数论初步

离散数学

南京大学计算机科学与技术系

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*）

整数的代数性质

- 下表给出$\forall a, b, c \in \mathbb{Z}$关于加法和乘法的性质：

性质	加法	乘法
封闭性	$a+b$ 是整数	$a \times b$ 是整数
结合律	$a+(b+c)=(a+b)+c$	$a \times (b \times c)=(a \times b) \times c$
交换律	$a+b=b+a$	$a \times b = b \times a$
存在单位元	$a+\mathbf{0}=a$	$a \times \mathbf{1} = a$
存在逆元	$a+(-\boldsymbol{a})=0$	在整数集中，只有1或 −1关于乘法存在整数逆元，其余整数a关于乘法的逆元为$\frac{1}{a}$，都不为整数。
分配律	$a \times (b+c)=(a \times b)+(a \times c)$	

- 以下介绍数论中的一些重要研究对象

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：

  $$(\exists!\, q, r \in \mathbb{Z} \land 0 \le r < d)(a = d \times q + r)$$

  - 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

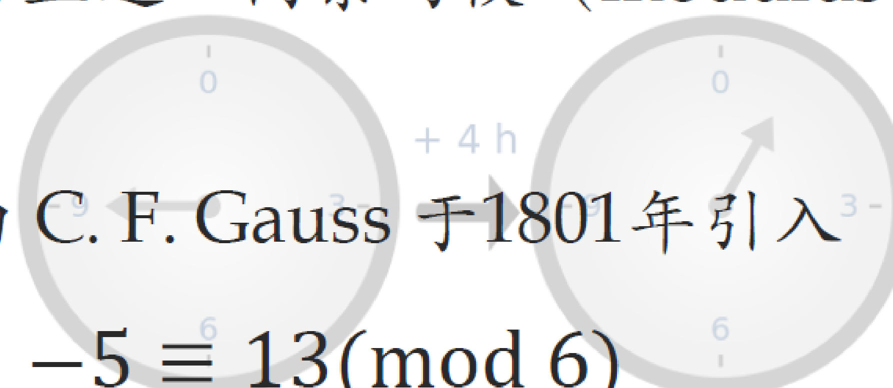
- 模的基本性质：令$a, b \in \mathbb{Z}, d \in \mathbb{Z}^+$，则：
  - $(a + b) \bmod d = (a \bmod d + b \bmod d) \bmod d$
  - $(a \times b) \bmod d = [(a \bmod d)(b \bmod d)] \bmod d$

同余

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

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

  - 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“≡”由 C. F. Gauss 于1801年引入



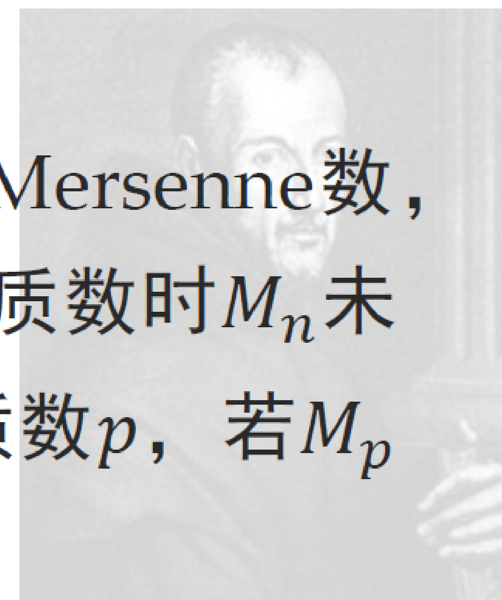
- **例**：$26 \equiv 14(\mathrm{mod}\, 12)$，$-5 \equiv 13(\mathrm{mod}\, 6)$

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
  - $\boldsymbol{n} = \boldsymbol{p}_1^{\alpha_1}\boldsymbol{p}_2^{\alpha_2}\cdots\boldsymbol{p}_k^{\alpha_k}\,(p_1 < p_2 < \cdots < p_k, \alpha_i \in \mathbb{Z}^+)$

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

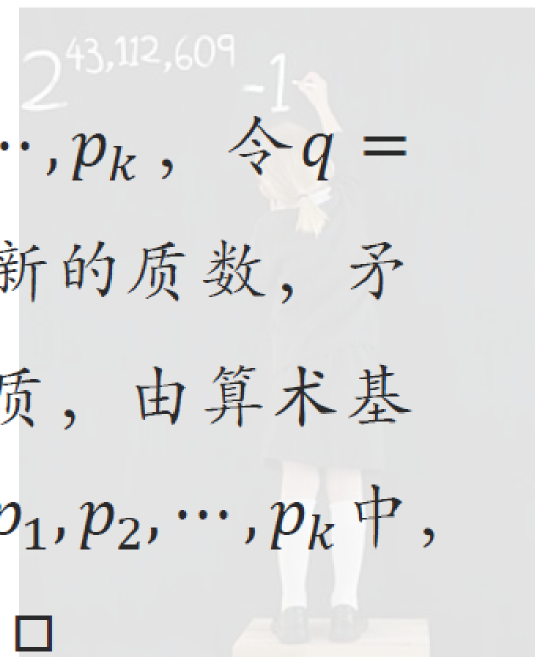


质数

- 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$p_1, p_2, \cdots, p_k$，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$p_1, p_2, \cdots, p_k$中，为新的质数，矛盾。原命题成立。 $\square$



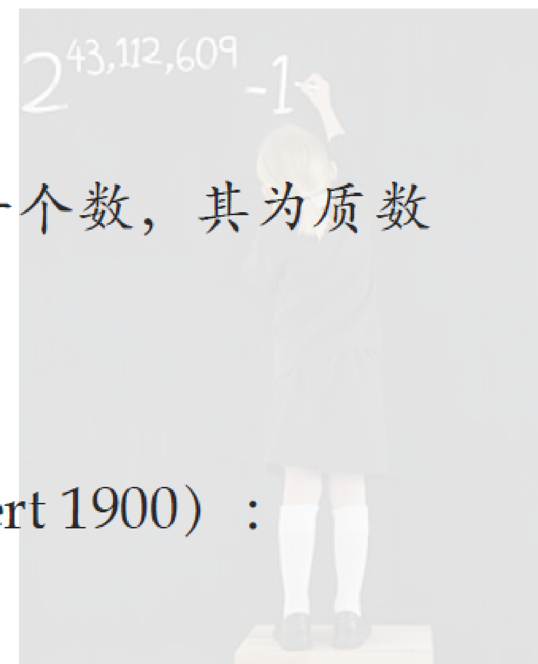
质数定理

- 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

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

  - 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）：

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

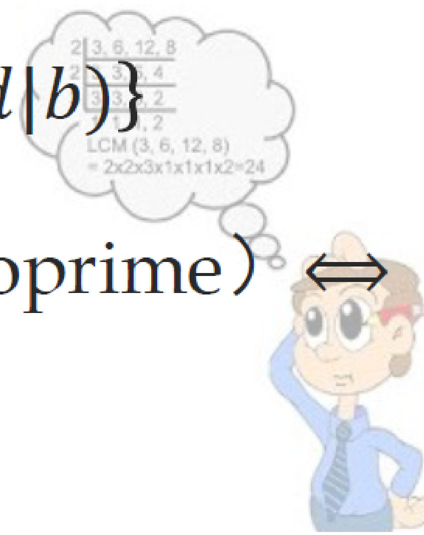


最大公约数

- 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：

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

- 称 $a, b \in \mathbb{Z}^+$互质（mutually prime, coprime）$\Leftrightarrow$ $\gcd(a, b) = 1$（常简记为$(a, b) = 1$）



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：

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

求最大公约数的Euclid算法

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

```
function gcd(a, b)  // 非全0正整数
  while b ≠ 0
      t := b
      b := a mod b
      a := t
  return a
```

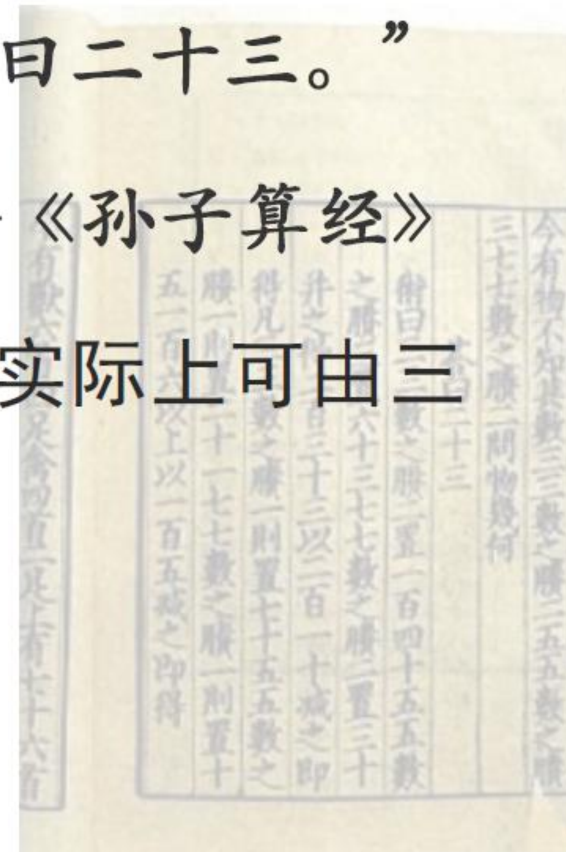
"欧几里得算法是所有算法的鼻祖，因为它是现存最古老的非凡算法。"

——高德纳，《计算机程序设计艺术，第二卷：半数值算法》，第二版（1981），p. 318.

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》


今有物不知其數三三數之賸二五五數之賸三
七七數之賸二問物幾何
答曰二十三

- 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：

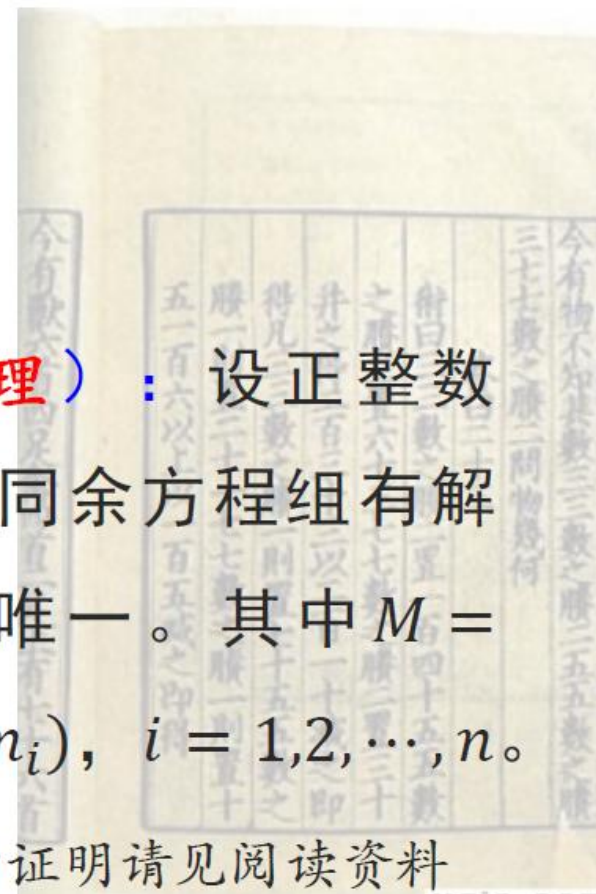
$$
\begin{cases}
x \equiv 2 \pmod 3 \\
x \equiv 3 \pmod 5 \\
x \equiv 2 \pmod 7
\end{cases}
$$

中国剩余定理

- 一元线性同余方程组可写为：

$$\begin{cases} x \equiv a_1 (\mathrm{mod}\, m_1) \\ x \equiv a_2 (\mathrm{mod}\, m_2) \\ \quad\vdots \\ x \equiv a_n (\mathrm{mod}\, m_n) \end{cases}$$

- 定理（线性同余方程组的解存在定理）：设正整数 $m_1, m_2, \cdots, m_n$ 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 $M = \prod_{i=1}^{n} m_i$，$M_i = M/m_i$，$t_i M_i \equiv 1 (\mathrm{mod}\, m_i)$，$i = 1,2,\cdots,n$。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$n \in \mathbb{Z}^+$，

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

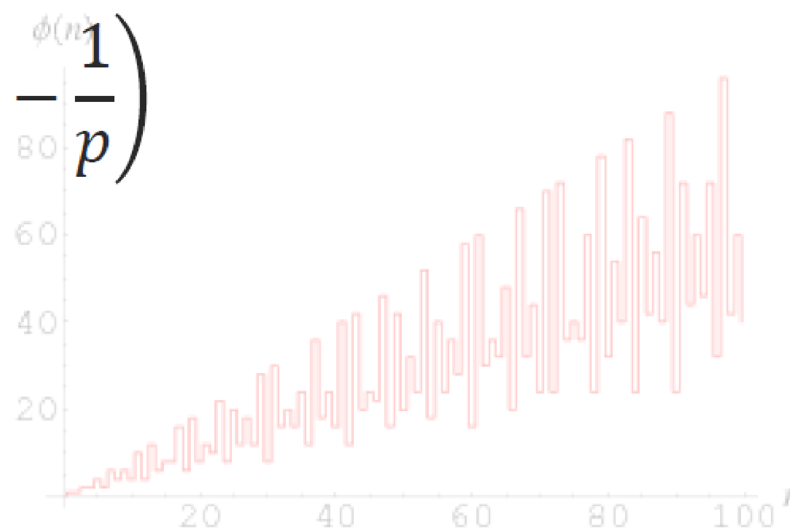
- 例：$\varphi(3) = 2$，$\varphi(4) = 2$，$\varphi(12) = 4$

- 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

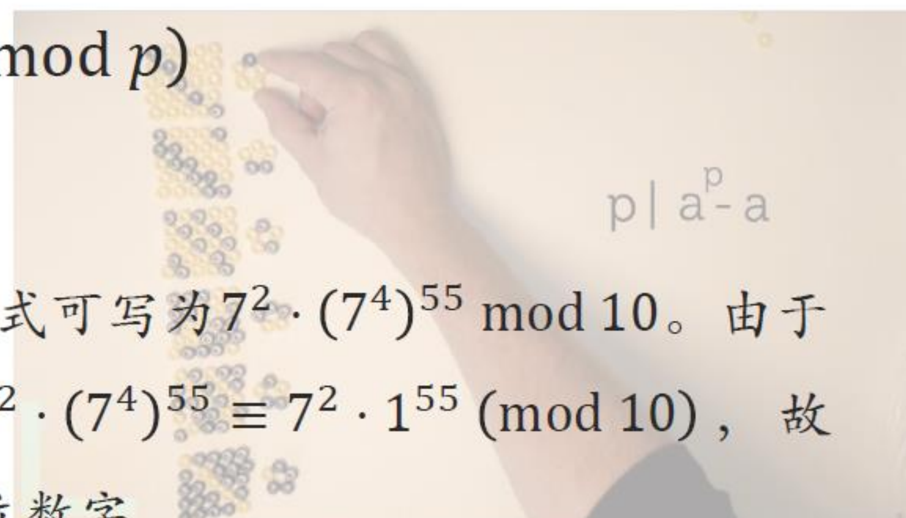
- 定理（**Euler定理**）：对$a,n\in\mathbb{Z}^+$，若$(a,n)=1$，则：

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

- 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：

$$a^{p-1}\equiv 1(\mathrm{mod}\ p)$$

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



归纳与递归

离散数学

南京大学计算机科学与技术系

提要

- 数学归纳法
- 强数学归纳法
- 运用良序公理来证明
- 递归定义
- 结构归纳法

什么是数学归纳法

- 数学归纳法（mathematical induction, MI）是利用归纳原理进行定理证明的一种逻辑方法
- 数学归纳法的理论基础独立地源自两种系统：一是在自然数的公理化系统中的无穷公理，二是存在于ZFC系统中的选择公理（等价于良序公理）
- 数学归纳法常用于证明有关正整数或自然数的命题

数学归纳法的逻辑基础

- 数学归纳法是建立在公理系统中的一个逻辑归纳推理过程：
  - Ⅰ. 基于皮亚诺自然数公理系统的（第一）数学归纳法

    $$\mathbf{P}(1), \forall x\big(\mathbf{P}(x) \to \mathbf{P}(x+1)\big) \Rightarrow \forall x \mathbf{P}(x)$$

  - Ⅱ. 基于选择公理（A.C.）的强数学归纳法（超限归纳法）

    $$\mathbf{P}(1), \forall x\big(\forall y < x, \mathbf{P}(y) \to \mathbf{P}(x)\big) \Rightarrow \forall x \mathbf{P}(x)$$

数学归纳法

- 证明目标
  - $\forall n\ P(n)$　//n的论域为正整数集合
- 证明框架
  - 基础步骤：$P(1)$为真
  - 归纳步骤：对任意正整数k, $P(k) \Rightarrow P(k+1)$.

    //即，证明$\forall k\ (P(k) \rightarrow P(k+1))$
  - 因此，对任意正整数n, $P(n)$ 成立. // 即：$\forall n\ P(n)$

数学归纳法（有效性）

- 良序公理
  - 正整数集合的非空子集都有一个最小元素
- 数学归纳法的有效性（归谬法）
  - 假设$\forall n\ P(n)$不成立，则 $\exists n\ (\neg P(n))$成立.
  - 令$S=\{\ n\in Z^+ \mid \neg P(n)\}$，S是非空子集.
  - 根据良序公理，S有最小元素，记为m, $m\neq 1$
  - $(m\text{-}1)\notin S$, 即$P(m\text{-}1)$成立.
  - 根据归纳步骤，$P(m)$成立，即$m\notin S$，矛盾.
  - 因此，$\forall n\ P(n)$成立.

数学归纳法（举例）

- $H_k=1+1/2+\ldots+1/k$ （k为正整数）
- 证明：$H_{2^n} \geq 1+n/2$ （n为正整数）
  - 基础步骤：$P(1)$为真，$H_2=1+1/2$
  - 归纳步骤：对任意正整数k, $P(k) \Rightarrow P(k+1)$.

$$H_{2^{k+1}} = H_{2^k} + 1/(2^k+1)+\ldots+1/2^{k+1}$$

$$\geq (1+k/2)+2^k(1/2^{k+1}) = 1+(1+k)/2$$

  - 因此，对任意正整数n, $P(n)$ 成立.

数学归纳法（举例）

- 猜测前n个奇数的求和公式，并证明之。
  - 1=1
  - 1+3=4
  - 1+3+5=9
  - 1+3+5+7=16
  - …
  - $1+3+\ldots+(2n-1)=n^2$（n为正整数）
  - 运用数学归纳法证明（练习）

数学归纳法证明时常见错误

- 例1：任意n个人，他们一定全部在同一天出生.
- 错误证明：
  - Basis： 当$n=1$时，只有一个人，命题显然成立；
  - I.H.：假设任意k个人，他们全部在同一天出生，则：
  - I.S.： 当有$k+1$个人时（编号为$1,2,\cdots,k,k+1$），根据归纳假设，第1人至第k人（共k个人）一定在同一天出生；第2至第 $k+1$ 人（共 k 个人）也一定在同一天出生。因此，这$k+1$人全部在同一天出生。根据数学归纳法，命题成立. □
  - 归纳基础错误：$P(1) \nrightarrow P(2)$！

数学归纳法证明时常见错误

- 例2：证明 $\sum_{i=1}^{n} 2i-1=n^2$
- 错误证明：
  - Basis：当 $n=1$ 时，$\sum_{i=1}^{1} 2i-1=1^2$ 命题成立；
  - I.H.：假设当 $n=k$ 时 $\sum_{i=1}^{k} 2i-1=k^2$ 成立，则：
  - I.S.：根据等差数列的求和公式，$\sum_{i=1}^{k+1} 2i-1=1+3+5+\cdots+2(k+1)-1=\frac{[1+2(k+1)-1](k+1)}{2}=(k+1)^2$。

    根据数学归纳法，命题成立. □
  - 归纳过程错误：未证明 $P(k)\rightarrow P(k+1)$！

强数学归纳法

- 证明目标
  - $\forall n\ P(n)$　//n的论域为正整数集合
- 证明框架
  - 基础步骤：$P(1)$为真
  - 归纳步骤：对任意正整数k, $P(1), \ldots, P(k) \Rightarrow P(k+1)$.

    //即，证明$\forall k\ (P(1) \wedge \ldots \wedge P(k) \rightarrow P(k+1))$
  - 因此，对任意正整数n, $P(n)$ 成立. // 即：$\forall n\ P(n)$

强数学归纳法（一般形式）

- 设$P(n)$是与整数n有关的陈述， a和b是两个给定的整数， 且$a \le b$.
- 如果能够证明下列陈述
  - $P(a), P(a+1), \ldots, P(b)$.
  - 对任意$k \ge b$, $P(a) \wedge \ldots \wedge P(k) \rightarrow P(k+1)$
- 则下列陈述成立
  - 对任意$n \ge a$, $P(n)$.

$\{ n \in \mathrm{Z} \mid n \ge a \}$是良序的

强数学归纳法（举例）

- 任意整数n(n ≥2)可分解为（若干个）素数的乘积
  - n = 2.
  - 考察 k+1.
- 用4分和5分就可以组成12分及以上的每种邮资.
  - $P(12)$, $P(13)$, $P(14)$, $P(15)$.
  - 对任意$k \geq 15$, $P(12)\wedge\ldots\wedge P(k)\rightarrow P(k+1)$

数学归纳法（举例）

- 对每个正整数$n \geq 4$，$n! > 2^n$
  - 基础步骤：$P(4)$为真，$24 > 16$
  - 归纳步骤：对任意正整数$k \geq 4$, $P(k) \Rightarrow P(k+1)$.

    $(k+1)! = (k+1)\ k! > (k+1)\ 2^k > 2^{k+1}$
  - 因此，对任意正整数$n \geq 4$, $P(n)$ 成立.

运用良序公理来证明（举例）

- 设a是整数, d是正整数, 则存在唯一的整数q和r满足
  - $0 \leq r < d$
  - $a = dq + r$
- 证明
  - 令$S=\{a-dq \mid 0 \leq a-dq，q \in Z\}$，S非空.
  - 非负整数集合具有良序性
  - S有最小元，记为$r_0 = a-dq_0$.
  - 可证 $0 \leq r_0 < d$

运用良序公理来证明（举例）

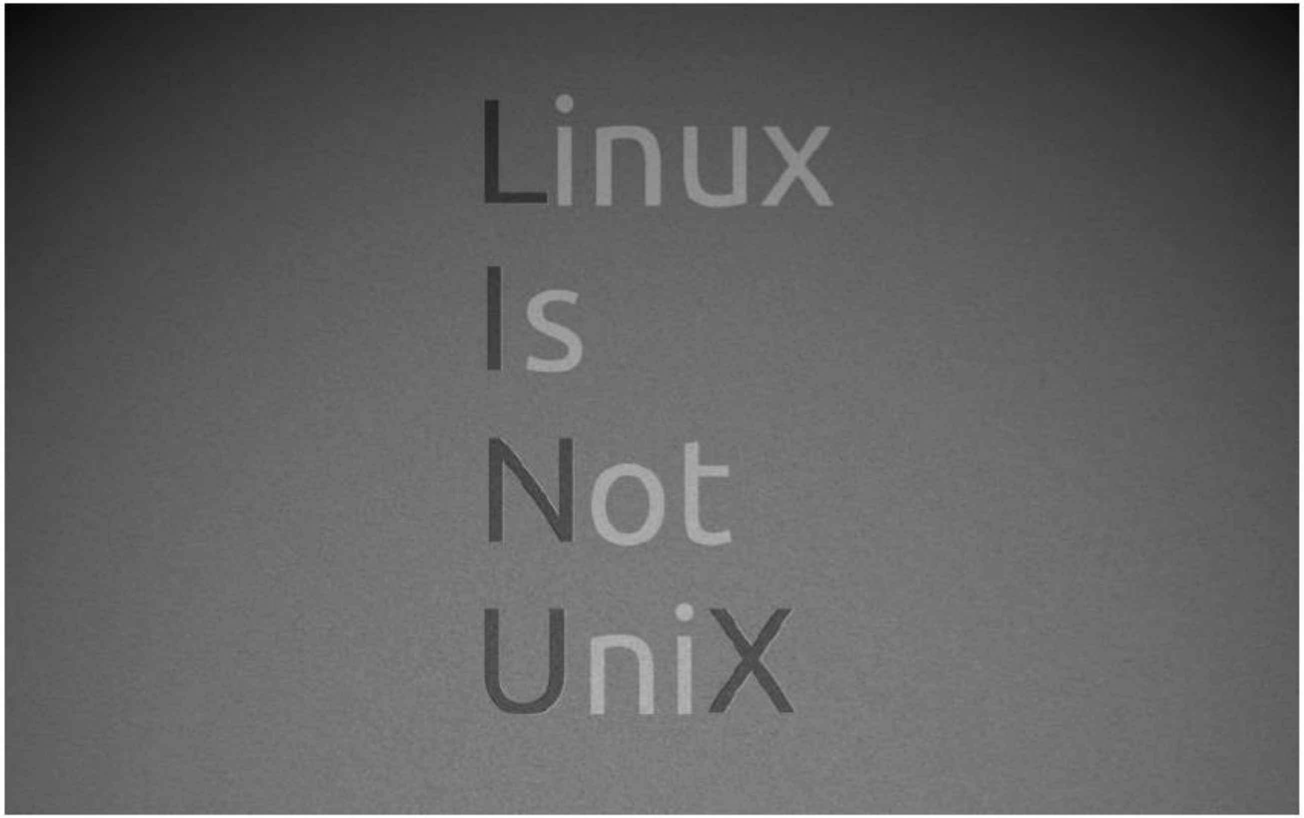
- 在循环赛胜果图中，若存在长度为m（$m \geq 3$）的回路，则必定存在长度为3的回路。

  备注：$a_i \rightarrow a_j$ 表示a_i赢了a_j

证明

- 设最短回路的长度为k（$k \geq 3$） //良序公理的保证
- $a_1 \rightarrow a_2 \rightarrow a_3 \rightarrow \ldots \rightarrow a_k \rightarrow a_1$
- 若$a_3 \rightarrow a_1$, 存在长度为3的回路，矛盾。
- 若$a_1 \rightarrow a_3$, 存在长度为$(k-1)$的回路，矛盾。

递归结构



递归结构

递归定义（N上的函数）

- 递归地定义自然数集合N上的函数。
  - 基础步骤：指定这个函数在0处的值；
  - 递归步骤：给出从较小处的值来求出当前的值之规则。
- 举例，阶乘函数F(n)=n！的递归定义
  - $F(0)=1$
  - $F(n)=n\cdot F(n-1)$ for $n>0$

Fibonacci 序列

- Fibonacci 序列 $\{f_n\}$ 定义如下
  - $f_0 = 0$,
  - $f_1 = 1$,
  - $f_n = f_{n-1} + f_{n-2}$, 对任意$n \geq 2$.
- 其前几个数
  - 0, 1, 1, 2, 3, 5, 8, …
- 证明：对任意$n \geq 0$，$$f_n = \frac{\alpha^n - \beta^n}{\alpha - \beta}$$

其中，$$\alpha = \frac{1+\sqrt{5}}{2}, \beta = \frac{1-\sqrt{5}}{2}.$$

归纳证明: Fibonacci 序列

- 验证：当n=0,1时，陈述正确。
- 对于k+1，

$$f_{k+1} = f_k + f_{k-1}$$

$$= \frac{\alpha^k - \beta^k}{\alpha - \beta} + \frac{\alpha^{k-1} - \beta^{k-1}}{\alpha - \beta}$$

$$= \frac{(\alpha^k + \alpha^{k-1}) - (\beta^k + \beta^{k-1})}{\alpha - \beta}$$

$$= \frac{\alpha^{k+1} - \beta^{k+1}}{\alpha - \beta}.$$

注意：$\alpha^2 = \alpha + 1$，且$\alpha^{n+1} = \alpha^n + \alpha^{n-1}$对任意$n \geq 1$.

递归定义（集合）

- 递归地定义集合。
  - 基础步骤：指定一些初始元素；
  - 递归步骤：给出从集合中的元素来构造新元素之规则；
  - 排斥规则（只包含上述步骤生成的那些元素）默认成立
- 举例，正整数集合的子集S
  - $x \in S$
  - 若$x \in S$且$y \in S$，则 $x+y \in S$。

递归定义（举例）

- 字母表Σ上的字符串集合Σ^*。
  - 基础步骤： $\lambda \in \Sigma^*$ （λ表示空串）；
  - 递归步骤：若$\omega \in \Sigma^*$ 且$x \in \Sigma$，则 $\omega x \in \Sigma^*$ 。
- 字符串的长度（ Σ^*上的函数l）。
  - 基础步骤：$l(\lambda)=0$;
  - 递归步骤：$l(\omega x) = l(\omega) + 1$, 若$\omega \in \Sigma^*$ 且$x \in \Sigma$

递归定义（举例）

- Σ^*上的字符串连接运算。
  - 基础步骤：若$\omega\in \Sigma^*$，则 $\omega \cdot \lambda=\omega$;
  - 递归步骤：若$\omega_1\in \Sigma^*$ 且$\omega_2\in \Sigma^*$ 以及$x \in \Sigma$，

    则 $\omega_1 \cdot (\omega_2\, x) = (\omega_1 \cdot \omega_2)\, x$ 。

    // $\omega_1 \cdot \omega_2$通常也写成$\omega_1\, \omega_2$

递归定义（举例）

- 复合命题的合式公式。
  - 基础步骤：T, F, s都是合式公式，其中s是命题变元;
  - 递归步骤：若E和F是合式公式，则 $(\neg E)$、$(E \wedge F)$、 $(E \vee F)$、$(E \rightarrow F)$和$(E \leftrightarrow F)$都是合式公式。

结构归纳法

- 关于递归定义的集合的命题，进行结构归纳证明。
  - 基础步骤：证明对于初始元素来说，命题成立;
  - 递归步骤：针对生产新元素的规则，若相关元素满足命题，则新元素也满足命题
- 结构归纳法的有效性源于自然数上的数学归纳法
  - 第0步（基础步骤），…

结构归纳法（举例）

- $l(xy) = l(x) + l(y)$, x和y属于 Σ^* 。
- 证明
  - 设$P(y)$表示：每当x属于 Σ^*，就有$l(xy) = l(x) + l(y)$ 。
  - 基础步骤：每当x属于 Σ^*，就有$l(x\lambda) = l(x) + l(\lambda)$ 。
  - 递归步骤：假设$P(y)$为真，a属于 Σ, 要证$P(ya)$为真。
    - 即：每当x属于 Σ^*，就有$l(xya) = l(x) + l(ya)$
    - $P(y)$为真，$l(xy) = l(x) + l(y)$
    - $l(xya)= l(xy)+1= l(x) + l(y)+1=l(x) + l(ya)$

广义结构归纳法（举例）

- N×N是良序的（字典序）
- 递归定义$a_{m,n}$
  - $a_{0,0} = 0$
  - $a_{m,n} = a_{m-1,n} + 1 \ \ (n=0, m>0)$
  - $a_{m,n} = a_{m,n-1} + n \ \ (n>0)$
- 归纳证明 $a_{m,n} = m+n(n+1)/2$

0	**1**	**3**
1	**2**	**4**
2	**3**	**5**

作业

- 教材内容：[Rosen] 4.2—4.3节
- 课后习题：
  - pp.210-213（第七版 pp.277-278）: 18, 22
  - pp.220-223（第七版 pp.290-291）: 7, 12, 36
  - pp.233-235（第七版 pp.302-304）: 25, 32, 47, 54
  - pp. 245 (第七版 pp.313): 37