Lec 06. 初等数论

整数：整数的加法运算形成群 $\{\mathbb{Z}, 0, +\}$；整数对加法和乘法运算形成整环 $\{\mathbb{Z}, +, \times, 0, 1\}$。

因数：a, b 为整数且 $b \neq 0$；如果有整数 c 使得 $a = bc$，则 a 为 b 的倍数，b 为 a 的因数，或称 b 整除 a，写作 $b|a$。

> Abel 证明：$n(n \geq 5)$ 次的一般代数方程没有根式解，引入群和域的概念。

群：设 G 是一个集合，定义 $G \times G \to G$ 上的二元运算 $\cdot$ ，若满足下列条件，则 $(G, \cdot)$ 为一个群；

- 封闭性：若 $a, b \in G$，则 $a \cdot b \in G$；
- 结合律：若 $a, b, c \in G$，则 $(a \cdot b) \cdot c = a \cdot (b \cdot c)$；
- 单位元：存在一个元素 $e \in G$，使得对于任意 $a \in G$ 有 $e \cdot a = a \cdot e = a$；
- 逆元：对于任意 $a \in G$，都存在一个元素 $b \in G$，使得 $a \cdot b = b \cdot a = e$。

交换群：若群 $(G, \cdot)$ 满足交换律，则称其为交换群，即 $\forall a, b \in G$ 有 $a \cdot b = b \cdot a$；交换群也称为 Abel 群。

有限群：若群 $(G, \cdot)$ 中的元素个数 $|G|$ 是有限的，称 G 为有限群；

阶：对于 G 中的的元素 a，计算 $a, a^2 = a \cdot a, a^3 = a^2 \cdot a, \cdots$；若 $\exists m$ 使 $a^m = 1$，称 a 的阶有限，并称使得 $a^m = 1$ 的最小的正整数 m 为元素 a 的阶；否则 a 的阶无穷。

子群：若 G 的元素 a 是 m 阶元，则 $\{1, a, a^2, \cdots, a^{m-1}\}$ 构成 G 的子群；

循环群：称形如 $\{1, a, a^2, \cdots, a^{m-1}\}$ 的群为循环群，且元素 a 为该群生成元。

【定理】设 G 为阶为 n 的群，那么它的所有子群的阶都可以整除 n。

同余：若两个整数 a 和 b 的差可以被 m 整除，即 $m \mid (a - b)$，称 a 和 b 关于模 m 是同余的，记作 $a \equiv b (\bmod m)$。

同余关系的性质：同余关系是等价关系。

- 先加（减、乘）再取模同余先取模再加（减、乘）；
- 一个数 a 同余自身；
- 若 $a \equiv b \pmod m$ 且 $c \equiv d \pmod m$，则 $ac \equiv bd \pmod m$。

素数：一个大于 1 的正整数，若只能被 1 和他本身整除且不能被其他正整数整除，这样的正整数叫素数（质数）。

复数：一个正整数除了能被 1 和他本身整除外，还能被其他正整数整除，这样的正整数叫复合数。

【引理】如果 a 是大于 1 的整数，则 a 的大于 1 的最小因数一定是素数。换句话说，任何大于 1 的整数都至少有一个素因数。

【引理】如果 a 是大于 a 的整数，所有 $\leq \sqrt{a}$ 的素数都除不尽 a，则 a 为素数。

【引理】素数个数无限。（反证）

素数分布：以 $\Pi(x)$ 代表不大于 x 的素数个数，则

$$\lim_{x\to+\infty}\frac{\Pi(x)}{x/\log x}=1,\lim_{x\to+\infty}\frac{\Pi(x)}{x}=0$$

即 x 越大，素数分布越稀疏。

最大公因数：最大的整数 d 使得 $d\mid a_1,d\mid a_2,\cdots,d\mid a_n$，则 d 为 $a_1,a_2,\cdots,a_n$ 最大公因数；

- 若 $n=2$，记 $\gcd(a_1,a_2)=(a_1,a_2)=d$;
- 若 $d=1$ 称 $a_1,a_2,\cdots,a_n$ 互素。

最小公倍数：最小的整数 m 使得 $a_1\mid m,a_2\mid m,\cdots,a_n\mid m$，则 m 为 $a_1,a_2,\cdots,a_n$ 最小公倍数；

- 若 $n=2$，记 $\operatorname{lcm}(a_1,a_2)=[a_1,a_2]=m$。

一次同余式：$a,b\in\mathbb{Z},m\in\mathbb{Z}^+$，当 $a\not\equiv 0\pmod m$，$ax+b\equiv 0\pmod m$ 称为模 m 的一次同余式。若 c 使得上式成立，则称 $x\equiv c\pmod m$ 是一次同余式的一个解。

结论：当 $(a,m)=1$ 时，$ax+b\equiv 0\pmod m$ 一定有整数解。

Euclid 算法：若 $a>b,a=qb+r\ (0\le r<b)$，则 $(a,b)=(b,r_1)$。

扩展 Euclid 算法：解决 $ax+by=c$ 的 x,y 整数解的问题。写出 Euclid 具体过程，先考虑最后一行，即

$$(a,b)x+0y=c$$

此时得到初始解答 $x=\frac{c}{(a,b)},y=0$；每次向上迭代一轮，已算出下一轮的解 (x^*,y^*)，则上一轮的解可以如下推出：

$$\begin{cases}ax+by=c\\ bx+(a-[a/b]\cdot b)y=c\end{cases}\Longrightarrow\begin{cases}x=y^*\\ y=x^*-[a/b]y^*\end{cases}$$

向上迭代直到最初轮即可。

整数的唯一因子分解：每个大于 1 的整数 a 都可以分解为素数的连乘积。

【唯一分解定理】如果不计素因子的次序，则只有一种方法可以把一个正整数分解为素因数的连乘积；即任意正整数 a，都可以唯一地因式分解为

$$a=p_1^{a_1}p_2^{a_2}\cdots p_l^{a_l}\quad p_1<p_2<\cdots<p_l\text{ are primes}$$

【引理】形如 p^j 的整数只能为 p^i 整除，其中 $i<j$。

等价类：用同余关系可以将整数集合 $\mathbb{Z}$ 分成 m 个等价类，这样同余类只有 m 个，每类都有无穷个元素，其中

$$[i]=\{a\mid a\in\mathbb{Z},a\equiv i\pmod m\}$$

完全剩余系：$a_i\in[i]$，则 $\{a_0,a_1,\cdots,a_{m-1}\}$ 称为模 m 的完全剩余系；其中 $\{0,1,\cdots,m-1\}$ 为模 m 的非负最小完全剩余系。

【定理】若 $(m,k)=1$，则 $\{ka_0,ka_1,\cdots,ka_{m-1}\}$ 也是模 m 的完全剩余系。

简化剩余系：在模 m 的完全剩余系中，去掉与 m 不互素的那些数，剩下的部分称为模 m 的简化剩余系。$\mathbb{Z}_m$ 的简化剩余系称为 $\mathbb{Z}_m^*$，读作模 m 的非负最小简化剩余系。

Euler 函数：简化剩余系中元素个数，即不超过 m 且与 m 互素的元素个数，记为 $\varphi(m)$。

【Euler定理】 设 $(a,n)=1$，则 $a^{\varphi(n)}\equiv 1 \pmod n$。（证明思路：给定非负最小简化剩余系 $\mathbb{Z}_n^*$，则 $a\mathbb{Z}_n^*$ 也是简化剩余系，两个简化剩余系中数乘积相等，故得证）

【Euler 定理等价形式】 设 $(a,n)=1$，则 $a^{\varphi(n)+1}\equiv a \pmod n$；特别地，当 $n=pq$ 且 p,q 为素数时，有

$$a^{\varphi(pq)+1}\equiv a^{(p-1)(q-1)+1}\equiv a \pmod n$$

此时即使 $(n,a)\neq 1$，等式也成立。

【引理】 设 m_1,m_2 为正整数，$(m_1,m_2)=1$；若 A,B 分别是模 m_1,m_2 的简化剩余系，则 m_2A+m_1B 是模 m_1m_2 的简化剩余系。

【结论】 $\varphi(m_1m_2)=\varphi(m_1)\varphi(m_2)\quad ((m_1,m_2)=1).$

欧拉函数的计算：$\varphi(m)=m\prod_{i=1}^{n}\left(1-\frac{1}{p_i}\right)$，特别地，若 $m=pq$ 且 p,q 为素数，有 $\varphi(m)=(p-1)(q-1)$。

【费马小定理】（Euler 定理推论）若 p 是素数，则有$a^{p-1}\equiv 1 \pmod p$。

利用 Euler 定理和 Fermat 小定理计算模幂：设 $(a,n)=1, b=k\varphi(n)+r$ 其中 $0\le r<\varphi(n)$，则 $a^b\equiv a^r \pmod n$。

素性测试：判断一个大整数是否为素数。目前的素性测试算法都是概率性的算法，而非确定性的算法。

Millar-Rabin 算法：素性测试算法，产生的结果几乎肯定是素数；返回否定结论一定正确，返回肯定结论出错概率低；迭代多次后均返回肯定结论则出错概率大大降低。

【中国剩余定理（孙子定理）】 若 $(m_1,m_2,\cdots,m_k)$ 是 k 个两两互素的整数，则线性同余式组

$$\begin{cases} x\equiv b_1 & \pmod{m_1} \\ x\equiv b_2 & \pmod{m_1} \\ \cdots & \\ x\equiv b_k & \pmod{m_1} \end{cases}$$

对于模 $M=m_1m_2\cdots m_k$ 有唯一解。

- **用途**：加快求模的速度，可以并行计算，特别适用于 M 长度为 150 位以上的情况。
- **求解方法**：令 $M=m_1m_2\cdots m_k$，定义 $M_i=\frac{M}{m_i}$ 且 $M_i'\equiv M_i^{-1} \pmod{m_i}$，则唯一解为 $x=\sum_{i=1}^{n} b_iM_iM_i^{-1}$。

次数：由欧拉定理 $a^{\varphi(m)}=1$，所以 $a^0,a^1,a^2,\cdots$ 一定出现周期性循环，使得上述序列出现重复的最小正整数 k 称为 a 模 m 的次数。一定有 $k\mid\varphi(m)$ 但 $k=\varphi(m)$ 不一定成立。

原根：如果 a 模 m 次数 $\varphi(m)$，则称 a 是模 m 的一个原根，并非所有 m 都有原根。

【定理】 m 是原根的充要条件是 m 形如 $2,4,2^np+1$。

【定理】 原根个数为 $\varphi(\varphi(m))$ 个。

【引理】 原根可以生成模 m 的简化剩余系。

离散对数问题：指数运算 $y = g^x \pmod m$ 的逆问题是计算一个数模 m 的离散对数，记为 $x = \log_g y \pmod m$。如果 g 是原根则一定有整数解。如果 g 不是原根可能无解。由 x, g, m 计算 y 容易而由 y, g, m 计算 x 困难。

- 离散指数问题可以通过迭代将复杂度降低至 $O(\log m)$。
- 离散对数问题没有特别好的算法。
  - 常规算法：$O(p)$；
  - BSGS 算法：$O(\sqrt{p})$，思想是 $m = \lceil \sqrt{p-1} \rceil$ 且 $x = im + j$，则 $y = g^x \equiv g^{im+j} \pmod p$ 即 $g^j \equiv yg^{-mi} \pmod p$，于是分别遍历所有可能的 i, j 即可。
  - Index Calculus 算法需要 $O(\sqrt{p_1})$ 次乘法，其中 p_1 为 p 最大素因子。
- 若 $p \sim 2^{256}$，则离散对数问题大约需要 $\sim 2^{128}$ 的复杂度，就目前计算机而言无法完成。

【Fermat 大定理】当 $n > 2$ 时，$x^n + y^n = z^n$ 的整数解都是平凡解。