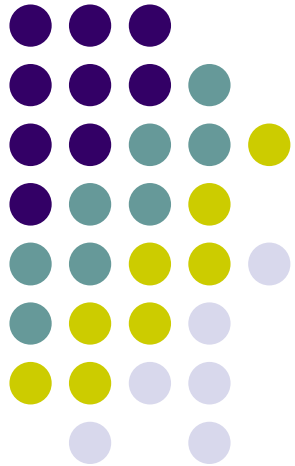
自然数及数论初步

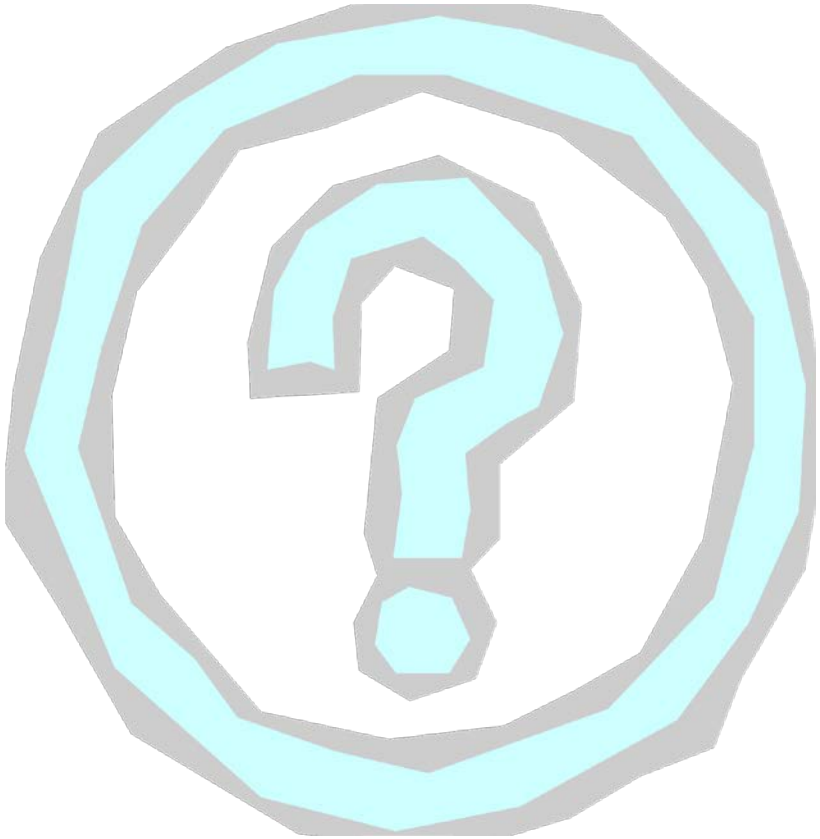
离散数学—集合论

南京大学计算机科学与技术系



内容提要

- 自然数
- 整数及基本运算
- 素数
- 欧拉函数



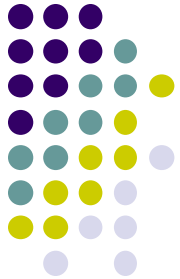
用集合定义自然数

- 设a为集合, 称$a \cup \{a\}$为a的后继, 记为$s(a)$，或a^+。
- 设A是集合，若A满足下列条件，称A为归纳集：
  - $\emptyset \in A$
  - $\forall a(a \in A \rightarrow s(a) \in A)$
- 自然数集合N:是所有归纳集的交集。
  - 因此：$N = \{ \emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}, \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}, \ldots \}$
  - N的每一个元素称为一个自然数。
  - $\emptyset$记为0，$s(0)$记为1，$s(1)$记为2， $s(2)$记为3，以此类推

再具体一点

- 记号0表示：　　Ø
- 记号1表示s(0)：Ø∪{Ø}={Ø}
- 记号2表示s(1)：{Ø}∪{{Ø}}={Ø,{Ø}}
- 记号3表示s(2)：{Ø,{Ø}, {Ø,{Ø}}}
- $1 \in 3$　$2 \in 3$
- $1 \subseteq 3$　$2 \subseteq 3$
- $1 \cup 3 = 3$　$2 \cap 3 = 2$

皮亚诺公理
(Peano axioms for natural numbers)



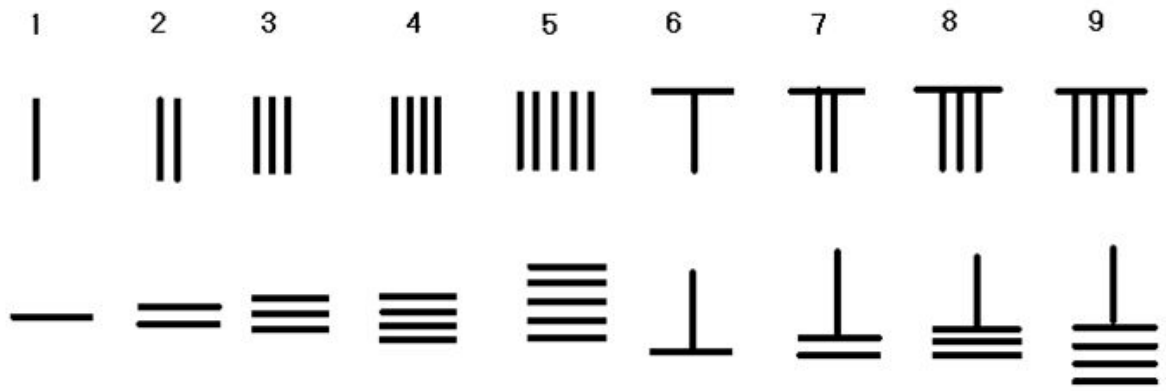
- 零是个自然数.
- 每个自然数都有一个后继（也是个自然数）.
- 零不是任何自然数的后继.
- 不同的自然数有不同的后继.
- （归纳公理）设由自然数组成的某个集合含有零，且每当该集合含有某个自然数时便也同时含有这个数的后继，那么该集合定含有全部自然数.

- 备注：另有4个与自然数相等有关的公理

自然数上的运算

- 加法（递归定义）
  - $m + 0 = m$
  - $m + s(n) = s(m+n)$
- 乘法（递归定义）
  - $m * 0 = 0$
  - $m * s(n) = m + m*n$

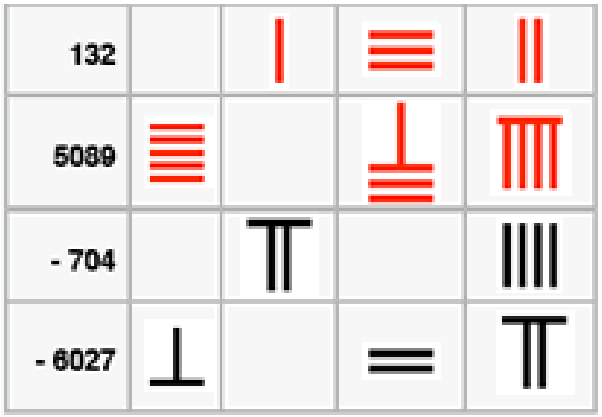
算筹（中国古代数学）

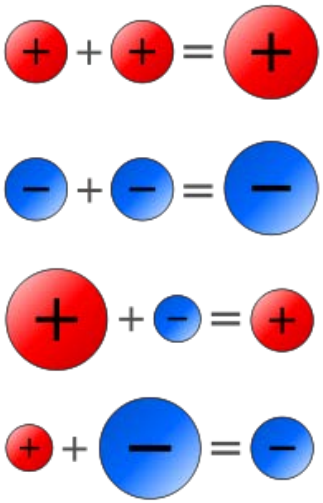


算筹数码，四则运算（九九表）、乘方、开方

“战国”或之前

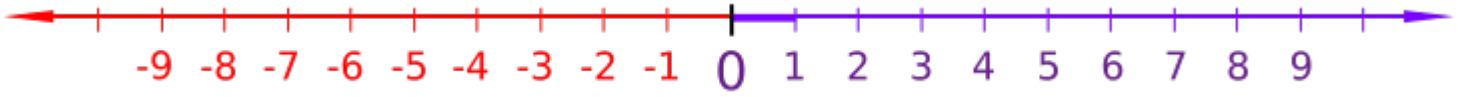
正整数(N^+)、零、负整数





刘徽(A.D. 225-295)

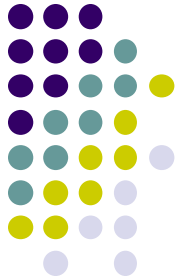
$$4x + 20 = 4$$



整数 $\mathbb{Z}$

	Addition	multiplication
Closure Property	a +b=an integer example 6+2=8	ax b=an integer example 3x4=12
Associative	a+(b +c)=(a +b)+c example 9+(2+4)=(9+2)+4=15	ax(b x c)=(ax b)x c example 3x[-2)x4]= [3x(-2)]x4=-24
Distributive	ax(b +c)=(ax b)+(a x c), (a +b) x c=(a x c)+(b x c) example5x[2+(-3)]=[5x2]+[5x(-3)]=10-15=-5	
Commutative	a+ b=b +a example 3+(-2)=(-2)+3=1	ax b=b x a example 3x(-2)=(-2)x3=-6
Identity	a+0=a example 6+0=6	ax1=a example (-6)x1=-6
Inverse element	a+(-a)=0 example 6+(-6)=0	No inverse element
Zero product property		If a x b=0,then either a=0, or b=0 or both=0

整数之间的整除



- 对任意整数a和b, $a \neq 0$, 我们说a整除b (记作$a|b$) , 如果存在整数c使得 $b = a\,c$.
- 设a, b和c是整数， $a \neq 0$,
  - 若$a|b$，且 $a|c$，则 $a|(b+c)$
  - 若$a|b$，则 $a|(b\,c)$
  - 若$a|b$，且 $b|c$，则 $a|c$

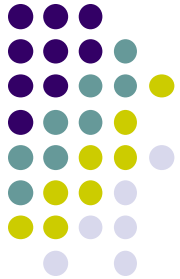
带余除法

- 令a为整数，d为正整数，则存在唯一的整数q和r，且 $0 \le r < d$，满足 $b = dq + r$.
  - d为除数，a为被除数，q为商，r为余数。
  - 记作 $q = a \text{ div } d$，$r = a \bmod d$. 举例：$-11 \bmod 3 = ?$
- 证明：
  - $S=\{r \in N \mid \exists q \in Z.\ r = b-dq\}$是N的非空子集
  - N是良序的，S有最小元素，记为r_0，即$r_0 = b-dq_0$
  - 用反证法易证$r_0<d$, 否则r_0-d是S中比r_0更小的元素, 矛盾
  - 唯一性证明，$0 \le r_1 - r_0 = d(q_0-q_1) < d$，因此，$q_1=q_0$

带余除法（续）

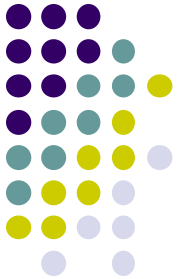
- 令a和b为整数，d为正整数，则
  - $(a + b) \bmod d = (a \bmod d + b \bmod d) \bmod d$.
  - $(a\ b) \bmod d = ((a \bmod d)\ (b \bmod d)) \bmod d$.

同余算术 (高斯, Gauss)



- 设a和b为整数，m为正整数，如果m整除$(b-a)$，就说a模m同余b. 记作 $a \equiv b \pmod{m}$.
- $a \equiv b \pmod{m}$ *iff* $a \pmod{m} = b \pmod{m}$
- $a \equiv b \pmod{m}$ *iff* $\exists k \in \mathbf{Z}.\ a = b + km$
- 举例 $-1 \equiv 5 \pmod 6$, $-2 \equiv 4 \pmod 6$, …, $-5 \equiv 1 \pmod 6$
  - [0]={…,-6, 0, 6, …}
  - [1]={…-5, 1, 7,…}
  - [2]={…,-4, 2, 8, …}
  - …

素数



- 大于1的正整数p称为素数，如果p仅有的正因子是1和p。大于1又不是素数的正整数称为合数。
- 正整数n是合数 *iff* $\exists a \in \mathbf{N}.\ 1 < a < n$, 且 $a \mid n$.
- 算术基本定理：每个大于1的正整数都可以唯一地写为一个素数或者若干个素数的乘积，其中素数因子以非递减序出现。
  - $n = p_1^{\alpha 1}\, p_2^{\alpha 2} \ldots p_k^{\alpha k}$
- 素数举例：2, 3, 5, 7, 11, 13, 17, 19, …
- 合数举例：$100 = 2^2\, 5^2$. $999 = 3^3\, 37$, $1024 = 2^{10}$.

埃拉托色尼筛选法(Eratosthenes, BC276–195)

- 用筛选法求质数（以25以内的为例）

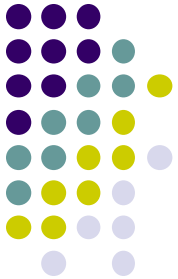
2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25

[2] 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25

[3] 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25

[5] 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25

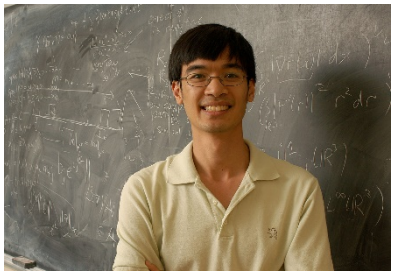
素数（续）



- 下列自然数哪些是素数？
  - 101
  - 2^2-1，2^3-1，2^5-1，…，2^p-1,…
  - 2^{11}-1=2047=23·89 （大数的因数分解有点难）
  - （搜寻尽可能大的梅森素数）
- 如果n是合数，那么n必有不大于$\sqrt{n}$的一个素因子.
- 存在无限多个素数
  - 证明. 反证法，假设只有有限个素数，$p_1, p_2 \ldots, p_k$
  - 令$q=1+p_1p_2 \ldots p_k$，q的素因子是新的素数，矛盾。

素数（续）

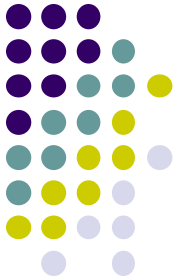
- 任意给定K，存在K个成等差级数的素数(陶哲轩,格林, 2004)
  - 举例：当K=3时，我们有3, 7, 11。



- 任一大于2的偶数都可以写成2个素数之和？
  - 1+1（哥德巴赫猜想，1742）
  - 1+2（陈景润证明，1966）

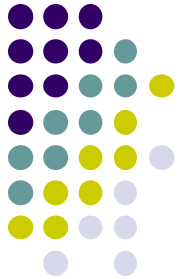
- 素数的分布？
  - 无穷多个“特殊形式的素数”，比如：搜寻尽可能大的梅森素数。
  - 不超过n的素数有多少个？接近于$n / \ln n$ (n充分大时）

最大公约数



- 能整除两个（正）整数的最大正整数称为这两个正整数的最大公约数。记法：gcd(*a*, *b*)
  - gcd(*a*, *b*) = *max*{ $d \in \mathbf{N}^+ \mid d|a, d|b$}，$a \neq 0$ 或者 $b \neq 0$
  - 我们称*a*和*b*是互素的，如果gcd(*a*, *b*) = 1
- 若 $a = p_1^{\alpha 1} p_2^{\alpha 2} \ldots p_k^{\alpha k}$，$b = p_1^{\beta 1} p_2^{\beta 2} \ldots p_k^{\beta k}$，
  则 $\gcd(a, b) = p_1^{\gamma 1} p_2^{\gamma 2} \ldots p_k^{\gamma k}$，$\gamma_i = \min\{\alpha_i, \beta_i\}$
- 求2个正整数的最大公约数
  - gcd(*a*, *b*) = gcd(*a*, *b*-*a*) //不妨假设 *a*<*b*。

欧几里德算法（求最大公约数）

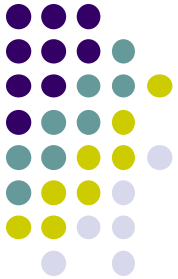


```
function gcd(a, b)  // a>0, b>0
  while a ≠ b
        if a > b
              a := a − b
        else
              b := b − a
  return a
```

```
function gcd(a, b)  // 不全为0的自然数
  while b ≠ 0
        t := b
        b := a mod b
        a := t
  return a
```

```
function gcd(a, b)  // a≥b≥0, a>0
  if b=0
        return a
 else
        return gcd(b, a mod b)
```

最大公约数（续）



- **gcd(a, b)一定是a和b的线性组合，即：**

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

  //欧几里德算法

- **非零整数a和b是互素的 *iff* $\exists s, t \in Z.\ sa+tb=1$**
  - **必要性显然。**
  - **以下证明其充分性。假设$\exists s, t \in Z.\ sa+tb=1$.**
  - **假设$\gcd(a, b)=d$，$\exists a_1, b_1 \in Z.\ a=a_1 d, b=b_1 d$.**
  - **我们有$sa_1 d+tb_1 d=1$. 即 $(sa_1+tb_1)d=1$.**
  - **因此$d=1$. 即$\gcd(a, b)=1$。**

中国剩余定理（孙子算经，5世纪）

$$(S):\ \begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \quad \vdots \\ x \equiv a_n \pmod{m_n} \end{cases}$$

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’。

- 假设正整数$m_1, m_2, \ldots, m_n$两两互素，一元线性同余方程组（S）有解，在模M同余下是唯一的。

$$M = m_1 \times m_2 \times \cdots \times m_n = \prod_{i=1}^{n} m_i \qquad M_i = M/m_i, \ \forall i \in \{1,2,\cdots,n\}$$

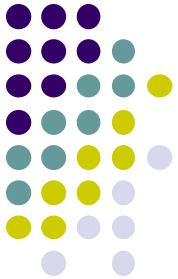
$$x = \sum_{i=1}^{n} a_i t_i M_i. \qquad t_i M_i \equiv 1 \pmod{m_i}, \ \forall i \in \{1,2,\cdots,n\}.$$

- 解的唯一性证明需要下列引理：

  设a, b和c是正整数, a和b是互素的, 若$a|bc$, 则$a|c$。

证明： $\exists s, t \in Z.\ sa+tb=1.\ c=(sa+tb)c=sac+tbc$, 因此, $a|c$。

Euler‘s totient (ϕ函数)



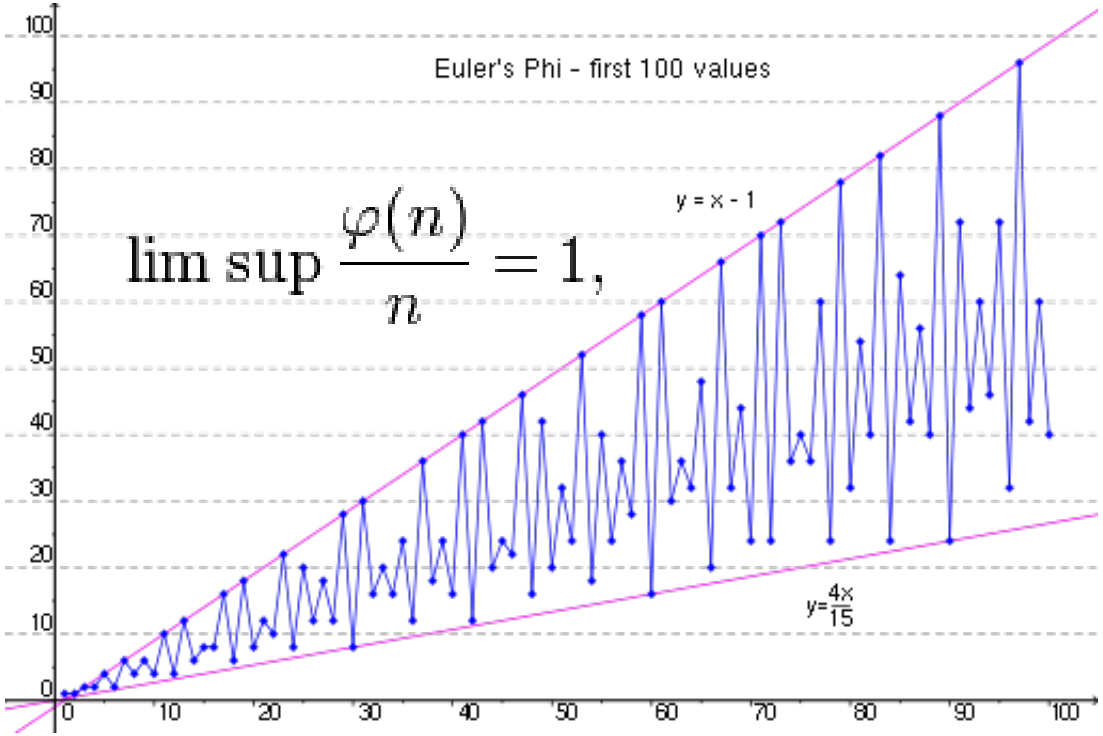
- 不大于n且与n互质的正整数的个数，记为 $\phi(n)$ 。
- $\phi(n) = |\{ k \mid 1 \le k \le n , \gcd(k, n) = 1\}|, n \in N^+$
  - $\phi(3) = 2, \phi(4) = 2, \phi(12) = 4$
- 设 $n = p_1^{\alpha 1} p_2^{\alpha 2} \ldots p_k^{\alpha k}$
- 令 $A_i = \{ x \mid 1 \le x \le n , p_i$整除$x\}$
- $\phi(n) = | \sim A_1 \cap \sim A_2 \cap \ldots \cap \sim A_k |$

$$= n - (n/p_1 + \ldots + n/p_k) + (n/p_1p_2 + \ldots + n/p_{k-1}p_k)$$

$$- \ldots + (-1)^k n/p_1p_2 \ldots p_k$$

$$= n(1 - 1/p_1)(1 - 1/p_2) \ldots (1 - 1/p_k)$$

欧拉函数(phi)



$$\limsup \frac{\varphi(n)}{n} = 1,$$

$$\liminf \frac{\varphi(n)}{n} \log\log n = e^{-\gamma}.$$

欧拉常数 γ = 0.577215665...

欧拉函数(phi)

- $\phi(p)=p-1$，p是素数
- 如果m与n互素，则$\varphi(mn) = \varphi(m)\varphi(n)$.

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

欧拉定理

- **Fermat小定理. 设正整数*a*不是*p*的倍数，则**

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

- **Euler定理. 若正整数*a*与*n*互素，则**

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

RSA的数学基础

- 若a与n互质，则 $a^{\varphi(n)} \equiv 1 \pmod{n}$,
  - 若$\alpha \equiv 1 \pmod{\varphi(n)}$, 则 $a^{\alpha} \equiv a \pmod{n}$
- 若$n=pq$, $\alpha \equiv 1 \pmod{\varphi(n)}$, $0<m<n$, 则$m^{\alpha} \equiv m \pmod{n}$
- 选取大质素p, q: $n=pq$ (n难以分解成质素乘积）.
- 令 $k= \varphi(n)$ (不知道n的质因子，k难以求出）.
- 设e为公钥，d为私钥，满足 $ed \equiv 1 \pmod{k}$.
- 加密： $S = m^e \pmod{n}$.
- 解密： $t = S^d \pmod{n}$. ($t = m$， why?)

作业

- 教材[3.4, 3.5, 3.7]
  - P156: 10, 13, 19, 25
  - P162: 2, 4, 7, 14, 17, 24
  - P182: 19, 20, 28, 41