CS 6260
Some number theory

Let $\mathbf{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$ denote the set of integers.
Let $\mathbf{Z+} = \{1, 2, \ldots\}$ denote the set of positive integers and
$\mathbf{N} = \{0, 1, 2, \ldots\}$ the set of non-negative integers.

If a, N are integers with $N > 0$ then there are unique integers r, q such that $a = Nq + r$ and $0 \le r < N$.

We associate to any positive integer N the following two sets:
$\mathbf{Z_N} = \{0, 1, \ldots, N-1\}$, $\mathbf{Z_N^*} = \{ i \in Z : 1 \le i \le N-1 \text{ and } \gcd(i,N)=1 \}$

Groups

- Def. Let G be a non-empty set and let $\cdot$ denote a binary operation on G. We say that G is a group if it has the following properties:
  1. Closure: For every $a, b \in G$ it is the case that $a \cdot b$ is also in G.
  2. Associativity: For every $a, b, c \in G$ it is the case that $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.
  3. Identity: There exists an element $1 \in G$ such that $a \cdot 1 = 1 \cdot a = a$ for all $a \in G$.
  4. Invertibility: For every $a \in G$ there exists a unique $b \in G$ such that $a \cdot b = b \cdot a = 1$.

inverse, denoted a^{-1}

- Fact. Let N be a positive integer. Then $\mathbf{Z_N}$ is a group under addition modulo N, and $\mathbf{Z_N^*}$ is a group under multiplication modulo N.
- In any group, we can define an exponentiation operation:
  if $i = 0$ then a^i is defined to be 1,
  if $i > 0$ then $a^i = a \cdot a \cdots a$ (i times)
  if $i < 0$ then $a^i = a^{-1} \cdot a^{-1} \cdots a^{-1}$ (j=-i times)
- For all $a \in \mathbf{G}$ and all $i,j \in \mathbf{Z}$:
  - $a^{i+j} = a^i \cdot a^j$
  - $(a^i)^j = a^{ij}$
  - $a^{-i} = (a^i)^{-1} = (a^{-1})^i$

- The order of a group is its size
- Fact. Let **G** be a group and let m = |**G**| be its order. Then $a^m = 1$ for all $a \in$ **G**
- Fact. Let **G** be a group and let m = |**G**| be its order. Then $a^i = a^{i \bmod m}$ for all $a \in$ **G** and all $i \in$ **Z**.
- Example. Let us work in the group $\mathbf{Z}_{21}^*$ ={1, 2, 4, 5, 8, 10, 11, 13, 16, 17, 19, 20} under the operation of multiplication modulo 21. m=12.

$5^{86} \bmod 21 = 5^{86 \bmod 12} \bmod 21 = 5^{2 \bmod 12} \bmod 21 = 25 \bmod 21 = 4$

- If **G** is a group, a set **S** ⊆ **G** is called a subgroup if it is a group in its own right, under the same operation as that under which **G** is a group.
- If we already know that **G** is a group, there is a simple way to test whether **S** is a subgroup:
  - it is one if and only if $x \cdot y^{-1} \in$ **S** for all x, y ∈ **S**. Here y^{-1} is the inverse of y in **G**.
- Fact. Let **G** be a group and let S be a subgroup of **G**. Then the order of **S** divides the order of **G**.

Algorithms and their running times

- Since in cryptography we will be working with BIG numbers, the complexity of algorithms taking numbers as inputs is measured as a function of the bit-length of the numbers.
- E.g. PrintinBinary (A), where $A=2^k$ takes k operations

Some basic algorithms

Algorithm	Input		Output	Running Time
INT-DIV	a, N	$(N > 0)$	(q, r) with $a = Nq + r$ and $0 \le r < N$	$O(\|a\| \cdot \|N\|)$
MOD	a, N	$(N > 0)$	$a \bmod N$	$O(\|a\| \cdot \|N\|)$
EXT-GCD	a, b	$((a, b) \neq (0, 0))$	$(d, \overline{a}, \overline{b})$ with $d = \gcd(a, b) = a\overline{a} + b\overline{b}$	$O(\|a\| \cdot \|b\|)$
MOD-ADD	a, b, N	$(a, b \in \mathbf{Z}_N)$	$(a + b) \bmod N$	$O(\|N\|)$
MOD-MULT	a, b, N	$(a, b \in \mathbf{Z}_N)$	$ab \bmod N$	$O(\|N\|^2)$
MOD-INV	a, N	$(a \in \mathbf{Z}_N^*)$	$b \in \mathbf{Z}_N^*$ with $ab \equiv 1 \pmod N$	$O(\|N\|^2)$
MOD-EXP	a, n, N	$(a \in \mathbf{Z}_N)$	$a^n \bmod N$	$O(\|n\| \cdot \|N\|^2)$
EXP_G	a, n	$(a \in G)$	$a^n \in G$	$2\|n\|$ G-operations

Cyclic groups and generators

- If $g \in \mathbf{G}$ is any member of the group, the order of g is defined to be the least positive integer n such that $g^n = 1$.
  We let <g> = $\{ g^i : i \in \mathbf{Z_n} \} = \{g^0, g^1, \ldots, g^{n-1}\}$ denote the set of group elements generated by g. This is a subgroup of order n.
- Def. An element g of the group is called a generator of **G** if <g>=**G**, or, equivalently, if its order is $m=|\mathbf{G}|$.
- Def. A group is cyclic if it contains a generator.
- If g is a generator of **G**, then for every $a \in \mathbf{G}$ there is a unique integer $i \in \mathbf{Z_m}$ such that $g^i = a$. This i is called the discrete logarithm of a to base g, and we denote it by $\mathrm{DLog}_{\mathbf{G},g}(a)$.
- $\mathrm{DLog}_{\mathbf{G},g}(a)$ is a function that maps **G** to $\mathbf{Z_m}$, and moreover this function is a bijection.
- The function of $\mathbf{Z_m}$ to **G** defined by $i \to g^i$ is called the discrete exponentiation function

---

- Example. Let p = 11. Then $\mathbf{Z}^*_{\mathbf{11}} = \{1,2,3,4,5,6,7,8,9,10\}$ has order p – 1 = 10. We find the subgroups generated by group elements 2 and 5. We raise them to the powers 0,...,9.

i	0	1	2	3	4	5	6	7	8	9
2^i mod 11	1	2	4	8	5	10	9	7	3	6
5^i mod 11	1	5	3	4	9	1	5	3	4	9

<2> = $\{1,2,3,4,5,6,7,8,9,10\} = \mathbf{Z}^*_{\mathbf{11}}$ <5> = {1,3,4,5,9}

2 is a generator and thus $\mathbf{Z}^*_{\mathbf{11}}$ is cyclic.

a	1	2	3	4	5	6	7	8	9	10
$\mathrm{DLog}_{\mathbf{Z}^*_{11},2}(a)$	0	1	8	2	4	9	7	3	6	5

Choosing cyclic group and generators

- The discrete log function is conjectured to be one-way (hard to compute) for some cyclic groups **G**. Due to this fact we often seek cyclic groups.
- Examples of cyclic groups:
  - $\mathbf{Z}^*_{\mathbf{p}}$ for a prime p,
  - a group of prime order
- We will also need generators. How to chose a candidate and test it?
- Fact. Let **G** be a cyclic group and let $m = |\mathbf{G}|$. Let $p_1^{\alpha_1} \cdot \cdot \cdot p_n^{\alpha_n}$ be the prime factorization of m and let $m_i = m/p_i$ for i = 1,...,n.
  Then $g \in \mathbf{G}$ is a generator of **G** if and only if for all i = 1, . . . , n: $g^{m_i} \neq \mathbf{1}$.
- Fact. Let **G** be a cyclic group of order m, and let g be a generator of **G**. Then $\mathrm{Gen}(\mathbf{G}) = \{ g^i \in G : i \in \mathbf{Z}^*_{\mathbf{m}} \}$ and $|\mathrm{Gen}(\mathbf{G})| = \phi(m)$.

- Example. Let us determine all the generators of the group $\mathbf{Z}^*_{\mathbf{11}}$. Its size is $m = \phi(11) = 10$, and the prime factorization of 10 is $2^1 \cdot 5^1$. Thus, the test for whether a given $a \in \mathbf{Z}^*_{\mathbf{11}}$ is a generator is that $a^2 \neq 1 \pmod{11}$ and $a^5 \neq 1 \pmod{11}$.

a	1	2	3	4	5	6	7	8	9	10
a^2 mod 11	1	4	9	5	3	3	5	9	4	1
a^5 mod 11	1	10	1	1	1	10	10	10	1	10

- $\mathrm{Gen}(\mathbf{Z}^*_{\mathbf{11}}) = \{2,6,7,8\}$.
- Double-checking: $|\mathbf{Z}^*_{\mathbf{11}}|=10$, $\mathbf{Z}^*_{\mathbf{10}} = \{1,3,7,9\}$
  $\{ 2^i \in G : i \in \mathbf{Z}^*_{\mathbf{10}} \} = \{ 2^1, 2^3, 2^7, 2^9 \pmod{11}\} = \{2,6,7,8\}$

Algorithm for finding a generator

- The most common choice of a group in crypto is $\mathbf{Z}_{\mathbf{p}}^*$ for a prime p.
- Idea. Pick a random element and test it. Chose p s.t. the prime factorization of the order of the group (p-1) is known. E.g., chose a prime p s.t. p=2q+1 for some prime q.
- Algorithm FIND-GEN(p)
  $q \leftarrow (p-1)/2$
- found $\leftarrow 0$
  While (found $\neq 1$) do
- $\quad g \xleftarrow{\$} \mathbf{Z}_p^* - \{1, p-1\}$
- $\quad$ If $(g^2 \bmod p \neq 1)$ and $(g^q \bmod p \neq 1)$ then found $\leftarrow 1$
  EndWhile
- Return g
- The probability that an iteration of the algorithm is successful in finding a generator is

$$\frac{|\mathsf{Gen}(\mathbf{Z}_p^*)|}{|\mathbf{Z}_p^*| - 2} = \frac{\varphi(p-1)}{p-3} = \frac{\varphi(2q)}{2q-2} = \frac{q-1}{2q-2} = \frac{1}{2}$$

Squares and non-squares

- Def. An element a of a group **G** is called a square, or quadratic residue if it has a square root, meaning there is some b ∈ G such that b^2 = a in **G**.
- We let QR(**G**) = { g ∈ **G** : g is quadratic residue in **G** }
- We are mostly interested in the case where the group **G** is $\mathbf{Z}_{\mathbf{N}}^*$ for some integer N.
- Defs. An integer a is called a square mod N or quadratic residue mod N if a mod N is a member of QR($\mathbf{Z}_{\mathbf{N}}^*$). If b^2 = a (mod N) then b is called a square-root of a mod N. An integer a is called a non-square mod N or quadratic non-residue mod N if a mod N is a member of $\mathbf{Z}_{\mathbf{N}}^*$ – QR($\mathbf{Z}_{\mathbf{N}}^*$).
- Def. Let p be a prime. Define the Legendre symbol of a

$$J_p(a) = \begin{cases} 1 & \text{if } a \text{ is a square mod } p \\ 0 & \text{if } a \bmod p = 0 \\ -1 & \text{otherwise.} \end{cases}$$

- Example. QR($\mathbf{Z}_{\mathbf{11}}^*$)?

a	1	2	3	4	5	6	7	8	9	10
$a^2 \bmod 11$	1	4	9	5	3	3	5	9	4	1

QR($\mathbf{Z}_{\mathbf{11}}^*$)={1, 3, 4, 5, 9}

Recall that $\mathbf{Z}_{\mathbf{11}}^*$ is cyclic and 2 is a generator.

Fact. A generator is always a non-square. (But not all non-squares are generators).

a	1	2	3	4	5	6	7	8	9	10
$\mathrm{DLog}_{\mathbf{Z}_{11}^*,2}(a)$	0	1	8	2	4	9	7	3	6	5
$J_{11}(a)$	1	-1	1	1	1	-1	-1	-1	1	-1

- Fact. Let p ≥ 3 be a prime and let g be a generator of $\mathbf{Z}_{\mathbf{p}}^*$. Then QR($\mathbf{Z}_{\mathbf{p}}^*$) = { g^i : i ∈ $\mathbf{Z}_{\mathbf{p-1}}$ and i is even } , and |QR($\mathbf{Z}_{\mathbf{p}}^*$)| = (p – 1)/2

Facts. Let p ≥ 3 be a prime. Then

- $J_p(a) \equiv a^{\frac{p-1}{2}} \pmod p$ for any a ∈ $\mathbf{Z}_{\mathbf{p}}^*$
- $g^{\frac{p-1}{2}} \equiv -1 \pmod p$ for any generator g of $\mathbf{Z}_{\mathbf{p}}^*$
- $J_p(ab \bmod p) = J_p(a) \cdot J_p(b)$ for any a ∈ $\mathbf{Z}_{\mathbf{p}}^*$
- $J_p(g^{xy} \bmod p) = 1$ if and only if $J_p(g^x \bmod p) = 1$ or $J_p(g^y \bmod p) = 1$

for any generator g of $\mathbf{Z}_{\mathbf{p}}^*$ and any x,y ∈ $\mathbf{Z}_{\mathbf{p-1}}$

- $\Pr\left[x \xleftarrow{\$} \mathbf{Z}_{p-1}\,;\, y \xleftarrow{\$} \mathbf{Z}_{p-1} \,:\, J_p(g^{xy}) = 1\right]$ =3/4

for any generator g of $\mathbf{Z}_{\mathbf{p}}^*$

Groups of prime order

- Def. An element h of a group **G** is called non-trivial if it is not equal to the identity element of the group.
- Fact. Any non-trivial member of a group of prime order is a generator of the group.
- Fact. Let q ≥ 3 be a prime such that p = 2q + 1 is also prime. Then QR($\mathbf{Z}_\mathbf{p}^*$) is a group of prime order q. Furthermore, if g is any generator of $\mathbf{Z}_\mathbf{p}^*$, then g^2 mod p is a generator of QR($\mathbf{Z}_\mathbf{p}^*$).
- Fact. Let g be a generator of a group of prime order q. Then for any element Z of the group

$$\Pr\left[x \stackrel{\$}{\leftarrow} \mathbf{Z}_q \,;\, y \stackrel{\$}{\leftarrow} \mathbf{Z}_q \,:\, g^{xy} = Z\right] \;=\; \begin{cases} \frac{1}{q}\left(1-\frac{1}{q}\right) & \text{if } Z \neq \mathbf{1} \\ \frac{1}{q}\left(2-\frac{1}{q}\right) & \text{if } Z = \mathbf{1} \end{cases}$$

- Example. Let q = 5 and p = 2q + 1 = 11.
- QR($\mathbf{Z}_{11}^*$) $= \{1, 3, 4, 5, 9\}$

We know that 2 is a generator of $\mathbf{Z}_{\mathbf{11}}^*$

Let's verify that 4 = 2^2 is a generator of QR($\mathbf{Z}_{\mathbf{11}}^*$).

i	0	1	2	3	4
4^i mod 11	1	4	5	9	3