数论入门

Weil.A

December 3, 2017

1

我们假定读者了解“集合”和“子集”的概念． $\in$表示“属于某个集合的元素”． 我们用$\mathbb{Z}$表示所有整数的集合，$\mathbb{Q}$表示所有有理数的集合． 我们假设整数和有理数的基本性质：

（1） $x+(y+z)=(x+y)+z$.

（2） $x+y=y+x$.

（3） 方程$a+x=b$存在唯一解x（如果a，b在$\mathbb{Z}$中，那么$x\in\mathbb{Z}$，如果a，b在$\mathbb{Q}$中，那么$x\in\mathbb{Q}$）.

（4） $0+x=x$.

（1’） $(xy)z=x(yz)$.

（2’） $xy=yx$.

（3’） 方程$ax=b$存在唯一解$x\in\mathbb{Q}$，如果a，b在$\mathbb{Q}$中，而且$a\neq 0$.

（4’） $1\cdot x=x$.

（5） $x(y+z)=xy+xz$（分配律）.

$a+x=b$的唯一解记为$b-a$，对于$a\neq 0$，$ax=b$的唯一解记为$\frac{b}{a}$.

有理数是正的(≥ 0) 或者负的(≤ 0)；只有0是两者都是.[1] $b\geq a$（或者$a\leq b$)意味着$b-a\geq 0$；$b>a$（或者$a<b$)意味着 $b\geq a$，$b\neq a$． 如果$x>0$，$y>0$，那么$x+y>0$以及$xy>0$.

如果a，b，x都是整数，$b=ax$，则称b为a的倍数；称a整除b或者是b的因子；此时我们记之为$a|b$.

最后，我们有：

（6） 非空的正整数集合包含一个最小整数.

[1]注意，这里正负的定义和我们平常的是不一样的.

事实上，这样的集合中包含某个整数n；于是$0,1,\ldots,n-1,n$中的第一个包含在这个集合中的整数即满足我们的要求．(6)的一个等价形式是“数学归纳原理”：

(6’) 如果关于正整数x的的断言对于$x=0$是正确的，并且对于所有的$x<n$成立可以推出$x=n$的时候这个断言也是正确的，那么它对所有的x正确.

证明．令F表示由使断言不成立的正整数构成的集合，如果F不是空的，应用(6)；可以推出与(6’)中假设矛盾的结论. □

习题

1. 证明等式$(-1)\cdot(-1)=1$是分配律的推论.

   证明

$$\begin{aligned}0&=(-1)\cdot 0\\&=(-1)\cdot(-1+1)\\&=(-1)\cdot(-1)+(-1)\cdot 1\\&=(-1)\cdot(-1)-1\end{aligned}$$

   因此:

$$(-1)\cdot(-1)=1$$

2. 证明任何一个整数$x>1$或者有一个>1而且$\leq\sqrt{x}$的因子，或者不存在任何>1而且$<x$的因子(在后一种情形下，这个整数称为素数；参考第4节).

   证明

   假设x不是素数，也就是说存在$a|x$，这里$1<a<x$，不妨设$x=ab$，因此可以知道b满足不等式

$$1<b<x,$$

   我们证明$\min(a,b)$满足题目中的条件$1<\min(a,b)\leq\sqrt{x}$，为了讨论方便，不妨设$a\leq b$，于是

$$x=ab\geq a^2$$

   也就是说

$$a\leq\sqrt{x},$$

   结论成立.

3. 使用归纳法证明

$$1^3+2^3+\cdots+n^3=[\frac{n(n+1)}{2}]^2.$$

这个证明比较简单，这里不讨论了. 对于这个题目，难点在于如何发现这个等式，考虑如下等式:

$$(k+1)^4=k^4+4k^3+6k^2+4k+1,\quad k=1,2,\cdots,n.$$

4. 使用归纳证明对于任何$n\geq 0$，$4^{2n+1}+3^{n+2}$是13的倍数.

这个证明也不难，这里给出递推部分，起点的验证省略. 令$a_n=4^{2n+1}+3^{n+2}$.

$$\begin{aligned}a_{n+1}&=4^{2n+3}+3^{n+3}\\&=4^2\cdot 4^{2n+1}+3\cdot 3^{n+2}\\&=13\cdot 4^{2n+1}+3(4^{2n+1}+3^{n+2})=13M+3a_n\end{aligned}$$

5. 给定一个天平，以及n个砝码：$1,3,3^2,\ldots,3^{n-1}$ 克. 证明可以通过允许在两边同时放置砝码，可以称出任何N 克重量，其中N为≥ 1以及$\leq 1/2(3^n-1)$的整数（提示：考虑所有如下形式的和式

$$e_0+3e_1+3^2e_2+\cdots 3^{n-1}e_{n-1},$$

其中每一个e_i为0，+1，或者-1).

这里实际上涉及到了数的3进位制的表示.

根据题目我们可以证明这些砝码能够表示的最大数为

$$1+3+\cdots+3^{n-1}=\frac{1-3^n}{1-3}=\frac{3^n-1}{2}.$$

6. 证明任意一个n个变量的d次多项式，最多包含$\frac{(n+d)!}{n!d!}$个项. （提示：对d使用归纳法，注意到下面的关系：n个变量的d次同类项多项式的项的数量，和$n-1$个变量的d次多项式的项的数量相等.）

用$a_{n,d}$来表示n个变量的d次多项式包含的最多的项数，那么$d=0$时，显然有

$$\begin{aligned}a_{n,0}&=1\\a_{n,1}&=n+1=\frac{(n+1)!}{n!1!}\\a_{1,d}&=d+1=\frac{(1+d)!}{1!d!}\end{aligned}$$

对于一般的n个变量，我们记其中某个变量为x，那么把多项式按照x^k合并各个项，这里$k = 1, 2, \cdots, d$. 那么x^k这里面包含的项数为$a_{n-1,d-k}$，由此可以得出如下等式:

$$\begin{aligned} a_{n,d} &= \sum_{k=0}^{d} a_{n-1,d-k} \\ &= \sum_{k=0}^{d} a_{n-1,k} \\ &= \sum_{k=0}^{d} \binom{k}{n+k-1} \end{aligned}$$

下面根据这个等式证明$a_{n,d} = \frac{(n+d)!}{n!d!} + \binom{d}{n+d}$. 使用归纳法即可，并且注意到如下几个等式:

$$\binom{0}{n-1} = 1 = \binom{0}{n},$$

以及

$$\binom{k-1}{n} + \binom{k}{n} = \binom{k}{n+1}.$$

也可以使用组合方法来获取上述等式：满足要求的每一个项满足

$$x_1^{i_1} \cdots x_n^{i_n}, \quad 0 \le i_k \le n$$

那么应该$i_1, i_2, \cdots, i_n$满足

$$i_1 + i_2 + \cdots + i_n \le d.$$

于是应该通过

$$i_1 + i_2 + \cdots + i_n = k$$

并且对k遍历0到d来获取. 有$n+k$(我们需要把i_k的取值保证至少为1)个球排成一列，使用$n-1$个木杆(这样得到的是n组)把这些球隔开，不算两边，一共有$n+k-1$个位置，这里每一个的数量是$\binom{n-1}{n+k-1} = \binom{k}{n+k-1}$.

2

引理 2.1. 设d, a 为整数, $d > 0$. 则存在唯一的d的最大倍数$dq \leq a$; 它具有特征为: $dq \leq a < d(q+1)$, 或者$a = dq + r$, $0 \leq r < d$.

(在这个关系中, r称为a被d除的余数; d称为除数, q称为商).

证明. 形如$a - dz$ ($z \in \mathbb{Z}$)的整数的集合包含正整数, 因为z可以取绝对值足够大的负数(例如, $z = -N$, N为足够大的正整数). 对于所有具有上述形式的正整数应用第1节的性质(6); 取它的最小元素r, 写为$a - dq$: 于是$0 \leq r < d$; 否则$a - d(q+1)$属于同一个集合并且$< r$. □

定理 2.2. 设M为非空的整数集, 对减法封闭. 那么存在唯一的$m \geq 0$, 使得M由m的所有倍数组成: $M = \{mz\}_{z \in \mathbb{Z}} = m\mathbb{Z}$.

证明. 如果$x \in M$, 根据假设, $0 = x - x \in M$, $-x = 0 - x \in M$. 如果$y \in M$, 那么$y + x = y - (-x) \in M$, 因此M对于加法也是封闭的. 如果$x \in M$, $nx \in M$, 其中n为任意一个正整数, 于是$(n+1)x = nx + x \in M$; 于是根据归纳法, 对任意$n \geq 0$有$nx \in M$, 从而对于所有的$n \in Z$也成立. 最后, 所有的M中的元素的整数系数的线性组合也是M中的元素; M的这个性质可以得出M在加法和减法下封闭, 它和我们的假设是等价的.

如果$M = \{0\}$, 定理是成立的, 取$m = 0$即可. 否则, M中大于0的元素组成的集合非空; 取m为其中的最小元素. m的所有倍数全部属于M. 任意$x \in M$, 根据引理有$x = my + r$, $0 \leq r < m$; 于是$r = x - my$也是M的元素. 根据m的定义, 应该有$r = 0$, $x = my$. 因此$M = m\mathbb{Z}$. 反过来, 既然m是$m\mathbb{Z}$中的最小的大于0的元素, 那么当给定M时, m也将被唯一确定. □

推论 2.3. 设$a, b, \ldots, c$为有限个整数, 则存在唯一的整数$d \geq 0$, 使得所有$a, b, \ldots, c$的整数系数的线性组合$ax + by + \cdots + cz$组成的集合是由d的所有倍数组成的.

证明. 应用定理2.2于上述集合即可. □

推论 2.4. 使用推论2.3同样的假设和符号，那么d是每一个整数$a, b, \ldots, c$的因子，并且这些整数的公因子也是d的因子.

证明. 注意整数$a, b, \ldots, c$本身也是它们的线性组合组成的集合的元素. 反过来，$a, b, \ldots, c$的公因子也是它们的每一个线性组合的因子，特别的也是d的因子. □

定义 2.5. 定理2.2的推论中定义的整数d称为$a, b, \ldots, c$的最大公因子；表示为$(a, b, \ldots, c)$.

既然最大公因数$(a, b, \ldots, c)$属于$a, b, \ldots, c$的线性组合的集合（它是大于0的元素中的最小者，除非$a, b, \ldots, c$都为0），它就应该可以表示为如下形式

$$(a, b, \cdots, c) = ax_0 + by_0 + \cdots + cz_0$$

其中$x_0, y_0, \ldots, z_0$都是整数.

习题

1. 证明$(a, b, c) = ((a, b), c) = (a, (b, c))$.

   证明. 注意本书中最大公约数的定义方式，这里应该使用这个定义来证明. 注意到a, b, c有对称性，由于$(a, b) = (b, a)$后面的两个式子没有本质差别，这里只证明第一个等式.

   设$d_1 = (a, b)$，则存在x_0, y_0，使得$d = ax_0 + by_0$. 我们证明集合$A = \{ax + by + cz\}$和集合$B = \{d_1 w + cz\}$是相等的，那么根据定义等式成立.

   (1) $A \subset B$，$\forall d \in A$，则$d = ax + by + cz$，根据d_1的定义(推论2.3)，应该有$ax + by = wd_1 = w(ax_0 + by_0)$，于是有$d = ax + by + cz = wd_1 + cz \in B$.

   (2) $B \subset A$，$\forall d \in B$，则$d = d_1 w + cz = (ax_0 + by_0)w + cz = awx_0 + bwy_0 + cz \in A$. □

2. 证明Fibonacci数列(1，2，3，5，8，13，…，数列中的第二项之后的每一项都是他前面的两个项之和）中任何连续的两个项的最大公因数为1.

   证明. 我们首先证明：$(a, b) = (a - b, b)$. 这只要注意到$ax + by = (a - b)x + b(x + y)$.

   根据Fibonacci数列的定义有：$a_{n+2} = a_{n+1} + a_n$，$a_n = a_{n+2} - a_{n+1}$，因此

$$\begin{aligned}(a_{n+2}, a_{n+1}) &= (a_{n+2} - a_{n+1}, a_{n+1}) \\ &= (a_n, a_{n+1}) = (a_{n+1}, a_n) \\ &= \cdots = (a_2, a_1) = 1\end{aligned}$$

□

3. 如果p，q，r，s为整数，满足$ps-qr=\pm1$，整数a,b,a',b'满足

$$a'=pa+qb, b'=ra+sb,$$

证明$(a,b)=(a',b')$（提示：从最后的两个方程种解出a，b）.

证明. 我们对$ps-qr=1$进行讨论，至于-1的情形类似.
首先我们可以从上述两个等式求出a，b的表达式：

$$\begin{aligned} a &= sa'-qb' \\ b &= -ra'+pb' \end{aligned}$$

由此，我们可以证明$A=\{ax+by\}=\{a'x+b'y\}=B$. 一方面：

$$\begin{aligned} ax+by &= (sa'-qb')x+(-ra'+pb')y \\ &= a'(sx-ry)+b'(-qx+py) \end{aligned}$$

另一方面

$$\begin{aligned} a'x+b'y &= (pa+qb)x+(ra+sb)y \\ &= a(px+ry)+b(qx+sy) \end{aligned}$$

$A=B$，因而$(a,b)=(a',b')$. □

4. a，b为大于0的整数，令$a_0=a$，$a_1=b$；当$n\geq1$时，a_{n+1}使用如下方式定义$a_{n-1}=a_nq_n+a_{n+1}$，$0\leq a_{n+1}<a_n$，$a_n>0$. 证明存在$N\geq1$使得$a_{N+1}=0$，并且$a_N=(a,b)$.

证明. 只要注意到$a_0>a_1>a_2>\cdots>a_n>\cdots$，可知最多经过$a$次即可达到$a_n=0$，令$N=n-1$即可. 难点在于后面的结论：$a_N=(a,b)$. 这一点我们只要证明$(a_{n-1},a_n)=(a_n,a_{n+1})$即可. 这样的话

$$(a,b)=(a_0,a_1)=(a_1,a_2)=\cdots=(a_N,a_{N+1})=(a_N,0)=a_N.$$

为了方便，改变一下记号：$a=qb+r$，然后需要证明$(a,b)=(b,r)$. 设$A=\{ax+by\}$，$B=\{bx+ry\}$.

$$\begin{aligned} ax+by=(qb+r)x+by=b(qx+y)+rx\in B \\ bx+ry=bx+(a-qb)y=ay+b(x-qy)\in A \end{aligned}$$

□

5. 使用习题4中的符号，证明a_n可以表示为$ax+by$，x，y为整数，$0 \le n \le N$.

证明. 使用归纳法即可. $a_0 = a \cdot 1 + b \cdot 0$，$a_1 = a \cdot 0 + b \cdot 1$，对于$a_0 = a_1 q_1 + a_2$，

$$a_2 = a_0 - a_1 q_1 = a + b \cdot (-q_1).$$

假若对于小于等于n的a_k能够由a和b表示出来，$a_k = ax_k + by_k$，那么对于a_{n+1}.

$$\begin{aligned} a_{n+1} &= a_{n-1} - a_n q_n \\ &= ax_{n-1} + by_{n-1} - q_n(ax_n + by_n) \\ &= a(x_{n-1} - q_n x_n) + b(y_{n-1} - q_n y_n) \end{aligned}$$

$x_{n+1} = x_{n-1} - q_n x_n$，$y_{n+1} = y_{n-1} - q_n y_n$，结论成立. □

6. 使用习题4，5的方法给出下列情形中的(a,b)，以及求解$ax+by=(a,b)$:

（i） a = 56， b = 35；

（ii） a = 309， b = 186；

（iii） a = 1024， b = 729.

（i） $7 = (a,b) = 56 \cdot 2 - 35 \cdot 3$；

（ii） $3 = (a,b) = 309 \cdot (-3) + 186 \cdot 5$；

（iii） $1 = (a,b) = 729 \cdot 361 - 1024 \cdot 257$.

7. $a,b,\ldots,c,m$为整数，$m>0$，证明

$$(ma, mb, \ldots, mc) = m \cdot (a, b, \ldots, c).$$

证明. 令$d = (a,b,\ldots,c)$，则$d|a$，$d|b$，$\cdots$，$d|c$，于是$md|ma$，$md|mb$，$\cdots$，$md|mc$，md是它们的公因子，于是$md|(ma,mb,\cdots,mc)$.

$d = ax + by + \cdots + cz$，于是$md = max + mby + \cdots + mcz$，于是$(ma,mb,\cdots,mc)|md$.

有了上面两个整除关系可以知道$(ma,mb,\cdots,mc) = md = m(a,b,\cdots,c)$. □

8. 证明每一个有理数可以表示为$\frac{m}{n}$，$(m,n)=1$，$n>0$，并且这种表示方式是唯一的.

证明. 所谓有理数，是指整数的比例，于是我们只需要证明$d = (a,b)$时，$(a/d, b/d) = 1$，并且$m_1/n_1 = m_2/n_2$, 并且m_i, n_i满足题设条件时，必有$m_1 = m_2$，$n_1 = n_2$.

利用上一题的结论$(a/d, b/d) \cdot d = (a,b) = d$，于是$(a/d, b/d) = 1$．至于后面部分，我们有$m_1 n_2 = m_2 n_1$．我们证明结论$d|ab$，$(a,d) = 1$，则必有$d|b$．证明比较简单，$(a,d) = 1$可以得出：$ax + dy = 1$，于是$abx + dby = b$，因此$d|b$．$m_1|m_2 n_1$，$(m_1, n_1) = 1$可知$m_1|m_2$，不妨设$m_2 = km_1$，于是有$n_2 = kn_1$，注意$n_1 > 0$，$n_2 > 0$，因此$k > 0$，如果$k > 1$，那么$(m_2, n_2) = (km_1, kn_1) = k > 1$，这与我们的假设矛盾，因此结论成立. $\square$

2.

3

定义 3.1. 整数a，b，...，c称作是互素的，如果他们的最大公因数为1.

换句话说，它们是互素的如果它们没有大于1的公因子.

如果整数a，b是互素的，那么就称a对于b不可约，b对于a不可约，而且，a的每一个因子对于b不可约，b的每一个因子对于a不可约.

定理 3.2. 整数$a,b,\ldots,c$是互素的当且仅当方程$ax+by+\cdots+cz=1$存在整数解$x,y,\ldots,z$.

事实上，如果$(a,b,\ldots,c)=1$，根据定理2.2的推论2.3，方程有解. 反过来，如果方程有解，那么每一个$a,b,\ldots,c$的公因子$d>0$必然整除1，因而必然是1.

推论 3.3. 如果d是整数$a,b,\ldots,c$的最大公因数，那么$\frac{a}{d},\frac{b}{d},\ldots,\frac{c}{d}$是互素的.

这一点立刻可以由这样一个事实得到：d可以表示为$ax_0+by_0+\cdots cz_0$.

定理 3.4. 如果a，b，c为整数，a和b互素，并且可以整除bc，那么a整除c.

既然$(a,b)=1$，我们有$ax+by=1$. 于是有

$$c=c(ax+by)=a(cx)+(bc)y.$$

而a可以整除右边的每一项，因而也整除c.

推论 3.5. 如果a，b，c为整数，a分别与b，c互素，那么a与bc互素.

令d为a和bc的正的公因子，它和b互素(因为它整除a)，根据定理3.4，d必然整除c，而$(a,c)=1$，d等于1.

推论 3.6. 如果一个整数和$a,b,\ldots,c$中的每一个整数互素，那么它也和这些数的乘积互素.

这可以通过对乘积的因子个数进行归纳得到.

习题

1. 如果$(a,b)=1$，a和b整除c，证明ab整除c.

证明. 从$(a,b)=1$, 存在整数x,y, 满足$1=ax+by$, 于是$c=acx+bcy$, 注意到$ab|ac$, $ab|bc$, 因此$ab|c$. □

另一个方法是：$a|c$, 说明$c=aa_1$, 根据$b|c$, 可知$b|aa_1$，而$(a,b)=1$, 从而$b|a_1$，因此$a_1=bb_1$, $c=aa_1=abb_1$, $ab|c$.

2. $m>1$，a和m互素，证明：m除$a,2a,\ldots,(m-1)a$得到的余数为$1,2,\ldots,m-1$的某个排序.

证明. 注意到$a,2a,\ldots,(m-1)a$一共有$m-1$个数，我们只要证明这些数中的任意两个数的余数不相同，并且不会出现余数为0的情形，那么结论成立.

首先m不整除ka，这里$1\le k\le m-1$，如果$m|ka$，由于$(m,a)=1$，于是$m|k$，这是不可能的.

其次，如果ka和la除以m的余数相同，这里$1\le k<l\le m-1$，那么就有$m|(l-k)a$，根据第一步证明的，这是不可能的. □

3. 证明：$N>0$为整数，N或者是完全平方数(即可以表示为n^2，这里n为大于0的整数)，或者$\sqrt{N}$不是有理数（提示：利用习题8）.

证明. 假设N不是完全平方数，我们证明$\sqrt{N}$不是有理数.

假设$\sqrt{N}$是有理数，于是存在$m,n>0$，$(m,n)=1$，$\sqrt{N}=m/n$，两边平方，$N=m^2/n^2$, 于是有

$$n^2N=m^2,$$

从$(m,n)=1$可知$(m^2,n^2)=1$，于是$m|N$，$m^2|N$，不妨设$N=m^2m_1$，于是有

$$\begin{aligned}n^2m^2m_1&=m^2\\ n^2m_1&=1\end{aligned}$$

由此得到$n=1$，$m_1=1$，这与N不是完全平方数矛盾. □

4. 任何大于1的不是2的幂的整数可以表示为两个或者更多个连续整数的和.

证明. 首先每一个数$N > 1$都可以表示为$N = 2^m a$的形式，这里$m \geq 0, a$为奇数. 根据题设，应该是$a \geq 3$，我们假设他能够表示成d个连续整数$b, b+1, \cdots, b+d-1$的和，则

$$2^m a = \frac{(b+d)(b+d-1)}{2} - \frac{b(b-1)}{2} = \frac{d(2b-1+d)}{2},$$

转化一下：

$$d(2b-1+d) = 2^{m+1}a$$

注意到d与$2b-1+d$必然是一个为奇数，另一个为偶数，如果$a < 2^{m+1}+1$，那么令$d = a$，此时$2b-1+d = 2^{m+1}$，$b = \frac{2^{m+1}+1-a}{2}$，否则令$d = 2^{m+1}$，$b = \frac{a+1-2^{m+1}}{2}$. 容易验证这是成立的，并且$a \geq 3$, $2^{m+1} \geq 2$. 因此数量个数至少为2. □

5. a，b为正整数，$(a,b) = 1$，证明每一个$\geq ab$的整数可以表示为$ax + by$的形式，x，y为正整数.

证明. 从$(a,b) = 1$, 存在$ax + by = 1$. 问题在于找到方程$n = ax + by$的正整数解, 这里$n \geq ab$，华罗庚的《数论导引》中有一个更强的结论$n > ab - a - b$.

首先根据前面讨论，方程必然有解. 不妨设x_0, y_0是其中一个解，则方程的所有解可以表示成如下形式：

$$\begin{cases} x = x_0 + bt \\ y = y_0 - at \end{cases} \quad t \in Z,$$

我们需要证明它有正整数解. 为此我们需要选择合适的$t \in Z$.

首先选择t使得，$0 \leq y_0 - at < a$，这是可能的，这实际上是带余除法的一个应用，我们说这个t能够使得$x = x_0 + bt > 0$, 因为此时$0 \leq by_0 - abt \leq ab$

$$(x_0 + bt)a = ax_0 + abt > by_0 - ab + ax_0 = n - ab \geq ab - ab = 0$$

获证. 这里注意的是本书中0包含在正整数之中. □

6. 利用习题5，对m使用归纳法，证明，如果$a_1, a_2, \ldots, a_m$是正整数，$d = (a_1, a_2, \ldots, a_m)$，$d$的足够大的倍数可以表示为$a_1x_1 + a_2x_2 + \cdots + a_mx_m$的形式，这里$x_i$都是正整数.

证明. 对于$m=2$，对a_1/d和a_2/d应用上一道题目，则当$N \geq (a_1a_2)/d$时，$ax+by=N$存在正整数解. 至于$m+1$来说，

$$d = ((a_1,\cdots,a_m),a_{m+1})$$

令$d_1=(a_1,\cdots,a_m)$，对于足够大的Kd_1，存在正整数x_i，使得$a_1x_1+\cdots+a_mx_m=Kd_1$，对于足够大的$Md$，存在正整数$y_1,y_2$使得，$d_1y_1+a_{m+1}y_2=Md$，当$Nd \geq Kd_1+Md$时，我们来看看是否存在正整数解. 首先对于任意的$Nd$，考虑$Nd-Kd_1 \geq Md$，存在正整数$y_1,y_2$，使得$d_1y_1+a_{m+1}y_2=Nd-Kd_1$，而对于$(y_1+K)d_1$来说，存在正整数$x_i$，使得$\sum a_ix_i=(y_1+K)d_1$，于是有$\sum a_ix_i=Nd$，这里$x_{m+1}=y_2$. 获证. 对于这道题目，只需要找到这个$Nd$，它不一定是满足条件的最小整数. $\square$

4

定义 4.1. 整数$p > 1$称为素数，如果它除了自己和1之外没有其它的正因子.

每一个大于1的整数至少有一个素因子，也就是它的最小的大于1的因子. 如果a为整数，p是素数，那么p或者整除a，或者和a互素.

定理 4.2. 如果一个素数整除某些整数的乘积，那么它必然整除至少其中一个因子.

否则，它将和所有的因子互素，于是根据定理3.4的推论3.6，它和这些数的乘积也是互素的.

定理 4.3. 每一个大于1的整数可以表示为素数的乘积；如果不考虑因子的顺序，这个表示方式还是唯一的.

设$a > 1$；令p为a的素因子. 如果$a = p$，定理成立，否则，$1 < \frac{a}{p} < a$；如果定理中的第一个结论对于$\frac{a}{p}$成立，那么对于a也成立. 对a使用归纳法，即可得出结论成立.

第二个结论可以通过归纳法加以证明. 假设a可以以两种方式表示为素数的乘积，即$a = pq \dots r$和$a = p'q' \dots s'$；p整除a，定理4.2表明p必整除素数$p', q', \dots s'$之一，假设为p'，那么$p = p'$；对$\frac{a}{p}$应用定理的第二部分，我们可以证明除了顺序之外，$q', \dots, s'$和$q, \dots, r$一样的. 根据归纳原理，就可以证明第二部分结论.

下面给出第二个证明. 把a表示为素数的乘积，$a = pq \dots r$；令P为任一素数；n为P在a的因子$p, q, \dots, r$中出现的次数. 即a是P^n的倍数；另一方面，由于$a \cdot P^{-n}$是不等于P的素数的乘积，由定理4.2，它不是P的倍数，因而a不是P^{n+1}的倍数. n可以唯一确定：n是满足P^n整除a的最大整数；我们使用$n = \upsilon_P(a)$来表示. 于是，任意的两种把a表示为素数乘积的方式中，必然包含相同的素数，以及相同的次数；这再一次证明了我们的定理的第二个结论.

2是素数；它是唯一的偶素数，所有其它的素数都是奇数. 前十个素数为

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29.$$

设$p_1 = 2, p_2, p_3, \ldots$是所有的素数，以它们的自然顺序(递增)排列. 令$a$为任一$\geq 1$的整数，对每一个$i \geq 1$，在把$a$表示为素数乘积的时候，$\alpha_i$为$a$的素因子中的$p_i$的次数(如果$p_i$不能整除$a$，则令$\alpha_i = 0$). 于是我们有

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$$

这里r足够大(也就是说a的所有的素因子都在$p_1, p_2, \ldots, p_r$之中).

定理 4.4. 存在无限多的素数.

事实上，如果只有有限个素数$p, q, \ldots, r$，那么$pq \ldots r + 1$的素因子显然不等于$p, q, \ldots, r$中的任意一个. (这是Euclid的证明，其它的证明方法可以参考习题).

习题

1. n为大于等于1的整数，p是素数. 对于任意的有理数x，我们用$[x]$表示小于或者等于x的最大整数，证明使得p^N整除$n!$的最大整数N可以由下式给出
$$N = \left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \left[\frac{n}{p^3}\right] + \cdots$$

   证明. 首先$[\frac{n}{m}]$表示的是不超过n的正整数中m的倍数的个数.

$$\frac{n}{m} - 1 < [\frac{n}{m}] \leq \frac{n}{m},$$

   如果我们用A_k表示1到n之间的p^k的倍数组成的集合, 那么有$A_{k+1} \subset A_k$, 如果用$|A_k|$表示集合中元素个数, 那么$|A_k| = [n/p^k]$, 并且有结论, 能被p^k整除但不能被p^{k+1}整除的数的个数应该是$|A_k| - |A_{k+1}|$. 这样$n!$中p的因子的个数(N)等于

$$\sum_{k=1}^{\infty} k(|A_k| - |A_{k+1}|),$$

   注意到一定程度之后必有$[n/p^k] = 0$, 把上式展开即可得到结论. □

2. 证明，$a, b, \ldots, c$为大于等于1的整数，那么

$$\frac{(a + b + \cdots + c)!}{a!b! \cdots c!}$$

   是整数. (提示：使用习题1，证明每一个素数在分子中的次数不小于它在分母中的次数.)

证明. 根据上一道题目,我们考察每一个素数p在分子分母中的次数,在分子中的次数为

$$\sum[\frac{a+b+\cdots+c}{p^k}],$$

在分母中的次数为

$$\sum[\frac{a}{p^k}]+\sum[\frac{b}{p^k}]+\cdots+\sum[\frac{c}{p^k}]$$
$$=\sum([\frac{a}{p^k}]+[\frac{b}{p^k}]+\cdots+[\frac{c}{p^k}]),$$

我们只要证明结论

$$[\frac{a+b}{m}]\geq[\frac{a}{m}]+[\frac{b}{m}]$$

即可. 而它是成立的, 因为

$$[\frac{a}{m}]\leq\frac{a}{m},\quad [\frac{b}{m}]\leq\frac{b}{m}$$

于是$[\frac{a}{m}]+[\frac{a}{m}]\leq\frac{a+b}{m}$, 而$[\frac{a+b}{m}]$是不超过$\frac{a+b}{m}$的最大整数, 所以前面的不等式成立. □

3. a, m, n为正整数, $m\neq n$, 证明$a^{2^m}+1$和$a^{2^n}+1$的最大公因数或者是1, 当a为偶数时; 或者是2, 当a为奇数时(提示: 使用这样一个事实, 当$n>m$时, $a^{2^n}-1$是$a^{2^m}+1$的倍数). 并依据此推出存在无限多的素数.

证明. 这里需要一个结论:

$$(a,b)=(a-kb,b),$$

$m\neq n$, 我们不妨设$m>n$, 那么根据提示有

$$(a^{2^m}+1,a^{2^n}+1)=(a^{2^m}+1-(a^{2^m}-1),a^{2^n}+1)=(2,a^{2^n}+1),$$

当a为偶数的时候, $a^{2^n}+1$为奇数, 最大公约数为1, 否则为偶数, 最大公约数等于2.

后一个结论可以这样来证明: 我们直接取$a=2$, 那么序列

$$\{2^{2^n}+1\}$$

任意两个数都是互素的. 那么他们的素因子也是互不相同的, 因此素数必然有无限多个. □

4. 如果$a = p^\alpha q^\beta \cdots r^\gamma$，$p, q, \dots, r$为不同的素数，$\alpha, \beta, \dots, \gamma$是正整数，证明$a$的不同的因子(包括$a$和1)的个数是

$$(\alpha+1)(\beta+1)\cdots(\gamma+1),$$

它们的和为

$$\frac{p^{\alpha+1}-1}{p-1}\cdot\frac{q^{\beta+1}-1}{q-1}\cdots\frac{r^{\gamma+1}-1}{r-1}.$$

证明. 我们需要结论:a的每个因子由乘积给出

$$p^{\alpha_1}q^{\beta_1}\cdots r^{\gamma_1},$$

这里$0 \le \alpha_1 \le \alpha, 0 \le \beta_1 \le \beta, 0 \le \gamma_1 \le \gamma$. 使用组合学的乘积原理可知不同的因子的个数就是

$$(\alpha+1)(\beta+1)\cdots(\gamma+1).$$

它们的和等于

$$\begin{aligned}&\sum_{\alpha_1,\beta_1,\gamma_1} p^{\alpha_1}q^{\beta_1}\cdots r^{\gamma_1}\\ =&\sum_{\beta_1,\gamma_1} q^{\beta_1}\cdots r^{\gamma_1}\sum_{\alpha_1} p^{\alpha_1}\\ =&\sum_{\alpha_1} p^{\alpha_1}\cdot\sum_{\beta_1} q^{\beta_1}\cdots\sum_{\gamma_1} r^{\gamma_1}\\ =&\frac{p^{\alpha+1}-1}{p-1}\cdot\frac{q^{\beta+1}-1}{q-1}\cdots\frac{r^{\gamma+1}-1}{r-1}.\end{aligned}$$

□

5. 证明，如果D是a的不同的因子的个数，这些因子的乘积为$a^{D/2}$.

证明. 令$A = \{a_1, a_2, \cdots, a_D\}$为$a$的不同的因子的集合, 只要注意到

$$B = \{\frac{a}{a_1}, \frac{a}{a_2}, \cdots, \frac{a}{a_D}\}$$

恰好也遍历了a的不同的因子, 那么就有素因子乘积的平方等于

$$\prod(a_i\cdot\frac{a}{a_i}) = a^D$$

结论成立. □

6. $n, a, b, \ldots, c$为大于1的整数， 不大于n的具有形式$a^\alpha b^\beta \cdots c^\gamma$的不同的数的个数满足

$$\leq (1+\frac{\log n}{\log a})(1+\frac{\log n}{\log b})\cdots(1+\frac{\log n}{\log c}).$$

使用这个结论，以及

$$\lim_{n\to+\infty}\frac{(\log n)^r}{n}=0$$

对任意$r > 0$， 证明素数个数是无限的(提示： 假设它是有限的，$a, b, \ldots, c$为所有的不同的素数).

证明. 具有上述形式的数的个数等于

$$(1+\alpha)(1+\beta)\cdots(1+\gamma),$$

注意到$a^\alpha \leq n$, 因此$\alpha < \log n/\log a$, 因此不等式部分成立.

至于后面部分, 假设素数只有有限个(k个), 它们就是$a, b, \cdots, c$, 并且a是最小的, 那么根据基本定理, 每一个数都能够表示为上述形式, 于是

$$n \leq (1+\frac{\log n}{\log a})(1+\frac{\log n}{\log b})\cdots(1+\frac{\log n}{\log c}),$$

另一方面,

$$\begin{aligned}&(1+\frac{\log n}{\log a})(1+\frac{\log n}{\log b})\cdots(1+\frac{\log n}{\log c}) < (1+\frac{\log n}{\log a})^k\\ &=\sum_{i=0}^{k} C_k^i(\frac{\log n}{\log a})^i\end{aligned}$$

于是

$$1 < \sum_{i=0}^{k}\frac{C_k^i}{\log^i a}\cdot\frac{(\log n)^i}{n}$$

令$n \to$, 而不等式右边是有限项, 并且每一项趋于0, 于是得到矛盾

$$1 \leq 0.$$

□

7. $(a, b) = 1$，a^2-b^2为完全平方数(参考习题3)，证明，或者$a+b$和$a-b$都是完全平方数，或者每一个都是一个完全平方数的二倍数(提示： 证明$a+b$和$a-b$的最大公约数是1或者2).

证明. 首先有

$$(a+b,a-b)=(a+b-(a-b),a-b)=(2a,a-b)=(2a,b)=(2,b),$$

当b为偶数的时候最大公约数为2, 否则为1.

其次我们有结论:如果$(m,n)=1$, 那么如果mn是完全平方数, 必有m和n都是完全平方数.

于是根据$(a+b,a-b)=1$和$(a+b,a-b)=2$分情形讨论, 第一种情形对应的就是$a+b$和$a-b$都是完全平方数. 至于后一情形, 只要注意到$((a+b)/2,(a-b)/2)=1$, 并且$(a^2-b^2)/4$仍旧是完全平方数即可. □

5

定义 5.1. 交换群(Abel群) 是指集合G, 以及G上的元素的二元运算, 满足以下公理(在这里把群的运算表示为+):

I (结合律). $(x+y)+z=x+(y+z)$, $\forall x,y,z\in G$.

II (交换律). $x+y=y+x$, $\forall x,y\in G$.

III $x,y\in G$, 方程$x+z=y$存在唯一解$z\in G$ (记$z=y-x$).

IV 存在一个元素属于G, 称为中性元(记之为0), 满足$0+x=x$, $\forall x\in G$.

举例来说, 整数集, 有理数集(以及实数集)在加法下构成交换群. 很多时候交换群的运算不一定是加法, 也就是可以不表示为+; 此时III中的$y-x$, IV中的0都应该作相应的修改. 如果这个运算以乘法表示, 那么在III中的z通常表示为$\frac{y}{x}$, 或者y/x, 或者yx^{-1}. 用1表示IV中的中性元. 非零的有理数在乘法下构成了一个交换群.

在本书中, 除了交换群之外, 不会出现其它的群; 因此“交换”一词通常就省略了. G的子集如果在同一个运算下仍旧构成一个群, 那么该子集就称为G的子群. 如果G表示为加法, G的子集是一个子群当且仅当它对加法和减法封闭, 甚至可以仅仅对减法封闭(参考定理2.2的证明). 定理2.2可以更加简洁地表述为Z的每一个子群具有形式mZ, $m\geq 0$.

下面给出有限群的例子.

定义 5.2. m, x, y为整数, $m>0$, 称x和y模m同余, 如果$x-y$是m的倍数; 可以表示为$x\equiv y(\mod m)$, 或更简洁表示为$x\equiv y(m)$.

第2章中的引理说明每一个整数必和$0,1,\ldots,m-1$之一, 而且只和其中的一个模m同余, 两个整数模m同余当且仅当它们除m的余数相同.

模m的同余关系具有下列性质:

(A) (自反性) $x\equiv x(\mod m)$;

(B) (传递性) 如果$x \equiv y$, $y \equiv z(\mod m)$, 则$x \equiv z(\mod m)$;

(C) (对称性) 若$x \equiv y(\mod m)$, 则$y \equiv x(\mod m)$.

(D) $x \equiv y$, $x' \equiv y'(\mod m)$, $x \pm x' \equiv y \pm y'(\mod m)$.

(E) $x \equiv y$, $x' \equiv y'(\mod m)$, $xx' \equiv yy'(\mod m)$.

(F) $d > 0$, 整除m, x和y;那么$x \equiv y(\mod m)$当且仅当$\frac{x}{d} \equiv \frac{y}{d}(\mod \frac{m}{d})$.

对于(E), 它是下面等式的推论

$$xx' - yy' = x(x' - y') + (x - y)y';$$

其它结论的验证也是比较简单的.

性质(A), (B), (C)可以表述为: 模m同余关系是整数之间的一个等价关系.

定义 5.3. 整数模m的同余类是所有这样的整数的集合, 这些整数和某个给定的整数模m同余.

x为任一整数, 我们用$(x \mod m)$ (或更简单的(x), 如果不会引起歧义的话)来表示与x模m同余的整数组成的同余类. 从(A)知x属于$(x \mod m)$; 它称为这个同余类的代表. 从(A), (B), (C)可知, 两个同余类$(x \mod m)$, $(y \mod m)$或者是相等的, 如果$x \equiv y(\mod m)$; 或者是不相交的(也就是说没有公共元素). 因而所有整数的集合被分成了m个不相交的同余类$(0 \mod m)$, $(1 \mod m)$, $\ldots$, $(m-1 \mod m)$.

我们使用如下方式定义同余类的加法:

$$(x \mod m) + (y \mod m) = (x + y \mod m);$$

这样做是允许的, 因为(D)表明等式右边仅仅依赖于左边的两个同余类, 而不依赖这些同余类的代表x, y的选择.

定理 5.4. 对任一整数$m > 0$, 模m的同余类在加法下构成一个m个元素的交换群.

这是显然的, 事实上, 对于给定的x, y, 方程

$$(x \mod m) + (z \mod m) = (y \mod m),$$

有唯一的解$(y - x \mod m)$, 而$(0 \mod m)$就是中性元.

习题

1. 如果$x_1,\ldots,x_m$为m个整数，证明存在一个合适的非空子集，使得这个子集中的元素的和是m的倍数（提示：考虑模m的由0，x_1，x_1+x_2，$\ldots$，$x_1+x_2+\cdots+x_m$决定的不同的同余类）.

   证明. 考虑m个数$y_1=x_1$，$y_2=x_1+x_2$，$\ldots$，$y_m=x_1+x_2+\cdots+x_m$，如果这些数中有m的倍数, 那么选择其中一个即可, 否则, 根据鸽笼原理, 至少有两个数模m同余, 不妨设为$y_i,y_j,1\le i<j\le m$, 于是数$x_i,\cdots,x_j$组成的集合满足条件. □

2. 证明每一个完全平方数(参考III的习题3)和0，1，或者4之一模8同余.

   证明. 把整数按照模4同余进行讨论即可:

$$\begin{aligned}(4m)^2=16m^2\equiv 0 \mod 8\\ (4m+1)^2=16m^2+8m+1\equiv 1 \mod 8\\ (4m+2)^2=16m^2+16m+4\equiv 4 \mod 8\\ (4m+3)^2=16m^2+24m+9\equiv 1 \mod 8\end{aligned}$$

   结论成立. □

3. 使用归纳法证明，如果n是正整数，那么

$$2^{2n+1}\equiv 9n^2-3n+2(\mod 54).$$

   证明. 既然题目中已经说明使用归纳法, 这里试试:

   $n=1$时, $2^{2n+1}=2^3=8, 9n^2-3n+2=8$, 显然有$2^{2n+1}\equiv 9n^2-3n+2(\mod 54)$.

   假设结论对于n成立, 那么对于$n+1$来说, 把2^{2n+3}分解并使用归纳假设有:

$$\begin{aligned}2^{2n+3}&=2^{2n+1}\cdot 2^2\equiv 4(9n^2-3n+2)\\ &=4(9n^2-3n+2)-(9(n+1)^2-3(n+1)+2)\\ &\quad+(9(n+1)^2-3(n+1)+2)\\ &=(9(n+1)^2-3(n+1)+2)+(27n^2-27n)\\ &=(9(n+1)^2-3(n+1)+2)+27n(n-1)\\ &\equiv(9(n+1)^2-3(n+1)+2) \mod 54\end{aligned}$$

   由此可知结论成立, 这里使用了$2|n(n-1)$, 并且$(27,2)=1$, 因此必有$27n(n-1)\equiv 0 \mod 54$. □

4. 证明，如果x，y，z是整数，$x^2+y^2=z^2$，那么$xyz \equiv 0 (\mod 60)$.

证明. 首先我们可以假设$(x,y,z)=1$. 其次如果x,y为偶数, 那么z必为偶数, 因此按照我们的假设, x,y不可能都是偶数, 第三, 根据完全平方数模4的结果, 我们可以证明x和y必然是一个为偶数, 另一个为奇数. 不妨设x为偶数, y为奇数, 于是z也是奇数. 如果$(x,y)=d>1$, 必有$d|z$, 因此在我们的假设下, 必有$(x,y)=1$.

通过模8可以得到x必然被4整除, 否则$x=4m+2$, 此时和y为奇数进行讨论, $x^2+y^2 \equiv 5 \mod 8$, 此时不可能是完全平方数. 另一个思路, 展开:

$$x_1^2+y_1^2+y_1=z_1^2+z_1$$
$$x_1^2=(z_1-y_1)(z_1+y_1+1)$$

而z_1-y_1和z_1+y_1有相同的奇偶性, 因此z_1-y_1和z_1+y_1+1至少有一个偶数, 于是$2|x_1^2$, $2|x_1$, 因此$4|x$. 于是必有$4|xyz$.

通过模3的讨论, 我们证明$3|x$和$3|y$至少有一个成立. 首先在于整数的完全平方数模3的余数只能是0和1. 如果3无法整除x和y, 那么$x^2+y^2 \equiv 2 \mod 3$, 不可能. 因此必有$3|xyz$.

通过模5的讨论, 我们证明它必有$5|x$, $5|y$, $5|z$至少有一个成立, 从而$5|xyz$. 首先是整数的完全平方数模5的余数只能是0, 1和4. 如果$5|x$和$5|y$都不成立, 那么x^2和y^2模5的余数只能是1和4, 但是两者不能同余, 如果同余, 此时x^2+y^2模5的余数或者是2, 或者是3, 都不可能让z成为完全平方数, 于是两者不同余, 此时$5|(x^2+y^2)=z^2$, $5|z$

综合上述的讨论, 并注意到3, 4, 5两两互素, 可知$3\cdot 4\cdot 5=60|xyz$. □

5. $x_0,x_1,\dots,x_n$是整数，证明

$$x_0+10x_1+\cdots+10^n x_n \equiv x_0+x_1+\cdots+x_n (\mod 9).$$

证明. 这个问题极为简单, 原因在于$10^k \equiv 1 \mod 9$, 这是所谓弃九法的依据. 使用这个方法就很容易判断一个整数能否被9整除. 关于$10^k \equiv 1 \mod 9$的证明, 可以使用归纳法或者二项式定理完成, $10^k=(9+1)^k$. □

6. 证明：同余组$x \equiv a (\mod m)$，$x \equiv b (\mod n)$有一个解的充分必要条件是$a \equiv b (\mod d)$，其中$d=(m,n)$. 如果$d=1$，证明这个解模mn唯一.

证明. 如果同余组有解, 那么有$m|(x-a), n|(x-b)$, 于是$x-a = ma_1, x-b = nb_1, a-b = nb_1 - ma_1$, 显然有$d|(a-b)$, 也就是$a \equiv b \mod d$.

反之, 如果$a \equiv b \mod d$, 那么$d|(a-b), a-b = kd$. 另一方面, $d = (m,n)$, 那么存在u, v使得$d = mu + nv$, 于是$kmu + knv = a - b$, 令$x = -kmu + a = knv + b$. 显然x满足同余组. 也就是同余组有解.

如果$d = 1$, 设x_1和x_2都是同余组的任意两个解, 我们需要证明$x_1 \equiv x_2 \mod mn$. 只要注意到此时有$x_1 \equiv x_2 \mod m$和$x_1 \equiv x_2 \mod n$. 当$d = 1$时, 有$x_1 \equiv x_2 \mod mn$. 它只是前面出现过的一个习题的另一种表示方式: 如果$(m,n) = 1, m|c, n|c$, 必有$mn|c$. 这里的$c = x_1 - x_2$. □

7. n是大于0的整数， 证明前面的$2n$个整数中的任意$n+1$个整数包含两个数x，y，使得$\frac{y}{x}$是2的幂（提示： 对于任意给定的整数$x_0, x_1, \ldots, x_n$，令x_i'为x_i的最大的奇因子， 证明它们之中至少有两个是相等).

   证明. 首先应该注意前面$2n$个整数中只有n个奇数, 其次, 每一个整数都可以表示为$2^k a$的形式, 这里a为奇数, 那么对于任意的$n+1$个数$x_0, x_1, \ldots, x_n$来说, 上述表达式的奇数部分最多只有n个, 因此至少有两个的奇数部分相等, 不妨假设x_i和x_j的奇数部分都是a, 即$x_i = 2^k a, x_j = 2^l a$, 那么令x为两者之中较小的一个, y为较大的一个即可. □

8. 对于任意的x， y是大于0的整数， 记$x \sim y$如果$\frac{y}{x}$为2的幂， 也就是为2^n， $n \in Z$； 证明这是一个等价关系， $x \sim y$当且仅当x的奇因子和y的奇因子是相同的.

   证明. 等价关系主要是三个关系: 自反性, 对称性, 传递性.

   自反性: $\frac{x}{x} = 1 = 2^0$, 因此$x \sim x$;

   对称性: $x \sim y$意味着$\frac{y}{x} = 2^n$, 于是$\frac{x}{y} = 2^{-n}, -n \in Z$, 因此$y \sim x$.

   传递性: $x \sim y, y \sim z$, 这意味着$\frac{y}{x} = 2^n, \frac{z}{y} = 2^m$, 于是$\frac{z}{x} = \frac{z}{y} \cdot \frac{y}{x} = 2^m \cdot 2^n = 2^{m+n}$, 因此$x \sim z$.

   如果x与y有相同的奇因子, 那么最大的奇因子也是相同的, 假设都是a, 于是应该有$x = 2^n a, y = 2^m a, \frac{y}{x} = 2^{m-n}, x \sim y$.

   反之, 如果$x \sim y$, 那么$y = 2^n x$, 如果$n < 0$, 我们考虑$x = 2^{-n} y$, 两者没有实质性差别. 于是如果奇数$a|x$, 显然有$a|y$, 反之如果$a|y$, 那么由于$(a, 2^n) = 1$, 于是$a|x$, 因此他们的奇因子相同. □

5.

6

设m为大于0的整数，我们定义同余类的乘法如下

$$(x \mod m) \cdot (y \mod m) = (xy \mod m);$$

事实上，第5章中的性质(E)，表明等式的右边仅仅依赖于左边的两个同余类，而不依赖于它们的代表x，y的选择.

定义 6.1. 环是集合R以及集合上的两个二元运算，加法(记为$+$)和乘法(记为$\cdot$或者$\times$)，并且满足下列公理:

I 在加法下，R为一个群.

II 乘法是结合的，交换的，以及对加法满足分配律：$(xy)z = x(yz)$，$xy = yx$，$x(y+z) = xy + xz$，$\forall x, y, z$.

如果R是一个环，根据分配律

$$(x \cdot 0) + (xz) = x(0+z) = xz,$$

依据加法群的性质，有$x \cdot 0 = 0$. 类似的有$x \cdot (-y) = -xy$.

如果R中包含一个元素e满足对于任意x成立$ex = x$，那么它是唯一的；因为，如果f也满足条件，那么$ef = f$，$ef = fe = e$. 这样的元素称为单位元，通常记为1_R或者1；一个环称作是幺环如果它包含一个单位元.

整数集，有理数集都是幺环.

定理 6.2. 对任意大于0的整数m，模m的同余类在加法和乘法下，构成一个m元的幺环.

很容易验证这个结论. 单位元就是同余类$(1 \mod m)$；这个同余类我们将记为1，用0来表示同余类$(0 \mod m)$；我们有$1 \neq 0$，除非$m = 1$. $m = 6$的情形表明在幺环中，即使x和y都不为0，也可能成立$xy = 0$（分别取x，y为2的模6同余类和3的模6同余类)；在这种情况下x，y称为零因子. 环Z和Q中没有零因子.

如果a与m互素，$a' = a + mt$，那么a'和m的每一个公因子必然整除$a = a' - mt$；这表明同余类$(a \mod m)$中的所有整数都和m互素. 此时称这个同余类和m互素. 如果$(a \mod m)$，$(b \mod m)$都和m互素，根据定理3.4的推论1表明$(ab \mod m)$也和m互素；特别的，模m的同余类环中这样的同余类不可能为零因子.

定理 6.3. 令m，a，b为整数，$m > 0$；$d = (a, m)$. 同余式$ax \equiv b(\mod m)$或者恰好有d个解模m，或者没有解；它有一个解当且仅当$b \equiv 0(\mod d)$；恰好有$\frac{m}{d}$个不同的b模m满足这个情况.

事实上，x为一个解当且仅当存在整数y使得$ax - b = my$，即$b = ax - my$；由定理2.2的推论1，这个方程有解当且仅当d整除b，即$b = dz$；我们可以通过分别令z取$0, 1, \ldots, \frac{m}{d} - 1$而得到$b$的模$m$不同的值. 如果$x$为$ax \equiv b(\mod m)$的解，那么$x'$也是方程的解当且仅当$a(x' - x) \equiv 0(\mod m)$；由同余的性质(F)，它等价于$\frac{a}{d}(x' - x) \equiv 0(\mod \frac{m}{d})$，于是根据定理3.4和定理3.2的推论有$x' \equiv x(\mod \frac{m}{d})$. 这表明$ax' \equiv b(\mod m)$的所有的解可以被表示为$x' = x + \frac{m}{d}u$；通过令$u$分别取$0, 1, \ldots, d - 1$可以得到模$m$的不同的解.

推论 6.4. 与m互素的模m同余类在乘法下构成一个群.

这一点可以在定理3.4的推论1，定理6.3，以及下面的事实获得：同余类$(1 \mod m)$为模m同余类环的乘法的中性元.

定义 6.5. 对任意大于0的整数m，与m互素的模m同余类的个数记为$\varphi(m)$，φ称为Euler函数.

于是，我们有

$$\varphi(1) = \varphi(2) = 1, \varphi(3) = \varphi(4) = 2, \varphi(5) = 4, \text{等等}.$$

如果$m \geq 2$，$\varphi(m)$也可以定义为与m互素的并且小于等于$m - 1$的正整数的个数. 如果p是素数，$\varphi(p) = p - 1$.

定义 6.6. 一个域是这样的一个环，它的非零元素在乘法下构成一个群.

有理数环Q是一个域；整数环Z不是域. 域中不存在零因子；例子Z表明反过来是不成立的.

定理 6.7. 对任意整数$m > 1$，模m同余类环是一个域当且仅当m是一个素数.

如果m是素数，除了0之外的所有的模m同余类都是和m互素的，因而根据定理6.3的推论可知构成一个乘法群，另一方面，如果m不是素数，它有一个因子d，$1 < d < m$；从而$1 < \frac{m}{d} < m$，因而同余类$(d \mod m)$，$(\frac{m}{d}$

$\bmod m$)不为0，然而它们的乘积为0．因此它们是零因子，因而模m环不是一个域．

如果p是素数，模p的同余类域将被记为$\mathbb{F}_p$；它包含p个元素．

习题

1. 设$F(X)$是整系数多项式，如果$x \equiv y(\mod m)$，那么$F(x) \equiv F(y)(\mod m)$.

   证明. 利用$x_1 \equiv y_1(\mod m), x_2 \equiv y_2(\mod m)$时有$x_1x_2 \equiv y_1y_2(\mod m)$, 以及归纳法即可证明. □

   这是上一节中的结论的简单应用.

2. 解同余方程组

   $$5x - 7y \equiv 9(\mod 12), 2x + 3y \equiv 10(\mod 12);$$

   证明解对于模12是唯一的.

   和普通的线性方程组有点类似, 只是需要注意模12.

3. 对所有的a和b模2，解

   $$x^2 + ax + b \equiv 0(\mod 2).$$

   首先注意到$x^2 \pm x \equiv 0$.

   如果$a \equiv 1$, 那么此时只有在$b \equiv 0$时有解(此时任意x都满足方程), 其余时候无解. 下面可以假设$a \equiv 0$. 此时有

   $$x^2 + ax + b \equiv x^2 + b = x^2 + x - x + b \equiv x - b \equiv 0,$$

   因此方程的解为$x \equiv b(\mod 2)$.

4. 解$x^2 - 3x + 3 \equiv 0(\mod 7)$.

5. 设$m > 1$，证明所有小于m的和m互素的正整数的算术平均值为$\frac{m}{2}$.

   证明. 只要注意到a和m互素的时候, $m-a$也与m互素, 假设$a_1, \cdots, a_r$是所有满足条件的整数, 那么$m - a_1, \cdots, m - a_r$同样是所有满足条件的整数, 求和得到

   $$\sum_1^r a_i = \frac{mr}{2},$$

   于是所求的算术平均值是$m/2$. □

6. 设m为奇数，证明

$$1^m + 2^m + \cdots + (m-1)^m \equiv 0(\mod m).$$

证明. 这只需要注意到$(m-k)^m \equiv (-k)^m = -k^m(\mod m)$即可. 两两分组. □

7. m，n为大于0的整数，$(m,n)=1$，证明$\varphi(mn)=\varphi(m)\varphi(n)$（提示：使用习题V.6）.

证明. 需要使用前面证明过的结论:$(m,n)=1$, 同余组$x \equiv a(\mod m)$和$x \equiv b(\mod n)$有解, 并且在模mn下唯一.

有了这个结论, 可以这样来证明: 对于每一个与m互素的a和与n互素的b，都存在唯一的一个与mn互素的x, 并且不同的a和b的组合, 对应不同的x. 反证即可, 如果不同的a和b组合, 对应到了同一个x, 将会发生矛盾. 即$m|(x-a_1), m|(x-a_2)$, 于是$m|(a_1-a_2)$, 也就是$a_1 \equiv a_2(\mod m)$.

反过来, 由于当$(x,mn)=1$时, 必有$(x,m)=1$和$(x,n)=1$. 因此对于每一个与mn互素的x, 必然对应与m互素的a和与n互素的b, 显然一个x只能属于一个模m或者n的同余类.

有了上述一一对应, 根据乘法原理应该有$\varphi(m)\varphi(n)=\varphi(mn)$. □

8. 证明：$m>1$，$p,q,\ldots,r$为m的所有的素因子，那么有

$$\varphi(m) = m\Big(1-\frac{1}{p}\Big)\Big(1-\frac{1}{q}\Big)\cdots\Big(1-\frac{1}{r}\Big).$$

证明. 这将需要使用上一道题目的结论以及算术基本定理. 首先要求出p为素数的时候, $\varphi(p^r)$的值, 这里$r \geq 1$, 我们发现除了$p, 2p, \cdots, p^{r-1}p$和p^r不是互素之外, 其余所有小于p^r的正整数都和p^r互素, 因此$\varphi(p^r) = p^r - p^{r-1} = p^r(1-1/p)$.

根据算术基本定理有$m = p^\alpha q^\beta \cdots r^\gamma$, 于是

$$\begin{aligned}\varphi(m) &= \varphi(p^\alpha)\cdot\varphi(q^\beta)\cdots\varphi(r^\gamma)\\ &= p^\alpha(1-\frac{1}{p})\cdot q^\beta(1-\frac{1}{q})\cdots r^\gamma(1-\frac{1}{r})\\ &= m(1-\frac{1}{p})(1-\frac{1}{q})\cdots(1-\frac{1}{r}).\end{aligned}$$

获证. □

9. p为任意素数, 利用二项式定理并对n使用归纳法证明: 对所有整数n成立$n^p \equiv n(\mod p)$.

证明. 这里只是给出递推部分:

$$n^p = (n-1+1)^p \equiv (n-1)^p + 1 \equiv n-1+1 = n.$$

□

10. p为任意素数, $n \geq 0$, 对n使用归纳法证明: 如果$a \equiv b(\mod p)$, 那么$a^{p^n} \equiv b^{p^n}(\mod p^{n+1})$.

证明. 这里只要注意到如果$A \equiv B$, 必有

$$\sum_0^{p-1} A^k B^{p-1-k} \equiv 0$$

和展开式$A^p - B^p = (A-B)(\sum_0^{p-1} A^k B^{p-1-k})$即可. □

11. p为奇素数, $x^2 \equiv y^2(\mod p)$, 证明x或者和y模p同余, 或者和$-y$模p同余, 但是两者不能同时成立, 除非p整除x和y; 因此$x^2 \equiv a(\mod p)$恰好对于$1, 2, \ldots, p-1$中的一半的整数a存在解x.

证明. 这里使用域的知识, 当p为素数时, 模p的同余类组成一个域, 而$x^2 \equiv y^2(\mod p)$等价于$(x-y)(x+y) \equiv 0(\mod p)$, 那么当$p$不整除$x$或者$y$时, 只能有$x-y \equiv 0$或者$x+y \equiv 0$, 如果两者同时成立, 由于$p$是奇素数, 将会得到$x \equiv 0$和$y \equiv 0$同时成立.

由此结论, 把a分成三部分, 一部分只有一个元素$a \equiv 0$, 其余的两部分拥有相等的数量, 也就是说对于a来说, 如果$x^2 \equiv a$有解, $x^2 \equiv -a = p-a$必然无解. □

12. 证明形如$x + y\sqrt{2}$ (x, y为整数)的数组成一个环; 如果x, y取遍所有的有理数, 它们组成一个域.

这个只是验证环和域的各个条件, 这里不讨论了, 注意到$0 = 0 + 0\sqrt{2}$和$1 = 1 + 0\sqrt{2}$即可.

7

群以及子群的定义表明群G的任意个子群(无论是有限的还是无限的)的交集仍旧是G的子群.

定义 7.1. $a, b, \ldots, c$为群G的元素. 那么所有包含$a, b, \ldots, c$的G的子群的交集G'称作是$a, b, \ldots, c$生成的，它们被称为G'的生成元.

另一种说法为G'是包含$a, b, \ldots, c$的G的最小子群；有可能出现这样的情形：G'就是G本身.

令G为一个群，x是G中元素，用G_x表示由x生成的子群. 假设G是用加法来表示的. 同往常一样，用$-x$来表示$0-x$；它必然属于G_x. 用$0 \cdot x$来表示0；对每一个大于0的整数n，用nx来表示n个都是x的项的和$x+x+\cdots+x$，$(-n)x$来表示$-(nx)$；对n进行归纳可知，所有这些元素都属于G_x. 同样使用归纳法，我们立即可以验证如下公式

$$mx + nx = (m+n)x, m(nx) = (mn)x.$$

对于Z中的所有m，n成立. 第一个公式说明所有元素nx（$n \in Z$）构成G的一个子群；显然，它就是G_x. 为了方便起见，我们仅仅把它作为G在乘法群下的一个定理；此时我们用x^0表示G中的中性元1，x^{-1}表示元素x'满足$x'x = 1$，用x^n表示n个x的乘积$x \cdot x \cdot \ldots \cdot x$，$x^{-n}$表示$(x^n)^{-1}$.

定理 7.2. 令G为乘法群；那么对任何的$x \in G$，由x生成的G的子群由元素x^n，$n \in Z$组成.

G和x的含义如定理7.2所示，M_x表示满足$x^a = 1$的整数a构成的集合. 由于$x^0 = 1$，因而M_x是非空的. 对于所有整数a，b，我们有

$$x^{a-b} = x^a \cdot (x^b)^{-1},$$

表明$x^a = x^b$成立当且仅当$a - b \in M_x$；特别的，M_x在减法下封闭. 因此M_x满足定理2.2的条件（也就是说，它是加法群Z的子群），由某个整数$m \geq 0$的倍数组成；如果m不是0，它是最小的大于0的整数满足$x^m = 1$. 如果$m = 0$，所有的元素x^a都是不同的；如果$m > 0$，x^a等于x^b当且仅当$a \equiv b (\mod m)$.

定义 7.3. 两个群G，G'之间的同构是一个G到G'的一一对应(双射)，把G上的群运算映射到G'上的群运算.

当存在这样的映射时，G和G'称作是同构的. 同构的概念可以以同样的方式推广到环和域.

依据这个定义，前面得到的结果可以按如下方式重新给出:

定理 7.4. 令G为乘法群，由单个元素x生成. 那么或者G是无限的，映射$x^a \to a$是G到加法群Z的一个同构，或者它由有限的m个元素组成，此时映射$x^a \to (a \mod m)$ 是G到Z中模m同余类加法群的同构.

当然，如果G是任一个群，x为G中元素，定理7.4可以应用到由x生成的G的子群上.

定义 7.5. 有限群的元素个数称为它的阶数. 如果有限群是由单个元素生成的，它就称为是循环的；如果群中元素x生成一个m阶的群，那么m称作元素x的阶.

习题

1. F为有限域，证明由1生成的F的加法群的子群具有素数p阶，是F的子域，同构于模p同余类域F_p.

   证明. 如果用S表示这个子群, 我们可以证明如果$m, n \in S$, 那么$mn \in S$, 如果p不是素数, 设$p = mn$, 则$mn = 0$, 由此必有$m = 0$或者$n = 0$, 矛盾. 至于它是子域, 只需要证明$m \in S$, 必有$n \in S$, 使得$mn = 1$即可, 这里$m, n \neq 0$, 由于$(m, p) = 1$, 存在整数x, y, 使得$mx + py = 1$, 令$n = x$即可. □

   上面论述过程对于整数m和子群中的元素不做区分, 实际上就是因为最后的结论, 他们之间存在同构关系.

2. 证明群G的非空的有限子集S是G的子群，当且仅当它在群运算下封闭（提示：如果$a \in S$，$a \to ax$是S到它自身的一个双射）.

   证明. 必要性显然, S是子群, 自然在群运算下封闭. 下面证明充分性, 设S在群运算下封闭.

   由于S非空, 存在$a \in S$, 于是考虑映射$x \to ax$, 这是一个双射(这里用到了有限这个条件, 只有在有限集合中, 单射同时是满射), 于是$\{ax : x \in S\} = S$, 也就是存在x使得$ax = a$. $x = 1$, 它说明$1 \in S$, 同时说明存在x, 满足$ax = 1$. 也就是$a^{-1} \in S$. □

3. 证明有限环是一个域当且仅当它没有零因子.

证明. 必要性显然, 域中不存在零因子. 至于充分性. 设F是有限环, 其中不存在零因子. 我们证明它是一个域, 也就是F的非零因子关于乘法构成一个群. 我们只需要证明非零元素中存在乘法单位元和乘法逆元. 设$a \in F, a \neq 0$, 那么对于所有的$x \in F, x \neq 0$, 有$ax \neq 0$, 这是利用了不存在零因子这个条件. 另一方面不存在零因子, 也意味着$x \to ax$是一个单射, 加上有限这个条件, 从而是一个双射, 和上一道题目类似, 说明F中的非零元素构成乘法群. □

4. 如果G是一个(交换)群, n为整数, 证明元素x^n, $x \in G$构成G的一个子群.

证明. 令$S = \{x^n : n \in Z\}, x^0 = 1$是$S$的单位元, $x^n \cdot x^{-n} = x^0 = 1$, 由此可知它们构成一个群. □

5. G', G''为(交换)群G的子群, 证明元素$x'x''$, $x' \in G'$, $x'' \in G''$, 组成G的一个子群.

证明. 令$S = \{x'x'', x' \in G', x'' \in G''\}$. 运算的封闭性很容易验证(需要交换性这个条件). G'和G''是子群, 说明单位元$1 \in G', 1 \in G''$, 于是$1 \in S$, 而$(x'x'')((x')^{-1}(x'')^{-1}) = 1$, 说明$x'x''$存在逆元, 有了这些就足够说明$S$是一个子群了. □

6. G为(交换)群, x为G中m阶元素, y为G中n阶元素. 证明, 如果$(m, n) = 1$, 那么$x^a y^b = 1$当且仅当$x^a = y^b = 1$: 由此可以证明由x, y生成的群是mn阶的, 并且由xy生成.

证明. 充分性显然, $x^a = y^b = 1$, 显然有$x^a y^b = 1$.

必要性: 设$x^a y^b = 1$, 我们需要证明$m|a, n|b$, 或者说如果有$0 \leq a < m, 0 \leq b < n$时, 必有$a = b = 0$. 显然如果$a = 0$, 必有$b = 0$.

$$x^a = y^{-b} \Rightarrow x^{am} = y^{-bm} = 1 \Rightarrow n|bm,$$

而$(m, n) = 1$, 因此$n|b, b = 0$, 于是可得到$a = 0$.

有了前面的结论, 显然x, y生成的子群可以$x^a y^b$的形式表示, 另一方面$(xy)^{mn} = 1$, 任何小于mn的正整数$p > 0$, 都有$(xy)^p \neq 1$. □

7. 证明: $m > 2$, $n > 2$, $(m, n) = 1$, 和mn互素的模mn同余类乘法群不是循环的 (提示: 利用习题V.6, 以及这样一个事实: 每一个循环群至多有一个2阶子群).

证明. 首先说明:每一个循环群至多有一个2阶子群. 循环群中的元素可以记为$\{1, a, a^2, \cdots, a^{n-1}\}$, 其中$a^n = 1$, 当$n$为偶数的时候, $a^{n/2}$是一个2阶元素, $\{1, a^{n/2}\}$构成一个2阶子群. 其余元素都不是2阶的, 当n为奇数时, 不存在2阶子群.

根据习题V. 6, 方程组$x \equiv 1(\mod m), x \equiv -1(\mod n)$存在模$mn$意义下的唯一解$x_1$, 方程组$x \equiv -1(\mod m), x \equiv 1(\mod n)$存在模$mn$意义下的唯一解$x_2$, 显然$x_1 \neq x_2, x_1 \neq 1, x_2 \neq 1$, 并且有$x_1^2 \equiv 1(\mod m), x_1^2 \equiv 1(\mod n)$, 由于$(m, n) = 1$, 于是$x_1^2 \equiv 1(\mod mn)$, 同理$x_2^2 \equiv 1(\mod mn)$, 这就是说这个群中至少存在两个2阶子群$\{1, x_1\}, \{1, x_2\}$. 因而不可能是循环群. □

8. 找出所有的n, 使得模2^n奇同余类乘法群是循环的.

$n = 1$, 或者$x = 2$, 满足条件; 当$x > 2$时, 模2^n奇同余类乘法群不可能是循环的, 此时$2^n - 1$和$2^{n-1} - 1$都是2阶元素, 这和循环群至多有一个2阶元素矛盾.

9. 证明, 如果G是(交换)群, $n > 0$为整数, G中所有其阶数能整除n的元素构成G的子群.

证明. 记G中所有其阶数能整除n的元素组成的集合为S, 于是如果$x \in S$, 则存在a, 使得$x^a = 1$, 且$a|n$. 首先, $1 \in S$, 如果$x, y \in S$, 则$(xy)^n = 1$, 于是xy的阶能够整除n, $xy \in S$, 其次$x^a = 1$, 则$(x^{-1})^a = 1$, 也就说, x^{-1}的阶也能整除n, 从而$x^{-1} \in S$. 剩余的条件容易验证, 可知S构成一个群. □

10. 证明, 如果G是有限(交换)群, G中所有元素的乘积或者是1, 或者是一个2阶元素.

证明. 我们把G中元素分成两类, 第一类是$a \neq a^{-1}$, 记为U, 第二类中元素满足$a = a^{-1}$, 记作V, 则$U \cap V = \emptyset, G = U \cup V$, U种元素的乘积必然等于1, 而且必然是偶数个元素, 但是V中元素的乘积不一定等于1, 但是他们的乘积的平方必然等于1. □

11. 如果p是一个素数, 证明$(p-1)! \equiv -1(\mod p)$ (提示: 考虑模p乘法群, 以及利用习题VII. 10的结论).

证明. 考虑模p乘法群, 这是一个有限群, 其元素恰好就是$1, 2, \cdots, p-1$. 那么根据上一道题目的结论, $(p-1)! \equiv 1(\mod p)$, 或者$[(p-1)!]^2 \equiv 1(\mod p)$. 我们如果说明不可能是前一个结论, 那么必然有$(p-1)! \equiv -1(\mod p)$.

根据前面题目的证明方法, 对于$1 \leq x \leq p-1$, 如果$x^2 \equiv 1(\mod p)$, 必有$(x-1)(x+1) \equiv 0(\mod p)$, 此时$x=1$, 或者$x=p-1$, 除此之外的$x$都有$x \neq x^{-1}$, 于是全部元素的乘积满足

$$(p-1)! \equiv p-1 \equiv -1(\mod p).$$

$\square$

8

定理2.2表明Z的任何子群M或者是0，或者由其中最小的大于0的元素m生成；在后一种情形，它由m生成的，也可以由$-m$生成，而不能由其它元素生成．对于循环群，我们有：

定理 8.1．设G是一个m阶的循环群，由元素x生成．G'是G的子群；那么存在m的因子d使得G'是由x^d生成的$\frac{m}{d}$阶循环群．

令M为所有使得$x^a \in G'$的整数a组成的集合．公式$x^{a-b} = (x^a)\cdot(x^b)^{-1}$表明$M$是$Z$的一个子群；它包含$m$，从而包含$m$的某个因子$d$的所有倍数．因此$G'$由元素$x^{da}$，$a \in Z$组成，也就是说由$x^d$生成．我们有$x^{da} = x^{db}$当且仅当$da \equiv db(\mod m)$；根据同余关系(§V)的性质(F)，这等价于$a \equiv b(\mod \frac{m}{d})$．

推论 8.2．对于m的每一个正因子n，m阶群有且仅有一个n阶子群．

设G的含义如定理VIII.1所示，令$d = \frac{m}{n}$；根据定理，如果G'是G的n阶的子群，它必然是由x^d生成，x^d也确实生成一个子群．

推论 8.3．G，m，x，G'的含义如定理VIII.1所示，G中的元素x^a可以生成G'当且仅当$(a,m) = d$．

如果$(a,m) = d$，$x^a \in G'$；根据定理VI.2，我们有$at \equiv d(\mod m)$，于是有$x^d = (x^a)^t$，因此由x^a生成的群包含x^d，因此就是G'．

推论 8.4．G，m，x含义同上，x^a生成G当且仅当$(a,m) = 1$，G恰好有$\varphi(m)$个不同的生成元．

推论 8.5．对每一个大于0的整数m，我们有

$$\sum_{d|m} \varphi(d) = m.$$

(在这里左边的求和是针对m的所有正因子d).

考虑m阶循环群G（例如模m同余类加法群），根据推论1，对于m的每个因子d，G恰好有一个d阶的子群G_d，$d \to G_d$是m的所有因子到G的所有子群之间的一一映射. 对每一个d，用H_d表示G_d的所有的不同的生成元的集合，根据推论3，它有$\varphi(d)$个元素. G的每一个元素属于而且只属于一个集合H_d，因为它能生成而且只能生成一个G的子群.

G为一个群，X是G的子集；对每一个$a \in G$，我们用aX表示所有元素ax（$x \in X$)组成的集合. 群的定义表明$x \to ax$是X到aX的一个双射，因此，如果X是有限的，那么所有集合aX拥有和X相等数量的元素.

定义 8.6. 设G是一个群，H是G的子群，任何一个形如xH（$x \in G$)的集合称为G中的H的陪集(coset).

引理 8.7. 设xH，yH为群G的子群H的两个陪集，那么它们或者没有公共元素，或者$xH = yH$.

如果它们有一个公共元素，假设它可以表示为xh，$h \in H$，也可以表示为yh'，$h' \in H$. 这可以得到$y^{-1}x = h'h^{-1} \in H$，因此$xH = y \cdot (y^{-1}x)H = y \cdot (h'h^{-1}H) = yH$.

定理 8.8. 如果H是有限群G的子群，那么H的阶整除G的阶.

事实上，G中的每一个元素x属于某个H的陪集(例如xH)，根据引理，只属于一个陪集.由于每一个陪集的元素个数都等于H的阶，G的阶必然是这个值的倍数.

定理 8.9. 如果x是m阶群的元素，它的阶整除m，$x^m = 1$.

由于x的阶d就是由x生成的G的子群的阶，定理VIII.2表明它整除m，因而$x^m = (x^d)^{m/d} = 1$.

(上面的结论，以及它们的证明，对其他交换群也成立，如前所述，它们不在我们的处理范围之内).

定理 8.10. m为任意大于0的整数，x是一个与m互素的整数，那么$x^{\varphi(m)} \equiv 1(\mod m)$.

这是上述推论的一个特殊情形，只要把它应用于与m互素的模m同余类乘法群（或者，简要的，但是不那么准确的说法是模m乘法群).

推论 8.11. p为素数，则对每一个和p互素的x有$x^{p-1} \equiv 1(\mod p)$；对每一个x有$x^p \equiv x(\mod p)$.

第一个结论是定理VIII.3的特例，第二个结论是其推论. 反过来，从定理VI.2可知，后一个结论也包含了前一个结论. 第二个结论的另外的证明参考习题VI.9.

这个推论属于Fermat，常称为Fermat定理；第一个证明由Euler给出，他同时给出了定理VIII.3的一个证明(基本上和上面给出的相同)，这个定理常称为Euler定理.

习题

1. G是m阶群，n和m互素，证明G的每一个元素可以表示为x^n（$x \in G$）的形式.

   证明. 首先对于G中元素x, 有$x^m = 1$, 其次, 由于$(m,n) = 1$, 存在整数u, v, 使得$mu + nv = 1$, 于是

   $$x = x^{mu+nv} = x^{nv} = (x^v)^n.$$

   获证. □

2. p是素数，证明每一个p^n（$n > 0$)阶的群，包含一个p阶元素，每一个p阶群是循环群.

   证明. 如果x的阶数为k, 则$k|p^n$, 由于p为素数, 于是$k = p^m, 0 \le m \le n$. 所要证明的是存在$m = 1$的情形, 对于$m = 0$, 只有单位元是这个情形.

   我们使用归纳法来证明, 当$n = 1$时, 群本身就是一个p阶的, 任何一个不等于1的元素都是p阶元素, 结论成立. 假设对于小于等于n的整数都成立, 那么对于$n+1$来说, 如果群中存在p^{n+1}阶的元素x, 那么群本身是一个循环群, 可以由x^k来表示, 于是x^{n+1}就是一个p阶的元素. 如果不存在这样的元素, 那么任取一个不等于1的元素x, x的阶为p^m, $m < n+1$, 于是$m \le n$, 这样由这个x生成的循环群中, 存在一个p阶元素. 获证.

   也可以直接证明, 前面说明了x的阶为p^m, 那么$x^{p^{m-1}}$的阶就是p.

   每一个p阶群来说, 由于p是素数, 它的任何一个不等于1的元素的阶必然等于p, 任何一个不等于1的元素都可以生成这个元素, 因而是循环群. □

3. 如果p是$a^{2^n} + 1$的奇素因子，$n \ge 1$，证明$p \equiv 1(\mod 2^{n+1})$（提示：找出模p乘法群中的$(a \mod p)$的阶）（Euler用此来证明$2^{32} + 1$不是素数，给出了Fermat猜想的一个反例：所有的整数$2^{2^n} + 1$是素数).

   证明. 根据条件, 有$a^{2^n}+1 \equiv 0(\mod p)$, 也就是$a^{2^n} \equiv -1(\mod p)$, $a^{2^{n+1}} \equiv 1(\mod p)$. 由此可以知道$a \mod p$的阶为$2^{n+1}$, 而模$p$乘法群的是$p-1$阶群, 于是$2^{n+1}|(p-1)$, 即$p - 1 \equiv 0(\mod 2^{n+1})$, $p \equiv 1(\mod 2^{n+1})$.

   有了这个结论, 我们寻找奇素数p满足$p \equiv 1(\mod 2^6)$, 通过计算机稍微试验几个, 就可以发现$p = 641$满足条件. $641|2^{32} + 1$. □

4. 如果a，b为大于0的整数，$a = 2^\alpha 5^\beta m$，m和10互素，证明$\frac{b}{a}$的小数形式的数字的周期整除$\varphi(m)$；证明，如果它不存在小于$m-1$个数字的周期，那么m是素数.

证明. 我们假设循环节出现的时候, 余数对应了模m的元素为a, 那么, 这里其实是元素$10^k (\mod m), k = 0, 1, 2, \cdots, r-1$, r为循环节的长度. 也就说$a10^r \equiv a (\mod m)$. 设10在模m同余乘法群中的阶为s, 则$r \leq s, s|\varphi(m)$, 因为10是与m互素的模m的同余乘法群的元素(一共有$\varphi(m)$个). 若能证明$r|s$, 则$r|\varphi(m)$, 首先对于所有$0 < t < r, a10^t \equiv a (\mod m)$是不成立的. 设$s = kr + t$, 则

$$a \equiv a10^s = a10^{kr+t} \equiv a10^t (\mod m),$$

于是必须有$t = 0, r|s$.

注意到如果m为素数, 那么$\varphi(m) = m-1$. 我们使用反证法, 如果m不是素数, $m = m_1 m_2, (m_1, m_2) = 1$, 我们只要找到一个$a$, 使得$r < m-1$即可. 对于$a$, 有$a10^{r_1} \equiv a \mod (m_1), b10^{r_2} \equiv b (\mod m_2)$,

$$\begin{aligned} ab10^{r_1 r_2} &\equiv ab (\mod m_1) \\ ab10^{r_1 r_2} &\equiv ab (\mod m_2) \\ ab10^{r_1 r_2} &\equiv ab (\mod m_1 m_2) \end{aligned}$$

于是$r_1 r_2 \leq \varphi(m_1)\varphi(m_2) \leq (m_1 - 1)(m_2 - 1) < m - 1$. 与题设矛盾, m为素数. □

注意反过来不一定成立, 也就是说m为素数的时候, 可能出现循环节的长度小于$m-1$, 例如1/3.

9

为了考虑系数在域F_p上的多项式，以及该域上的方程，我们先复习任意域K上的多项式的一些基本性质；它们独立于域的性质，它们类似于前面II，III，IV上描述的整数的性质.

在这一节中，域K始终保持不变. K上的一个不定元X的多项式P（也就是说系数在K上），由下列形式给出

$$P(X) = a_0 + a_1 X + \cdots + a_n X^n$$

其中$a_0, a_1, \ldots, a_n$属于K. 如果$a_n \neq 0$，P称作是n次的,我们用$n = \deg(P)$表示；任意非0多项式都有次数. 加法和乘法以往常的方式定义，这些多项式构成一个环，常表示为$K[X]$. 如果P，Q是非0多项式，则$\deg(PQ) = \deg(P) + \deg(Q)$.

引理 9.1. A，B为两个多项式，$B \neq 0$；$m = \deg(B)$. 存在唯一的多项式Q使得$A - BQ$或者等于0，或者是小于m次的多项式.

（可以和第II节的引理比较一下）. 如果$A = 0$，那是不证自明的；我们对$n = \deg(A)$实施归纳法：首先我们证明Q的存在性. 如果$n < m$，我们取$Q = 0$. 否则，令bX^m为B的m次项，aX^n为A的n次项；由于多项式$A' = A - B \cdot (\frac{a}{b} X^{n-m})$的次数小于$n$，利用归纳假设，我们可以把它表示为$BQ' + R$，这里或者$R = 0$，或者$R$的次数小于$n$. 于是$A = BQ + R$，这里$Q = Q' + \frac{a}{b} X^{n-m}$. 至于$Q$的唯一性，令$A - BQ$和$A - BQ_1$为0或者其次数小于$m$；因而这一点对于$B(Q - Q_1)$也是成立；它的次数为$m + \deg(Q - Q_1)$，除非$Q - Q_1 = 0$，从而$Q$必须等于$Q_1$.

如果$R = 0$，$A = BQ$，A就称为B的倍式，而B为A的因式. 如果$B = X - a$，那么R必然为0，或者是0次多项式，也就是说是常数(K中元素)，因此我们有

$$A = (X - a)Q + r$$

$r \in K$. 用a代替两边的X，我们有$A(a) = r$；如果它是0，就称a为A的根. 因此A是$X - a$的倍式当且仅当a是A的根.

正如第2节中的引理推导出定理II.1一样，我们有

定理 9.2. 设$\mathfrak{M}$是(域K)上的非空的多项式集合,对加法封闭, 因此, 如果A属于$\mathfrak{M}$, 那么所有的A的倍式也属于$\mathfrak{M}$. 那么$\mathfrak{M}$由所有的某个多项式D的所有倍式成的, 在忽略乘以一个非零常数的情形下D是唯一决定的.

如果$\mathfrak{M} = \{0\}$, 定理成立, 取$D = 0$. 否则, 在$\mathfrak{M}$中选择具有最小次数d的非0多项式D. 如果A属于$\mathfrak{M}$, 我们应用引理于A和D, 有$A = DQ + R$, R或者是0, 或者次数小于d. 于是$R = A + D \cdot (-Q)$也属于$\mathfrak{M}$, 根据D的定义R等于0, $A = DQ$. 如果D_1也有和D一样的性质, 那么它是D的倍数, D是D_1的倍数, 因此它们有相同的次数; $D_1 = DE$, 我们可知E的次数是0, 是非零常数.

称aX^d为D的d次项; 在这些和D只相差一个非零常数因子的所有多项式之中, 有且仅有一个多项式的最高项系数为1, 即$a^{-1}D$; 这样的多项式称为是规范化的.

正如在第2节中的那样, 我们可以对所有多项式$A, B, \ldots, C$的线性组合组成的集合$\mathfrak{M}$应用定理IX.1; 这里$P, Q, \ldots, R$是任意的多项式. 如果$\mathfrak{M}$是由D的倍数组成的, D或者是0, 或者是一个规范化的多项式, D被称为$A, B, \ldots, C$的最大公因式, 并表示为$(A, B, \ldots, C)$. 和第2节一样, D是$A, B, \ldots, C$的因式, 并且$A, B, \ldots, C$的每一个公因式整除D. 如果$D = 1$, 则称$A, B, \ldots, C$互素; 它成立当且仅当存在多项式$P, Q, \ldots, R$满足

$$AP + BQ + \cdots + CR = 1.$$

如果$(A, B) = 1$, 则称A对B不可约, B对A不可约.

一个$n > 0$次多项式A称为是素的, 或者不可约的, 如果它没有大于0次小于n次的因式. 任何一个1次的多项式都是不可约的. 我们需要注意到多项式的不可约性会随着域的改变而有所不同: 例如$X^2 + 1$在Q上不可约, 在实数域上也不可约, 但是在复数域上是可约的, $X^2+1 = (X+i)(X-i)$.

正如第4节一样, 我们可以证明每一个大于0次的多项式可以被唯一地表示为不可约多项式的乘积. 我们需要的是一个稍弱一点的结果:

定理 9.3. A是K上的$n > 0$次多项式, 它能够在不考虑因子次序的情况下被唯一地表示为如下形式

$$A = (X - a_1)(X - a_2) \cdots (X - a_m)Q,$$

这里$0 \leq m \leq n$, $a_1, a_2, \ldots, a_m \in K$, Q在K中没有根.

如果A没有根, 这是显然的; 否则, 我们对n使用归纳法. 如果A有一个根a, $A = (X - a)A'$; A'的次数为$n - 1$, 我们可以对它应用这个定理; 把A'表示为前面的形式, 我们得到类似的乘积. 如果A能够以上述方式表示, 并有如下形式

$$A = (X - b_1)(X - b_2) \cdots (X - b_r)R$$

其中R在K中没有根, 于是A的根a必然是a_i之一, 也是b_j之一, 除以$X-a$之后, 我们得到A'的两个乘积, 根据归纳假设, 它们必然相等.

推论 9.4. $n > 0$次多项式至多有n个不同的根.

习题

1. 给出Q上的多项式的最大公因式:

$$X^5 - X^4 - 6X^3 - 2X^2 + 5X + 3, X^3 - 3X - 2.$$

找出它们在域F_3上的最大公因式, 这里系数解释为模3同余类.

使用辗转相除法:

$$\begin{aligned} X^5 - X^4 - 6X^3 - 2X^2 + 5X + 3 &= (x^2 - x - 3)(x^3 - 3x - 2) \\ &\quad + (-3x^2 - 6x - 3) \\ (x^3 - 3x - 2) &= \frac{-1}{3}(x-2)(-3x^2 - 6x - 3) \end{aligned}$$

于是在Q上的最大公因式为$x^2 + 2x + 1 = (x+1)^2$.

在F_3上的最大公因式也可以表示为上述形式.

2. 证明$X^4 + 1$是Q上的素多项式, 但是在习题VI.12中定义的域上有2次因式.

证明. $X^4 + 1$没有实数根, 因此在R上没有一次因式, 在Q上也没有, 所以如果$X^4 + 1$可以分解, 我们可以设

$$X^4 + 1 = (X^2 + aX + b)(X^2 + cX + d)$$

展开, 比较对应项可以得到

$$\begin{aligned} a + c &= 0 \\ d + ac + b &= 0 \\ ad + bc &= 0 \\ bd &= 1 \end{aligned}$$

如果$a = 0$, 那么$c = 0$, $b = -d$, 于是由$bd = 1$, 可知在R上无解.

$a \neq 0, a = -c, b = d, -a^2 + 2b = 0, b^2 = 1$, 如果$b = -1$, 无解, 必须$b = d = 1$, $a = \sqrt{2}, c = -\sqrt{2}$, 或者$a = -\sqrt{2}, c = \sqrt{2}$, 这是唯一的实数解.

$$X^4 + 1 = (X^2 - \sqrt{2}X + 1)(X^2 + \sqrt{2}X + 1).$$

获证. □

3. Let K be any field, and R a subring of $K[X]$ containing K. Prove that there exists a finite set of polynomials $P_1, P_2, \cdots, P_N$ in R such that R consists of all the polynomials in $P_1, \cdots, P_N$ with coefficients in K (Hint: call d the g.c.d. of the degrees of all polynomials in R, take $P_1, \cdots, P_m$ in R such that the g.c.d. of their degrees is d, and then apply the conclusion in exercise III.6).

   设K是任意的域, R是包含K的$K[X]$的子环, 证明存在R中的有限个多项式集合$P_1, P_2, \ldots, P_N$, 使得R由系数在K上$P_1, P_2, \ldots, P_N$的组合的多项式组成. (提示: 令d为R中所有的多项式的次数的最大公约数, 选择R中的$P_1, P_2, \ldots, P_m$使得它们的次数的最大公约数为d, 然后对习题III.6应用这个结论).

   这道题目不是很理解,首先,根据习题3.6,存在L,使得$l \geq l$时,对于每一个ld,存在正整数$x_1, \cdots, x_m$,使得

$$\sum x_i \deg(P_i) = ld.$$

   是不是说把次数小于Ld的所有的R中的多项式取出来就是呢? 例如$X^n, n \leq Ld$. 需要证明能够取出有限个.

10

引理 10.1. 设G为m阶群. 如果对于m的每一个因子d，G中只有d个元素满足$x^d=1$，那么G是循环的.

对于m的每一个因子d， 令$\psi(d)$为G中d阶元素的个数； 我们需要证明$\psi(m)>0$. 在每一种情形下， 由于G的每一个元素的阶整除m， 我们有

$$m=\sum_{d|m}\psi(d).$$

如果对某个d，$\psi(d)>0$，于是G包含有d阶元素，它生成d阶循环群G'. G'中的所有d个元素满足$x^d=1$，我们的假设说明G的所有$\psi(d)$个d阶的元素全部属于G'；根据定理VIII.1的推论3，它恰好有$\psi(d)$个这样的元素. 因此，如果$\psi(d)$不是0，它等于$\varphi(d)$. 既然$\sum\psi(d)$等于m，根据定理VIII.1的推论4，$\sum\varphi(d)$也等于m，这意味着对于所有的d，$\psi(d)=\varphi(d)$；特别的，$\psi(m)=\varphi(m)>0$.

现在我们考虑任意一个域K，用$K^\times$表示K的非零元素组成的乘法群，我们来考虑$K^\times$的元素以及有限阶子群. 如果x是$K^\times$的m阶元素，则$x^m=1$，$x^a=x^b$当且仅当$a\equiv b(\mod m)$；习惯上，x称作单位根，或者更准确地说m次单位元根. 对每一个n，K中满足$x^n=1$的元素x是单位根，其阶整除n. 在复数域，数

$$e^{2\pi i/m}=\cos\frac{2\pi}{m}+i\sin\frac{2\pi}{m}$$

是m次单位元根；对于$(a,m)=1$的时候$e^{2\pi ia/m}$也是.

定理 10.2. 如果K是任意的域，$K^\times$的每一个有限子群都是循环的.

对每一个$n>0$，K中满足$x^n=1$的元素是多项式X^n-1的根；根据定理IX.2的推论，K中至多只有n个这样的元素. 我们的定理立刻可以由引理得到.

推论 10.3. 如果K是有限域，则$K^\times$是循环的.

推论 10.4. K是任意的域，n是大于0的整数，K中满足$x^n=1$的元素组成一个循环群，其阶整除n.

很显然它们构成$K^\times$的子群；由定理X.1知它是循环的；如果它是由x生成的，x的阶，同时也就是这个群的阶，整除n.

定理 10.5. p为任一素数，存在和p互素的整数r，使得$1,r,r^2,r^3,\ldots,r^{p-2}$，在某种顺序下，分别模$p$同余于$1,2,\ldots,p-1$.

这只是以下事实的一个传统说法：与p互素的模p同余类组成模p同余类域F_p的乘法群$F_p^\times$，根据定理X.1的推论，它是循环的；如果$(r \mod p)$是这个群的生成元，r具有定理X.2所述的性质.

设m为大于1的整数，和m互素的模m同余类乘法群并不总是循环的（参考习题VII.7和VII.8）. 它是循环的，当且仅当存在和m互素的整数r，使得$(r \mod m)$在该群中是$\varphi(m)$阶的，也就是说，当且仅当满足$r^x\equiv 1(\mod m)$的大于0的最小整数x等于$\varphi(m)$；如果这一点成立,则称r为模m原根. 于是对于和m互素的每一个整数a，存在整数x使得$r^x\equiv a(\mod m)$；整数x仅仅由模$\varphi(m)$决定，称为a的指标，并记之为$\mathrm{ind}_r(a)$. 根据定理VII.2，如果r是模m原根，映射

$$(a \mod m)\to(\mathrm{ind}_r(a) \mod \varphi(m))$$

是与m互素的模m同余类乘法群到模$\varphi(m)$的同余类群的一个同构. 特别的，对于和m互素的a和b，我们有：

$$\mathrm{ind}_r(ab)\equiv\mathrm{ind}_r(a)+\mathrm{ind}_r(b)(\mod \varphi(m)).$$

和对数法则类似.

习题

1. m为大于1的整数，证明模m的原根的个数或者等于0，或者等于$\varphi(\varphi(m))$.

   证明. 假设r为模m的原根,那么与m互素的模m同余类是循环的,并且可以由r生成,可以表示为

   $$r,r^2,\cdots,r^{\varphi(m)}=1,$$

   所有与$\varphi(m)$互素的k,r^k也是模m原根,于是一共有$\varphi(\varphi(m))$个. □

2. 找出模13的原根；对于$1\le a\le 12$求出$\mathrm{ind}_r(a)$；利用这张表找出所有的模13原根，以及模13的5次幂和29次幂.

   如果r为模13的原根,那么$r^{12}=1,r^n\neq 1,0\le n<12$,另一方面,$r^k=1$,必有$k|12$,12的因子为$1,2,3,4,6,12$,逐个验证.

3. 当p是素数时，利用模p原根的存在性，证明$1^n+2^n+\cdots+(p-1)^n$模p同余于0或者-1，依据不同的整数$n\geq 0$.

证明. 存在与p互素的r, 使得$1, r, r^2, \cdots, r^{p-2}$与$1, 2, \cdots, p-1$模$p$同余, 于是

$$\begin{aligned} 1^n+2^n+\cdots+(p-1)^n &\equiv 1^n+r^n+r^{2n}+\cdots+r^{(p-2)n} \\ &\equiv \frac{1-(r^n)^{p-1}}{1-r^n} (\mod p) \end{aligned}$$

当$(p-1)|n$时, 分子为零, 需要特别考虑, 此时

$$1^n+2^n+\cdots+(p-1)^n \equiv 1+1+\cdots+1 = p-1 \equiv -1(\mod p).$$

否则, 根据前面的$1-(r^n)^{p-1}=0$, 可知

$$1^n+2^n+\cdots+(p-1)^n \equiv 0(\mod p).$$

□

4. 证明一个模$m>1$的原根同时也是模m的每一个因子的原根. (提示: 使用习题V. 6)

5. 使用二项式定理, 通过归纳法证明, 如果p是奇素数, 那么对所有的$n\geq 0$:

$$(1+px)^{p^n} \equiv 1+p^{n+1}x(\mod p^{n+2})$$

(参考习题VI. 10). 并由此证明: 如果r是一个模p原根, 它是模p^n的原根的充要条件是p^2不能整除$r^{p-1}-1$, 此时, r和$r+p$都是模p^n原根.

证明. $n=0$时, 结论显然成立.

$n=1$时,

$$(1+px)^p = 1+p(px)+\frac{p(p-1)}{2}(px)^2+\cdots+(px)^p \equiv 1+p^2x(\mod p^3)$$

假设结论对于n成立, 对于$n+1$来说, 由于

$$(1+px)^{p^n} \equiv (1+p^{n+1}x)(\mod p^{n+2}),$$

于是

$$(1+px)^{p^{n+1}} = [(1+px)^{p^n}]^p \equiv (1+p^{n+1}x)[(1+px)^{p^n}]^{p-1}(\mod p^{n+2}),$$

另一方面

$$(1+p^{n+1}x)^p \equiv 1+p^{n+2}x(\mod p^{n+3}),$$

□

6. 求出所有的$m > 1$，使得模m原根存在.（提示：使用习题X.4，X.5，VII.7，VII.8，以及这样的事实：如果r是模某个奇数m的原根，那么r和$r + m$均是模$2m$的原根）.

7. 整数$m > 0$称作是不含平方因子的，如果它没有形如n^2的因子，这里$n > 1$. 对每一个$m > 0$，令$\mu(m) = (-1)^r$，如果m是不含平方因子的并且是r个素数的乘积（当$m = 1$时$r = 0$），否则$\mu(m) = 0$. 证明当ab互素时有$\mu(ab) = \mu(a)\mu(b)$；从而有$\sum_{d|m} \mu(d) = 1$，在$m = 1$时，而在$m > 1$时和式为0.（提示：用习题IV.4的方式来表示m）.

8. 令K为包含m次单位原根x的域；对于m的每一个因子d，$F_d(X)$为$X - x^a$（$0 \le a < m$，$(a, m) = \frac{m}{d}$）的乘积. 证明F_d是$\varphi(d)$阶的，并有

$$X^m - 1 = \prod_{d|m} F_d(X);$$

从而，可以使用习题X.7证明

$$F_m(X) = \prod_{d|m} (X^{m/d} - 1)^{\mu(d)}.$$

9. K的含义同习题X.8，证明K中所有的m次单位原根之和等于$\mu(m)$. 特别的请给出当$K = F_p$，$m = p - 1$时的结果.

11

现在我们考虑域K（有时在环上)上的形如$x^m = a$的方程；$a = 1$的情形已经在第10节中讨论过了．而$a = 0$的情形是平凡的，故我们假定$a \neq 0$．在域K中，x为$x^m = a$的解，则x'也是它的一个解的充要条件是$(x'/x)^m = 1$．因此如果$x^m = a$在K上有解，那么它的解的个数和K中m次原根一样，也就是$X^m - 1$的根的个数一样.

这里我们主要考虑模p同余类域F_p.

定理 11.1. p为素数，整数$m > 0$，整数a和p互素；$d = (m, p-1)$．同余式$x^m \equiv a(\mod p)$或者恰好有d个模p的解，或者没有解；它有解当且仅当同余式$y^d \equiv a(\mod p)$有解；这等价于$a^{(p-1)/d} \equiv 1(\mod p)$，这样的$a$(模$p$)恰好有$\frac{p-1}{d}$个.

我们使用这个事实：群$F_p^\times$是循环群，或者说存在模p的原根r(参考第10节)．令$a \equiv r^t, x \equiv r^u(\mod p)$，即$t = \mathrm{ind}_r(a)$，$u = \mathrm{ind}_r(x)$．于是同余式$x^m \equiv a(\mod p)$等价于$mu \equiv t(\mod p-1)$，我们的结论可以由定理VI.2得出，只要我们注意到$t \equiv 0(\mod d)$等价于$\frac{p-1}{d}t \equiv 0(\mod p-1)$，即$a^{(p-1)/d} \equiv 1(\mod p)$.

举个例子，考虑同余式$x^3 \equiv a(\mod p)$，a和p互素．若$p = 3$，它等价于$x \equiv a(\mod 3)$．对于$p \equiv 1(\mod 3)$的情形；即$p \neq 2$，$p \equiv 1(\mod 2)$，因而可以表示为$6n+1$；我们有$d = 3$，$\frac{p-1}{d} = 2n$；同余式$x^3 \equiv a(\mod p)$有解的充要条件是a和$1, r^3, \ldots, r^{p-4}$之一模p同余，此时，如果x是一个解，$xr^{2nz}(z = 0, 1, 2)$模p给出所有的解．如果$p \equiv 2(\mod 3)$，此时p或者是2，或者为$6n-1$，同余式$x^3 \equiv a(\mod p)$对于和p互素的每一个a有且仅有一个解.

从此开始，我们只考虑$m = 2$的情形．于是$x^2 \equiv 1(\mod p)$在$p = 2$时，只有一个解1，而在$p > 2$时有两个解± 1.

定义 11.2. p为奇素数(单质数)，整数a和p互素，分别称作模p二次剩余或者二次非剩余，如果同余式$x^2 \equiv a(\mod p)$有解或者无解.

对于$m = 2$不会再有其它可能，单词“二次”通常被省略；对于$m = 3$常常被称作“三次剩余”，$m = 4$时称作“四次剩余”，等等.

p是一个奇素数；$p=2n+1$，r为模p原根. 定理XI.1说明存在n个模p二次剩余，即$1, r^2, \ldots, r^{2n-2}$，以及n个二次非剩余，即$r, r^3, \ldots, r^{2n-1}$. 如果x是$x^2 \equiv a(\mod p)$的解，同余式有两个解$\pm x$，而没有其他解.

定理 11.3. 令$p=2n+1$为奇素数，整数a和p互素. 则a^n或者和$+1$模p同余，或者和-1模p同余；根据$a^n \equiv +1(\mod p)$或者$a^n \equiv -1(\mod p)$，a分别为模p二次剩余或者二次非剩余.

令$b=a^n$；根据Fermat定理（即定理VIII.3的推论），我们有$b^2 \equiv 1(\mod p)$，因此$b \equiv \pm 1(\mod p)$. 至此我们可以运用定理XI.1了.

推论 11.4. 对于奇素数p，根据$p \equiv 1(\mod 4)$，或者$p \equiv -1(\mod 4)$，-1分别是模p的二次剩余，或者二次非剩余.

事实上，$(-1)^n=1$当n为偶数的时候，$(-1)^n=-1$当n为奇数的时候.

习题

1. p为a^2+b^2的奇素数因子，a，b为整数，证明p和1模4同余，除非它整除a和b.

2. p为奇素数，a和p互素，证明同余式$ax^2+bx+c \equiv 0(\mod p)$分别有两个解，一个解，无解，分别对应于$b^2-4ac$是模$p$二次剩余，0，或者二次非剩余.

3. $m>0$，$n>0$是互素的整数，F是整系数多项式，证明同余式$F(x) \equiv 0(\mod mn)$有解的充要条件是$F(x) \equiv 0(\mod m)$和$F(x) \equiv 0(\mod n)$都有解.（提示：使用习题V.6和VI.1）

4. p是奇素数，$n>0$，a和p互素，通过对n使用归纳法证明：同余式$x^2 \equiv a(\mod p^n)$有解的充要条件是a为模p二次剩余. 并证明，如果x是一个解，那么除了$\pm x$之外再没有其它解.

5. 证明，a为一奇数，$n>2$，同余式$x^2 \equiv a(\mod 2^n)$有解当且仅当$a \equiv 1(\mod 8)$.（提示：对n进行归纳，注意到，如果x是一个解，则x和$x+2^{n-1}$是$y^2 \equiv a(\mod 2^{n+1})$的解）. 如果$x$是一个解，找出其它的解.

6. 使用习题XI.3，4，5，给出同余式$x^2 \equiv a(\mod m)$有解的判断准则. 这里m为大于1的整数，a和m互素.

7. 如果对于某个$m>1$以及某个和m互素的a，同余式$x^2 \equiv a(\mod m)$恰好有n个不同的解模m，证明恰好存在$\frac{\varphi(m)}{n}$个不同的和m互素的a满足条件.

12

设p是一个奇素数；$p=2n+1$．用G表示和p互素的模p同余类乘法群$F_p^\times$；它包含一个由同余类$(\pm 1 \mod p)$组成的2阶子群H；我们对G和H应用第VIII节的定义和引理． 如果$x\in G$，那么它属于而且仅属于一个陪集xH；它由两个元素$(\pm x \mod p)$组成；存在n个这样的陪集，即陪集$(\pm 1 \mod p), (\pm 2 \mod p), \ldots, (\pm n \mod p)$． 我们在每一个陪集中选择一个元素，我们把它们表示为$u_1,\ldots,u_n$，它就是G中H的陪集的代表集合；于是每一个和p互素的整数和$\pm u_1,\ldots,\pm u_n$之一模p同余． 下面的引理属于Gauss，常称作Gauss引理，这样的集合$\{u_1,\ldots,u_n\}$称作模p“Gauss集”．这样的集合中最简单的是$\{1,2,\ldots,n\}$．

引理 12.1．$p=2n+1$为奇素数，$\{u_1,\ldots,u_n\}$是模p的Gauss集．a是和p互素的整数；$1\le i\le n$，$e_i=\pm 1$，i'满足$au_i\equiv e_i u_{i'}(\mod p)$． 那么分别对应于乘积$e_1e_2\cdots e_n$等于$+1$或者$-1$，$a$是模$p$的二次剩余或者二次非剩余．

在n个同余式$au_i\equiv e_i u_{i'}(\mod p)$中，没有两个$i'$是相等的，否则，存在$i\ne k$，有$au_i\equiv \pm au_k(\mod p)$，因此$u_i\equiv \pm u_k(\mod p)$，这和Gauss集的定义矛盾．因此，我们把所有这些同余式相乘，可以得到

$$a^n(u_1u_2\cdots u_n)\equiv (e_1e_2\cdots e_n)\cdot(u_1u_2\cdots u_n)(\mod p)$$

既然所有的u_i和p互素，因此

$$a^n\equiv e_1e_2\cdots e_n(\mod p).$$

根据定理XI.2可以得到我们的结论．

定理 12.2．p是奇素数，在$p\equiv 1(\mod 8)$或$p\equiv 7(\mod 8)$时2是模p二次剩余，而在$p\equiv 3(\mod 8)$或$p\equiv 5(\mod 8)$时是二次非剩余．

$p=2n+1$，对$a=2$和Gauss集$\{1,2,\ldots,n\}$应用Gauss引理．当$n=4m$或者$4m+1$时，e_i在$1\le i\le 2m$时等于1，其它情形等于-1；于是e_i的乘积为$(-1)^{n-2m}=(-1)^n$． 若$n=4m+2$或者$4m+3$，e_i在$1\le i\le 2m+1$时等于1，其它情形下为-1，e_i的乘积为$(-1)^{n-2m-1}=(-1)^{n-1}$． 引理的一个简单的应用即可给出上述结论．

定义 12.3. p是奇素数，整数a和p互素，我们定义$\left(\frac{a}{p}\right)$在a是模p二次剩余的时候等于$+1$，而在a是模p的二次非剩余的时候等于-1；这个符号称为Legendre符号.

给定p，符号$(\frac{a}{p})$仅仅依赖于a的模p同余类. 根据定义有对于和p互素的a有$(\frac{a^2}{p}) = 1$.

如果r是模p原根，若$a \equiv r^x(\mod p)$，即$x = \mathrm{ind}_r(a)$，我们有$(\frac{a}{p}) = (-1)^x$；这里我们需要注意到它并不依赖于x的选择，x定义为模一个偶数$p-1$. 从指标(参考第X节的最后一个公式)的基本性质可知，Legendre符号具有如下性质：对于所有和p互素的a，b有

$$(\frac{ab}{p}) = (\frac{a}{p}) \cdot (\frac{b}{p}).$$

定理XI.2，它的推论，定理XII.1分别为

$$a^{(p-1)/2} \equiv (\frac{a}{p})(\mod p), (\frac{-1}{p}) = (-1)^{(p-1)/2}, (\frac{2}{p}) = (-1)^{(p^2-1)/8}.$$

(对于最后一个公式，注意到$\frac{p^2-1}{8}$总是一个整数，$p \equiv 1,7(\mod 8)$时为偶数，而$p \equiv 3,5(\mod 8)$时为奇数).

下面的定理常称为“二次互反律”：

定理 12.4. p和q是不同的奇素数，那么有

$$(\frac{p}{q}) \cdot (\frac{q}{p}) = (-1)^{[(p-1)/2]\cdot[(q-1)/2]}$$

令$p = 2n+1$，$q = 2m+1$. 对$a = q$和模p的Gauss集$\{1, 2, \ldots, n\}$运用Gauss引理. 对于$1 \le x \le n$，我们有$qx \equiv e_x u(\mod p)$，这里$e_x = \pm 1$，$1 \le u \le n$；这也可以表示为$qx = e_x u + py$，这里e_x，u，y在x给定的时候由这些条件唯一确定. 特别的，$e_x = -1$当且仅当$qx = py - u$，也就是$py = qx + u$，$1 \le u \le n$. 这意味着$y > 0$，并有

$$y \le \frac{1}{p}(q+1)n < \frac{q+1}{2} = m+1.$$

换句话说，$e_x = -1$的充要条件是能够找到y使得数对(x, y)满足条件

$$1 \le x \le n, 1 \le y \le m, 1 \le py - qx \le n.$$

因此，如果数对(x, y)的数量是N，Gauss引理给出$(\frac{q}{p}) = (-1)^N$.

类似的，$(\frac{p}{q}) = (-1)^M$，如果M是满足如下条件的数对(x, y)的数量：

$$1 \le x \le n, 1 \le y \le m, 1 \le qx - py \le m.$$

由于当x和p互素的时候$qx-py$不可能等于0，特别的，若$1\le x\le n$，我们的定理中的等式的左边等于$(-1)^{M+N}$，这里$M+N$是满足如下条件的数对(x,y)的数量：

$$1\le x\le n, 1\le y\le m, -n\le qx-py\le m.$$

现在用S表示满足如下条件的数对(x,y)的数量

$$1\le x\le n, 1\le y\le m, qx-py<-n,$$

用T表示满足如下条件的数对(x',y')的数量

$$1\le x'\le n, 1\le y'\le m, qx'-py'>m.$$

在最后面的两个集合之间，存在一个一一映射

$$x'=n+1-x, y'=m+1-y;$$

事实上，根据我们的定义，我们有

$$qx'-py'-m=-(qx-py+n).$$

因此$S=T$. 另一方面，$M+N+S+T$是所有的数对(x,y)的数量，这里$1\le x\le n$，$1\le y\le m$，因此它等于mn. 最后我们有

$$(\frac{p}{q})\cdot(\frac{q}{p})=(-1)^{M+N}=(-1)^{M+N+S+T}=(-1)^{mn},$$

正是我们要证明的.

习题

1. p为奇素数；定义在和p互素的整数a上的函数$f(a)$如下：$f(a)$从±1中取值，并且
$$f(ab)=f(a)f(b); f(a)=f(b)\text{如果}a\equiv b(\mod p).$$
证明或者对所有的a有$f(a)=1$；或者对所有的a有$f(a)=(\frac{a}{p})$.

2. p是a^2+2b^2的奇因子，a，b为整数，证明p和1或者3模8同余，除非它整除a和b.

3. p，q是素数，$p=2q+1$，$q\equiv1(\mod 4)$，证明2是模p原根.

4. 仅使用Gauss引理，找出所有的素数$p>3$，使得3是一个二次剩余.

5. a为非零整数. 证明如果p，q是奇素数，但不是a的因子，使得$p\equiv q(\mod 4|a|)$，那么$(\frac{a}{p})=(\frac{a}{q})$. （提示：令$a=\pm n^2b$，这里$b$是不含平方因子的(参考习题X.7)；对$b$的每一个奇素因子和$p$，$q$应用二次互反律；当$b$为偶数的时候应用定理XII.1，当$a<0$时运用定理XI.2的推论).

13

我们回忆一下复数的概念；它是形如$x+iy$的数，其中x，y是实数；i满足$i^2=-1$，加法和乘法规则正如我们已经了解的．特别的，乘法规则如下

$$(x+iy)(x'+iy')=(xx'-yy')+i(yx'+xy').$$

复数集C在加法和乘法下构成一个幺环，它的单位元是$1=1+i\cdot 0$（参考第VI节）．如果$a=x+iy$，$\bar{a}=x-iy$称为a的共轭虚数；$\bar{a}$的共轭虚数就是a．映射$a\to\bar{a}$是C到它自身的一个保持加法和乘法的一一映射；因此它是一个C的自同构，也就是C到它自身的一个同构．

我们记$N(a)=a\bar{a}$，并称之为a的范数．根据乘法规则，如果$a=x+iy$，则$N(a)=x^2+y^2$；从乘法的交换性有$N(ab)=N(a)N(b)$．a的范数等于0当且仅当$a=0$；否则它是大于0的实数．因此对任意$a=x+iy\neq 0$，我们有

$$a'=N(a)^{-1}\bar{a}=\frac{x}{N(a)}-i\frac{y}{N(a)},$$

则$aa'=1$，对每一个b，$a(a'b)=b$；反过来，如果$az=b$，我们有$a'(az)=a'b$，因此，根据结合律有$z=a'b$．这说明C实际上是一个域．通常，我们都把复数$a=x+iy$和平面上的点(x,y)联系起来；它到原点0的Euclid距离为$|a|=N(a)^{1/2}$；它也被称作是a的绝对值．

我们的目的不是要考虑域C，而是它的子集，那些复数$x+iy$(其中$x,y\in Z$，也就是为常规整数)组成的集合．很容易验证它是一个环；这个环称为Gauss环，其元素称为Gauss整数．显然$a\to\bar{a}$是这个环的一个自同构．如果a是一个Gauss整数，$N(a)=a\bar{a}$是Z中的正整数．我们偶尔也会考虑数$x+iy(x,y\in Q$，即x，y为有理数)；可以证明它们构成一个域（Gauss域）．

a，b，x为Gauss整数，$b=ax$，b称为a的倍数，a整除b，或者说a是b的因子；此时$N(a)$整除$N(b)$．每一个Gauss整数整除它的范数．

1的因子称为是单元；如果$a=x+iy$是一个单元，$N(a)$整除1因而必然等于1；由于x，y是整数，这意味着它们中的一个是± 1，而另一个为0．因此Gauss单元是± 1，$\pm i$．

两个非零的Gauss整数a，b相互整除的充要条件是它们只相差一个单元因子，即若$b = ea$，$e = \pm 1, \pm i$；则称它们是联合的．给定的Gauss整数$a \neq 0$的四个联合之中，有且仅有一个$b = x + iy$满足$x > 0, y \geq 0$；它称作是规范(normalized)的．例如，$1 + i$的四个联合$\pm 1 \pm i$中，$1 + i$是唯一的规范的Gauss整数．从几何意义上看，平面上对应于a的联合的点，可以通过点a绕着0分别旋转$\frac{\pi n}{2}$ (n = 0，1，2，3)角度得到；其中的规范整数或者在正实数轴上，或者在第一象限．

范数大于1的Gauss整数称为Gauss素数，如果它除了单元以及它的联合之外没有其它因子．一个等价的说法是q为Gauss素数，如果它既不是0也不是单元，并且没有一个因子其范数大于1而且小于$N(q)$．通常意义上的普通的素数(参考第IV节)将被称作是有理素数 (或者常规素数)．如果q是Gauss整数，$N(q)$是有理素数，那么q是Gauss素数；正如我们将看到的，它的逆命题不成立．Gauss素数的联合还是Gauss素数；这些数中有且仅有一个在上述意义上是规范的．如果q是Gauss素数，$\bar{q}$也是Gauss素数．a为一个既不是0也不是单元的Gauss整数，它的最小范数大于1的因子必然是Gauss素数．

Gauss把Gauss整数引入数论之中，他发现Gauss整数可以唯一地分解为Gauss素数的乘积，类似于通常的整数．下面会给出这个证明；证明方法类似第II，III，IV，IX节．我们首先证明一个类似第II，IX节的引理．

引理 13.1. a，b为Gauss整数，$b \neq 0$，那么存在b的倍数bq使得

$$N(a - bq) \leq \frac{1}{2} N(b).$$

对于任意实数t，存在一个最大的整数$m \leq t$，有$m \leq t < m + 1$；对于离t最近的整数m'，依$t - m$是否$\leq m + 1 - t$而分别等于m或者$m + 1$；于是有$|t - m'| \leq \frac{1}{2}$．令$z = x + iy$为任意的复数；$m$为最接近$x$的整数，$n$为最接近$y$的整数，$q = m + in$．于是$q$是Gauss整数，我们有

$$N(z - q) = (x - m)^2 + (y - n)^2 \leq \frac{1}{2}.$$

对$z = \frac{a}{b}$应用此不等式，这里a，b是引理中定义的Gauss整数．于是按照如上方法构造的Gauss整数q满足条件．

定理 13.2. $\mathfrak{M}$为非空的Gauss整数集，对加法下封闭，于是若$a \in \mathfrak{M}$，则所有的a的倍数都属于$\mathfrak{M}$．那么$\mathfrak{M}$是由某个Gauss整数d的所有倍数组成，d在相差一个单元因子的情形下是唯一确定的．

若$\mathfrak{M} = \{0\}$，定理成立，只要取$d = 0$．否则，选择最小范数大于0的元素$d \in \mathfrak{M}$．若$a \in \mathfrak{M}$，我们应用引理有$a = dq + r$，$N(r) \leq \frac{1}{2} N(d)$．因而$r = a - dq \in \mathfrak{M}$，这样会和$d$的定义产生矛盾，除非$r = 0$，$a = dq$．至于

唯一性，假设d'具有和d一样的性质，d和d'必然是相互的倍数，因此d'是d的联合.

和在第II，IX节一样，我们可以对于给定的Gauss整数$a, b, \ldots, c$的所有的线性组合$ax + by + \cdots + cz$(这里$x, y, \ldots, z$是任意Gauss整数)的集合应用定理XIII.1，并由此定义最大公约数$(a, b, \ldots, c)$；如果我们规定它必须为规范的，那么它是唯一确定的. 如果它等于1，我们称$a, b, \ldots c$是互素的. 我们现在可以重复第III，IV节的主题了，只是定理IV.2的证明是对整数a进行归纳，而现在需要对$N(a)$进行归纳. 结论是

定理 13.3. 每一个非零的Gauss整数能本质上唯一地表示为单元和Gauss素数的乘积.

在这里“本质上唯一”是以下意义. 令

$$a = eq_1q_2\cdots q_r = e'q_1'q_2'\cdots q_s'$$

为两种乘积表示方式($a \neq 0$)，这里e，e'是单元，q_j和q_k'都是Gauss素数. 定理说明$r = s$，并且可以通过重新排列q_k'使得q_j'是q_j的联合，$1 \leq j \leq r$；若a为单元，则$r = 0$. 如果规定a的素因子是规范的，那么乘积在不要求因子的顺序的情形下是唯一确定的.

常规整数也是Gauss整数；为了把它们分解为Gauss素数的乘积，只需要分解为常规素数即可.

定理 13.4. p是奇有理素数. 它或者是一个Gauss素数，或者是某个Gauss素数q的范数；在后一种情形，$p = q\bar{q}$，q，$\bar{q}$不是联合，p除了q，$\bar{q}$以及它们的联合之外没有Gauss素数因子.

如定理XIII.2，令$p = eq_1q_2\cdots q_r$. 对于范数，我们发现p^2等于$N(q_j)$的乘积. 若有某个$N(q_j)$等于p^2，那么$r = 1$，$p = eq_j$，p本身就是Gauss素数. 否则每一个$N(q_j)$等于p，我们有$p = N(q) = q\bar{q}$，q为Gauss素数；$\bar{q}$也是Gauss素数. 令$q = x + iy$；如果$\bar{q}$是q的联合，那么它等于$\pm q$或者$\pm iq$；这样或者有$y = 0$，$p = x^2$，或者有$x = 0$，$p = y^2$，或者有$y = \pm x$，$p = 2x^2$；但是p是奇素数，因而这是不可能的.

对于$p = 2$，它的分解方式为

$$2 = N(1 + i) = (1 + i)(1 - i) = i^3(1 + i)^2;$$

它的唯一的规范的素因子为$1 + i$.

定理 13.5. p是奇有理素数. 那么依p和3或者1模4同余，p分别是一个Gauss素数，或者是某个Gauss素数的范数.

如果它是$q = x + iy$的范数，我们有$p = x^2 + y^2$，这里的x，y必然是一为奇数，一为偶数. 平方数x^2和y^2有一个模4和1同余，而另一个模4和0同余，因此$p \equiv 1 \pmod 4$. 反过来，定理XI.2的推论说明-1是模p二次剩余，因而存在x使得$x^2 + 1$是p的倍数. 而$x^2 + 1 = (x + i)(x - i)$，如果p是Gauss素数，这意味着p或者整除$x + i$，或者整除$x - i$. 很显然这是不可能的.

推论 13.6. 每一个Gauss素数或者是$\pm 1 \pm i$，或者是和3模4同余的有理素数的联合，或者它的范数是和1模4同余的有理素数.

事实上，每一个Gauss素数q必然整除其范数$q\bar{q}$的某个有理素数因子p；当p是奇数时应用定理XIII.4，以及当$p = 2$时使用上述备注，我们可以得到我们的结论.

推论 13.7. 有理素数可以表示为两个平方数之和的充要条件为它等于2或者和1模4同余.

事实上，若$p = x^2 + y^2$，由于p有因子$x \pm iy$，它不可能是Gauss素数.
有必要指出这是一个已经在一个更大的环即Gauss整数中证明过的结论.
习题

1. 如果一个正整数能够表示为形式$n^2 a$，这里$a > 1$并且无平方因子，证明它能够表示为两个平方数之和的充要条件是a的每一个奇素数因子满足$\equiv 1 \pmod 4$. 如果是这样，a有r个素因子，找出把a表示为两个平方数之和的方式个数.

2. 如果一个整数是两个互素的平方数之和，证明该整数的每一个因子也是两个互素的平方数之和.

3. 使用复数在平面上的点的表示，证明，如果z是任意的复数，那么存在Gauss整数q到z的距离$\leq \frac{\sqrt{2}}{2}$；证明至少存在一个Gauss整数到z的距离最小，同时最多不会超过4个具有这样的性质. （提示：参考第XIII节的引理的证明）

4. 和常规整数一样的定义在Gauss整数中的同余关系$f(m)$，对于所有的Gauss整数$m \neq 0$，$f(m)$等于不同的模mGauss同余类的个数；证明对任意的非零Gauss整数m，n，$f(mn) = f(m)f(n)$. （提示：在模m的同余类中选择代表x_i，$1 \leq i \leq f(m)$，在模n的同余类中选择代表y_j，$1 \leq j \leq f(n)$，然后证明$x_i + my_j$是模mn的同余类的代表).

5. 使用习题XIII.4证明对每一个m，$f(m) = m\bar{m}$. （提示：对m和$n = \bar{m}$应用习题XIII.4).

6. 证明，m是范数大于1的Gauss整数，模m的Gauss同余类组成一个域的充要条件是m是Gauss素数. 证明，如果$N(m)$是有理素数，每一个Gauss整数和某个有理整数模m同余.

7. $\omega = -\frac{1}{2} + i\frac{\sqrt{3}}{2}$，证明复数$x + y\omega$(其中$x$，$y$为常规整数)组成环$R$，其中单元为$\pm 1$，$\pm\omega$，$\pm\omega^2$. 证明，如果$z$是一个任意的复数，存在环$R$中的元素$q$使得$N(z-q) \leq \frac{1}{3}$. （提示：参考习题XIII.3). 因此对环$R$证明定理XIII.1的一个类似结论，以及唯一分解定理. [1]

8. 使用习题XIII.7证明大于3的有理素数可以表示为x^2+xy+y^2(x，y为整数)的充要条件是它$\equiv 1 \pmod 3$.

参 考 文 献

[1] 华罗庚 数论导引

[2] Hardy 数论导引

索 引