IERG5590: Advanced Blockchain **Spring 2020**

Notes 1: Mathematics for Cryptography

Instructor: Sherman S. M. Chow

1.1 Basic Number Theory

1.1.1 Modular Arithmetic

- Consider $\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}$ and $\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$.
- We say that "a is congruent to b modulo n", or $a \equiv b \pmod{n}$, if $a = nx + b$ for some $x \in \mathbb{Z}$.
- Usual arithmetic rules apply:
  1. $a \equiv a \pmod{n}$
  2. if $a \equiv b \pmod{n}$, then $b \equiv a \pmod{n}$
  3. if $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$, then $a \equiv c \pmod{n}$
  4. if $a \equiv b \pmod{n}$ and $c \equiv d$, then $a + c \equiv b + d \pmod{n}$ and $ac \equiv bd \pmod{n}$
  5. if $a \equiv b \pmod{n}$, then $a + c \equiv b + c \pmod{n}$ and $ac \equiv bc \pmod{n}$
  6. if $a \equiv b \pmod{n}$, then $a^k \equiv b^k \pmod{n}$ for all positive integer k
- Except:
  - if $ac \equiv bc \pmod{n}$, then $a \equiv b \pmod{n/d}$ where $d = \gcd(c, n)$

1.1.2 Euclidean Algorithm

Notations and Terminologies:

- The greatest common divisor (GCD) d of two integers a and b is the maximum of the integers that divides both a and b, denoted as $d = \gcd(a, b)$.
- The integers a and b are said to be *coprime* if $\gcd(a, b) = 1$.
- $a \mid b$ means "a divides b". $a \nmid b$ means "a does not divide b".

Lemma 1.1 *If $a = qb + r$, then $\gcd(a, b) = \gcd(b, r)$.*

Proof: Let $d = \gcd(a, b)$, then $d \mid a$ and $d \mid b$. Then $d \mid (r = a - qb)$. Suppose c is a common divisor of b and r, then $c \mid (a = qb + r)$. By definition of d, $c \leq d$. Therefore $d = \gcd(b, r)$. ■

Theorem 1.2 *For non-zero integers a and b, there exists integers x and y such that $\gcd(a, b) = ax + by$.*

Proof: We provide a constructive proof, *i.e.* we state the (extended) Euclidean algorithm which computes the GCD, x and y. Without loss of generality, assume $a > b > 0$. Compute the following:

$$\begin{array}{rcl} a = q_1 b + r_1 & & 0 < r_1 \le b \\ b = q_2 r_1 + r_2 & & 0 < r_2 \le r_1 \\ r_1 = q_3 r_2 + r_3 & & 0 < r_3 \le r_2 \\ \vdots & & \\ r_{n-2} = q_n r_{n-1} + r_n & & 0 < r_n < r_{n-1} \\ r_{n-1} = q_{n+1} r_n + 0 & & \end{array}$$

By Lemma **??**, $\gcd(a,b) = \gcd(b, r_1) = \ldots = \gcd(r_{n-1}, r_n) = \gcd(r_n, 0) = r_n$.

Now, we work backward from the second last equation.

$$\begin{aligned} r_n &= r_{n-2} - q_n r_{n-1} \\ &= (1 + q_n q_{n-1}) r_{n-2} + (-q_n) r_{n-3} \\ &= \ldots \\ &= ax + by \end{aligned}$$

■

Example 1.3 *Compute* $\gcd(360, 924)$.

$$\begin{aligned} 924 &= 2 \times 360 + 204 \\ 360 &= 1 \times 204 + 156 \\ 204 &= 1 \times 156 + 48 \\ 156 &= 3 \times 48 + 12 \\ 48 &= 4 \times 12 + 0 \end{aligned}$$

$$\begin{aligned} \gcd(360, 924) = 12 &= 156 - 3 \times 48 \\ &= 156 - 3 \times (204 - 156) \\ &= 4 \times 156 - 3 \times 204 \\ &= 4 \times (360 - 1 \times 204) - 3 \times 204 \\ &= 4 \times 360 - 7 \times 204 \\ &= 4 \times 360 - 7 \times (924 - 2 \times 360) \\ &= 18 \times 360 - 7 \times 924 \end{aligned}$$

1.1.3 Euler's Phi / Totient Function

Euler's totient function: $\phi(n) =$ "# of positive integers that are less than and coprime with n".

Properties: Let p be prime. Let m, n be positive integers such that $\gcd(m, n) = 1$.

- $\phi(p) = p - 1$
- $\phi(p^k) = p^{k-1}(p-1)$
- $\phi(mn) = \phi(m)\phi(n)$.

  Proof: Consider the following array:

$$\begin{array}{cccccc} 1 & 2 & \ldots & r & \ldots & m \\ m+1 & m+2 & & m+r & & 2m \\ 2m+1 & 2m+2 & & 2m+r & & 3m \\ \vdots & \vdots & & \vdots & & \vdots \\ (n-1)m+1 & (n-1)m+2 & & (n-1)m+r & & nm \end{array}$$

For each row, we know by Lemma **??** that $\gcd(km + r, m) = \gcd(r, m)$. Therefore there are exactly $\phi(m)$ columns in each row that are coprime with m. Now consider the r-th column, none of them are congruent to each other modulo n. Therefore they are congruent to $0, 1, \ldots, n-1$ in some order, and exactly $\phi(n)$ of them are coprime with n.

■

1.1.4 Fermat's Little Theorem and Euler's Generalization

Theorem 1.4 *(Fermat's Little Theorem) Let p be a prime and $p \nmid a$. Then $a^{p-1} \equiv 1 \pmod{p}$.*

Theorem 1.5 *(Euler's Generalization of Fermat's Little Theorem)*

If $n \geq 1$ and $\gcd(a, n) = 1$, then $a^{\phi(n)} \equiv 1 \pmod{n}$.

Proof: Let $a_1, a_2, \ldots, a_{\phi(n)}$ be positive integers that are less than and coprime with n. Since $\gcd(a, n) = 1$, $aa_1, aa_2, \ldots, aa_{\phi(n)}$ are congruent to $a_1, a_2, \ldots, a_{\phi(n)}$ in some order. Let $aa_i \equiv a'_i \pmod{n}$ for $i = 1, 2, \ldots, \phi(n)$. Then

$$\begin{aligned}(aa_1)(aa_2)\ldots(aa_{\phi(n)}) &\equiv a'_1 a'_2 \ldots a'_{\phi(n)} \pmod{n} \\ &\equiv a_1 a_2 \ldots a_{\phi(n)} \pmod{n}\end{aligned}$$

and so

$$a^{\phi(n)}(a_1 a_2 \ldots a_{\phi(n)}) \equiv a_1 a_2 \ldots a_{\phi(n)} \pmod{n}$$

Since $\gcd(a_i, n) = 1$ for all i, we have $\gcd(a_1 a_2 \ldots a_{\phi(n)}, n) = 1$. Therefore $a^{\phi(n)} \equiv 1 \pmod{n}$. ■

Definition 1.6 (Orders and Primitive Roots) *Given $a \in \mathbb{Z}$, let $k \leq \phi(n)$ be the smallest positive integer such that $a^k \equiv 1 \pmod{n}$. Then k is called the* order *of a. If a has the highest order, namely $\phi(n)$, then a is called a* primitive root *of n. A primitive root a* generates *all the integers less than and coprime with n by self multiplication.*

Example 1.7 3 *is a primitive root of* 7*.*

x	1	2	3	4	5	6
$3^x \pmod{7}$	3	2	6	4	5	1

1.1.5 Fast Exponentiation Algorithm

How to calculate $a^x \pmod{n}$ for large x, say $5^{110} \pmod{131}$?

1. Expand x in binary representation: $110 = 64 + 32 + 8 + 4 + 2$
2. Complete the following table by repeated squaring:

$$\begin{array}{ll} 5^2 \equiv 25 \pmod{131} & 5^4 \equiv 25^2 \equiv 101 \pmod{131} \\ 5^8 \equiv 101^2 \equiv 114 \pmod{131} & 5^{16} \equiv 114^2 \equiv 27 \pmod{131} \\ 5^{32} \equiv 27^2 \equiv 74 \pmod{131} & 5^{64} \equiv 74^2 \equiv 105 \pmod{131} \end{array}$$

3. $5^{110} = 5^{64+32+8+4+2} = 5^{64} \cdot 5^{32} \cdot 5^8 \cdot 5^4 \cdot 5^2 \equiv 105 \cdot 74 \cdot 114 \cdot 101 \cdot 25 \equiv 60 \pmod{131}$.

1.2 Basic Abstract Algebra

Definition 1.8 (Groups) *Let $\mathbb{G}$ be a set and "$\cdot$" be an operation defined over $\mathbb{G}$. $(\mathbb{G}, \cdot)$ or simply $\mathbb{G}$ is called a group if the following holds.*

1. *Closed: If $a, b \in \mathbb{G}$, then $a \cdot b \in \mathbb{G}$*
2. *Associative: If $a, b, c \in \mathbb{G}$, then $(a \cdot b) \cdot c = a \cdot (b \cdot c)$*
3. *Existence of Identity: $\exists\ e \in \mathbb{G}$ such that $a \cdot e = e \cdot a = a\ \forall\ a \in \mathbb{G}$*
4. *Existence of Inverses: If $a \in \mathbb{G}$, then $\exists\ a^{-1} \in \mathbb{G}$ such that $a \cdot a^{-1} = a^{-1} \cdot a = e$*

Furthermore, if $\mathbb{G}$ is commutative, i.e. "if $a, b \in \mathbf{G}$, then $a \cdot b = b \cdot a$", then $\mathbf{G}$ is said to be an Abelian group. If the number of elements in $\mathbb{G}$ is finite, $\mathbb{G}$ is said to be a finite group. In this case, the number of elements $|\mathbb{G}|$ is called the order of the group $\mathbb{G}$. Otherwise, $\mathbb{G}$ is said to be an infinite group.

Definition 1.9 (Cyclic Groups and Generators) *Let $\mathbb{G}$ be a finite group with order n and identity element $1_{\mathbb{G}}$. If there exists an element $g \in \mathbb{G}$ such that $\mathbb{G}$ can be written as $\{g, g^2, g^3, \ldots, g^n = 1_{\mathbb{G}}\}$, then $\mathbb{G}$ is said to be a cyclic group, and g is said to be a generator of $\mathbb{G}$.*

Example 1.10 *Let $n \in \mathbb{Z}$. $(\mathbb{Z}_n, +)$ is a cyclic group of order n, and any $g \in \mathbb{Z}_n^*$ is a generator of $\mathbb{Z}_n$. Furthermore, if $n = 2, 4, p^k$ or $2p^k$ for some odd prime p and positive integer k, then $(\mathbb{Z}_n^*, \times)$ is a cyclic group of order $\phi(n)$, and any primitive root of n is also a generator of $\mathbb{Z}_n^*$.*

Definition 1.11 (Rings) *Let $(R, +)$ be an Abelian group and "$\cdot$" be an additional operation defined over R. $(R, +, \cdot)$ or simply R is called a ring if the following holds.*

1. *Associative w.r.t. $\cdot$: If $a, b, c \in R$ then $(a \cdot b) \cdot c = a \cdot (b \cdot c)$*
2. *Existence of Identity w.r.t. $\cdot$: $\exists\ e \in R$ such that $a \cdot e = e \cdot a = a\ \forall\ a \in R$*
3. *Distributive w.r.t. $+$: If $a, b, c \in R$ then $(a + b) \cdot c = (a \cdot c) + (b \cdot c)$ and $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$*

Furthermore, if R is commutative w.r.t. $\cdot$, i.e."if $a, b \in R$, then $a \cdot b = b \cdot a$", then R is said to be a commutative ring.

Definition 1.12 (Fields) *A commutative ring $(\mathbb{F}, +, \cdot)$ is called a field if multiplicative inverses exist except for the additive identity.*

1.3 Computationally Hard Problems

Definition 1.13 (Discrete Logarithm Problem (DLP)) *Let $\mathbb{G}$ be a cyclic group of λ-bit long prime order p. Given $(g, y = g^x, p)$ where $g \in \mathbb{G}$ is a generator, and $1 \leq x \leq p$ is randomly chosen, find x.*

Definition 1.14 (RSA Problem) *Given a tuple (N, e, c), where $N = pq$ for some randomly chosen λ-bit long primes p and q, $e \leftarrow \mathbb{Z}^*\phi(n)$, and $c = m^e \pmod{n}$ for some $m \leftarrow \mathbb{Z}_n^*$, find m.*