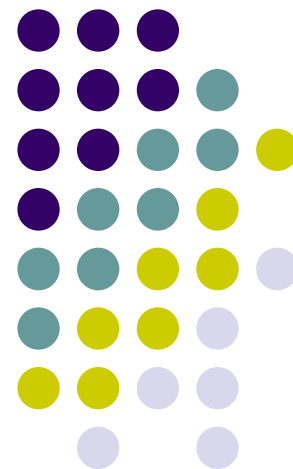


数论初步

离散数学
南京大学计算机学院



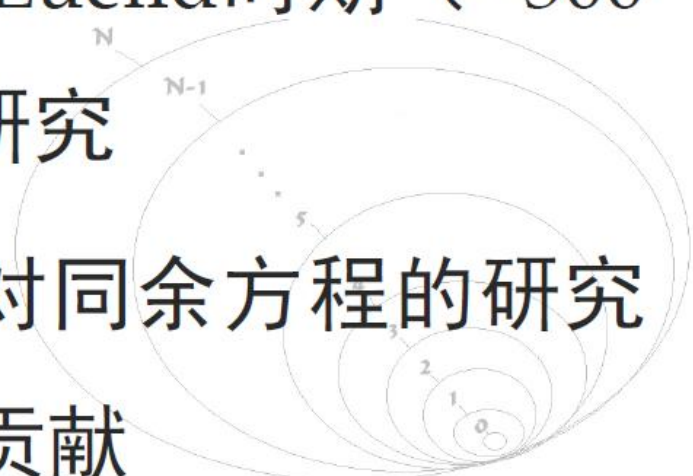
提要

- 整数的性质
- 整数的基本运算
- 质数
- Euler函数与Euler定理



什么是数论?

- 数论是纯数学的一个分支，也是纯数学的代表，它主要研究**整数**的性质
- 数论的早期研究可追溯至Euclid时期（~300 B.C.）：对质数和整除的研究
- 中国古代（~400 A.D.）对同余方程的研究为现代数论作出了基础性贡献





现代数论的早期铺垫

- 证明质数无穷

——Euclid: *Elements* (~300 A.D.)

- 筛法寻找质数

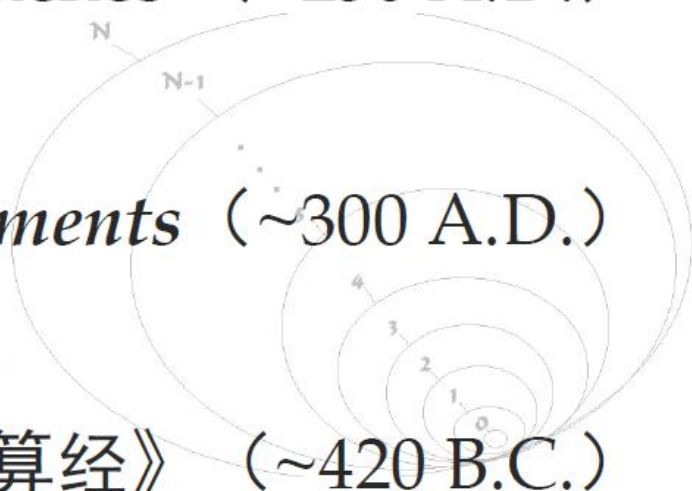
——Eratosthenes (~250 A.D.)

- 辗转相除法求最大公约数

——Euclid: *Elements* (~300 A.D.)

- 求解同余方程的中国剩余定理

——《孙子算经》 (~420 B.C.)





整数集

- 整数集一般记为 \mathbb{Z} （来源于德语“数”：*Zahlen* 的首字母），同时用 \mathbb{Z}^+ 表示正整数集（ $\mathbb{N} - \{0\}$ ），用 \mathbb{Z}^- 表示负整数集（ $\mathbb{Z} - \mathbb{N}$ ）
- \mathbb{Z} 为可列集： $\mathbb{Z} \approx \mathbb{N}$ ，基数为 \aleph_0
- \mathbb{Z} 是全序集（未来课程详述），无上界和下界
- \mathbb{Z} 和加法运算形成一个循环群（未来课程详述）；和加法运算及乘法运算形成一个环（参见抽象代数资料*）

整除

- 整除 (divisible) 是定义在 \mathbb{Z} 上的二元关系：
设 $a, b \in \mathbb{Z}, a \neq 0$, $a|b \Leftrightarrow (\exists c \in \mathbb{Z})(b = a \times c)$
- $a|b$ 读作 “ a 整除 b ”
- 设 $a, b, c \in \mathbb{Z}$ 且 $a \neq 0$, 有:
 - $(a|b) \wedge (a|c) \rightarrow a|(b + c)$
 - $a|b \rightarrow a|(b \times c)$
 - $(a|b) \wedge (b|c) \rightarrow a|c$





余数

- 余数 (remainder) 来源于带余除法
- 定义 (带余除法) : 令 $a \in \mathbb{Z}, d \in \mathbb{Z}^+$, 则:
$$(\exists! q, r \in \mathbb{Z} \wedge 0 \leq r < d)(a = d \times q + r)$$
 - 其中, a 称为被除数 (dividend), d 称为除数 (divisor), q 称为商 (quotient), r 称为余数
 - 记: $q = a \operatorname{div} d, r = a \bmod d$, 后者读作 “ a 模 b ”
- 例: $\because -11 = 3 \times (-4) + 1, \therefore -11 \bmod 3 = 1$

余数



- 模的基本性质：令 $a, b \in \mathbb{Z}, d \in \mathbb{Z}^+$ ，则：
 - $(a + b) \bmod d = (a \bmod d + b \bmod d) \bmod d$
 - $(a \times b) \bmod d = [(a \bmod d)(b \bmod d)] \bmod d$



同余

- **同余** (congruence modulo) 是定义在 \mathbb{Z} 上的二元关系：设 $a, b \in \mathbb{Z}$,

$$a \equiv b(\text{mod } m) \Leftrightarrow (\exists m \in \mathbb{Z}^+)(m|(a - b))$$

- 上式读作“ a 与 b 模 m 同余 (a is congruent to b modulo m)”，称 m 为上述“同余的模 (modulus of the congruent)”
- 同余关系及符号“ \equiv ”由 C. F. Gauss 于1801年引入
- **例**： $26 \equiv 14(\text{mod } 12)$, $-5 \equiv 13(\text{mod } 6)$



最大公约数

- 设 $a, b \in \mathbb{Z}^+$ 且 $a \neq 0$ 或者 $b \neq 0$ ，可同时整除 a, b 的最大正整数称为 a 与 b 的 **最大公约数**（greatest common divisor, GCD），记为：

$$\gcd(a, b) = \max\{d \in \mathbb{Z}^+ \mid (d|a) \wedge (d|b)\}$$

- 称 $a, b \in \mathbb{Z}^+$ **互质**（mutually prime, coprime） \Leftrightarrow

$$\gcd(a, b) = 1 \quad (\text{常简记为 } (a, b) = 1)$$

2 | 3, 6, 12, 8
3 | 3, 4
2 | 2
1, 2
LCM(3, 6, 12, 8)
= 2x2x3x1x1x1x2=24





最大公约数的性质

- 定理（线性合成）：设 $a, b \in \mathbb{Z}^+$ ，则：

$$(\exists s, t \in \mathbb{Z})(\gcd(a, b) = sa + tb)$$

- 定理（辗转相减）：设 $a, b \in \mathbb{Z}^+, a < b$ ，则：

$$\gcd(a, b) = \gcd(a, b - a)$$

- 定理（辗转相除）：设 $a, b \in \mathbb{Z}^+, a > b$ ，则：

$$\gcd(a, b) = \gcd(b, a \bmod b)$$



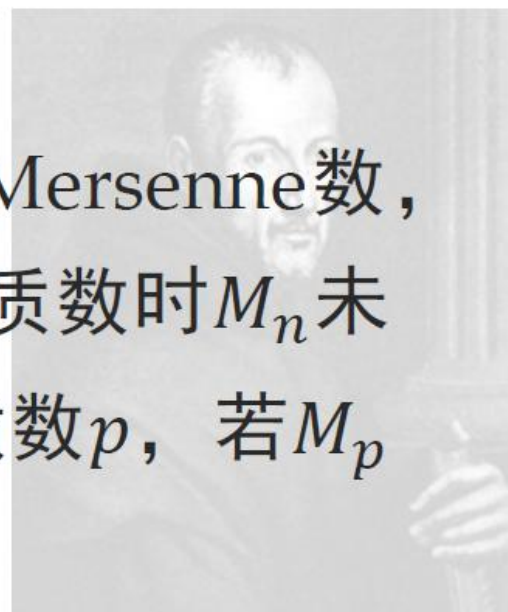
- If d is $GCD(a, b)$, then $d = sa + tb$ for some integer s and t .
 - Let x be the smallest positive integer that can be written as $sa + tb$. For any common divisor c of a, b , $c|(sa + tb)$, which means that x is no less than any common divisor of a, b .
 - Let $a = qx + r$ ($0 \leq r < x$), then $r = a - q(sa + tb) = (1 - qs)a - qtb$. Since r is also of the form of $sa + tb$, r can not be positive, and must be 0. So, $a = qx$, that is, $x|a$. Similarly, $x|b$.
 - Conclusion: $x = sa + tb$ is the largest common divisor of a and b . And it is a multiple of any other common divisors.

质数

- 仅含2个正因子（1和自身）的大于1的整数称为**质数**（prime number），大于1的非质数整数称为**合数**（composite number）
- **定理（算术基本定理）**：每个大于1的整数皆可分解为有限个质数之积（这些质数称为**质因子**），若不考虑顺序，则分解唯一
 - $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ ($p_1 < p_2 < \cdots < p_k, \alpha_i \in \mathbb{Z}^+$)

质数

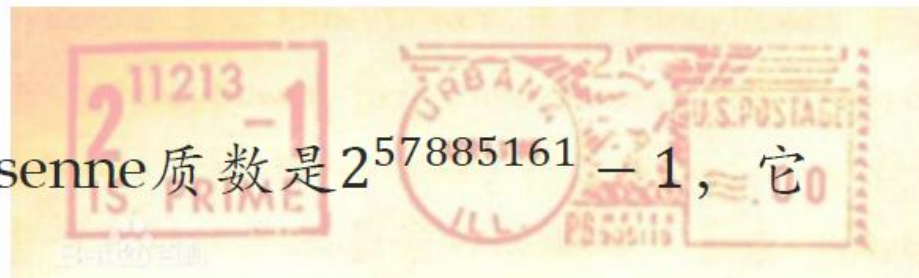
- 关于质数的命题可追溯到Euclid时期，最著名的命题之一为《几何原本》所提之：若 $2^p - 1$ 为质数，则 $2^{p-1}(2^p - 1)$ 为完全数（本身为其所有真因子之和的数）
- 对 $n \in \mathbb{Z}^+$ ，整数 $M_n = 2^n - 1$ 被称为Mersenne数，当 n 为合数时 M_n 必为合数，但当 n 为质数时 M_n 未必——甚至极少——为质数。对某质数 p ，若 M_p 为质数，则称 M_p 为Mersenne质数





质数

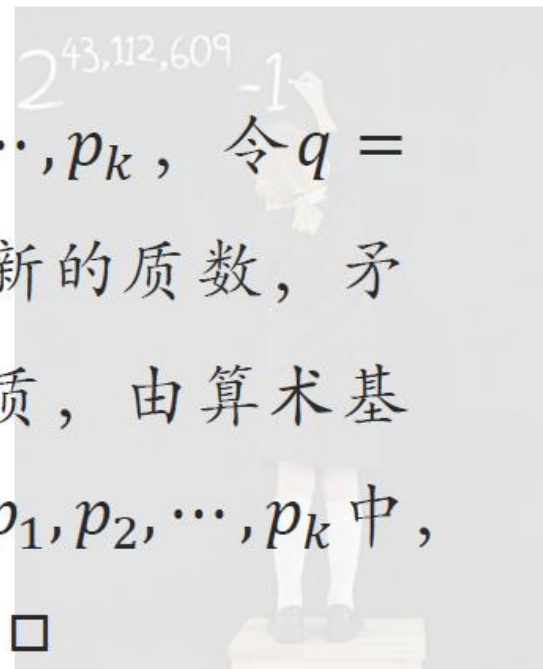
- 截至今日，人类共发现48个Mersenne质数
 - M_2, M_3, M_5, M_7 于公元前被发现
 - 前12个Mersenne质数发现于手算时代
 - 在1952—1994年的计算机时代，发现了第13—34个Mersenne质数
 - 在1996年至今，互联网时代的分布式大规模计算发现了第35—48个Mersenne质数（但不知道第44到第48个之间是否还有其它Mersenne质数）
 - 目前已知最大的第48个Mersenne质数是 $2^{57885161} - 1$ ，它有17425170位





质数的性质

- **命题：** 若 n 为合数，则其必含有不大于 \sqrt{n} 的质因子
- **命题（Euclid）：** 有无穷多质数
 - **证明：** 反设质数有穷，列为 p_1, p_2, \dots, p_k ，令 $q = \prod_{i=1}^k p_i + 1$ ，则若 q 为质数，则其为新的质数，矛盾；若 q 为合数，因为 $\prod_{i=1}^k p_i$ 与 q 互质，由算术基本定理， q 的分解式中的质数均不在 p_1, p_2, \dots, p_k 中，为新的质数，矛盾。原命题成立。 □



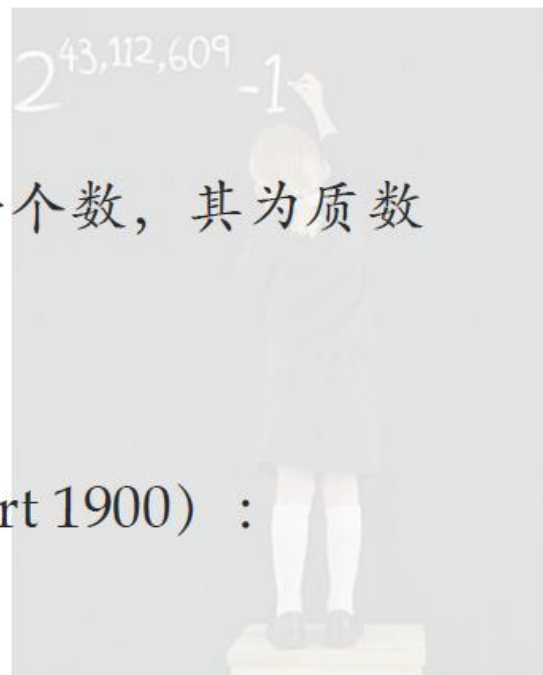
质数定理

- **定理***（**质数定理**）：设 $x \in \mathbb{R}^+$ ， $\pi(x)$ 为质数计数函数（*i.e.* 不大于 x 的质数的个数），有

$$\lim_{x \rightarrow \infty} \frac{\pi(x)}{x / \ln x} = 1$$

- 质数定理表明从不大于 n 的自然数中随机选一个数，其为质数的**概率约为 $1 / \ln n$**
- 质数的分布随着 n 的增大**逐渐稀疏**
- 孪生质数猜想（twin prime conjecture, Hilbert 1900）：

$$\liminf_{n \rightarrow \infty} (p_{n+1} - p_n) = 2$$





张益唐 与 孪生素数猜想



生于1955-

庾信平生最萧瑟，
暮年诗赋动江关

2013: $\liminf_{n \rightarrow \infty} (p_{n+1} - p_n) < 7 \times 10^7$



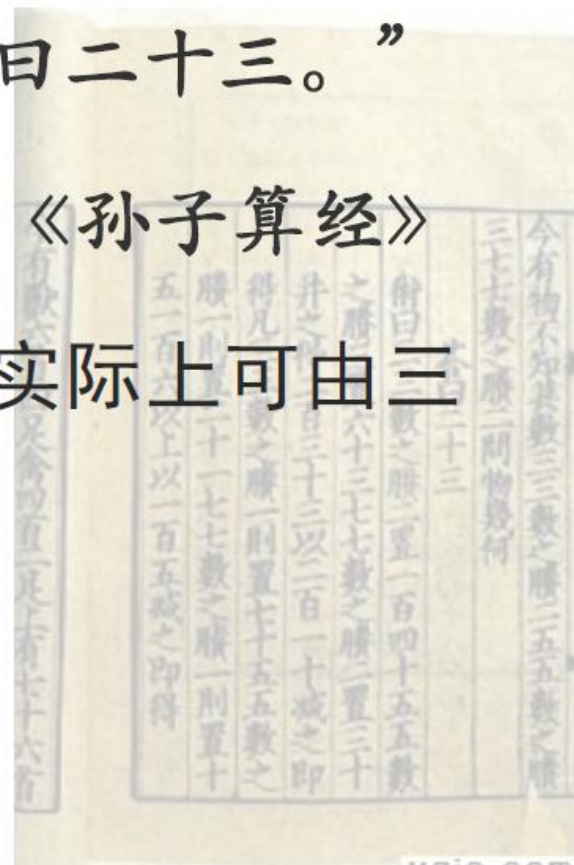
中国剩余定理（孙子定理）

“今有物不知其数，三三数之剩二，五五数之剩三，七七数之剩二，问物几何？答曰二十三。”

——《孙子算经》

上述问题中的三个“ x 数之剩几”实际上可由三个线性同余方程描述：

$$\begin{cases} x \equiv 2 \pmod{3} \\ x \equiv 3 \pmod{5} \\ x \equiv 2 \pmod{7} \end{cases}$$



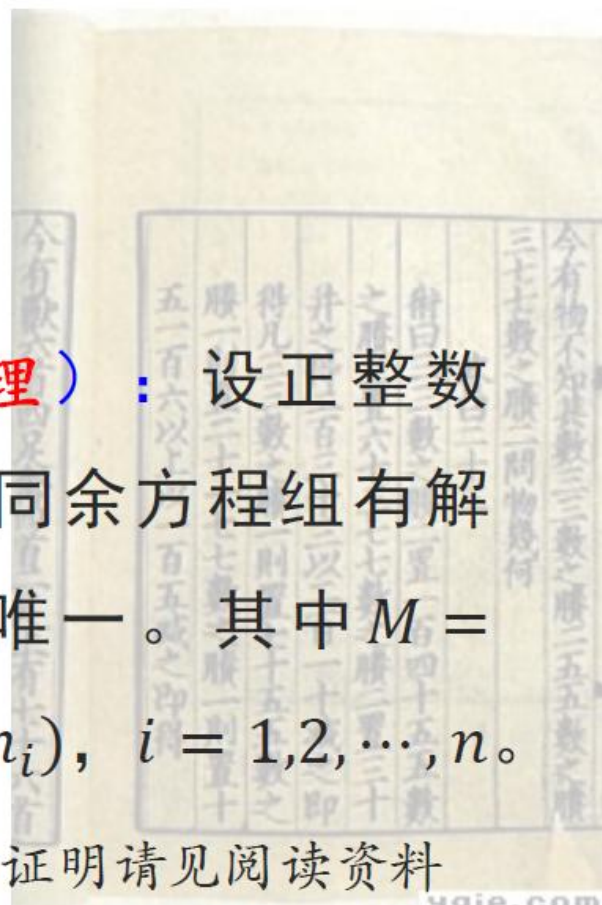


中国剩余定理

- 一元线性同余方程组可写为：

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

- 定理（线性同余方程组的解存在定理）：设正整数 m_1, m_2, \dots, m_n 两两互质，则一元线性同余方程组有解 $x = \sum_{i=1}^n a_i t_i M_i$ ，且解在模 M 同余下唯一。其中 $M = \prod_{i=1}^n m_i$ ， $M_i = M/m_i$ ， $t_i M_i \equiv 1 \pmod{m_i}$ ， $i = 1, 2, \dots, n$ 。上述 t_i 称为 M_i 的“数论倒数”。该定理的证明请见阅读资料



欧拉函数

- 定义（欧拉函数）：对任意 $n \in \mathbb{Z}^+$,

$$\varphi(n) = |\{m \in \mathbb{Z}^+ | m \leq n \wedge (m, n) = 1\}|$$

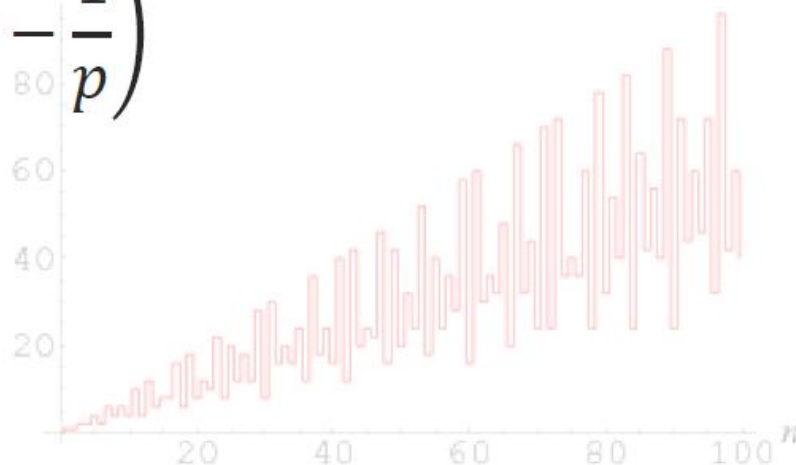
- 例： $\varphi(3) = 2$, $\varphi(4) = 2$, $\varphi(12) = 4$

- 由容斥原理(未来课程详述) 可证：

$$\varphi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right)$$

其中 $\{p\}$ 为 n 的所有质因子

- $(m, n) = 1 \rightarrow \varphi(mn) = \varphi(m)\varphi(n)$
- p 为质数 $\rightarrow \varphi(p) = p - 1$





欧拉定理

- **定理（Euler定理）**：对 $a, n \in \mathbb{Z}^+$ ，若 $(a, n) = 1$ ，则：

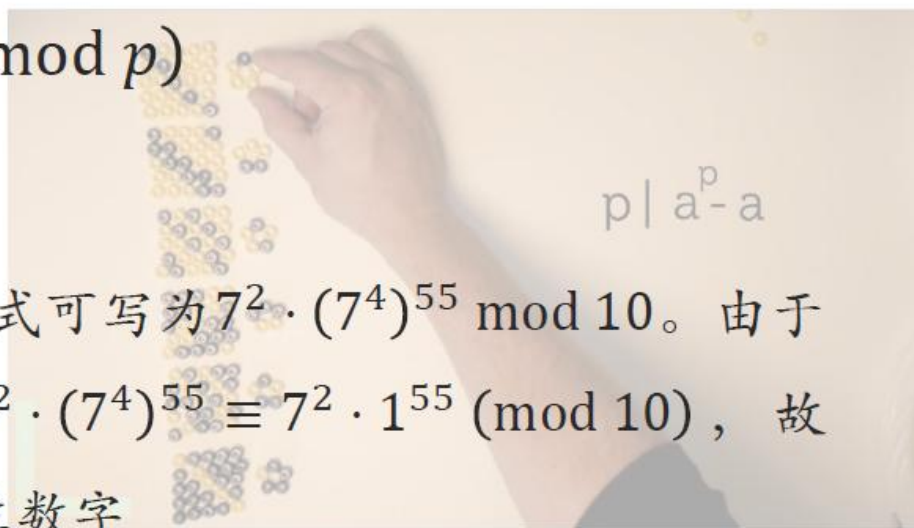
$$a^{\varphi(n)} \equiv 1 \pmod{n}$$

- 若上述 $n \in \mathbb{Z}^+$ 为质数，由欧拉函数的性质易得到：
- **定理（Fermat小定理）**：设正整数 a 不是质数 p 之倍数，则：

$$a^{p-1} \equiv 1 \pmod{p}$$

- **例**：求 7^{222} 的个位数字

- **解**：待求即为 $7^{222} \bmod 10$ ，上式可写为 $7^2 \cdot (7^4)^{55} \bmod 10$ 。由于 $(7, 10) = 1$ ，由Euler定理， $7^2 \cdot (7^4)^{55} \equiv 7^2 \cdot 1^{55} \pmod{10}$ ，故 $7^{222} \bmod 10 = 9$ 即为 7^{222} 之个位数字



作业

- 教材内容: [Rosen] 4.2—4.3节
- 课后习题:
 - 见课程主页

