Lecture 8

Integers module a prime

e.g. a mod 23 (prime)

Multiplication mod 23 (prime)

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22
1	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22
2	2	4	6	8	10	12	14	16	18	20	22	1	3	5	7	9	11	13	15	17	19	21
3	3	6	9	12	15	18	21	1	4	7	10	13	16	19	22	2	5	8	11	14	17	20
4	4	8	12	16	20	1	5	9	13	17	21	2	6	10	14	18	22	3	7	11	15	19
5	5	10	15	20	2	7	12	17	22	4	9	14	19	1	6	11	16	21	3	8	13	18
6	6	12	18	1	7	13	19	2	8	14	20	3	9	15	21	4	10	16	22	5	11	17
7	7	14	21	5	12	19	3	10	17	1	8	15	22	6	13	20	4	11	18	2	9	16
8	8	16	1	9	17	2	10	18	3	11	19	4	12	20	5	13	21	6	14	22	7	15
9	9	18	4	13	22	8	17	3	12	21	7	16	2	11	20	6	15	1	10	19	5	14
10	10	20	7	17	4	14	1	11	21	8	18	5	15	2	12	22	9	19	6	16	3	13
11	11	22	10	21	9	20	8	19	7	18	6	17	5	16	4	15	3	14	2	13	1	12
12	12	1	13	2	14	3	15	4	16	5	17	6	18	7	19	8	20	9	21	10	22	11
13	13	3	16	6	19	9	22	12	2	15	5	18	8	21	11	1	14	4	17	7	20	10
14	14	5	19	10	1	15	6	20	11	2	16	7	21	12	3	17	8	22	13	4	18	9
15	15	7	22	14	6	21	13	5	20	12	4	19	11	3	18	10	2	17	9	1	16	8
16	16	9	2	18	11	4	20	13	6	22	15	8	1	17	10	3	19	12	5	21	14	7
17	17	11	5	22	16	10	4	21	15	9	3	20	14	8	2	19	13	7	1	18	12	6
18	18	13	8	3	21	16	11	6	1	19	14	9	4	22	17	12	7	2	20	15	10	5
19	19	15	11	7	3	22	18	14	10	6	2	21	17	13	9	5	1	20	16	12	8	4
20	20	17	14	11	8	5	2	22	19	16	13	10	7	4	1	21	18	15	12	9	6	3
21	21	19	17	15	13	11	9	7	5	3	1	22	20	18	16	14	12	10	8	6	4	2
22	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1

* Inverses exist for every integer in $\mathbb{Z}_{23}^*$

* We can do multiplication and it follows all the rules from last lecture

* We can do a type of division.

* $a / b \Rightarrow a \cdot b^{-1}$ → invert and multiply.
  ↑ not defined.

* $22/5 \stackrel{?}{=} 22 \cdot 5^{-1} = 22 \cdot 14 = 9$

* $8^9 = \underbrace{(8 \cdot 8 \cdot 8 \cdot 8 \ldots 8)}_{9}$

$= (8 \cdot 8)(8 \cdot 8)(8 \cdot 8)(8 \cdot 8)(8)$

$= (18)(18)(18)(18)(8)$

$= (2)(2)(8)$

$= 48$

$= 9$

$r^c \bmod 23$ → exponentiation.

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
2	1	2	4	8	16	9	18	13	3	6	12	1	2	4	8	16	9	18	13	3	6	12	1
3	1	3	9	4	12	13	16	2	6	18	8	1	3	9	4	12	13	16	2	6	18	8	1
4	1	4	16	18	3	12	2	8	9	13	6	1	4	16	18	3	12	2	8	9	13	6	1
5	1	5	2	10	4	20	8	17	16	11	9	22	18	21	13	19	3	15	6	7	12	14	1
6	1	6	13	9	8	2	12	3	18	16	4	1	6	13	9	8	2	12	3	18	16	4	1
7	1	7	3	21	9	17	4	5	12	15	13	22	16	20	2	14	6	19	18	11	8	10	1
8	1	8	18	6	2	16	13	12	4	9	3	1	8	18	6	2	16	13	12	4	9	3	1
9	1	9	12	16	6	8	3	4	13	2	18	1	9	12	16	6	8	3	4	13	2	18	1
10	1	10	8	11	18	19	6	14	2	20	16	22	13	15	12	5	4	17	9	21	3	7	1
11	1	11	6	20	13	5	9	7	8	19	2	22	12	17	3	10	18	14	16	15	4	21	1
12	1	12	6	3	13	18	9	16	8	4	2	1	12	6	3	13	18	9	16	8	4	2	1
13	1	13	8	12	18	4	6	9	2	3	16	1	13	8	12	18	4	6	9	2	3	16	1
14	1	14	12	7	6	15	3	19	13	21	18	22	9	11	16	17	8	20	4	10	2	5	1
15	1	15	18	17	2	7	13	11	4	14	3	22	8	5	6	21	16	10	12	19	9	20	1
16	1	16	3	2	9	6	4	18	12	8	13	1	16	3	2	9	6	4	18	12	8	13	1
17	1	17	13	14	8	21	12	20	18	7	4	22	6	10	9	15	2	11	3	5	16	19	1
18	1	18	2	13	4	3	8	6	16	12	9	1	18	2	13	4	3	8	6	16	12	9	1
19	1	19	16	5	3	11	2	15	9	10	6	22	4	7	18	20	12	21	8	14	13	17	1
20	1	20	9	19	12	10	16	21	6	5	8	22	3	14	4	11	13	7	2	17	18	15	1
21	1	21	4	15	16	14	18	10	3	17	12	22	2	19	8	7	9	5	13	20	6	11	1
22	1	22	1	22	1	22	1	22	1	22	1	22	1	22	1	22	1	22	1	22	1	22	1

Multiplicative order (order)

Given an element of a group, $g \in G_q$, what is the order of $g \bmod p$?

$ord(g)$ → smallest t s.t. $g^t \equiv 1 \bmod p$ ($t \neq 0$)

Example:

$ord(7) = 22$

$ord(13) = 11$ (22 is also a 1 but 11 is smaller)

$ord(9) = 11$

Fermat's little theorem.

$$g^{p-1} \bmod p = 1$$

↳ order of g will always be $p-1$ or less.

What are the orders of the integers mod 23?

* We see four orders:

$\{1, 2, 11, 22\}$ ← set.

$ord(1)$ ↑ ↑ $ord(22)$ ← set

In general, given a prime p, the order of $g \in \mathbb{Z}_p^*$ for any g:

$$\text{ord}(g) \mid p-1$$

Example: $p = 23$

↳ $11 \mid p-1 = 1 \mid 22$

$22 \mid 22$

$2 \mid 22$

$11 \mid 22$

$(1 \cdot 22 = 22$
$2 \cdot 11 = 22)$

Safe Prime

$p-1$ → always have 1 and $p-1$ as divisors (and thus orders)

↕ prime

↳ always have 2 b/c p is an odd integer

↳ ∴ always have $\frac{p-1}{2}$

↳ we can stop if

$\frac{p-1}{2}$ is prime

Safe primes:

$p = 2q + 1 \qquad \left(q = \frac{p-1}{2}\right)$

↑ prime ↑ prime

↑ prime

Example: $23 = 2 \cdot 11 + 1$

prime ↑ ↑ prime

For any safe prime p, all elements of $\mathbb{Z}_p^*$ will have order

$\{1, 2, \frac{p-1}{2} = q, p-1\}$

How many elements of $\mathbb{Z}^*_{23}$ have order 11?

10 of them:

G_{11}

$\{1, 2, 3, 4, 6, 8, 9, 12, 13, 16, 18\}$

↑ add 1 to the set.

Set of 11 integers (or a prime number of integers.

* We can consider each element to be a generator:

a sequence of integers generated by multiplying a number by itself repeatedly

↳ hit a 1 (order) and repeat

* All the elements that have order 11 (q in general) generate the same set of integers (G_q)

* In general, all elements of G_q generate G_q.

* G_q is closed under multiplication

Mult	1	2	3	4	6	8	9	12	13	16	18
1	1	2	3	4	6	8	9	12	13	16	18
2	2	4	6	8	12	16	18	1	3	9	13
3	3	6	9	12	18	1	4	13	16	2	8
4	4	8	12	16	1	9	13	2	6	18	3
6	6	12	18	1	13	2	8	3	9	4	16
8	8	16	1	9	2	18	3	4	12	13	6
9	9	18	4	13	8	3	12	16	2	6	1
12	12	1	13	2	3	4	16	6	18	8	9
13	13	3	16	6	9	12	2	18	8	1	4
16	16	9	2	18	4	13	6	8	1	3	12
18	18	13	8	3	16	6	1	9	4	12	2

Exp	0	1	2	3	4	5	6	7	8	9	10
1	1	1	1	1	1	1	1	1	1	1	1
2	1	2	4	8	16	9	18	13	3	6	12
3	1	3	9	4	12	13	16	2	6	18	8
4	1	4	16	18	3	12	2	8	9	13	6
6	1	6	13	9	8	2	12	3	18	16	4
8	1	8	18	6	2	16	13	12	4	9	3
9	1	9	12	16	6	8	3	4	13	2	18
12	1	12	6	3	13	18	9	16	8	4	2
13	1	13	8	12	18	4	6	9	2	3	16
16	1	16	3	2	9	6	4	18	12	8	13
18	1	18	2	13	4	3	8	6	16	12	9

Definition: G_q

G_q is a subgroup of integers in $\mathbb{Z}_p^*$ where $p = 2q + 1$ such that:
(prime)

* the size of G_q is q (prime)
* G_q is closed under multiplication and exponentiation.
* the order of all elements in G_q is q (except ord(1) = 1)

$\hookrightarrow$ $g^q = 1$

$g^{q+1} = (g^q)(g^1) = g$

$g^a = g^{[a \bmod q]} \bmod p$

* every element of G_q is invertible.

* exponents in G_q can be reduced mod q:

$$g^{a \sim Z_q} \bmod p = g^{a \bmod q} \bmod p$$

↳ $G_q \leq Z_p^*$

* Computing inverses.

$$g^{-1} \bmod p = g^{-1 \bmod q} \bmod p$$

$$= g^{q-1} \bmod p$$

* Finding inverses is efficient.

* If $\exists b$ s.t. $a^2 = b$ then

b is a quadratic residue (QR)

↳ $b \in G_q$

↳ $QR = G_q$.

↑ set of all such b

Applications for crypto:

* Safe prime $p = 2q+1$ $\left(q = \frac{p-1}{2} \approx \frac{1}{2}p\right)$

↳ $|p| \geq 2048$ bits.

$|q| \geq 2047$ bits.

(in practice, we use non-safe-prime groups ($p = 2aq+1$, a prime) where $q \geq 256$ bits)

NO exam.

* How to find an element of G_q?

① Try 1, 2, 3..., take the order:

$\text{ord}(3)$? $\stackrel{?}{=} 1 \rightarrow 3^1 \stackrel{?}{=} 1$

$\stackrel{?}{=} 2 \rightarrow 3^2 \stackrel{?}{=} 1$

$\stackrel{?}{=} q \rightarrow 3^q \stackrel{?}{=} 1$

$\stackrel{?}{=} q-1 \quad 3^{q-1} = 1$

② Choose any integer in $\mathbb{Z}_p^*$ and square it

↳ answer is in G_q.

Other algorithms in G_q.

↳ group operations

↳ given x and y, find a.

$$\begin{cases} y = ax \\ y = xa \\ y = a^x \\ y = x^a \end{cases}$$

↳ if we have to scan along an entire row/column, this will be infeasible for large primes

↳ need to jump directly to answer.

(1) $y = a \cdot x \mod p$.

↳ $a = y \cdot x^{-1} \mod p$

↳ no division so we invert and multiply.

↳ exists always.

$= y(x^{-1 \bmod q}) \mod p$

$= y(x^{q-1}) \mod p$.

↑ one exp
↑ one mult. } efficient.

(2) $y = x \cdot a \mod p$

↳ same as (1) because multiplication is communitive.

↳ efficient.

(3) $y = a^x = (\overbrace{a \cdot a \cdot a \cdot a \ldots a}^{x}) \mod p$

$a = \sqrt[x]{y}$

↑ roots are defined.

$$= y^{(1/x)}$$

$$= y^{(x^{-1})}$$

$$= y^{(x^{-1} \bmod q-1)}$$

$$= y^{(x^{q-2} \bmod q)} \bmod p$$

(1 exp. + 1 exp.) } efficient.

Aside:

$g^{a^b \bmod q-1 \bmod q} \bmod p$.

Example:

$y = a^x$ $\quad (23 = 2 \cdot 11 + 1)$, p, q

$6 = a^9 \bmod 23$.

$a = \sqrt[9]{6} \bmod 23$

$= 6^{(9^{-1})} \bmod 23$

$= 6^{(9^{-1} \bmod 11)} \bmod 23$

$= 6^5 \bmod 23 = 2$

$9^{-1} \bmod q$

$= 9^{-1 \bmod q-1} \bmod q$

$= 9^{-1 \bmod 10} \bmod 11$

$= 9^9 \bmod 11$

$= 5$

④ $y = x^a \mod p$

↳ $a = \log_x(y)$

↳ exists because

$x^1, x^2, x^3, x^4 \ldots$

will generate G_q.

and $y \in G_q$.

↳ $y = x^a \mod p$

$3 = 6^a \mod p$

$a = 7$ (start at row

6 and slide until you

get 3 → column 7)

↳ "modular" logarithm

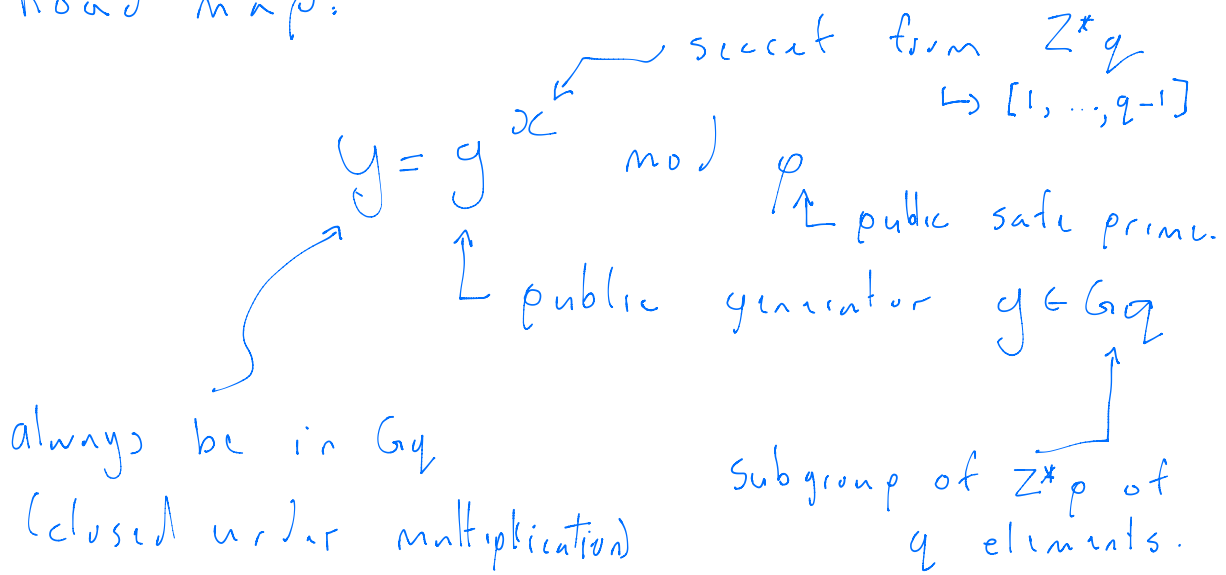
or discrete logarithm

↳ no efficient algorithm

that is known.

↳ $p \geq 2048$ and we work in G_q where q is prime: discrete log problem is hard

Road map:



Generally $\{p, q, g\}$ will be pre-chosen by e.g. NIST

Discrete logarithm problem (DLP):

Given safe prime p ($2q+1 = p$ for prime q) where p is a large prime ($|p| \geq 2048$ bits), it is infeasible to compute x such that $y = g^x \bmod p$ given $\langle g, y, p, q \rangle$