Discrete Mathematics
Lec5: Number Theory

馬誠佑

- ***Number theory*** is the part of mathematics devoted to the study of the integers and their properties.
- Key ideas in number theory include divisibility and the primality of integers.
- Representations of integers, including binary and hexadecimal representations, are part of number theory.
- We'll use many ideas developed in Chapter 1 about proof methods and proof strategy in our exploration of number theory.

Division

- **Definition**: If a and b are integers with $a \neq 0$, then *a divides b* if there exists an integer c such that $b = ac$.
  - When a divides b we say that a is a *factor* or *divisor* of b and that b is a multiple of a.
  - The notation $a \mid b$ denotes that a divides b.
  - If $a \mid b$, then b/a is an integer.
  - If a does not divide b, we write $a \nmid b$.
- **Example**: Determine whether $3 \mid 7$ and whether $3 \mid 12$.

  $3|-12$?

  "b is even" $\equiv 2|b$.

  Is 0 even ?

  Is -4 even ?

Properties of Divisibility

Theorem 1: Let a, b, and c be integers, where $a \neq 0$.

i. If $a \mid b$ and $a \mid c$, then $a \mid (b + c)$; $a \mid (mb + nc)$, $\forall m, n \in Z$

ii. If $a \mid b$, then $a \mid bc$ for all integers c;

iii. If $a \mid b$ and $b \mid c$, then $a \mid c$.

Proof: (i) Suppose $a \mid b$ and $a \mid c$, then it follows that there are integers s and t with $b = as$ and $c = at$. Hence,

$b + c = as + at = a(s + t)$. Hence, $a \mid (b + c)$

(Exercises 3 and 4 ask for proofs of parts (ii) and (iii).)

Corollary: If a, b, and c be integers, where $a \neq 0$, such that $a \mid b$ and $a \mid c$, then $a \mid mb + nc$ whenever m and n are integers.

Can you show how it follows easily from (ii) and (i) of Theorem 1?

Division Algorithm

When an integer is **divided** by a **positive integer**, there is a quotient and a remainder. This is traditionally called the "Division Algorithm," but is really a theorem.

Division Algorithm: If a is an integer and d a positive integer, then there are unique integers q and r, with $0 \leq r < |d|$, such that $a = dq + r$ (*proved in Section* 5.2).

- d is called the *divisor*.
- a is called the *dividend*.
- q is called the *quotient*.
- r is called the *remainder*.

We can find q and r by:

$$q = \lfloor a/d \rfloor,$$
$$r = a - qd$$
$$where\ d \neq 0, r \in N$$

Definitions of Functions **div** and **mod**

$q = a$ **div** d

$r = a$ **mod** d

Examples:

- What are the quotient and remainder when 101 is divided by 11?
- **Solution**: The quotient when 101 is divided by 11 is 9 = 101 **div** 11, and the remainder is 2 = 101 **mod** 11. (101 = 11 x 9 + 2)
- What are the quotient and remainder when −11 is divided by 3?
- **Solution**: The quotient when −11 is divided by 3 is −4 = −11 **div** 3, and the remainder is 1 = −11 **mod** 3. (-11 = 3 x (-4) + 1)

The Mod Operator
(An integer "division remainder" operator)

Def : Let a, d∈ $Z\ with\ d > 1$. Then a mod d denotes the remainder r from the division "algorithm" with dividend *a* and divisor d; i.e. the remainder when *a* is divided by d.

- *We can compute (a mod d) by:* $a - d \cdot \left\lfloor \frac{a}{d} \right\rfloor$.
- In C programming language, "%"= mod.

Congruence Relation

Definition: If a and b are integers and m is a positive integer, then a is *congruent* to b *modulo* m if m divides $a - b$.

- The notation $a \equiv b \pmod{m}$ says that a is congruent to b modulo m.
- We say that $a \equiv b \pmod{m}$ is a *congruence* and that m is its *modulus.*
- Two integers are congruent mod m if and only if they have the same remainder when divided by m. $a \equiv b \pmod{m} \leftrightarrow m \mid a - b$
- If a is not congruent to b modulo m, we write $a \not\equiv b \pmod{m}$

Example: Determine whether 17 is congruent to 5 modulo 6 and whether 24 and 14 are congruent modulo 6.

Solution:

- $17 \equiv 5 \pmod{6}$ because 6 divides $17 - 5 = 12$.
- $24 \not\equiv 14 \pmod{6}$ since $24 - 14 = 10$ is not divisible by 6.

More on Congruences

Theorem 4: Let m be a positive integer. The integers a and b are congruent modulo m if and only if there is an integer k such that $a = b + km$.

Proof:

- If $a \equiv b \pmod{m}$, then (by the definition of congruence) $m \mid a - b$. Hence, there is an integer k such that $a - b = km$ and equivalently $a = b + km$.
- Conversely, if there is an integer k such that $a = b + km$, then $km = a - b$. Hence, $m \mid a - b$ and $a \equiv b \pmod{m}$.

The Relationship between (mod m) and **mod** m Notations

The use of "mod" in $a \equiv b \pmod{m}$ and $a \bmod m = b$ are different.

- $a \equiv b \pmod{m}$ is a relation on the set of integers.
- In $a \bmod m = b$, the notation **mod** denotes a function.

The relationship between these notations is made clear in this theorem.

Theorem 3: Let a and b be integers, and let m be a positive integer. Then $a \equiv b \pmod{m}$ if and only if $a \bmod m = b \bmod m$. (*Proof in the exercises*)

Useful Congruence Theorems

- $Let\ a, b \in Z\ and\ m \in Z^{+}. Then, a \equiv b (mod\ m) \leftrightarrow \exists k \in Z: a = b + km.$
- $Let\ a, b, c, d \in Z\ and\ m \in Z^{+}. Then, if\ a \equiv b\ mod\ m\ and\ c \equiv d\ mod\ m, we\ have$
  1. $a + c \equiv b + d (mod\ m)$
  2. $ac \equiv bd (mod\ m)$
  3. $a + b \equiv \big((a\ mod\ m) + (b\ mod\ m)\big) (mod\ m)$
  4. $ab \equiv ((a\ mod\ m)(b\ mod\ m)) (mod\ m)$

Pf: $a + c \equiv b + d(mod\ m)$

$$a \equiv b(mod\ m)$$
$$m|a - b \rightarrow a - b = mk_1$$
$$c \equiv d(mod\ m)$$
$$m|c - d \rightarrow c - d = mk_2$$
$$(a + c) - (b + d) = m(k_1 + k_2)$$
$$a + c \equiv b + d(mod\ m)$$

Pf: $ac \equiv bd(mod\ m)$

$$a = b + mk_1$$
$$c = d + mk_2$$
$$ac = (b + mk_1)(d + mk_2) = bd + mk_2b + mk_1\text{d+}m^2k_1\ k_2$$
$$ac - bd = m(\dots)$$

Pf: $a + b \equiv \big((a \bmod m) + (b \bmod m)\big) \pmod m$

$$a \equiv (a \bmod m) \pmod m$$
$$\text{b} \equiv (b \bmod m) \pmod m$$
$$a + b \equiv \big((a \bmod m) + (b \bmod m)\big) \pmod m$$

Pf: $ab \equiv ((a \bmod m)(b \bmod m)) \pmod m$

Example: Because 7 ≡ 2 (mod 5) and 11 ≡ 1 (mod 5) , it follows from 3 and 4 that

18 = 7 + 11 ≡ 2 + 1 = 3 (mod 5)

77 = 7 · 11 ≡ 2 · 1 = 2 (mod 5)

Algebraic Manipulation of Congruences

Multiplying both sides of a valid congruence by an integer preserves validity.

If $a \equiv b \pmod{m}$ holds then $c \cdot a \equiv c \cdot b \pmod{m}$, where c is any integer, holds by Theorem 2 with $d = c$.

Adding an integer to both sides of a valid congruence preserves validity.

If $a \equiv b \pmod{m}$ holds then $c + a \equiv c + b \pmod{m}$, where c is any integer, holds by Theorem 1 with $d = c$.

Dividing a congruence by an integer does not always produce a valid congruence.

Example: The congruence $14 \equiv 8 \pmod{6}$ holds. But dividing both sides by 2 does not produce a valid congruence since $14/2 = 7$ and $8/2 = 4$, but $7 \not\equiv 4 \pmod{6}$.

Arithmetic Modulo m 1

Definitions: Let $\mathbf{Z}_m$ be the set of nonnegative integers less than m: {0,1, …., $m-1$}

- The operation $+_m$ is defined as $a +_m b = (a + b)$ **mod** m. This is *addition modulo m*.
- The operation $\cdot_m$ is defined as $a \cdot_m b = (a \cdot b)$ **mod** m. This is *multiplication modulo m*.
- Using these operations is said to be doing *arithmetic modulo m*.

Example: Find $7 +_{11} 9$ and $7 \cdot_{11} 9$.

Solution: Using the definitions above:

- $7 +_{11} 9 = (7 + 9)$ **mod** $11 = 16$ **mod** $11 = 5$
- $7 \cdot_{11} 9 = (7 \cdot 9)$ **mod** $11 = 63$ **mod** $11 = 8$

Arithmetic Modulo m 2

The operations $+_m$ and $\cdot_m$ satisfy many of the same properties as ordinary addition and multiplication.

- *Closure*: If a and b belong to $\mathbf{Z}_m$, then $a +_m b$ and $a \cdot_m b$ belong to $\mathbf{Z}_m$.
- *Associativity*: If a, b, and c belong to $\mathbf{Z}_m$, then $(a +_m b) +_m c = a +_m (b +_m c)$ and $(a \cdot_m b) \cdot_m c = a \cdot_m (b \cdot_m c)$.
- *Commutativity*: If a and b belong to $\mathbf{Z}_m$, then $a +_m b = b +_m a$ and $a \cdot_m b = b \cdot_m a$.
- *Identity elements*: The elements 0 and 1 are identity elements for addition and multiplication modulo m, respectively.
  - If a belongs to $\mathbf{Z}_m$, then $a +_m 0 = a$ and $a \cdot_m 1 = a$.

Arithmetic Modulo m 3

- *Additive inverses*: If $a \neq 0$ belongs to $\mathbf{Z}_m$, then $m - a$ is the additive inverse of a modulo m and 0 is its own additive inverse.
  - $a +_m (m - a) = 0$ and $0 +_m 0 = 0$
- *Distributivity*: If a, b, and c belong to $\mathbf{Z}_m$, then
  - $a \cdot_m (b +_m c) = (a \cdot_m b) +_m (a \cdot_m c)$ and $(a +_m b) \cdot_m c = (a \cdot_m c) +_m (b \cdot_m c)$.

Exercises 42-44 ask for proofs of these properties.

Multiplicatative inverses have not been included since they do not always exist. For example, there is no multiplicative inverse of 2 modulo 6.

Prove the set of real number R is uncountable

Pf: (一個可數的集合他的任一子集合也是可數的)
(0,1)

$$r_1 = 0.d_{11}d_{12}d_{13}\ldots$$
$$r_2 = 0.d_{21}d_{22}d_{23}\ldots$$
$$r_3 = 0.d_{31}d_{32}d_{33}\ldots$$

$$r = 0.d_1d_2d_3\ldots$$
$$d_i = \begin{cases} 4, d_{ii} \neq 4 \\ 5, d_{ii} = 4 \end{cases}$$

Ex: $r_1 = 0.21354, r_2 = 0.24221$

$$a = bq + r$$

$$a \div b = q \ldots r$$

$$0 \leq r < |b|$$

Ex:

$$10 \div 2 = 5 \ldots 0$$

$$(11) \div 3 = 3 \ldots 2$$

$$(-11) \div 3 = -4 \ldots 1 \Rightarrow -11 = 3\,(-4) + 1$$

$$11 \div (-3) = \ \ldots \Rightarrow 11 = (-3) \times ? + ?$$

$$(-11) \div (-3) = \ \ldots \Rightarrow -11 = (-3) \times ? + ?$$

Prime

- $P \geq 2\ is\ a\ prime\ if\ the\ only\ factors\ of\ p\ are\ 1\ and\ p.$
- If $q \geq 2 \wedge q\ is\ not\ a\ prime, q\ is\ composite$（合數）.
- 1~100 的prime 記～！

TABLE 1 **The Sieve of Eratosthenes.**

Integers divisible by 2 other than 2 receive an underline.

1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

Integers divisible by 3 other than 3 receive an underline.

1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

Integers divisible by 5 other than 5 receive an underline.

1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

Integers divisible by 7 other than 7 receive an underline; integers in color are prime.

1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

Factoring

- 100 = 2 x 2 x 5 x 5 = $2^2 \times 5^2$
- $a = p_1^{n_1} p_2^{n_2} p_3^{n_3} \dots p_k^{n_k}$
- gcd(a,b) = max$\{m: m|a \wedge m|b\}$
- lcm(a,b) = min$\{m \in Z^+: a|m \wedge b|m\}$

- Theorem: If n is a composite integer, then n has a prime divisor less than or equal to $\sqrt{n}$.

Pf:

$\because n\ is\ composite\ \ \therefore n = pq, \mathrm{p} \leq \mathrm{q}\ \text{and}\ \mathrm{p}, \mathrm{q} > 1\ \text{and}\ \mathrm{p}, \mathrm{q}! = 1\ \text{or}\ \mathrm{n}$

$suppose\ p, q > \sqrt{n}$

$pq > \sqrt{n} \cdot \sqrt{n} = \mathrm{n}\ \text{contradiction !!!}$

$\therefore p, q$有一個小於等於$\sqrt{n}$

Representations of Integers

In the modern world, we use *decimal,* or *base* 10, *notation* to represent integers. For example when we write 965, we mean $9 \cdot 10^2 + 6 \cdot 10^1 + 5 \cdot 10^0$.

We can represent numbers using any base *b*, where *b* is a positive integer greater than 1.

The bases *b* = 2 (*binary*), *b* = 8 (*octal*) , and *b* = 16 (*hexadecimal*) are important for computing and communications

The ancient Mayans used base 20 and the ancient Babylonians used base 60.

Base *b* Representations

We can use positive integer *b* greater than 1 as a base, because of this theorem:

Theorem 1: Let $b \geq 2, \forall n \in Z^+$, it can be expressed uniquely in the form:

$$n = a_k b^k + a_{k-1} b^{k-1} + \ldots + a_1 b + a_0$$

where *k* is a nonnegative integer, $a_0, a_1, \ldots a_k$ are nonnegative integers less than *b*, and $a_k \neq 0$. The a_j, $j = 0,\ldots,k$ are called the base-*b* digits of the representation.
(We will prove this using mathematical induction in Section 5.1.)

The representation of n given in Theorem 1 is called the *base b expansion of n* and is denoted by $(a_k a_{k-1} \ldots a_1 a_0)_b$.

We usually omit the subscript 10 for base 10 expansions.

Binary Expansions

Most computers represent integers and do arithmetic with binary (base 2) expansions of integers. In these expansions, the only digits used are 0 and 1.

Example: What is the decimal expansion of the integer that has $(1\ 0101\ 1111)_2$ as its binary expansion?

Solution:

$(1\ 0101\ 1111)_2 = 1\cdot 2^8 + 0\cdot 2^7 + 1\cdot 2^6 + 0\cdot 2^5 + 1\cdot 2^4 + 1\cdot 2^3 + 1\cdot 2^2 + 1\cdot 2^1 + 1\cdot 2^0 = 351.$

Example: What is the decimal expansion of the integer that has $(11011)_2$ as its binary expansion?

Solution: $(11011)_2 = 1\cdot 2^4 + 1\cdot 2^3 + 0\cdot 2^2 + 1\cdot 2^1 + 1\cdot 2^0 = 27.$

Octal Expansions

The octal expansion (base 8) uses the digits {0,1,2,3,4,5,6,7}.

Example: What is the decimal expansion of the number with octal expansion $(7016)_8$?

Solution: $7 \cdot 8^3 + 0 \cdot 8^2 + 1 \cdot 8^1 + 6 \cdot 8^0 = 3598$

Example: What is the decimal expansion of the number with octal expansion $(111)_8$?

Solution: $1 \cdot 8^2 + 1 \cdot 8^1 + 1 \cdot 8^0 = 64 + 8 + 1 = 73$

Hexadecimal Expansions

The hexadecimal expansion needs 16 digits, but our decimal system provides only 10. So letters are used for the additional symbols. The hexadecimal system uses the digits {0,1,2,3,4,5,6,7,8,9,A,B,C,D,E,F}. The letters A through F represent the decimal numbers 10 through 15.

Example: What is the decimal expansion of the number with hexadecimal expansion $(2AE0B)_{16}$?

Solution:

$2\cdot16^4 + 10\cdot16^3 + 14\cdot16^2 + 0\cdot16^1 + 11\cdot16^0 = 175627$

Example: What is the decimal expansion of the number with hexadecimal expansion $(E5)_{16}$?

Solution: $14\cdot16^1 + 5\cdot16^0 = 224 + 5 = 229$

Base Conversion 1

To construct the base b expansion of an integer n:

- Divide n by b to obtain a quotient and remainder.
  $n = bq_0 + a_0 \quad 0 \le a_0 \le b$
- The remainder, a_0, is the rightmost digit in the base b expansion of n. Next, divide q_0 by b.
  $q_0 = bq_1 + a_1 \quad 0 \le a_1 \le b$
- The remainder, a_1, is the second digit from the right in the base b expansion of n.
- Continue by successively dividing the quotients by b, obtaining the additional base b digits as the remainder. The process terminates when the quotient is 0.

Algorithm: Constructing Base b Expansions

procedure *base b expansion*(n, b: positive integers with $b > 1$)

$q := n$

$k := 0$

while ($q \neq 0$)

$a_k := q$ **mod** b

$q := \lfloor q / b \rfloor$

$k := k + 1$

return($a_{k-1}, \ldots, a_1, a_0$){$(a_{k-1} \ldots a_1 a_0)_b$ is base b expansion of n}

q represents the quotient obtained by successive divisions by b, starting with $q = n$.

The digits in the base b expansion are the remainders of the division given by q **mod** b.

The algorithm terminates when $q = 0$ is reached.

Example (From decimal expansion to non-decimal expansiion)

$$
\begin{aligned}
139 &= 34 \times 4 + 3 \\
&= (8 \times 4 + 2) \times 4 + 3 \\
&= 8 \times 4^2 + 2 \times 4 + 3 \\
&= (2 \times 4 + 0) \times 4^2 + 2 \times 4 + 3 \\
&= 2 \times 4^3 + 0 \times 4^2 + 2 \times 4 + 3 \\
&= (2023)_4
\end{aligned}
$$

Comparison of Hexadecimal, Octal, and Binary Representations

TABLE 1 Hexadecimal, Octal, and Binary Representation of the Integers 0 through 15.

Decimal	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Hexadecimal	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
Octal	0	1	2	3	4	5	6	7	10	11	12	13	14	15	16	17
Binary	0	1	10	11	100	101	110	111	1000	1001	1010	1011	1100	1101	1110	1111

Initial 0s are not shown

Each octal digit corresponds to a block of 3 binary digits.

Each hexadecimal digit corresponds to a block of 4 binary digits.

So, conversion between binary, octal, and hexadecimal is easy.

Conversion Between Binary, Octal, and Hexadecimal Expansions

Example: Find the octal and hexadecimal expansions of $(11\ 1110\ 1011\ 1100)_2$.

Solution:

- To convert to octal, we group the digits into blocks of three $(011\ 111\ 010\ 111\ 100)_2$, adding initial 0s as needed. The blocks from left to right correspond to the digits 3,7,2,7, and 4. Hence, the solution is $(37274)_8$.
- To convert to hexadecimal, we group the digits into blocks of four $(0011\ 1110\ 1011\ 1100)_2$, adding initial 0s as needed. The blocks from left to right correspond to the digits 3,E,B, and C. Hence, the solution is $(3EBC)_{16}$.

Binary Addition of Integers

Algorithms for performing operations with integers using their binary expansions are important as computer chips work with binary numbers. Each digit is called a *bit*.

procedure *add*(a, b: positive integers)
{the binary expansions of a and b are $(a_{n-1},a_{n-2},\ldots,a_0)_2$ and $(b_{n-1},b_{n-2},\ldots,b_0)_2$, respectively}
    $c := 0$
    for $j := 0$ to $n - 1$
        $d := \lfloor (a_j + b_j + c)/2 \rfloor$
        $s_j := a_j + b_j + c - 2d$
        $c := d$
    $s_n := c$
    return$(s_0,s_1,\ldots, s_n)$ {the binary expansion of the sum is $(s_n,s_{n-1},\ldots,s_0)_2$}

The number of additions of bits used by the algorithm to add two n-bit integers is $O(n)$.

EXAMPLE 8 Add $a = (1110)_2$ and $b = (1011)_2$.

Solution: Following the procedure specified in the algorithm, first note that

$$a_0 + b_0 = 0 + 1 = 0 \cdot 2 + 1,$$

so that $c_0 = 0$ and $s_0 = 1$. Then, because

$$a_1 + b_1 + c_0 = 1 + 1 + 0 = 1 \cdot 2 + 0,$$

it follows that $c_1 = 1$ and $s_1 = 0$. Continuing,

$$a_2 + b_2 + c_1 = 1 + 0 + 1 = 1 \cdot 2 + 0,$$

so that $c_2 = 1$ and $s_2 = 0$. Finally, because

$$a_3 + b_3 + c_2 = 1 + 1 + 1 = 1 \cdot 2 + 1,$$

follows that $c_3 = 1$ and $s_3 = 1$. This means that $s_4 = c_3 = 1$. Therefore, $s = a + b = (1\ 1001)_2$. This addition is displayed in Figure 1, where carries are shown in color. ◀

$$\begin{array}{r} \textit{1}\ \ \textit{1}\ \ \textit{1} \\ 1\ 1\ 1\ 0 \\ +\ 1\ 0\ 1\ 1 \\ \hline 1\ 1\ 0\ 0\ 1 \end{array}$$

Binary Multiplication of Integers

Algorithm for computing the product of two n bit integers.

procedure multiply(a, b: positive integers)
{the binary expansions of a and b are $(a_{n-1},a_{n-2},\ldots,a_0)_2$ and $(b_{n-1},b_{n-2},\ldots,b_0)_2$, respectively}
  for $j := 0$ to $n - 1$
    if $b_j = = 1$ **then** c_j = a left shifted j places
    else $c_j := 0$ {$c_o,c_1,\ldots, c_{n-1}$ are the partial products}
$p := 0$
for $j := 0$ to $n - 1$
  p **:=** $p + c_j$
return p {p is the value of ab}

The number of additions of bits used by the algorithm to multiply two n-bit integers is $O(n^2)$.

EXAMPLE 10 Find the product of $a = (110)_2$ and $b = (101)_2$.

Solution: First note that

$$ab_0 \cdot 2^0 = (110)_2 \cdot 1 \cdot 2^0 = (110)_2,$$

$$ab_1 \cdot 2^1 = (110)_2 \cdot 0 \cdot 2^1 = (0000)_2,$$

and

$$ab_2 \cdot 2^2 = (110)_2 \cdot 1 \cdot 2^2 = (11000)_2.$$

To find the product, add $(110)_2$, $(0000)_2$, and $(11000)_2$. Carrying out these additions (using Algorithm 2, including initial zero bits when necessary) shows that $ab = (1\ 1110)_2$. This multiplication is displayed in Figure 2. ◀

```
    1 1 0
  × 1 0 1
  -------
    1 1 0
  0 0 0
1 1 0
-------
1 1 1 1 0
```

GURE 2

Euclidean Algorithm[1]

The Euclidian algorithm is an efficient method for computing the greatest common divisor of two integers. It is based on the idea that gcd(a,b) is equal to gcd(b,c) when $a > b$ and c is the remainder when a is divided by b.

Euclid
(325 B.C.E. – 265 B.C.E.)

Example: Find gcd(91, 287):

- $287 = 91 \cdot 3 + 14$
- $91 = 14 \cdot 6 + 7$
- $14 = 7 \cdot 2 + 0$

Divide 287 by 91

Divide 91 by 14

Divide 14 by 7

Stopping condition

gcd(287, 91) = gcd(91, 14) = gcd(14, 7) = 7

Correctness of Euclidean Algorithm[1]

Lemma 1: Let $a = bq + r$, where a, b, q, and r are integers. Then gcd(a,b) = gcd(b,r).

Proof:

- If c is a common divisor of a and b, then c is also a common divisor of b and r.

$$\because r = a - bq \; and \; c|a \wedge c|b \; \therefore c|a - bq \; i.e. c|r$$

- If c is a common divisor of b and r, then c is also a common divisor of a and b.

$$\because a = bq + r \; and \; c|b \wedge c|r \; \therefore c|bq + r \; i.e. c|a$$

- Therefore, gcd(a,b) = gcd(b,r).

Ex: gcd(528, 30) = gcd(30, 18) = gcd(18,12) = gcd(6,0) = 6

Euclidean Algorithm 2

The Euclidean algorithm expressed in pseudocode is:

```
procedure gcd(a, b: positive integers)
x := a
y := b
while   y ≠ 0
        r := x mod y
        x := y
        y := r
return x {gcd(a,b) is x}
```

In Section 5.3, we'll see that the time complexity of the algorithm is $O(\log b)$, where $a > b$.

gcds as Linear Combinations

Étienne Bézout

(1730-1783)

Bézout's Theorem: If a and b are positive integers, then there exist integers s and t such that $\gcd(a,b) = sa + tb$.

(*proof in exercises of Section* 5.2)

Definition: If a and b are positive integers, then integers s and t such that $\gcd(a,b) = sa + tb$ are called *Bézout coefficients* of a and b. The equation $\gcd(a,b) = sa + tb$ is called *Bézout's identity.*

By Bézout's Theorem, the gcd of integers a and b can be expressed in the form $sa + tb$ where s and t are integers. This is a *linear combination* with integer coefficients of a and b.

- $\gcd(6,14) = (-2)\cdot 6 + 1\cdot 14$

Example: Reverse the Euclidean Algorithm

gcd(528, 35) = gcd(35,3) $\quad\quad$ 3 = 528-15 x 35

= gcd(3,2) $\quad\quad$ 2 = 35 – 11 x 3

= gcd(2,1) $\quad\quad$ 1 = 3-1x2

= 1

Then, reverse the process.

1 = 3-1x2 = 3- (35-11x 3)

= 12 x 3 - 35 = 12 x (528 – 15 x 35) – 35

= 12 x 528 – 181 x 35 = 12 x 528 – 181 x 35

Theorem

$$a, b, c \in Z^{+}. If \gcd(a, b) = 1 \; and \; a|bc, then \; a|c$$

Pf:

$$\because \gcd(a, b) = 1 \therefore \exists s, t \; s.t. \; sa + tb = 1.$$

We have (sa+tb)x c = sac + tbc = c.

$$\because a|sac \wedge a|tbc \therefore a|sac + tbc \;\; i.e. a|c$$

Theorem:

If p is a prime and $p|a_1 \cdot a_2 \cdot \cdots \cdot a_n where \; a_1 \cdot \; a_2 \cdot \; \cdot \; \cdot a_n \in Z, then \; p| \; a_i \; for \; some \; i.$

Theorem (Cancellation Rule)

$$m \in Z^+, a, b, c \in Z.$$

$$If\ ac \equiv bc(mod\ m) \wedge \gcd(c, m) = 1, then\ a \equiv b(mod\ m)$$

Pf:

$$\because ac \equiv bc(mod\ m)\ \therefore m|ac - bc\ i.e. m|(a - b) \cdot c$$

$$\because \gcd(c, m) = 1\ \therefore m|a - b\ i.e.\ a \equiv b(mod\ m)$$

Theorem

$$If\ \gcd(a,m) = 1\ and\ m > 1, then\ an\ inverse\ of\ a\ modulo\ m\ exists.$$
$$Furthermore, this\ inverse\ is\ unique\ modulo\ m.$$
$$In\ other\ words, there\ exists\ a\ unique\ s\ modulo\ m\ such\ that$$
$$sa \equiv 1\ mod\ m. In\ addition, we\ denote\ a^{-1} \equiv s(mod\ m).$$

Pf:

$\because \gcd(a,m) = 1 \therefore \exists s,t\ s.t.\ sa + tm \equiv 1(mod\ m)$

$$sa \equiv 1\ (mod\ m)$$
$$(a^{-1})a \equiv 1\ (mod\ m)$$

$\gcd(a,m) = 1\ \exists b\ \text{s.t.}\ ab \equiv 1\ (mod\ m) \Rightarrow$

$$b \equiv a^{-1}(\ mod\ m)$$
$$a \equiv b^{-1}\ (mod\ m)$$

Example

Given a = 5, m=3 ∵ $\gcd(a, m) = 1$ 求s 使得 $sa \equiv 1 \ (mod\ m)$

$$sa + tm = 1$$

gcd(5,3) = gcd(3,2). $2 = 5 - 1 \times 3$

=gcd(2,1) $1 = 3 - 1x2$

Ex: 5 x a^{-1} mod 3 = 5 x 2 mod 3 = 1

1= 3-1x2 = 3-1 x (5 – 1x3) = 2x3 -1 x5

$(a^{-1}) \equiv -1 \ (mod\ 3) \equiv 2 \ (mod\ 3)$

Example Finding Inverses 2

Example: Find an inverse of 101 modulo 4620.

Solution: First use the Euclidian algorithm to show that gcd(101,4620) = 1.

$4620 = 45 \cdot 101 + 75$

$101 = 1 \cdot 75 + 26$

$75 = 2 \cdot 26 + 23$

$26 = 1 \cdot 23 + 3$

$23 = 7 \cdot 3 + 2$

$3 = 1 \cdot 2 + 1$

$2 = 2 \cdot 1$

Since the last nonzero remainder is 1, gcd(101,4620) = 1

Working Backwards:

$1 = 3 - 1 \cdot 2$

$1 = 3 - 1 \cdot (23 - 7 \cdot 3) = -1 \cdot 23 + 8 \cdot 3$

$1 = -1 \cdot 23 + 8 \cdot (26 - 1 \cdot 23) = 8 \cdot 26 - 9 \cdot 23$

$1 = 8 \cdot 26 - 9 \cdot (75 - 2 \cdot 26) = 26 \cdot 26 - 9 \cdot 75$

$1 = 26 \cdot (101 - 1 \cdot 75) - 9 \cdot 75$

$= 26 \cdot 101 - 35 \cdot 75$

$1 = 26 \cdot 101 - 35 \cdot (4620 - 45 \cdot 101)$

$= -35 \cdot 4620 + 1601 \cdot 101$

Bézout coefficients : – 35 and 1601

1601 is an inverse of 101 modulo 4620

The Chinese Remainder Theorem[1]

In the first century, the Chinese mathematician Sun-Tsu asked:

There are certain things whose number is unknown. When divided by 3, the remainder is 2; when divided by 5, the remainder is 3; when divided by 7, the remainder is 2. What will be the number of things?

This puzzle can be translated into the solution of the system of congruences:

$x \equiv 2 \pmod 3$,

$x \equiv 3 \pmod 5$,

$x \equiv 2 \pmod 7$?

We'll see how the theorem that is known as the *Chinese Remainder Theorem* can be used to solve Sun-Tsu's problem.

The Chinese Remainder Theorem 2

Theorem 2: (*The Chinese Remainder Theorem*) Let $m_1, m_2, \ldots, m_n$ be pairwise relatively prime positive integers greater than one and $a_1, a_2, \ldots, a_n$ arbitrary integers. Then the system

$x \equiv a_1 \pmod{m_1}$

$x \equiv a_2 \pmod{m_2}$

.

.

.

$x \equiv a_n \pmod{m_n}$

has a unique solution modulo $m = m_1 m_2 \cdots m_n$.

(That is, there is a solution x with $0 \leq x < m$ and all other solutions are congruent modulo m to this solution.)

Proof: We'll show that a solution exists by describing a way to construct the solution. Showing that the solution is unique modulo m is Exercise 30.

Example

$$\begin{cases} x \equiv 1 \, mod \, 3 \\ x \equiv 2 \, mod \, 5 \end{cases}$$

$$x = 7 + 15k, k \in Z$$

$$x \equiv 7 \, mod \, 15$$

$$\begin{cases} x \equiv 1 \, mod \, 3 \\ x \equiv 2 \, mod \, 5 \\ x \equiv 3 \, mod \, 7 \end{cases}$$

$$x \equiv ? \, mod \, 3 \times 5 \times 7 \Rightarrow m = m_1 \times m_2 \times m_3$$

$$M_i \; i = 1,2,3$$

$$M_1 = \frac{m}{m_1} = 35$$

$$M_2 = \frac{m}{m_2} = 21$$

$$M_3 = \frac{m}{m_3} = 15$$

$$y_i, i = 1,2,3$$

$$M_1 y_1 \equiv 1 \, mod \, m_1$$

$$M_2 y_2 \equiv 1 \, mod \, m_2$$

$$M_3 y_3 \equiv 1 \, mod \, m_3$$

=>

$$35 y_1 \equiv 1 \, mod \, 3$$

$$21 y_2 \equiv 1 \, mod \, 5$$

$$15 y_3 \equiv 1 \, mod \, 7$$

$$y_1 = 2$$

$$y_2 = 1$$

$$y_3 = 1$$

$$x \equiv \sum_{i=1}^{3} a_i \, M_i y_i \; (mod \, 105)$$

$$\equiv 1 \times 35 \times 2 + 2 \times 21 \times 1 + 3 \times 15 \times 1 \equiv 157$$

$$(\text{mod } 105) \equiv 52 \; (mod \; 105)$$

The Chinese Remainder Theorem 3

To construct a solution first let $M_k = m/m_k$ for $k = 1,2,\ldots,n$ and $m = m_1 m_2 \cdots m_n$.
Since $\gcd(m_k, M_k) = 1$, by Theorem 1, there is an integer y_k, an inverse of M_k modulo m_k, such that

$$M_k\, y_k \equiv 1 \pmod{m_k}.$$

Form the sum

$$x = a_1 M_1 y_1 + a_2 M_2 y_2 + \cdots + a_n M_n y_n .$$

Note that because $M_j \equiv 0 \pmod{m_k}$ whenever $j \neq k$, all terms except the kth term in this sum are congruent to 0 modulo m_k.
Because $M_k\, y_k \equiv 1 \pmod{m_k}$, we see that $x \equiv a_k M_k y_k \equiv a_k \pmod{m_k}$, for $k = 1,2,\ldots,n$.
Hence, x is a simultaneous solution to the n congruences.

$$x \equiv a_1 \pmod{m_1}$$
$$x \equiv a_2 \pmod{m_2}$$
$$\vdots$$
$$x \equiv a_n \pmod{m_n}$$

The Chinese Remainder Theorem

Example: Consider the 3 congruences from Sun-Tsu's problem:

$x \equiv 2 \pmod 3$, $x \equiv 3 \pmod 5$, $x \equiv 2 \pmod 7$.

- Let $m = 3 \cdot 5 \cdot 7 = 105$, $M1 = m/3 = 35$, $M3 = m/5 = 21$, $M3 = m/7 = 15$.
- We see that
  - 2 is an inverse of $M1 = 35$ modulo 3 since $35 \cdot 2 \equiv 2 \cdot 2 \equiv 1 \pmod 3$
  - 1 is an inverse of $M2 = 21$ modulo 5 since $21 \equiv 1 \pmod 5$
  - 1 is an inverse of $M3 = 15$ modulo 7 since $15 \equiv 1 \pmod 7$
- Hence,
  $x = a1M1y1 + a2M2y2 + a3M3y3$
  $= 2 \cdot 35 \cdot 2 + 3 \cdot 21 \cdot 1 + 2 \cdot 15 \cdot 1 = 233 \equiv 23 \pmod{105}$
- We have shown that 23 is the smallest positive integer that is a simultaneous solution. Check it!

Example

Find the solution of the system

$$x \equiv 2(mod\ 3)$$
$$x \equiv 3(mod\ 5)$$
$$x \equiv 2(mod\ 15)$$

Sol:

$$x \equiv 2\ mod\ 15 \equiv \begin{cases} \cancel{x \equiv 2\ (mod\ 3)} \\ x \equiv 2\ (mod\ 5) \end{cases}$$

Contradiciton!! 無解

Fermat's Little Theorem

Theorem 3: (*Fermat's Little Theorem*) If p is prime and a is an integer not divisible by p, then $a^{p-1} \equiv 1 \pmod{p}$

Furthermore, for every integer a we have $a^p \equiv a \pmod{p}$

(*proof outlined in Exercise 19*)

Pierre de Fermat
(1601-1665)

Fermat's little theorem is useful in computing the remainders modulo p of large powers of integers.

Example: Find 7^{222} **mod** 11.

By Fermat's little theorem, we know that $7^{10} \equiv 1 \pmod{11}$, and so $(7^{10})^k \equiv 1 \pmod{11}$, for every positive integer k. Therefore,

$$7^{222} = 7^{22 \cdot 10 + 2} = (7^{10})^{22} 7^2 \equiv (1)^{22} \cdot 49 \equiv 5 \pmod{11}.$$

Hence, 7^{222} **mod** 11 = 5.

Hashing Functions

Definition: A *hashing function h* assigns memory location $h(k)$ to the record that has k as its key.

- A common hashing function is $h(k) = k \bmod m$, where m is the number of memory locations.
- Because this hashing function is onto, all memory locations are possible.

Example: Let $h(k) = k \bmod 111$. This hashing function assigns the records of customers with social security numbers as keys to memory locations in the following manner:

h(064212848) = 064212848 **mod** 111 = 14

h(037149212) = 037149212 **mod** 111 = 65

h(107405723) = 107405723 **mod** 111 = 14, but since location 14 is already occupied, the record is assigned to the next available position, which is 15.

The hashing function is not one-to-one as there are many more possible keys than memory locations. When more than one record is assigned to the same location, we say a *collision* occurs. Here a collision has been resolved by assigning the record to the first free location.

For collision resolution, we can use a *linear probing function*:
$h(k,i) = (h(k) + i) \bmod m$, where i runs from 0 to $m - 1$.

There are many other methods of handling with collisions. You may cover these in a later CS course.

RSA Systems

- Choose two large prime p and q
  - $n = pq: modulus$
  - $e: encryption\ key\ (public\ key) which\ is\ coprime\ to\ (p-1)(q-1)$
  - d: $decryption\ key\ (private\ key)\ such\ that\ d = e^{-1} \equiv 1\ mod\ (p-1)(q-1)$
- M: message
- RSA encryption:
  - $C \equiv M^e\ mod\ n: ciphertext\ (the\ encrypted\ message)$
- RSA decryption:
  - M≡ $C^d\ mod\ n$

Example

Here is an example of RSA

- Let p =43, q = 59, and n = pq = 2537
- Choose e = 13 and d = 937
  - gcd(13, (p-1)(q-1)) = gcd(13, 42 x 58) = 1
  - $d = e^{-1}$ mod (p-1)(q-1)
- Assume M = 1819
- Encryption: $C \equiv M^e \; mod \; n$
  - $C = 1819^{13} \; mod \; 2537 = 2081$
- Decryption: $M \equiv C^d \; mod \; n$
- $M = 2081^{937} \; mod \; 2537 = 1819$