = O(n)$
- **Modular multiplication in \mathbb{Z}_N :** naively $T_x = O(n^2)$
- **Modular exponentiation in \mathbb{Z}_N (g^x):**

$$O((\log x) \cdot T_x) \leq O((\log x) \cdot n^2) \leq O(n^3)$$

End of Segment

Intro. Number Theory

Intractable problems

Easy problems

- Given composite N and x in Z_N find x^{-1} in Z_N
- Given prime p and polynomial $f(x)$ in $Z_p[x]$
find x in Z_p s.t. $f(x) = 0$ in Z_p (if one exists)

Running time is linear in $\deg(f)$.

... but many problems are difficult

Intractable problems with primes

Fix a prime $p > 2$ and g in $(\mathbb{Z}_p)^*$ of order q .

Consider the function: $x \mapsto g^x$ in \mathbb{Z}_p

Now, consider the inverse function:

$$\text{Dlog}_g(g^x) = x \quad \text{where } x \text{ in } \{0, \dots, q-2\}$$

Example:

in \mathbb{Z}_{11} :	1,	2,	3,	4,	5,	6,	7,	8,	9,	10
------------------------	----	----	----	----	----	----	----	----	----	----

$\text{Dlog}_2(\cdot)$:	0,	1,	8,	2,	4,	9,	7,	3,	6,	5
--------------------------	----	----	----	----	----	----	----	----	----	---

DLOG: more generally

Let **G** be a finite cyclic group and **g** a generator of G

$$G = \{ 1, g, g^2, g^3, \dots, g^{q-1} \} \quad (q \text{ is called the order of } G)$$

Def: We say that **DLOG is hard in G** if for all efficient alg. A:

$$\Pr_{g \leftarrow G, x \leftarrow \mathbb{Z}_q} [A(G, q, g, g^x) = x] < \text{negligible}$$

Example candidates:

- (1) $(\mathbb{Z}_p)^*$ for large p , (2) Elliptic curve groups mod p

Computing Dlog in $(\mathbb{Z}_p)^*$ (n-bit prime p)

Best known algorithm (GNFS): run time $\exp(\tilde{O}(\sqrt[3]{n}))$

<u>cipher key size</u>	<u>modulus size</u>	<u>Elliptic Curve group size</u>
80 bits	1024 bits	160 bits
128 bits	3072 bits	256 bits
256 bits (AES)	<u>15360</u> bits	512 bits

As a result: slow transition away from (mod p) to elliptic curves

An application: collision resistance

Choose a group G where Dlog is hard (e.g. $(\mathbb{Z}_p)^*$ for large p)

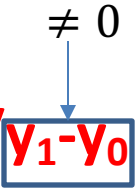
Let $q = |G|$ be a prime. Choose generators g, h of G

For $x, y \in \{1, \dots, q\}$ define $H(x, y) = g^x \cdot h^y$ in G

Lemma: finding collision for $H(.,.)$ is as hard as computing $\text{Dlog}_g(h)$

Proof: Suppose we are given a collision $H(x_0, y_0) = H(x_1, y_1)$

then $g^{x_0} \cdot h^{y_0} = g^{x_1} \cdot h^{y_1} \Rightarrow g^{x_0 - x_1} = h^{y_1 - y_0} \Rightarrow h = g^{x_0 - x_1 / y_1 - y_0}$



Intractable problems with composites

Consider the set of integers: (e.g. for $n=1024$)

$$\mathbb{Z}_{(2)}(n) := \{ N = p \cdot q \text{ where } p, q \text{ are } n\text{-bit primes} \}$$

Problem 1: Factor a random N in $\mathbb{Z}_{(2)}(n)$ (e.g. for $n=1024$)

Problem 2: Given a polynomial $\mathbf{f}(\mathbf{x})$ where $\text{degree}(\mathbf{f}) > 1$
and a random N in $\mathbb{Z}_{(2)}(n)$

find x in \mathbb{Z}_N s.t. $\mathbf{f}(x) = 0$ in \mathbb{Z}_N

The factoring problem

Gauss (1805): *“The problem of distinguishing prime numbers from composite numbers and of resolving the latter into their prime factors is known to be one of the most important and useful in arithmetic.”*

Best known alg. (NFS): run time $\exp(\tilde{O}(\sqrt[3]{n}))$ for n-bit integer

Current world record: **RSA-768** (232 digits)

- Work: two years on hundreds of machines
- Factoring a 1024-bit integer: about 1000 times harder
 \Rightarrow likely possible this decade

Computational Diffie-Hellman Problem (CDH)

Consider a **cyclic group** G of order q . The CDH assumption states that, given

$$(g, g^a, g^b)$$

for a randomly chosen generator g and random

$$a, b \in \{0, \dots, q-1\},$$

it is **computationally intractable** to compute the value

$$g^{ab}.$$

From Wiki: https://en.wikipedia.org/wiki/Computational_Diffie-Hellman_assumption

Decisional Diffie–Hellman Problem (DDH)

Consider a (multiplicative) **cyclic group** G of order q , and with **generator** g . The DDH assumption states that, given g^a and g^b for uniformly and independently chosen $a, b \in \mathbb{Z}_q$, the value g^{ab} "looks like" a random element in G .

This intuitive notion can be formally stated by saying that the following two probability distributions are **computationally indistinguishable** (in the **security parameter**, $n = \log(q)$):

- (g^a, g^b, g^{ab}) , where a and b are randomly and independently chosen from \mathbb{Z}_q .
- (g^a, g^b, g^c) , where a, b, c are randomly and independently chosen from \mathbb{Z}_q .

Triples of the first kind are often called **DDH triplet** or **DDH tuples**.

If CDH is solvable, then DDH can be broken.

From Wiki: https://en.wikipedia.org/wiki/Decisional_Diffie–Hellman_assumption

Further reading

- A Computational Introduction to Number Theory and Algebra, V. Shoup, 2008 (V2), Chapter 1-4, 11, 12

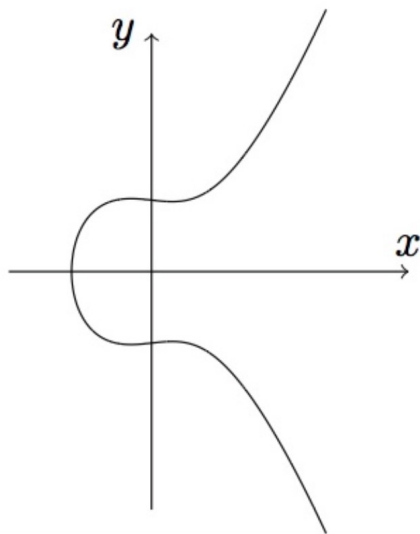
Available at [//shoup.net/ntb/ntb-v2.pdf](http://shoup.net/ntb/ntb-v2.pdf)

End of Segment

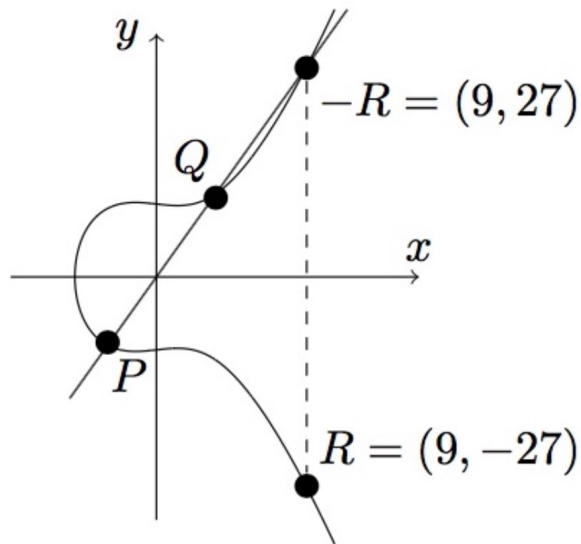
Elliptic curve cryptography

- DL problem on multiplicative group (or subgroup) of integers modulo a sufficiently large prime p is subjected to GNFS attack which runs in time $\exp(\tilde{O}((\log p)^{1/3}))$, thus p should be at least 2048 bits.
- The best DL attack algorithm on addition group built on elliptic curve of size q runs in time $O(\sqrt{q})$.
- As a result, to provide security comparable to AES-128, it is enough for q to be $q \approx 2^{256}$ ($\sqrt{q} = 2^{128}$)
- Much more efficient under the same security level.

The group of points of an elliptic curve



(a) The curve



(b) Adding $P = (-1, -3)$ and $Q = (1, 3)$

The curve $y^2 = x^3 - x + 9$ over the reals

Elliptic curves over finite fields

*Let $p > 3$ be a prime. An **elliptic curve** E defined over \mathbb{F}_p is an equation*

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

where $a, b \in \mathbb{F}_p$ satisfy $4a^3 + 27b^2 \neq 0$.

We write E/\mathbb{F}_p to denote the fact that E is defined over \mathbb{F}_p .

(x_1, y_1) is a point on the curve if it satisfies the curve equation,
and it is defined over the field F_p , or extended field F_{p^e}

Elliptic curves over finite fields

$E(\mathbb{F}_{p^e})$: the set of all points on the curve E defined over \mathbb{F}_{p^e} , including an point at infinity \mathcal{O} .

Example: $E : y^2 = x^3 + 1$ defined over \mathbb{F}_{11}

Enumerate all points on E .

$$E(\mathbb{F}_{11}) = \{\mathcal{O}, (-1, 0), (0, \pm 1), (9, \pm 2), (6, \pm 3), (8, \pm 4), (3, \pm 5)\}$$

Hasse Theorem: The number of points on curve is $|E(\mathbb{F}_{p^e})| = p^e + 1 - t$, $|t| \leq 2\sqrt{p^e}$.

Can be computed efficiently even for large p

Addition Law

let $P = (x_1, y_1)$ and $Q = (x_2, y_2)$ be two points in $E(\mathbb{F}_{p^e})$.


The sum $P \boxplus Q = (x_3, y_3)$ is computed as follows:

- if $x_1 \neq x_2$ we use the chord method. Let $s_c := \frac{y_1 - y_2}{x_1 - x_2}$ be the slope of the chord through the points P and Q . Define

$$x_3 := s_c^2 - x_1 - x_2 \quad \text{and} \quad y_3 := s_c(x_1 - x_3) - y_1.$$

- if $x_1 = x_2$ and $y_1 = y_2$ (i.e., $P = Q$), but $y_1 \neq 0$, we use the tangent method. Let $s_t := \frac{3x_1^2 + a}{2y_1}$ be the slope of the tangent at P . Define

$$x_3 := s_t^2 - 2x_1 \quad \text{and} \quad y_3 := s_t(x_1 - x_3) - y_1.$$

- if $x_1 = x_2$ and $y_1 = -y_2$ then define $P \boxplus Q := \mathcal{O}$.  Identity element, point at infinity

This addition law makes the set $E(\mathbb{F}_{p^e})$ into a group. **Please verify by yourself!**

$$y^2 = x^3 + x + 6 \text{ over GF}(11)$$

x	$x^3 + x + 6 \bmod 11$	QR?	y
0	6		
1	8		
2	5		
3	3		
4	8		
5	4		
6	8		
7	4		
8	9		
9	7		
10	4		

$$y^2 = x^3 + x + 6 \text{ over GF}(11)$$

x	$x^3 + x + 6 \bmod 11$	QR?	y
0	6	No	
1	8	No	
2	5	Yes	4,7
3	3	Yes	5,6
4	8	No	
5	4	Yes	2,9
6	8	No	
7	4	Yes	2,9
8	9	Yes	3,8
9	7	No	
10	4	yes	2,9

The set is the point at infinity and (2,4),(2,7),(3,5),(3,6) (5,2),(5,9),(7,2),(7,9), (8,3), (8,8),(10,2),(10,9).

13 elements. Since the order is prime, every element other than the point at infinity is a generator.

The elliptic curve specifies how elements are added.

Example: Given $E: y^2 = x^3 + 2x + 2 \pmod{17}$ and point $P = (5, 1)$

Goal: Compute $2P = P + P = (5, 1) + (5, 1) = (x_3, y_3)$

■ **Example:** Given $E: y^2 = x^3 + 2x + 2 \pmod{17}$ and point $P = (5, 1)$

Goal: Compute $2P = P + P = (5, 1) + (5, 1) = (x_3, y_3)$

$$s = \frac{3x_1^2 + a}{2y_1} = (2 \cdot 1)^{-1}(3 \cdot 5^2 + 2) = 2^{-1} \cdot 9 \equiv 9 \cdot 9 \equiv 13 \pmod{17}$$

$$x_3 = s^2 - x_1 - x_2 = 13^2 - 5 - 5 = 159 \equiv 6 \pmod{17}$$

$$y_3 = s(x_1 - x_3) - y_1 = 13(5 - 6) - 1 = -14 \equiv 3 \pmod{17}$$

Finally $2P = (5, 1) + (5, 1) = (6, 3)$

■ 椭圆曲线上的点构加上无穷远点成一个循环子群

$$2P = (5,1) + (5,1) = (6,3)$$

$$3P = 2P + P = (10,6)$$

$$4P = (3,1)$$

$$5P = (9,16)$$

$$6P = (16,13)$$

$$7P = (0,6)$$

$$8P = (13,7)$$

$$9P = (7,6)$$

$$10P = (7,11)$$

$$11P = (13,10)$$

$$12P = (0,11)$$

$$13P = (16,4)$$

$$14P = (9,1)$$

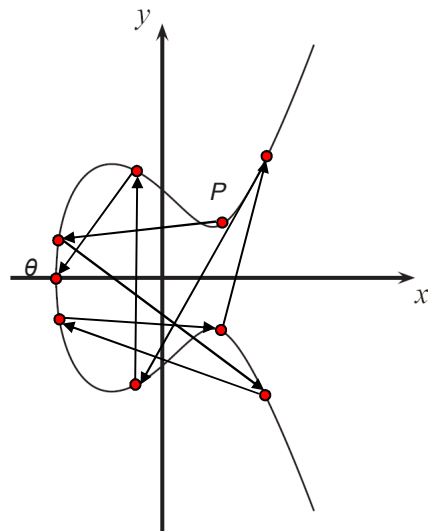
$$15P = (3,16)$$

$$16P = (10,11)$$

$$17P = (6,14)$$

$$18P = (5,16)$$

$$19P = \theta$$



这个椭圆曲线的位数为19，因为其包含19个点

Hard problems on Elliptic curve

- Please write down the following hard problems of the EC version
 - Discrete logarithm problem (DL)
 - Computational Diffie-Hellman problem (CDH)
 - Decisional Diffie-Hellman problem (DDH)

Pairing

Definition 15.2. Let $\mathbb{G}_0, \mathbb{G}_1, \mathbb{G}_T$ be three cyclic groups of prime order q where $g_0 \in \mathbb{G}_0$ and $g_1 \in \mathbb{G}_1$ are generators. A **pairing** is an efficiently computable function $e : \mathbb{G}_0 \times \mathbb{G}_1 \rightarrow \mathbb{G}_T$ satisfying the following properties:

1. *bilinear*: for all $u, u' \in \mathbb{G}_0$ and $v, v' \in \mathbb{G}_1$ we have

$$e(u \cdot u', v) = e(u, v) \cdot e(u', v) \quad \text{and} \quad e(u, v \cdot v') = e(u, v) \cdot e(u, v'),$$

2. *non-degenerate*: $g_T := e(g_0, g_1)$ is a generator of \mathbb{G}_T .

When $\mathbb{G}_0 = \mathbb{G}_1$ we say that the pairing is a **symmetric pairing**. We refer to \mathbb{G}_0 and \mathbb{G}_1 as the **pairing groups** or **source groups**, and refer to \mathbb{G}_T as the **target group**.

The group operation is written multiplicatively.

Central Property: for all $\alpha, \beta \in \mathbb{Z}_q$ $e(g_0^\alpha, g_1^\beta) = e(g_0, g_1)^{\alpha \cdot \beta} = e(g_0^\beta, g_1^\alpha)$.

Direct Consequences 1

$$e : \mathbb{G}_0 \times \mathbb{G}_1 \rightarrow \mathbb{G}_T$$

If $\mathbb{G}_0 = \mathbb{G}_1$, then the decision Diffie-Hellman(DDH) problem in \mathbb{G}_0 is easy.

Proof. given a triple $(u, v, w) = (g_0^\alpha, g_0^\beta, g_0^\gamma) \in \mathbb{G}^3$, we can test if $\gamma = \alpha \cdot \beta$ in \mathbb{Z}_q by

$$e(u, v) = e(g_0, w).$$

equality holds if and only if $e(g_0, g_0)^{\alpha\beta} = e(g_0, g_0)^\gamma$, $\Rightarrow \gamma = \alpha \cdot \beta$.

DDH assumption is believed to be held in \mathbb{G}_0 and \mathbb{G}_1 for most efficient asymmetric pairings

Direct Consequences 2

Computing DL in either G_0 or G_1 is no harder than computing DL in GT

Proof.

Given $u_0 = g_0^\alpha \in \mathbb{G}_0$, try to derive $\alpha \in \mathbb{Z}_q$.

Compute $u := e(u_0, g_1)$ and set $g_T := e(g_0, g_1)$.

Obviously, $u = (g_T)^\alpha$; so we can derive α by solving the DL in GT .
So if DL in GT is easy, so is the DL in G_0 (same for G_1).

For discrete log to be hard in either G_0 or G_1 , we must choose the groups so that DL in the target group GT is also hard.

Constructing Pairings from EC

$$e : \mathbb{G}_0 \times \mathbb{G}_1 \rightarrow \mathbb{G}_T :$$

Base field

Larger extended field

- \mathbb{G}_0 is an order q subgroup of $E(\mathbb{F}_p)$, for some prime q ,
 - \mathbb{G}_1 is an order q subgroup of $E(\mathbb{F}_{p^d})$, for some $d > 0$, where $\mathbb{G}_1 \cap \mathbb{G}_0 = \{\mathcal{O}\}$,
 - \mathbb{G}_T is an order q multiplicative subgroup of the finite field \mathbb{F}_{p^d} .
-
- d is called embedding degree, and should be small (< 16) to be efficient (pairing friendly curve).
 - The representation of elements in \mathbb{G}_0 is much shorter than in \mathbb{G}_1 . To minimize ciphertext length, we prefer that group elements that appear in ciphertext exist in \mathbb{G}_0 .

Pairing Performance

	time (milliseconds)
exponentiation: in \mathbb{G}_0	0.22
in \mathbb{G}_1	0.44
in \mathbb{G}_T	0.95
pairing: $\mathbb{G}_0 \times \mathbb{G}_1 \rightarrow \mathbb{G}_T$	2.32

Table 15.1: Benchmarks for pairings on the curve bn256¹.