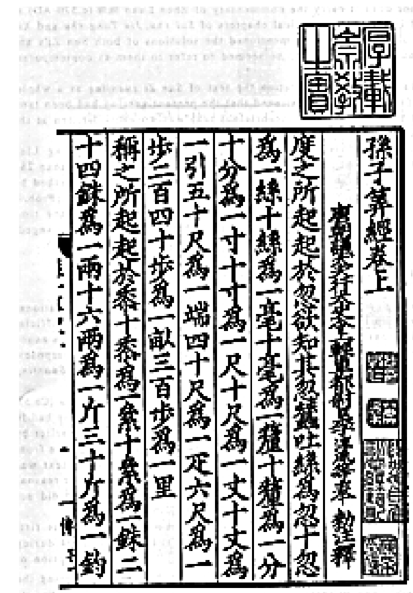
# Part II: Number Theory



孫子算經卷上

度之所起起於忽欲知其忽蠶吐絲爲忽十忽
爲一絲十絲爲一毫十毫爲一氂十氂爲一分
十分爲一寸十寸爲一尺十尺爲一丈十丈爲
一引五十尺爲一端四十尺爲一疋六尺爲一
步二百四十步爲一畝三百步爲一里
稱之所起起於黍十黍爲一絫十絫爲一銖二
十四銖爲一兩十六兩爲一斤三十斤爲一鈞

- Number theory is the part of mathematics devoted to the study of the integers and their properties.
- Number theory has a long history.
  - E.g.: Chinese Remainder Theorem 1700 years old
- For a long time, it had been regarded as pure mathematics and useless.
  - G. H. Hardy (prominent British mathematician): Pure mathematics is “beautiful” and “useless”. Applied mathematics is “trivial”, “ugly”, and “dull”
- However, number theory has found numerous applications in computer science in recent decades.

# L05: Modular Arithmetic

- **Divisibility**
- Modular Arithmetic
- Congruences
- Applications of Modular Arithmetic

- Reading: Rosen 4.1, 4.5

# Divisibility

- **Definition**:
  Let $a$ and $b$ be integers with $a \neq 0$. Then $a$ divides $b$ if there exists an integer $c$ such that $b = ac$.
  - 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 $a \nmid b$.
- When $a$ divides $b$ we say that $a$ is a factor or divisor of $b$ and that $b$ is a multiple of $a$.
- **Example**:
  Determine whether $3 \mid 7$ and whether $3 \mid 12$.

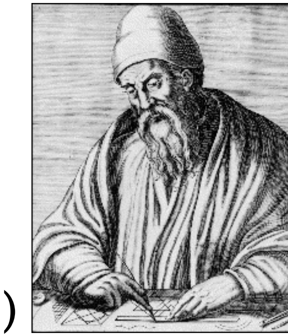
# Properties of Divisibility

- **Theorem:**
  Let $a$, $b$, and $c$ be integers, where $a \neq 0$.
  i. If $a \mid b$ and $a \mid c$, then $a \mid (b + c)$;
  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,
  $$b + c = as + at = a(s + t)$$
  Therefore, $a \mid (b + c)$.
- Proofs for (ii) and (iii) are left as exercises.

# Example

- **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.
- **Proof:**
  By (ii) of the theorem, we have $a \mid mb$ and $a \mid nc$.
  By (i) of the theorem, we have $a \mid mb + nc$.

# Euclid's Division Theorem



Euclid
(325 B.C.E. – 265 B.C.E.)

- **Theorem:**
  For any $a \in \mathbf{Z}, d \in \mathbf{Z}^+$, there exist unique integers $q$ and $r$, with $0 \le r < d$, such that $a = dq + r$.
  - $d$ is called the divisor.
  - $a$ is called the dividend.
  - $q$ is called the quotient.
  - $r$ is called the remainder.
- Examples
  - $11 \operatorname{div} 3 = 3, \;\; 11 \bmod 3 = 2.$
  - $-11 \operatorname{div} 3 = -4, \;\; -11 \bmod 3 = 1.$

Notation:

$$q = a \operatorname{div} d$$
$$r = a \bmod d$$

# Proof of Existence

- Let $S = \{x \mid x = a - dq, x \geq 0, q \in \mathbf{Z}\}$.
  - Note: The set is nonempty since $-dq$ can be made as large as needed.
- Let $r$ be the smallest integer in $S$. By the definition of $S$, there is a $q \in \mathbf{Z}$ such that
$$r = a - dq$$
- By the definition of $S$, we have $r \geq 0$.
- We must also have $r < d$. If not, then there would be a smaller nonnegative integer in $S$, which is
$$a - d(q+1) = a - dq - d = r - d > 0$$
- We will see an alternative proof by induction later.

# Proof of Uniqueness

- Suppose there are $q_1, r_1, q_2, r_2$ such that
$$a = dq_1 + r_1 \quad (1)$$
$$a = dq_2 + r_2 \quad (2)$$
$$0 \leq r_1 < d$$
$$0 \leq r_2 < d$$
- $(1) - (2)$:
$$0 = d(q_1 - q_2) + (r_1 - r_2)$$
$$d(q_1 - q_2) = r_2 - r_1$$
- So, $d \mid (r_2 - r_1)$
- Since $-d < r_2 - r_1 < d$ and $d \mid (r_2 - r_1)$, we must have $r_2 - r_1 = 0$, so $r_1 = r_2$ and thus $q_1 = q_2$ too.

# Outline

- Divisibility
- **Modular Arithmetic**
- Congruences
- Applications of Modular Arithmetic

# Modular Arithmetic

- **Lemma**
  For any $a, k \in \mathbf{Z}, m \in \mathbf{Z}^+$, $a \bmod m = (a + km) \bmod m$.
- **Proof**
  - By Euclid's Division Theorem, there exist unique $q, r, 0 \le r < m$, s.t.
  $$a = mq + r \qquad (1)$$
  - Similarly, there exist unique $q', r', 0 \le r' < m$, s.t.
  $$a + km = mq' + r' \qquad (2)$$
  - Adding $km$ to both sides of (1):
  $$a + km = m(q + k) + r$$
  - By the uniqueness in Division Theorem, we have
  $$r = r'$$
  - By definition of mod, $a \bmod m = (a + km) \bmod m$.

# Modular Arithmetic

- **Example**
  Prove the property
  $$(a \bmod mn) \bmod n = a \bmod n$$
- **Proof**:
  - $a = qmn + s, \; 0 \le s < mn$
  - $s = pn + r, 0 \le r < n$
  - Then, $(a \bmod mn) \bmod n = r$
  - On the other hand
    $$a = (qm + p)n + r,$$
  - So, $a \bmod n = r$
  - The equation is proved.

# Modular Arithmetic

- **Theorem**
  For any $a, k \in \mathbf{Z}, m \in \mathbf{Z}^+$,
  $$(a + b) \bmod m = \big((a \bmod m) + (b \bmod m)\big) \bmod m$$
- **Proof**:
  - By Euclid's Division Theorem, there exist unique $q_1, q_2$, s.t.
    $$a = q_1 m + (a \bmod m)$$
    $$b = q_2 m + (b \bmod m)$$
  - Adding these 2 equations and take modulo $m$
    $(a + b) \bmod m$
    $= \big((q_1 + q_2)m + (a \bmod m) + (b \bmod m)\big) \bmod m$
  - The theorem then follows from the previous Lemma.

# Modular Arithmetic

- **Theorem**
  For any $a, k \in \mathbf{Z}, m \in \mathbf{Z}^{+}$,
  $$(a \cdot b) \bmod m = \big((a \bmod m) \cdot (b \bmod m)\big) \bmod m$$
- **Proof**:
  - Similar to the previous theorem.
- **Theorems**
  For any $a, k \in \mathbf{Z}, m \in \mathbf{Z}^{+}$,
  $$(a + b) \bmod m = \big(a + (b \bmod m)\big) \bmod m$$
  $$(a + b) \bmod m = \big((a \bmod m) + b\big) \bmod m$$
  $$(a \cdot b) \bmod m = \big(a \cdot (b \bmod m)\big) \bmod m$$
  $$(a \cdot b) \bmod m = \big((a \bmod m) \cdot b\big) \bmod m$$

# Modular Arithmetic on $\mathbf{Z}_m$

- **Definition**

$$\mathbf{Z}_m = \{0,1,\ldots,m-1\}$$

- **Definition**
  For $a, b \in \mathbf{Z}_m$
  - $a +_m b = (a+b) \bmod m$
  - $a \cdot_m b = (a \cdot b) \bmod m$
- Examples
  - $7 +_{11} 9 = (7+9) \bmod 11 = 16 \bmod 11 = 5$
  - $7 \cdot_{11} 9 = (7 \cdot 9) \bmod 11 = 63 \bmod 11 = 8$

# Properties of Arithmetic Modulo *m*

- 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
$$(a +_m b) +_m c = a +_m (b +_m c)$$
$$(a \cdot_m b) \cdot_m c = a \cdot_m (b \cdot_m c)$$
- Commutativity: If $a$ and $b$ belong to $\mathbf{Z}_m$, then
$$a +_m b = b +_m a$$
$$a \cdot_m b = b \cdot_m a$$
- Distributivity: If *a*, *b*, and *c* belong to $\mathbf{Z}_m$ , then
$$a \cdot_m (b +_m c) = (a \cdot_m b) +_m (a \cdot_m c)$$

# Proof of Associativity

$$
\begin{aligned}
& a +_m (b +_m c) \\
& = \big(a + (b +_m c)\big) \bmod m \\
& = \Big(a + \big((b + c) \bmod m\big)\Big) \bmod m \\
& = \big(a + (b + c)\big) \bmod m \\
& = \big((a + b) + c\big) \bmod m \\
& = \big((a + b) \bmod m + c\big) \bmod m \\
& = \big((a +_m b) + c\big) \bmod m \\
& = (a +_m b) +_m c
\end{aligned}
$$

Proof of other properties are similar.

# Additive inverses and multiplicative inverses

- Identity elements: The elements 0 and 1 are identity elements for addition and multiplication modulo $m$, respectively.
  - For $a \in \boldsymbol{Z}_m$, $a +_m 0 = a$ and $a \cdot_m 1 = a$.
- Additive inverses
  For $a \in \mathbf{Z}_m$, $(-a \bmod m)$ is the additive inverse of $a$:
  - $a +_m (-a \bmod m\,) = \big(a + (-a \bmod m)\big) \bmod m$
    $= \big(a + (-a)\big) \bmod m = 0$
- Example: What is the additive inverse of 27 in $\mathbf{Z}_{58}$?
- Answer: 31
- For $a \in \mathbf{Z}_m$, $b$ is its multiplicative inverse if $a \cdot_m b = 1$
- Example: Let $m = 4$. What is the multiplicative inverse of 3? What is the multiplicative inverse of 2?

# Outline

- Divisibility
- Modular Arithmetic
- **Congruences**
- Applications of Modular Arithmetic

# Congruences

- **Definition**
  Let $a, b \in \mathbf{Z}, m \in \mathbf{Z}^+$. Then $a$ is congruent to $b$ modulo $m$ if $a \bmod m = b \bmod m$.
  - Notation: $a \equiv b \pmod{m}$
  - $a \equiv b \pmod{m}$ is a congruence; $m$ is its modulus.
  - Alternative definitions: (i) $m | (a - b)$;
    (ii) $\exists t \in \mathbf{Z}\ (a = b + mt)$
- **Examples**
  - $17 \equiv 5 \pmod{6}$ $\qquad$ $24 \not\equiv 14 \pmod{6}$
- **Note**
  - In $a \bmod m$, $\bmod$ is a binary operator
  - $a \equiv b \pmod{m}$ denotes an equivalence relationship between $a$ and $b$.

# Modular Arithmetic and Congruences

- Congruences provide another way to express modular arithmetic, by replacing $+_m$, $\cdot_m$, $=$ with $+$, $\cdot$, $\equiv$, adding $(\mathrm{mod}\ m)$ in the end.
- For any integer $a, b, c$, positive integer $m$
  - Associativity:
$$(a+b)+c \equiv a+(b+c) \pmod{m}$$
$$(a \cdot b) \cdot c \equiv a \cdot (b \cdot c) \pmod{m}$$
  - Commutativity:
$$a+b \equiv b+a \pmod{m}$$
$$a \cdot b \equiv b \cdot a \pmod{m}$$
  - Distributivity:
$$a(b+c) \equiv ab+ac \pmod{m}$$

# Modular Arithmetic and Congruences

- Difference:
  - $+_m$ and $\cdot_m$ are defined only on elements of $\mathbf{Z}_m$
  - Congruences are defined over $\mathbf{Z}$
- Examples
  - $6 +_8 7 = 5$
  - $6 + 15 \equiv 5 \pmod{8}$
  - $6 + 15 \equiv 21 \pmod{8}$
  - Can't write $6 +_8 7 = 13$ or $6 +_8 15 = 5$

# More on Congruences

- **Theorem**
  Let $m$ be a positive integer. If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then
  $$a + c \equiv b + d \pmod{m}$$
  $$ac \equiv bd \pmod{m}$$
  Proof in textbook
- **Example**
  Because $7 \equiv 2 \pmod{5}$ and $11 \equiv 1 \pmod{5}$, it follows that
  $$18 = 7 + 11 \equiv 2 + 1 = 3 \pmod{5}$$
  $$77 = 7 \cdot 11 \equiv 2 \cdot 1 = 2 \pmod{5}$$

# More on Congruences

- **Corollary**
  If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then
  $$a - c \equiv b - d \pmod{m}$$
- Note: $a/c \not\equiv b/d \pmod{m}$
- Corollary
  If $a \equiv b \pmod{m}$, then for any $c \in \mathbf{Z}$,
  $$a + c \equiv b + c \pmod{m}$$
  $$a - c \equiv b - c \pmod{m}$$
  $$ac \equiv bc \pmod{m}$$

# Outline

- Divisibility
- Modular Arithmetic
- Congruences
- **Applications of Modular Arithmetic**

# Parity Bits

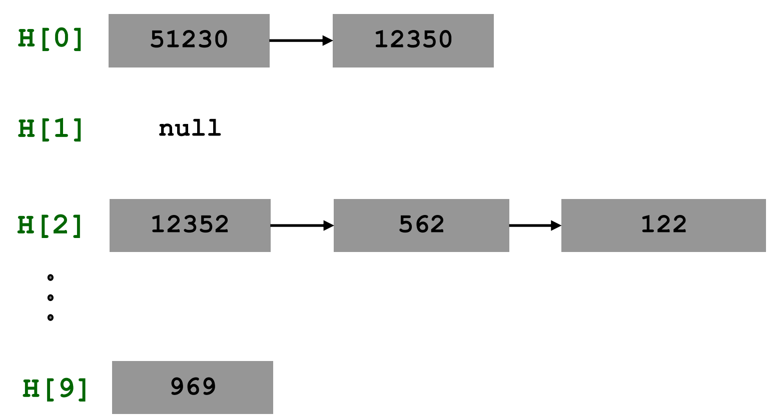
- Digital information is transmitted as a bit stream 00010010101111010101010101010101
- Denote the bits as $x_1, x_2, \dots, x_n$
- At the end of the stream, we often add a parity bit
$$x_{n+1} = (x_1 + x_2 + \cdots + x_n) \bmod 2$$
- This can detect one wrong bit
  - Or an odd number of wrong bits
- It cannot detect if there are an even number of wrong bits
  - Will come back to this later

# Hash Functions

- **Example**
  During exam checking, how to organize the exam papers so that the TA can quickly find the paper for any given student?
- **Solution**
  - $h(id) = id \bmod 10$
  - Hash by initials
- A hash function maps a universe of keys to a small set of locations

# Hash Table

- **Example**
  - Build a student database, where each student had id, name, address, phone, GPA, etc.
  - Given a student id, wants to quickly retrieve it.
- **Solution**
  - Suppose there are $n$ students. Create an array $H$ of size $m$.
  - Put student with id $x$ at location $H[h(x)]$.
  - Resolving collision: $H[i]$ stores a linked list of elements $x$ with $h(x) = i$.



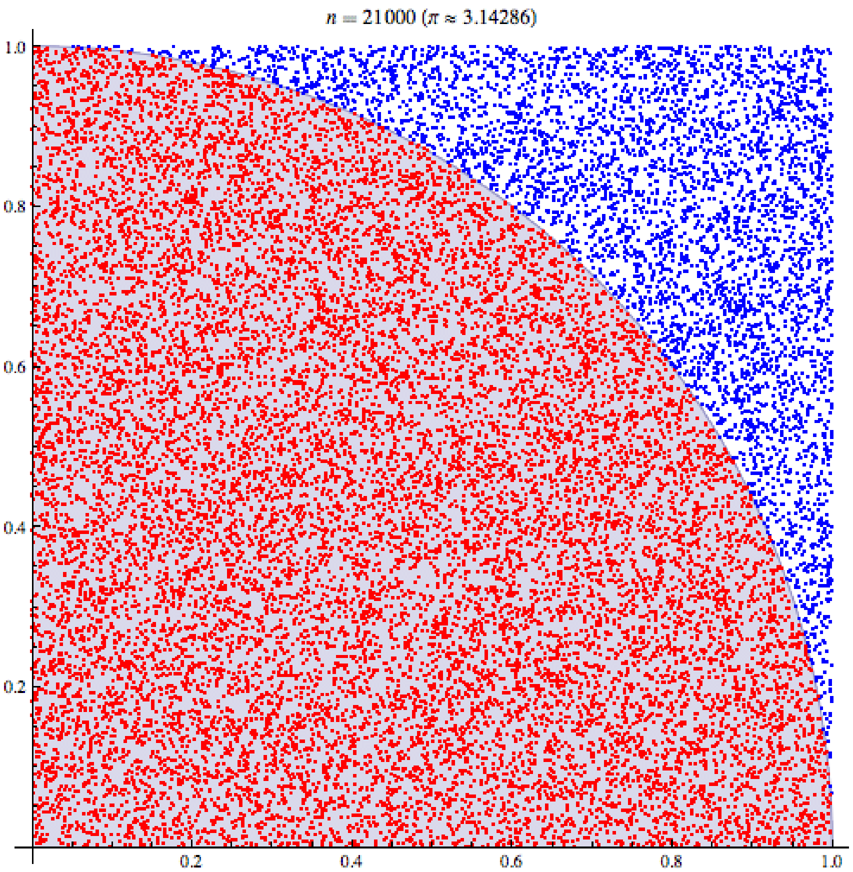
# Hashing Strings

- Each character is an integer between 0 and 255
- Need to take all characters into account
- A commonly used hash function
  Suppose characters of a $s$ are accessed as $s[0], s[1], \ldots$
  $$h(s) = \Big(\big((s[0] \cdot 31 + s[1]) \cdot 31 + s[2]\big) \cdot 31 + \cdots\Big) \bmod n$$
- Hash function in Java string library (note that overflows are equivalent to modular arithmetic)

```
int h(String s, int n) {
   int hash = 0;
   for (int i = 0; i < s.length(); i++)
      hash = ((31 * hash) + s[i]);
   return hash % n;
}
```

# Random Numbers

- Random numbers are needed for many purposes
  - Computer games
  - Computer simulation
  - Gambling
  - ...
- But how to generate random numbers?
  - `rand()`



# Pseudorandom Numbers

- Pseudorandom numbers are generated by deterministic methods. (So they are not truly random!)
- Linear congruential method
  - Given modulus $m$, the multiplier $a$, the increment $c$, and seed $x_0$
    - The seed is usually given by user (often use system time)
    - The other two are hard-coded
  - Generate a sequence of pseudorandom numbers:

$$x_{n+1} = (ax_n + c) \bmod m$$

- Example:
  - $m = 9, a = 7, c = 4, x_0 = 3$
  - $3, 7, 8, 6, 1, 2, 0, 4, 5, 3, 7, 8, 6, 1, 2, 0, 4, 5, 3, \ldots$

# Pseudorandom Numbers

- The linear congruential method generates repeating patterns
  - It has been found that with $m = 2^{31} - 1, a = 7^5, c = 0$, it generates $2^{31} - 2$ different numbers before repeating
  - Take another mod if random numbers in a certain range are needed
- It generates uniformly distributed numbers
- But they are not random!
- Don't use for lotteries, etc.
- Whole theory about pseudorandom number generators
- [http://www.random.org](http://www.random.org) provides truly random numbers (from atmospheric noise)