Number Theory and Cryptographic Hardness Assumptions

Michele Ciampi

Introduction to Modern Cryptography, Lecture 12, Part 2

Modular Arithmetic

- Let $a, b, N \in \mathbb{Z}$ with $N > 1$. We use the notation $a \bmod N$ to denote the remainder of a upon division by N.
- We say that a and b are *congruent* modulo N, written $a = b \bmod N$, if they have the same remainder when divided by N. Note that $a = b \bmod N$ if and only if $N | (a - b)$.

Modular Arithmetic

- Congruence modulo N obeys the standard rules of arithmetic with respect to addition and multiplication: if $a = a' \bmod N$ and $b = b' \bmod N$, then $(a + b) = (a' + b') \bmod N$ and $ab = a'b' \bmod N$.
- Example: compute $(1093028 \cdot 190301) \bmod 100$. Since $1093028 = 28 \bmod 100$ and $190301 = 1 \bmod 100$, we have

$$1093028 \cdot 190301 = 28 \cdot 1 = \bmod 100 \, .$$

Modular Arithmetic

- Congruence modulo N does not respect (in general) division. For this reason, $ab = cb \bmod N$ does not necessarily imply that $a = c \bmod N$.
- Example: $N = 24$. Then $3 \cdot 2 = 6 = 15 \cdot 2 \bmod 24$, but $3 \neq 15 \bmod 24$.

Modular Arithmetic

- If for a given integer b there exists an integer c such that $bc = 1 \bmod N$, we say that b is *invertible* modulo N and call c a *multiplicative inverse* of b modulo N.
- $c \bmod N$ is the unique multiplicative inverse of b that lies in the range $\{1, \ldots, N-1\}$ and is denoted by b^{-1}.
- When b is invertible modulo N, we define division by b as multiplication by b^{-1}.
- If $ab = cb \bmod N$ and b is invertible, then we have that

$$(ab) \cdot b^{-1} = (cb) \cdot b^{-1} \bmod N \Rightarrow a = c \bmod N \,.$$

Modular Arithmetic

Which numbers are invertible modulo N?

Modular Arithmetic

Which numbers are invertible modulo N?

Theorem

Let b, N integers with $b \geq 1$ and $N > 1$. Then b is invertible modulo N if and only if $\gcd(b, N) = 1$.

Groups

A *group* is a set $\mathbb{G}$ along with a binary operation $\circ$ for which the following conditions hold:

- *Closure*: For all $g, h \in \mathbb{G}$, $g \circ h \in \mathbb{G}$.
- *Existence of identity*: There exists an identity element $e \in \mathbb{G}$ such that for all $g \in \mathbb{G}$, $e \circ g = g = g \circ e$.
- *Existence of inverse*: For all $g \in \mathbb{G}$ there exists an element $h \in \mathbb{G}$ such that $g \circ h = e = h \circ g$. Such an h is called an inverse of g.
- *Associativity*: For all $g_1, g_2, g_3 \in \mathbb{G}$, $(g_1 \circ g_2) \circ g_3 = g_1 \circ (g_2 \circ g_3)$.

A group $\mathbb{G}$ with operation $\circ$ is *abelian* if the following holds:

- *Commutativity*: For all $g, h \in \mathbb{G}$, $g \circ h = h \circ g$.

Groups

- The inverse h of $g \in \mathbb{G}$ is unique.
- A set $\mathbb{H} \subseteq \mathbb{G}$ is a *subgroup* of $\mathbb{G}$ if itself forms a group under the same operation associated with $\mathbb{G}$.
- If $\mathbb{G}$ has finite number of elements, we say it is *finite*. The number of elements is called the *order* of $\mathbb{G}$, denoted by $|\mathbb{G}|$.

Examples

- The set of integers $\mathbb{Z}$ is an abelian group under addition with identity 0. The set of the multiples of 2 $\{\cdots, -6, -4, -2, 0, 2, 4, 6, \cdots\}$ is a subgroup of $\mathbb{Z}$.
- The set of non-zero real numbers $\mathbb{R} \setminus \{0\}$ is an abelian group under multiplication with identity 1.
- The set $\{0, \ldots, N-1\}$ with respect to addition modulo N is an abelian group of order N with identity 0. The inverse of a is $(N-a) \bmod N$. We denote this group by $\mathbb{Z}_N$.

Examples: the group $\mathbb{Z}_N^*$

The set of invertible elements modulo N is an abelian group under multiplication with identity 1. Namely,

$$\mathbb{Z}_N^* \stackrel{def}{=} \left\{ b \in \{1, \ldots, N-1\} \middle| \gcd(b, N) = 1 \right\} .$$

- *Commutativity* and *associativity* follow from the integers' properties.
- *Inverse* of b: use extended Euclidean algorithm to find x, y such that $bx + Ny = \gcd(b, N) = 1$. Then, $x \bmod N$ is the inverse of b modulo N.
- *Closure*: let $a, b \in \mathbb{Z}_N^*$. Then $(ab) \bmod N$ has inverse $(b^{-1}a^{-1}) \bmod N$, so $ab \in \mathbb{Z}_N^*$.

Examples: the group $\mathbb{Z}_{15}^*$

Let $N = 15 = 5 \cdot 3$. The set of invertible elements modulo 15 is $\{1, 2, 4, 7, 8, 11, 13, 14\}$.

- The inverse of 2 is 8 since $2 \cdot 8 = 16 = 1 \bmod 15$.
- The inverse of 4 is 4 since $4 \cdot 4 = 16 = 1 \bmod 15$.
- The inverse of 7 is 13 since $7 \cdot 13 = 91 = 1 \bmod 15$.
- The inverse of 11 is 14 since $11 \cdot 14 = 151 = 1 \bmod 15$.

Examples: the group $\mathbb{Z}_N^*$

The set of invertible elements modulo N is an abelian group under multiplication with identity 1. Namely,

$$\mathbb{Z}_N^* \stackrel{def}{=} \left\{ b \in \{1, \ldots, N-1\} \middle| \gcd(b, N) = 1 \right\} .$$

– Special case: for prime p, it holds that

$$\mathbb{Z}_p^* = \{1, 2, \ldots, p-1\} .$$

Multiplicative notation for groups

We use multiplicative notation $\cdot$ instead of $\circ$. We define

$$g^m = \underbrace{g \cdots g}_{m \text{ times}} \ .$$

The familiar rules of exponentiation hold: $g^m \cdot g^n = g^{m+n}$, $(g^m)^n = g^{mn}$, $g^1 = g$, $g^0 = 1$. If $\mathbb{G}$ is abelian, then $g^m \cdot h^m = (g \cdot h)^m$.

Theorem

Let $\mathbb{G}$ be a finite group with $m = |\mathbb{G}|$, the order of the group. Then for every element $g \in \mathbb{G}$, $g^m = 1$.

Proof. We prove for $\mathbb{G}$ abelian. Fix arbitrary $g \in \mathbb{G}$ and let $g_1, \ldots, g_m$ be the elements of $\mathbb{G}$. We claim that

$$g_1 \cdots g_m = (gg_1) \cdots (gg_m) \ .$$

To see this, note that $gg_i = gg_j \Rightarrow g^{-1}gg_i = g^{-1}gg_j \Rightarrow g_i = g_j$. So each of the m elements in parentheses on the right-hand are distinct. Because there are exactly m elements in $\mathbb{G}$, the m elements multiplied together on the right hand side are all the elements in $\mathbb{G}$ in permuted order. Since $\mathbb{G}$ is abelian the order in which elements are multiplied does not matter, so the right-hand side and the left-hand side are equal.
Again using that $\mathbb{G}$ is abelian we obtain

$$g_1 \cdots g_m = (gg_1) \cdots (gg_m) = g^m (g_1 \cdots g_m) \Rightarrow g^m = 1 \ .$$

□

Theorem

Let $\mathbb{G}$ be a finite group with $m = |\mathbb{G}|$, the order of the group. Then for every element $g \in \mathbb{G}$, $g^m = 1$.

Theorem

Let $\mathbb{G}$ be a finite group with $m = |\mathbb{G}|$, the order of the group. Then for every element $g \in \mathbb{G}$, $g^m = 1$.

Corollary

Let $\mathbb{G}$ be a finite group with $m = |\mathbb{G}| > 1$. Then for every $g \in \mathbb{G}$ and every integer x, we have $g^x = g^{x \bmod m}$.

Proof.

For some integers a, r, where $r = x \bmod m$, we have that
$x = am + r$, so

$$g^x = g^{am+r} = (g^m)^a \cdot g^r = 1^a \cdot g^r = g^r \ .$$

$\square$

Definition

Let $\mathbb{G}$ be a finite group and $g \in \mathbb{G}$. The *order* of g is the smallest positive integer i with $g^i = 1$.

Let i the order of $g \in \mathbb{G}$. We define the set (subgroup)

$$\langle g \rangle \stackrel{def}{=} \{g^0, \ldots, g^{i-1}\} .$$

Cyclic groups

Definition

A finite group $\mathbb{G}$ of order m is *cyclic* if it can be generated by a single element $g \in \mathbb{G}$ (of order m), i.e.,

$$\mathbb{G} = \langle g \rangle \stackrel{def}{=} \{g^0, \ldots, g^{m-1}\} .$$

We say that g is a *generator* of $\mathbb{G}$.

If g is a generator of $\mathbb{G}$, then every element $h \in \mathbb{G}$ is equal to g^x for some $x \in \{0, \ldots, m-1\}$.

Cyclic groups

Theorem

If $\mathbb{G}$ is a group of prime order p, then $\mathbb{G}$ is cyclic. Furthermore, all elements of $\mathbb{G}$ except the identity are generators of $\mathbb{G}$.

Theorem

If p is prime, then $\mathbb{Z}_p^*$ is a cyclic group of order $p - 1$.

Example

Consider the cyclic group $\mathbb{Z}_7^*$. We have that $\langle 2 \rangle = \{1, 2, 4\}$ so 2 is not a generator. However,

$$\langle 3 \rangle = \{1, 3, 2, 6, 4, 5\} = \mathbb{Z}_7^* \ ,$$

so 3 is a generator of $\mathbb{Z}_7^*$.

The discrete logarithm problem

Let $\mathcal{G}$ denote a generic PPT *group generation algorithm*. $\mathcal{G}$ on input 1^n outputs a description of a cyclic group $\mathbb{G}$, its order q (with length of q, $|q| = n$) and a generator $g \in \mathbb{G}$.

Since $\mathbb{G} = \langle g \rangle = \{g^0, \ldots, g^{q-1}\}$, for every $h \in \mathbb{G}$ there is a *unique* $x \in \mathbb{Z}_q$ such that $g^x = h$. We call x the *discrete logarithm of h with respect to g*.

The discrete logarithm problem

Consider the following experiment for a group generation algorithm $\mathcal{G}$ and an adversary $\mathcal{A}$.

The discrete-logarithm experiment $\mathsf{DLog}_{\mathcal{A},\mathcal{G}}(n)$**:**

1. Run $\mathcal{G}(1^n)$ to obtain $(\mathbb{G}, q, g)$.
2. Choose a uniform $h \in \mathbb{G}$.
3. $\mathcal{A}$ is given $(\mathbb{G}, q, g, h)$ and outputs $x \in \mathbb{Z}_q$.
4. Output 1 if $g^x = h$, and 0 otherwise.

Definition

We say that *the discrete logarithm problem is hard relative to* $\mathcal{G}$, if for all PPT adversaries $\mathcal{A}$, it holds that

$$\Pr\left[\mathsf{DLog}_{\mathcal{A},\mathcal{G}}(n) = 1\right] \leq \mathsf{negl}(n) \ .$$

The computational Diffie-Hellman problem

Consider the following experiment for a group generation algorithm $\mathcal{G}$ and an adversary $\mathcal{A}$.

The CDH experiment $\mathsf{CDH}_{\mathcal{A},\mathcal{G}}(n)$**:**

1. Run $\mathcal{G}(1^n)$ to obtain $(\mathbb{G}, q, g)$.
2. Choose uniform $x, y \in \mathbb{Z}_q$ and compute g^x, g^y.
3. $\mathcal{A}$ is given $(\mathbb{G}, q, g, g^x, g^y)$ and outputs $h \in \mathbb{G}$.
4. Output 1 if $h = g^{xy}$, and 0 otherwise.

Definition

We say that *the CDH problem is hard relative to* $\mathcal{G}$, if for all PPT adversaries $\mathcal{A}$, it holds that

$$\Pr\left[\mathsf{CDH}_{\mathcal{A},\mathcal{G}}(n) = 1\right] \leq \mathsf{negl}(n) \ .$$

The decisional Diffie-Hellman problem

Consider the following experiment for a group generation algorithm $\mathcal{G}$ and an adversary $\mathcal{A}$.

The DDH experiment $\mathsf{DDH}_{\mathcal{A},\mathcal{G}}(n)$**:**

1. Run $\mathcal{G}(1^n)$ to obtain $(\mathbb{G}, q, g)$.
2. Choose uniform $x, y, z \in \mathbb{Z}_q$.

Definition

We say that *the DDH problem is hard relative to* $\mathcal{G}$*, if for every PPT adversary* $\mathcal{A}$*, it holds that*

$$\left| \Pr\left[\mathcal{A}(\mathbb{G}, q, g, g^x, g^y, g^z) = 1\right] - \Pr\left[\mathcal{A}(\mathbb{G}, q, g, g^x, g^y, g^{xy}) = 1\right] \right| \leq$$

$\leq \mathsf{negl}(n)$, where in each case the probabilities are taken over the experiment $\mathsf{DDH}_{\mathcal{A},\mathcal{G}}(n)$.

Relations between the problems

- Hardness of the CDH problem relative to $\mathcal{G}$ implies hardness of the discrete-logarithm problem relative to $\mathcal{G}$.
- Hardness of the DDH problem relative to $\mathcal{G}$ implies hardness of the CDH problem relative to $\mathcal{G}$.

Relations between the problems

Via reduction, we can show that

- If there is an algorithm that solves discrete-logarithm problem relative to $\mathcal{G}$ (with some probability), then we can construct an algorithm for solving the CDH problem relative to $\mathcal{G}$.
- If there is an algorithm that solves CDH problem relative to $\mathcal{G}$, then we can construct an algorithm that solves the DDH problem relative to $\mathcal{G}$ (i.e., distinguishes g^{xy} from a uniform element $g^z \in \mathbb{G}$).

Exercise!

Groups with DLog/CDH/DDH hardness

- Large prime order subgroups of $\mathbb{Z}_p^*$, where p prime, are believed to be safe.

Theorem

Let $p = rq + 1$, where p, q prime. Then

$$\mathbb{G} \stackrel{def}{=} \{h^r \bmod p \mid h \in \mathbb{Z}_p^*\}$$

is a subgroup of $\mathbb{Z}_p^*$ of order q.

We usually select $r = 2$, i.e., we choose p, q primes such that $p = 2q + 1$.

End

References: Sec 8.1.1, 8.1.2, 8.1.3, 8.1.4, 8.3.1, 8.3.2, 8.3.3 (only the proofs in slides).