MATH2081: Math for Computing
Lecturer: Dr. Nguyen Hieu Thao
Email: thao.nguyenhieu@rmit.edu.vn

RMIT UNIVERSITY

Lecture Notes 7: Number Theory

(2024A, Week 8, Monday, April 22, 10:30-12:00)[1]

Divisors and prime numbers

(a) Let n and d be integers, $d \neq 0$. We say that d **divides** n if there exists an integer q satisfying $n = dq$. We call q the **quotient** and d a **divisor** or **factor** of n. If d divides n, we write $d \mid n$. If d does not divide n, we write $d \nmid n$.

(b) An integer greater than 1 whose only positive divisors are itself and 1 is a **prime**.

(c) An integer greater than 1 that is not prime is a **composite**.

(d) Let m and n be integers with not both zero. A **common divisor** of m and n is an integer that divides both m and n. The **greatest common divisor** of m and n is denoted by $\texttt{gcd}(m, n)$.

(e) Two integers m and n are **relatively prime** if $\texttt{gcd}(m, n) = 1$.

(f) Let m and n be positive integers. A **common multiple** of m and n is an integer that is divisible by both m and n. The **least common multiple** of m and n, denoted by $\texttt{lcm}(m, n)$, is the smallest *positive* common multiple of m and n.

Theorems

(a) Let m, n and d be integers. If $d \mid m$ and $d \mid n$, then $d \mid (m + n)$ and $d \mid (m - n)$.

(b) The number of primes is infinite.

(c) A positive integer n greater than 1 is composite if and only if n has a divisor d satisfying $2 \leq d \leq \sqrt{n}$.

(d) **Fundamental theorem of arithmetic.** Any integer greater than 1 can be written as a product of primes. Moreover, if the primes are written in nondecreasing order, the factorization is unique. In symbols, if

$$n = p_1 p_2 \cdots p_i \ \text{ and } n = p'_1 p'_2 \cdots p'_j,$$

where p_k and p'_k are primes and

$$p_1 \leq p_2 \leq \cdots \leq p_i \ \text{ and } \ p'_1 \leq p'_2 \leq \cdots \leq p'_j,$$

then $i = j$ and

$$p_k = p'_k, \quad \forall k = 1, 2, \ldots, i.$$

[1] Most of the content of this document is taken from the book [1].

(e) Let m and n be integers, $m > 1$, $n > 1$, with prime factorizations

$$m = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k} \quad \text{and} \quad n = p_1^{b_1} p_2^{b_2} \cdots p_k^{b_k}.$$

If the prime p_i is not a factor of m, we let $a_i = 0$. Similarly, if the prime p_i is not a factor of n, we let $b_i = 0$. Then

$$\texttt{gcd}(m, n) = p_1^{\min(a_1,b_1)} p_2^{\min(a_2,b_2)} \cdots p_k^{\min(a_k,b_k)},$$

and

$$\texttt{lcm}(m, n) = p_1^{\max(a_1,b_1)} p_2^{\max(a_2,b_2)} \cdots p_k^{\max(a_k,b_k)}.$$

(f) For any positive integers m and n,

$$\texttt{gcd}(m, n) \cdot \texttt{lcm}(m, n) = mn.$$

(g) If a is a nonnegative integer, b is a positive integer, and $r = a \;\texttt{mod}\; b$, then

$$\texttt{gcd}(a, b) = \texttt{gcd}(b, r).$$

(h) If a and b are nonnegative integers, not both zero, there exist integers s and t such that

$$\texttt{gcd}(a, b) = sa + tb.$$

(i) For two integers $n > 0$ and $\varphi > 1$ with $\texttt{gcd}(n, \varphi) = 1$, there exists a unique integer s, $0 < s < \varphi$, such that $ns \;\texttt{mod}\; \varphi = 1$. We call s the **multiplicative inverse** of n modulo φ.

(j) If a, b, and z are positive integers,

$$ab \;\texttt{mod}\; z = [(a \;\texttt{mod}\; z)(b \;\texttt{mod}\; z)] \;\texttt{mod}\; z.$$

(k) (Fermat's theorem) If p is prime, then

$$a^{p-1} \equiv 1 \;\texttt{mod}\; p, \quad \forall a \in Z_p^*,$$

where $Z_p^* = \{1, 2, 3, \ldots, p-1\}$.

(l) If p, q are pairwise relatively prime and $n = pq$, then for all integers x and a,

$$x \equiv a \;\texttt{mod}\; p \;\text{ and }\; x \equiv a \;\texttt{mod}\; q \quad \Longleftrightarrow \quad x \equiv a \;\texttt{mod}\; n.$$

RSA public-key cryptosystems

1. Select at random two large prime numbers p and q, $p \neq q$.
2. Compute $n = pq$.
3. Select a small odd integer e that is relatively prime to $\phi(n) = (p-1)(q-1)$.
4. Compute d as the *multiplicative inverse* of e modulo $\phi(n)$.
5. Publish the pair $P = (e, n)$ as the participant's **RSA public key**.
6. Keep secret the pair $S = (d, n)$ as the participant's **RSA secret key**.

To encode/encrypt a message M associated with a public key $P = (e, n)$, compute

$$P(M) = M^e \bmod n, \quad \forall M \in Z_n.$$

To decode/decrypt a *ciphertext* C associated with a secret key $S = (d, n)$, compute

$$S(C) = C^d \bmod n, \quad \forall M \in Z_n.$$

Theorem. $S(P(M)) = P(S(M)) = M$ for all $M \in Z_n$.

Representations of integers

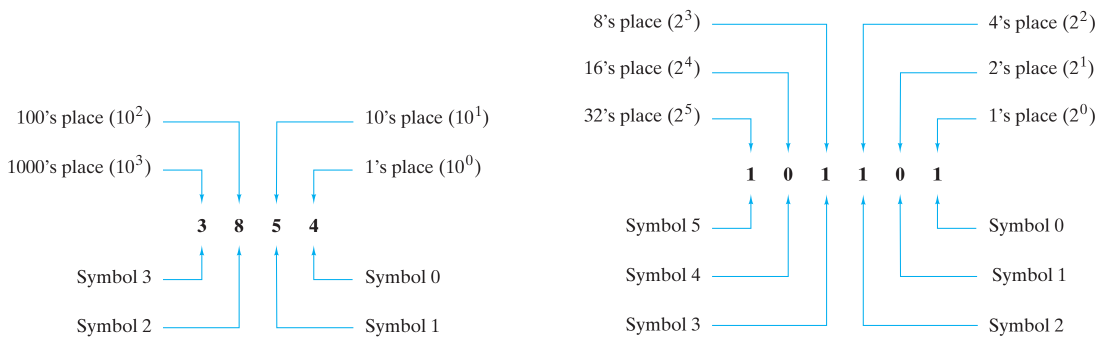

Figure 1: The decimal (left) and the binary (right) number systems.

A **bit** is a binary digit, that is, 0 or 1. In digital computers, data and instructions are encoded as bits. Technology determines how the bits are physically represented within a computer system. Hardware relies on the state of an electronic circuit to represent a bit. The circuit must be capable of being in two states - one representing 1, the other 0.

The **binary number system** represents integers using bits (0 and 1). Other important bases for number systems in computer science are base 8 (or **octal**) and base 16 (or **hexadecimal**). In the **hexadecimal number system**, to represent integers we use the symbols $0-9$, $A-F$. The symbols $A-F$ are interpreted as decimal $10-15$, respectively.

In general, in the **base N number system**, N distinct symbols, representing $0, 1, 2, \ldots, N-1$ are required. In representing an integer, reading from the right, the first symbol represents the number of 1 (i.e., N^0), the next symbol the number of N (i.e., N^1), the next symbol the number of N^2, and so on.

References

1. Johnsonbaugh, R.: Discrete Mathematics - Eighth Edition. *Pearson Education*, New York (2018).