- 教材讨论
  - TC第31章第1、2、3、4、5、6节

# 问题1：GCD和(Extended-)Euclid

- Define $\mathrm{lcm}(a_1, a_2, \ldots, a_n)$ to be the ***least common multiple*** of the $n$ integers $a_1, a_2, \ldots, a_n$, that is, the smallest nonnegative integer that is a multiple of each $a_i$. Show how to compute $\mathrm{lcm}(a_1, a_2, \ldots, a_n)$ efficiently using the (two-argument) gcd operation as a subroutine.

# 问题1：GCD和(Extended-)Euclid (续)

- 什么是 $(\mathbb{Z}_n, +_n)$ 和 $(\mathbb{Z}_n^*, \cdot_n)$？它们为什么是交换群？
- How to compute multiplicative inverses in $(\mathbb{Z}_n^*, \cdot_n)$？（我们上次课讨论过）

# 问题1：GCD和(Extended-)Euclid (续)

- 什么是 $(\mathbb{Z}_n, +_n)$ 和 $(\mathbb{Z}_n^*, \cdot_n)$？它们为什么是交换群？
- How to compute multiplicative inverses in $(\mathbb{Z}_n^*, \cdot_n)$? （我们上次课讨论过）
  - 1 = ax+ny
    利用Extended-Euclid求gcd(a,n)=1，得到的x即$a^{-1}$

# 问题2：$Z_n$和$Z_n$*

- 什么是<a>？
  （注意TC与TJ在定义上的区别）
- 什么时候$<a>=Z_n$？
  如果$<a>\neq Z_n$，那么a、<a>分别有什么特征？

# 问题2：$Z_n$和$Z_n$* (续)

- 你理解Euler’s phi function了吗？

  $$\phi(n) = n \prod_{p\,:\,p \text{ is prime and } p \mid n} \left(1 - \frac{1}{p}\right)$$

  它和 $(\mathbb{Z}_n^*, \cdot_n)$ 有什么关系？
  当n是质数时，你能算出φ(n)吗？
- 当m和n互质时，φ(mn)=φ(m)φ(n)，你能证明吗？

# 问题2：$Z_n$和$Z_n$* (续)

***Theorem 31.27 (Chinese remainder theorem)***
Let $n = n_1 n_2 \cdots n_k$, where the $n_i$ are pairwise relatively prime. Consider the correspondence

$$a \leftrightarrow (a_1, a_2, \ldots, a_k)\,, \tag{31.27}$$

where $a \in \mathbb{Z}_n$, $a_i \in \mathbb{Z}_{n_i}$, and

$$a_i = a \bmod n_i$$

for $i = 1, 2, \ldots, k$. Then, mapping (31.27) is a one-to-one correspondence (bijection) between $\mathbb{Z}_n$ and the Cartesian product $\mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \cdots \times \mathbb{Z}_{n_k}$. Operations performed on the elements of $\mathbb{Z}_n$ can be equivalently performed on the corresponding $k$-tuples by performing the operations independently in each coordinate position in the appropriate system. That is, if

$$\begin{aligned} a &\leftrightarrow (a_1, a_2, \ldots, a_k)\,, \\ b &\leftrightarrow (b_1, b_2, \ldots, b_k)\,, \end{aligned}$$

then

$$(a + b) \bmod n \leftrightarrow ((a_1 + b_1) \bmod n_1, \ldots, (a_k + b_k) \bmod n_k)\,, \tag{31.28}$$

$$(a - b) \bmod n \leftrightarrow ((a_1 - b_1) \bmod n_1, \ldots, (a_k - b_k) \bmod n_k)\,, \tag{31.29}$$

$$(ab) \bmod n \leftrightarrow (a_1 b_1 \bmod n_1, \ldots, a_k b_k \bmod n_k)\,. \tag{31.30}$$

# 问题2：$Z_n$和$Z_n$* (续)

*Proof:* Let $\mathbb{Z}_m \times \mathbb{Z}_n$ denote the set of all pairs $(X, Y)$ such that $X \in \mathbb{Z}_m$ and $Y \in \mathbb{Z}_n$. We define a function $f : \mathbb{Z}_{mn} \to \mathbb{Z}_m \times \mathbb{Z}_n$ by the formula $f([a]_{mn}) = ([a]_n, [a]_m)$.

Since $m$ and $n$ divide $mn$, this function is well defined (does not depend on the choice of the representative $a$). Since $\gcd(m, n) = 1$, the Chinese remainder theorem implies that this function establishes a one-to-one correspondence between the sets $\mathbb{Z}_{mn}$ and $\mathbb{Z}_m \times \mathbb{Z}_n$.

Furthermore, an integer $a$ is coprime with $mn$ if and only if it is coprime with $m$ and with $n$. Therefore the function $f$ also establishes a one-to-one correspondence between $G_{mn}$ and $G_m \times G_n$, the latter being the set of pairs $(X, Y)$ such that $X \in G_m$ and $Y \in G_n$. It follows that the sets $G_{mn}$ and $G_m \times G_n$ consist of the same number of elements. Thus $\phi(mn) = \phi(m)\phi(n)$.

这里的G就是我们说的Z*

# 问题2：$Z_n$和$Z_n$* (续)

- Draw the group operation tables for the groups $(\mathbb{Z}_4, +_4)$ and $(\mathbb{Z}_5^*, \cdot_5)$. Show that these groups are isomorphic by exhibiting a one-to-one correspondence $\alpha$ between their elements such that $a + b \equiv c \pmod 4$ if and only if $\alpha(a) \cdot \alpha(b) \equiv \alpha(c) \pmod 5$.

# 问题2：$Z_n$和$Z_n$* (续)

- Draw the group operation tables for the groups $(\mathbb{Z}_4, +_4)$ and $(\mathbb{Z}_5^*, \cdot_5)$. Show that these groups are isomorphic by exhibiting a one-to-one correspondence $\alpha$ between their elements such that $a + b \equiv c \pmod 4$ if and only if $\alpha(a) \cdot \alpha(b) \equiv \alpha(c) \pmod 5$.

- 任意$Z_i$，是不是一定能找到$Z_j$*与之同构？
  任意$Z_j$*，是不是一定能找到$Z_i$与之同构？
  如果能，请说明原因；如果不能，请给出反例。

# 问题2：$Z_n$和$Z_n$* (续)

- Draw the group operation tables for the groups $(\mathbb{Z}_4, +_4)$ and $(\mathbb{Z}_5^*, \cdot_5)$. Show that these groups are isomorphic by exhibiting a one-to-one correspondence $\alpha$ between their elements such that $a + b \equiv c \pmod 4$ if and only if $\alpha(a) \cdot \alpha(b) \equiv \alpha(c) \pmod 5$.

- 任意$Z_i$，是不是一定能找到$Z_j$*与之同构？
  任意$Z_j$*，是不是一定能找到$Z_i$与之同构？
  如果能，请说明原因；如果不能，请给出反例。

φ(n) is the number of numbers k, with 1≤k≤n, such that gcd(n,k)=1.
Clearly, if gcd(k,n)=1, then gcd(n−k,n)=1 as well, so (for n>2) all the numbers relatively prime to n can be matched up into pairs {k,n−k}. So φ(n) is even.
(In particular, k=n−k means that n=2k and gcd(n,k)=gcd(2k,k)=k>1.)

# 问题3：powers of an element

- 在这个算法中，c的作用是什么？
  你能简要解释这个算法的正确性证明吗？

Just prior to each iteration of the **for** loop of lines 4–9,

1. The value of $c$ is the same as the prefix $\langle b_k, b_{k-1}, \ldots, b_{i+1} \rangle$ of the binary representation of $b$, and
2. $d = a^c \bmod n$.

- 你会分析这个算法的运行时间吗？

```
MODULAR-EXPONENTIATION(a, b, n)
1   c = 0
2   d = 1
3   let ⟨b_k, b_{k-1}, ..., b_0⟩ be the binary representation of b
4   for i = k downto 0
5       c = 2c
6       d = (d · d) mod n
7       if b_i == 1
8           c = c + 1
9           d = (d · a) mod n
10  return d
```