讲稿

张文泰

rchardx@gmail.com

20100122-rev8

1 整除

1.1 自然数、Peano 公理

主要是最小自然数原理以及数学归纳法。

例题 1.1. 设$n \neq 1$。证明：$(n-1)^2|n^k-1$的充要条件是$(n-1)|k$。

证. $n^k-1=[(n-1)+1]^k-1=A(n-1)^2+k(n-1)$，这里$A$是一个整数，又$(n-1)^2|n^k-1$，所以必然有$(n-1)|k$，反过来命题同样成立。得证。 □

1.2 整除和素数

素数的检验。

例题 1.2. 证明：形如$4m+1$的素数有无穷多个。

证. 设$p_1, p_2, \ldots, p_r$是所有$4m+1$形式的素数，且$p_i=4m_i+1$。我们令$n=p_1p_2\cdots p_r+1$，则$n \equiv 2 \pmod 4$。那么如果n的素因数全都是$4m+3$形式，那么$n \equiv 1 \pmod 4$或$n \equiv 3 \pmod 4$，绝不会$n \equiv 2 \pmod 4$，所以一定存在一个$p=4m+1|n$，但是这个p没有在$p_1, p_2, \ldots, p_r$中出现，所以矛盾。 □

1.3 带余除法、辗转相除法

重点是辗转相除法及其扩展，并介绍相关的 Euclid's Algorithm。

使用 Euclid 辗转相除法，我们还可以求出$ax+by=d$的解。从后面的内容我们知道，这个不定方程有解的充要条件是$(a,b)|d$。我们先求

出$ax+by=(a,b)$的解，然后可以得到原方程的解。具体的做法是使用迭代。我们先考虑和原始的辗转相除法相同的过程，当最后$b=0$时，$a'x=a'$的解是$x=1,y=0$。对于$ax+by=(a,b)$，下一层的运算结果是$bx'+(a \bmod b)y'=(a,b)$，那么可以解得$x=y',y=x'-\lfloor\frac{a}{b}\rfloor y'$，因为$\lfloor\frac{a}{b}\rfloor\times b+(a \bmod b)=a$。

例题 1.3. *设$a>2$是奇数。证明*

(i) 一定存在正整数$d\le a-1$，使得$a|2^d-1$。

(ii) 设d_0是满足上面的最小正整数d。那么，$a|2^h-1$的充要条件是$d_0|h$。

证. 先证 (i)。考虑以下a个数：

$$2^0,2^1,2^2,\dots,2^{a-1}$$

显然，$a\nmid 2^j(0\le j<a)$。由定理知，对于每一个j，$0\le j<a$，

$$2^j=q_ja+r_j,\quad 0<r_j<a$$

所以a个余数$r_0,r_1,\dots,r_{a-1}$仅可能取$a-1$个值。因此其中必有两个相等，设为r_i,r_k，不妨设$0\le i<k<a$。因而有

$$a(q_k-q_i)=2^k-2^i=2^i(2^{k-i}-1)$$

所以，$a|2^{k-i}-1$，则$d=k-i\le a-1$，(i) 得证。

下面证 (ii)。易证充分性，所以只要证必然性。

$$h=qd_0+r,\quad 0\le r<d_0$$

因而有

$$2^h-1=2^{qd_0+r}-2^r+2^r-1=2^r(2^{qd_0}-1)+(2^r-1)$$

易得$a|2^r-1$，由此及d_0的最小性得$r=0$，即$d_0|h$。 □

例题 1.4. *给定a,d,n,m，求$\sum_{i=0}^{n-1}\lfloor\frac{a+di}{m}\rfloor$。*

1.4 最大公约数

几个证明和性质。整系数线性组合。

第一个途径：

定理 1.1. $a_j|c(1 \le j \le k)$的充要条件是$[a_1,\dots,a_k]|c$。

证. 充分性显然。设$L=[a_1,\dots,a_k]$。得

$$c = qL + r, \quad 0 \le r < L$$

由此及$a_j|c$推出$a_j|r$，所以r是公倍数。进而，又由$0 \le r < L$得$r=0$，所以$L|c$。 □

例题 1.5. 设p是素数。证明：若$(a,p)=1$，则$p|a^{p-1}-1$。

证. 首先要说明组合数的一个性质

$$\binom{p}{j} = \frac{p!}{j!(p-j)!}$$

是整数，即$j!(p-j)!|p!$。由于p是素数，所以，对任意$1 \le i \le p-1$有$(p,i)=1$。因此

$$(p, j!(p-j)!) = 1, \quad 1 \le j \le p-1$$

进而推出，当$1 \le j \le p-1$时$j!(p-j)!|(p-1)!$，也就是$p|\binom{p}{j}$。

我们先证$p|a^p-a$。用归纳法。当$a=1$时显然成立，若$a=n$时成立，$(n+1)^p-(n+1)=n^p-n+pA$，这里A是一个整数。显然，$a=n+1$时也成立，所以$p|a^p-a$。再由$(a,p)=1$，命题得证。 □

第二个途径:

定理 1.2. 设$a_1,\dots,a_k$是不全为零的整数。我们有

(i) $(a_1,\dots,a_k)=\min\{s=a_1x_1+\dots+a_kx_k : x_j \in \boldsymbol{Z}(1 \le j \le k), s>0\}$，即$a_1,\dots,a_k$的最大公约数等于$a_1,\dots,a_k$的所有整系数线性组合组成的集合$S$中最小的整数。

(ii) 一定存在一组整数$x_{1,0},\dots,x_{k,0}$使得

$$(a_1,\dots,a_k) = a_1x_{1,0} + \dots + a_kx_{k,0} \tag{1}$$

证. 由于$0 < a_1^2+\dots+a_k^2 \in S$，所以集合$S$中有正整数。由最小自然数原理得$S$中必有最小数$s_0$。显然，对于任一公约数$d|a_j(1 \le j \le k)$，则必有$d$整除$S$任一元素，那么$d|s_0$。所以，$|d| \le s_0$。另外

$$a_j = q_js_0 + r_j, \quad 0 \le r_j < s_0$$

因为s_0可以被$x_1,\dots,x_k$表示，a_j也可以，而$r_j=a_j-q_js_0$，所以$r_j \in S$。如果$r_j>0$，则与s_0最小矛盾，所以$r_j=0$。即s_0是最大公约数。 □

例题 1.6. 设m,n是正整数。证明$(2^m-1,2^n-1)=2^{(m,n)}-1$。

证. 不妨设$m\geq n$。由带余除法得$m=qn+r,0\leq r<n$。我们有

$$2^m-1=2^{qn+r}-2^r+2^r-1=2^r(2^{qn}-1)+2^r-1$$

由此及$2^n-1|2^{qn}-1$得

$$(2^m-1,2^n-1)=(2^n-1,2^r-1)$$

注意到$(m,n)=(n,r)$，若$r=0$，则$(m,n)=n$，结论成立。若$r>0$，则继续对$(2^n-1,2^r-1)$做同样的处理，由辗转相除法可以知道结论成立。

值得注意的是，这里的 2 用任何一个大于 1 的自然数替代都是成立的。

（联想：$(F_m,F_n)=F_{(m,n)}$。） □

例题 1.7. 设p是奇素数，q是2^p-1的素因数。证明$q=2kp+1$。

证. 首先有$q|2^{q-1}-1$。再得$q|2^{(p,q-1)}-1$，所以$p|q-1$，再由p为奇素数得$q=2kp+1$。 □

例题 1.8. $13|a^2-7b^2$的充要条件是$13|a,13|b$。

证. 充分性显然，证必要性。若$13\nmid a$，那么$13\nmid b$，则一定有x,y使得$13x+by=1$。由此及$13|y^2(a^2-7b^2)=(ay)^2-7(by)^2$，($(by)^2=(13x)^2+1-26x$)得到$13|(ay)^2-7$。这个式子不可能被 13 整除，矛盾。所以$13|a,13|b$。 □

1.5 算术基本定理

重点在于分解式。

例题 1.9. 给你一个正整数$n(n\leq 9\times 10^{14})$，求有多少种方式使得n能表示为若干个连续正整数的和。

例题 1.10. 练习题 *Factor*（练习题之后讨论）。

2 同余

2.1 同余、同余类、剩余系

简单地给出 Euler 函数$\varphi(p^k)$的公式。

例题 2.1. 给定k,n，求$\sum_{i=1}^{n}(k \mod i)$。

证. 对于当前的i，令$p = k \mod i, q = \lfloor \frac{k}{i} \rfloor$；如果$\left\lfloor \frac{k}{i+1} \right\rfloor$的值不变，$k \mod (i+1)$的值必然比当前的余数小$q$，所以可以把$p$一直减$q$直到小于0为止（减$\left\lfloor \frac{p}{q} \right\rfloor$次），将所得的和加入结果中。同时$i$增加$\left\lfloor \frac{p}{q} \right\rfloor$。 □

例题 2.2. 当正整数m满足什么条件时$1^3 + 2^3 + \cdots + (m-1)^3 + m^3 \equiv 0 \pmod m$一定成立。

证. 因为$k^3 + (m-k)^3 \equiv 0 \pmod m$，所以$1^3 + 2^3 + \cdots + (m-1)^3 + m^3 \equiv 0 \equiv m^3 + (1^3 + (m-1)^3) + \cdots \pmod m$。

当$2 \nmid m$，此式成立；当$2|m$时，若$4|m$，仍然成立。综上当$2 \nmid m$或$4|m$成立；当$2|m$且$4 \nmid m$时不成立。 □

2.2 Euler 函数与 Fermat-Euler 定理

定理的证明：既约剩余系乘积相同。

例题 2.3. 给出n,m，求$x_1,\ldots,x_n$的数量，这里$0 < x_i \le m$，且$(x_1,\ldots,x_n,m) = 1$。

证. 我们考察扩展的欧拉函数$\varphi(m,n)$。讨论。 □

例题 2.4. 练习题 *Sum*（练习题之后讨论）。

2.3 Wilson 定理

定理 2.1 (Wilson)**.** 设p是素数，$r_1,\ldots,r_{p-1}$是模p的既约剩余系，我们有

$$r_1 \cdots r_{p-1} \equiv -1 \pmod p$$

特别的

$$(p-1)! \equiv -1 \pmod p$$

证. 当$p = 2$时，结论成立。所以设$p \ge 3$。

对这一组给定的既约剩余系中每一个r_i，必然存在一个唯一的r_j使得

$$r_i r_j \equiv 1 \pmod p \tag{2}$$

使$r_i = r_j$的充要条件是

$$r_i^2 \equiv 1 \pmod p$$

即

$$(r_i - 1)(r_i + 1) \equiv 0 \pmod p$$

由于p是素数且$p \geq 3$，所以上式成立当且仅当

$$r_i - 1 \equiv 0 \pmod p$$

或

$$r_i + 1 \equiv 0 \pmod p$$

由于$p \geq 3$，所以这两个条件不能同时成立。因此，在既约剩余系中，除了

$$r_i \equiv 1, -1 \pmod p$$

这两个数以外，对其它的r_i必有$r_j \neq r_i$使得式 2成立。不妨设$r_1 \equiv 1 \pmod p$，$r_{p-1} \equiv -1 \pmod p$。这样，在这组剩余系中除去满足上式的两个数以外，其它的数恰好可以按照式 2两两分完，即满足

$$r_2 \cdots r_{p-2} \equiv 1 \pmod p$$

所以定理得证。 □

例题 2.5. 设p是奇素数，证明

$$1^2 \cdot 3^2 \cdots (p-2)^2 \equiv (-1)^{(p+1)/2} \pmod p$$

证. 注意到当p是奇素数时

$$\begin{aligned}(p-1)! &= (1 \cdot (p-1))(3 \cdot (p-3)) \cdots ((p-2)(p-(p-2))) \\ &\equiv (-1)^{(p-1)/2} \cdot 1^2 \cdot 3^2 \cdots (p-2)^2 \pmod p\end{aligned}$$

由此可以得证。 □

例题 2.6. 设素数$p > 5$。证明$(p-1)! + 1$不可能是素数的方幂。

证. 显然，$p|(p-1)!+1$，那么如果$(p-1)!+1$为某个素数的方幂，那么这个素数一定是p。注意到$p-1|(p-2)!$，我们设$(p-1)!+1 = p^k$，得到$p-1|k$ (数学归纳法)。然后可以导出矛盾。

数学归纳法：$p^n - 1 = (p-1+1)^n - 1 = A(p-1)^2 + n(p-1)$。

矛盾：$(p-1)! + 1 = p^k \leq p^(p-1)$，而左边明显小于右边。 □

例题 2.7. 练习题 *Color*（练习题做完后讨论）。

3 同余方程

注意多项式同余的最高“有效”次数。

3.1 一次同余方程

3.2 一次同余方程组、孙子定理

例题 3.1. 设k是给定的正整数。证明：一定存在k个相邻整数，其中任何一个数都能被大于1的立方数整除。

证. 设$p_1, \ldots, p_k$，考虑$x \equiv -j+1 \pmod{p_j^3}, j=1,\ldots,k$。若$x_0$是一个解，那么$x_0, x_0+1, \ldots, x_0+k-1$就是答案。 □

3.3 模为素数的二次同余方程

定理 3.1 (Euler 判别法). 设素数$p>2$，$p \nmid d$。那么，d是模p的二次剩余的充要条件是

$$d^{(p-1)/2} \equiv 1 \pmod p \tag{3}$$

d是模p的二次非剩余的充要条件是

$$d^{(p-1)/2} \equiv -1 \pmod p \tag{4}$$

证. 我们先证明上述两个式子有且仅有一个成立。我们有

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

所以

$$(d^{(p-1)/2}-1)(d^{(p-1)/2}+1) \equiv 0 \pmod p$$

由于素数$p>2$以及

$$(d^{(p-1)/2}-1, d^{(p-1)/2}+1)|2$$

所以，上面两个判别式有且仅有一个成立。

下面证式 3成立是d为p的二次剩余的充要条件。先证必要性。若d是p的二次剩余，则必有x_0使得

$$x_0^2 \equiv d \pmod p$$

因而

$$x_0^{p-1} \equiv d^{(p-1)/2} \pmod p$$

由于$p \nmid d$，所以$p|x_0$，因而

$$x_0^{p-1} \equiv 1 \pmod p$$

必要性得证。

再证充分性。证明方法和我们证明 Wilson 定理的方法一样。设式 3成立，此时必然有$p \nmid d$。考虑

$$ax \equiv d \pmod p$$

对于$1 \leq i < j \leq (p-1)/2$，我们有

$$i^2 \not\equiv j^2 \pmod p$$

所以，p的既约剩余系中两两可以搭配成上式的解，所以

$$(p-1)! \equiv d^{(p-1)/2} \equiv -1 \pmod p$$

矛盾，充分性得证。 □

例题 3.2. *对于给定的n,*

- *求出$x^2 \equiv 1 \pmod n$的解数；*
- *求出所有x满足$x^2 \equiv 1 \pmod n$。*

证. 我们先假定n的不同素因数个数是r。考察$x^2 \equiv 1 \pmod{p^k}$，我们发现由于$(x-1)(x+1) \equiv 1 \pmod{p^k}$，所以当$p > 2$时只能完全分配到一边，就是两个解。当$p = 2$时，由于$(x-1)$和$(x+1)$只相差2，只能同时被2整除。我们令符号$[p]$表示命题$p$成立时值为1，否则为0。那么$p = 2$时的解数就是$2^{[8|p^k]+[4|p^k]-[2|p^k]}$。我们考虑到各个不同的同余方程是独立的，不同的素因数之间可以分开计算，所以总的解数是$2^{r+[8|n]+[4|n]-[2|n]}$。 □

3.4 Legendre 符号、Gauss 二次互反律

4 不定方程

4.1 Pythagoras 方程

例题 4.1. 不定方程

$$x^4 + y^4 = z^2$$

无$xyz \neq 0$的解。

证. 该命题即要证无正整数解。假若有正整数解，那么在全体正整数解中，必有一组解x_0, y_0, z_0，使得z_0取最小值。

(i) 必有$(x_0, y_0) = 1$。若不然，有素数$p|x_0, p|y_0$，则推出$p^2|z_0$，与z_0的最小性矛盾。由x_0^2, y_0^2, z_0为方程$x^2 + y^2 = z^2$的本原解得，x_0, y_0必为一奇一偶，不妨设$2|y_0$，以及$(z_0, y_0) = 1$。

(ii) $g_1 = (z_0 - y_0^2, z_0 + y_0^2) = 1$。因为$g_1|(2z_0, 2y_0^2) = 2(z_0, y_0^2) = 2$，由此及$2 \nmid z_0 - y_0^2$即得$g_1 = 1$。由此及

$$(z_0 - y_0^2)(z_0 + y_0^2) = x_0^4$$

我们令

$$z_0 - y_0^2 = u^4, \quad z_0 + y_0^2 = v^4$$

这里$v > u > 0, (u, v) = 1, 2 \nmid uv$。进而有

$$y_0^2 = (v^2 - u^2)\frac{v^2 + u^2}{2} \tag{5}$$

(iii) $g_2 = (v^2 - u^2, (v^2 + u^2)/2) = 1$。因为

$$g_2|(v^2 - u^2, v^2 + u^2)|(2v^2, 2u^2) = 2(v^2, u^2) = 2$$

由$2 \nmid uv$得到$2 \nmid (v^2 + u^2)/2$，因此$g_2 = 1$。我们再令

$$v^2 - u^2 = a^2, \quad (v^2 + u^2)/2 = b^2$$

这里$a > 0, b > 0, (a, b) = 1$，及$2|a, 2 \nmid b$。

(iv) 由u, v满足的条件及a, b得

$$0 < b < v < z_0$$

及u, a, v是方程$x^2 + y^2 = z^2$的本原解且$2|a$。因此得到

$$u = r^2 - s^2, \quad a = 2rs, \quad v = r^2 + s^2$$

所以

$$r^4 + s^4 = b^2$$

而$b < z_0$，与z_0的最小性矛盾，命题得证。

□

4.2 Lagrange 定理

每个正整数一定可以表示为四个平方数之和，即对任意的$n \geq 1$，不定方程

$$x_1^2 + x_2^2 + x_3^2 + x_4^2 = n$$

有解。

如果需要证明这个定理，下面的恒等式是必须引进的：

$$\begin{aligned}
&(a_1^2 + a_2^2 + a_3^2 + a_4^2)(b_1^2 + b_2^2 + b_3^2 + b_4^2) \\
&= (a_1b_1 + a_2b_2 + a_3b_3 + a_4b_4)^2 + (a_1b_2 - a_2b_1 + a_3b_4 - a_4b_3)^2 \\
&+(a_1b_3 - a_3b_1 + a_4b_2 - a_2b_4)^2 + (a_1b_4 - a_4b_1 + a_2b_3 - a_3b_2)^2
\end{aligned}$$