第二章 整除性、线性方程与最大公因数

张志强
智能信息处理研究中心
http://rciip.hrbeu.edu.cn

基本概念

- 整除
  - 假设m与n是整数，m≠0，m整除n是指n是m的倍数，即存在整数k使得n=km，记做m|n，如果m不整除n，则记做 m∤n
  - 称整除n的数为n的因数
- 公因数
  - 已知两个整数，所谓公因数就是指能够同时整除这两个数的数，如4是12和20的公因数

基本概念

- 最大公因数
  - 两个数a和b的最大公因数就是指整除它们两个的最大数，记做gcd(a,b)，如果gcd(a,b)=1，则称a和b互素
  - 求gcd(225,120),gcd(36,132)
    - 分解因数方法：$225=3^2*5^2$, $120=2^3*3*5$
    - 列出a和b的所有因数，然后找出同时出现这两个列表中的最大数
  - Try gcd(1 160 718 174, 316 258 250)=?

欧几里得算法

- 例子，gcd(225,120)

  225=1*120+105

  120=1*105+15

  105=7*15+0
- 求最大公因数问题转化为求商和余数的问题
  - 课堂练习：

    gcd(1 160 718 174, 316 258 250)=?

欧几里得算法

- 一般情形

$$a=q_1*b+r_1$$
$$b=q_2*r_1+r_2$$
$$r_1=q_3*r_2+r_3$$
$$r_2=q_4*r_3+r_4$$
$$\cdots\cdots$$
$$r_{n-3}=q_{n-1}*r_{n-2}+r_{n-1}$$
$$r_{n-2}=q_n*r_{n-1}+r_n$$
$$r_{n-1}=q_{n+1}*r_n+0$$

- 第一步证明r_n是a和b的公因数
- 第二步证明r_n是最大公因数

- 为什么该算法是正确的？

欧几里得算法

- 定理：要计算两个整数a和b的最大公因数，先令r_{-1}=a，r_0=b，然后计算相继的商和余数

$$r_i=q_{i+1}*r_i+r_{i+1} \qquad (i=0,1,2,\ldots)$$

- 直到余数r_{i+1}为0，最后的余数r_n就是a和b的最大公因数

提问：为什么欧几里得算法总能结束？

作业

- 编写程序计算两个整数a和b的最大公因数，即使a和b中的一个等于零，程序也应正常运行，不会出现死循环。

线性方程

- 已知两个整数a和b，我们观察由a的倍数和b的倍数得到的所有可能的整数，即ax+by的所有整数，其中x和y可为任何整数，例如　取a=42，b=30，其线性组合的值为

	x=-3	*x =-2*	*x =-1*	*x =0*	*x =1*	*x =2*	*x =3*
y=-3	-216	-174	-132	-90	-48	-6	36
y=-2	-186	-144	-102	-60	-18	24	66
y=-1	-156	-114	-72	-30	12	54	96
y=0	-126	-84	-42	0	42	84	126
y=1	-96	-54	-12	30	72	114	156
y=2	-66	-24	18	60	102	144	186
y=3	-36	6	48	90	132	174	216

线性方程

- 观察
  - 每个结果均被6整除，因为42和30均是6的倍数，一般地，形如ax+by均被gcd(a,b)整除，这个结论显然
  - 42与30的最大公因数6出现在上述表中，这一点并不显然，42*(-2)+30*3=6，这是否是一个普适的结论？即“形如ax+by的最小正整数等于gcd(a,b)”
    - ax+by=gcd(a,b)的解如何求？

线性方程

- 例，试解60x+22y=gcd(60,22)
- 回忆欧几里得算法计算最大公因数

60=2*22+16 (1)
22=1*16+6 (2)
16=2*6+4 (3)
6=1*4+2 (4)
4=2*2+0

- 令a=60，b=22代入上面的第一个式子，得16=a-2b，用此式代入第二个式子得b=(a-2b)+6 => 6=-a+3b，现将16和6的表达式代入第三式得a-2b=2*(-a+3b)+4 => 4=3a-8b，代入第四式得11b-4a=2 → x=-4,y=11,

线性方程

- 从几何上来看ax+by=g是平面上的一条斜率为-a/b的直线，则如果(x_0,y_0)是上面方程的一个解，那么这条直线上的坐标均为整数的点也都是方程的解
- 定理(线性方程定理)：设a和b是非零整数，g=gcd(a,b)，方程ax+by=g总有一个整数解(x_0,y_0)，它可以通过欧几里得算法得到，则方程的每一个解均可由下式得到，其中k为任意整数

$$\left(x_0 + k\cdot\frac{b}{g}, y_0 - k\cdot\frac{a}{g}\right)$$

线性方程

- 例如，60x+22y=gcd(60,22)=2
  有解x=-4,y=11，于是线性方程定理表明每个解均可由公式(-4+11k, 11-30k)得到
- 结论
  - 方程ax+by=gcd(a,b)总有解。
  - 这个结论在理论上和实践上都很重要，后面的内容就需要用到它。例如在密码学研究中就需要解方程ax+by=1

练习

- 求方程的所有整数解

  105x+121y=1

  x_0=-53, y_0=46

  (-53+121k,46-105k)