初 等 数 论 习 题 解 答

第一章　整除性以及算术基本定理

(1)找出$180, 270, 520$所有因子

略.

(3)在$m = 2, 3, 7, 9$时计算687的m进制展开

解　仅以$m = 2$为例,其他情形类似可得,当$m = 2$时,由除法算法知$m = 2^9 + 2^7 + 2^5 + 2^3 + 2^2 + 2^1 + 1$. □

(5)令a, x, y, z, w为整数.证明如果$a \mid (2006x - y)$且$a \mid (2006z - w)$,那么$a \mid (xw - yz)$.

证明　由$a \mid (2006x - y), a \mid (2006z - w)$.我们有$2006x - y = at_1, 2006z - w = at_2$,其中$t_1, t_2$为整数. 所以有$2006xz - yz = at_1z, 2006zx - wx = at_2x$,两式相减有$wx - yz = at_1z - at_2x$,从而我们有$a \mid (xw - yz)$. □

(7)计算$(206, 208), [168, 252, 294]$.

解　$(206, 208) = 2, [168, 252, 294] = 3528$. □

(9)证明若n为奇数时,$(n, n + 2) = 1$,n为偶数时,$(n, n + 2) = 2$.

证明　由辗转相除法,$(n, n + 2) = (n, 2)$,当n为奇数,则$n = 2k + 1$,从而$(2k + 1, 2) = (1, 2) = 1$.当n为偶数,则$n = 2k$,从而$(2k, 2) = 2$. □

(11)利用Euclid算法计算14和91的最大公因子,将$(14, 91)$表为14和91的整的线性组合.计算$\frac{91}{14}$的简单连分数表示.

解　$91 = 6 \cdot 14 + 7, 14 = 2 \cdot 7 + 0$,所以$\gcd(91, 14) = 7$.从而$\gcd(91, 14) = 7 = 91 - 6 \cdot 14, \frac{91}{14} =< 6, 2 >$. □

(13)找出$a = 2^8 5^5 7^3 11^7, b = 3^7 5^9 11^3 13^8$的最大公因子和最小公倍数.

解　$\gcd(a, b) = \prod\limits_p p^{min\{v_p(a), v_p(b)\}} = 5^5 11^3$. $\mathrm{lcm}(a, b) = \prod\limits_p p^{max\{v_p(a), v_p(b)\}} = 2^8 3^7 5^9 11^7 13^8$. □

(15)令$n > 2$,证明当$k = 2, \cdots, n + 1$时,$(n + 1)! + k$均为复合数.

证明　对任意的k在$2, \cdots, n+1$之间,我们有$(n+1)! = 1 \cdot 2 \cdots (k-1) \cdot k \cdot (k+1) \cdots (n+1)$, 所以$(n + 1)! + k = k(1 \cdot 2 \cdots (k - 1) \cdot (k + 1) \cdots (n + 1) + 1)$,从而

表明$k \mid k+(n+1)!$,且显然$k < k+(n+1)!$,即k为$k < k+(n+1)!$的非平凡因子.故$k < k+(n+1)!$为复合数.

此题表明,连续出现的复合数列的长度可以任意长,或者两素数之间的间隔可以趋于无穷. □

(17)证明$\mathrm{rad}(mn) = \mathrm{rad}(m)\,\mathrm{rad}(n)$当且仅当$(m,n) = 1$

证明　设m,n的标准分解式分别为$m = \prod_{p_i} p_i^{e_i}$,$n = \prod_{q_i} q_i^{f_i}$,其中$e_i, f_i$均大于等于1. 从而$\mathrm{rad}(m) = \prod_{p_i} p_i$,$\mathrm{rad}(n) = \prod_{q_i} q_i$ 若$\mathrm{rad}(mn) = \mathrm{rad}(m)\,\mathrm{rad}(n)$,那么表明$\mathrm{rad}(mn) = \prod_{p_i} p_i \prod_{q_i} q_i$,如果存在某个$p_i = q_j$,对某个$i,j$成立,那么则表明$\mathrm{rad}(mn)$有某个素因子的幂次大于等于2,这与$\mathrm{rad}(n)$定义矛盾.所以,$(m,n) = 1$. 反过来,如果$(m,n) = 1$,那么对任意的$i,j$均有$p_i \neq q_j$.

于是$\mathrm{rad}(mn) = \prod_{p_i} p_i \prod_{q_i} q_i = \mathrm{rad}(m)\,\mathrm{rad}(n) = \prod_{p_i} p_i \prod_{q_i} q_i$. □

(19)令S为一个正整数的集合.如果对任意的$x,y \in S$,我们都有$(x,y) \in S$(对应$[x,y] \in S$),我们就说S是$\gcd-$闭的(对应$\mathrm{lcm}-$闭的).

对任意实数e,我们定义S的e次幂$S^e := \{x^e \mid x \in S\}$.证明若$e$为一个正整数,则集合$S$是$\gcd-$闭的(对应$\mathrm{lcm}-$闭的)当且仅当$S^e$是$\gcd-$闭的(对应$\mathrm{lcm}-$ 闭的).

证明　我们先证明一个小结果.对任意的x,y,如果$\gcd(x,y) = d$,那么对任意的正整数e,我们有$\gcd(x^e,y^e) = d^e$,$\mathrm{lcm}(a^e,b^e) = \mathrm{lcm}(a,b)^e$.由于$\gcd(x,y) = d$, 所以我们有$x = dt_1, y = dt_2$,其中$t_1,t_2$互素.

从而我们有$\gcd(x^e,y^e) = \gcd(d^e t_1^e, d^e t_2^e) = d^e \gcd(t_1^e,t_2^e) = d^e$.

再由$\gcd(a,b)\,\mathrm{lcm}(a,b) = ab$,我们有$\mathrm{lcm}(a^e,b^e) = \mathrm{lcm}(a,b)^e$.

我们只证明S时$\gcd-$闭的,当S是$\mathrm{lcm}-$闭的时候,类似可证.

若对任意的$x,y \in S$,有$\gcd(x,y) \in S$.那么对任意的$x^e,y^e \in S^e$,$\gcd(x^e,y^e) = \gcd(x,y)^e \in S^e$.所以由定义$S^e$也是$\gcd-$闭的.反过来,如果$S^e$ 是$\gcd-$闭的,即是对任意的x,y,$\gcd(x^e,y^e) \in S^e$,于是我们有$\gcd(x,y)^e \in S^e$,即$\gcd(x,y) \in S$.所以由定义S是$\gcd-$闭的. □

(21)令$2 = p_1 < p_2 < \cdots$为一个素数的递增序列.证明$p_n \leq 2^{2^{n-1}}$对所有$n \geq 1$成立.

证明　我们用数学归纳法证明该题.当$n=1$时,命题是显然成立的.我们假设命题在$n=k$时成立,我们证明命题在$n=k+1$时也成立.

考虑$N=p_1p_2\cdots p_k+1$,显然$p_1,p_2,\cdots,p_k$均不为N的因子,又注意到$\{p_i\}_{i=1}^{\infty}$是素数列的一个升序排列,所以对任意p整除N,$p_{k+1}\leq p\leq N$,由归纳假设$N=p_1p_2\cdots p_k+1\leq\prod_{i=1}^{k}2^{2^{i-1}}+1=2^{\sum_{i=1}^{k}2^{i-1}}=2^{2^k-1}+1\leq 2\cdot 2^{2^k-1}=2^{2^k}$.即命题在$n=k+1$也成立. □

(23)设a,n为两个正整数,其中$n>1$.

(i)证明只有在$a=2$且$n=p$为一个素数时,a^n-1为素数.具有$M_p=2^p-1$形式的素数称为梅森素数.

(ii)计算前5个梅森素数.

证明

(i)当$a=1$时,$a^n-1=0$,所以a^n-1不为素数.当$a>2$时,$a^n-1=(a-1+1)^n-1=(a-1)^n+\binom{n}{1}(a-1)^{n-1}+\cdots+\binom{n}{n-1}(a-1)+1-1=(a-1)K$. 其中$K$为某一个正整数.所以$(a-1)\mid(a^n-1)$,当$a>2$时,由于$n>1,1<a-1<a^n-1$,从而$a-1$为$a^n-1$的非平凡因子.故而当$a>2$时,$a^n-1$不为素数.

下面设$a=2$,若n不为素数,则存在d,d',满足$1<d\leq d'<n$,使得$n=dd'$.从而有$2^n-1=2^{dd'}-1=(2^d-1)(2^{d(d'-1)}+2^{d(d'-2)}+\cdots+2^d+1)$.这样$2^d-1$为$2^n-1$的一个非平凡因子.故而$a^n-1$不为素数.

(ii)简单计算知前5个素数为$2^2-1,2^3-1,2^5-1,2^7-1,2^{13}-1$. □

(25)x_1,x_2,x_3为三个非负整数,找到所有不能表示成$3x_1+10x_2+14x_3$形式的非负整数.计算$G(3,10,14)$.

解　由书上定理1.5.2知当整数$b\geq(3-1)(10+14-1)=46$时,则b一定可以用形式$3x_1+10x_2+14x_3$表示.所以,我们只需找出满足$0\leq b\leq 46$的整数b,判断哪些整数不可以表出就可以了. 注意到12到21均可以被表出,所以将x_2变成x_2+k,我们就可以得到$12+10k$到$21+10k$的所有值. 也就是说,大于等于12的值都可以表示.简单验算知$1,2,4,5,7,8,11$均不能表出,所以$G(3,10,14)=12$.

□

(27)令n,k为整数,且$k>0$,证明(i)$(n-1)^2\mid(n^k-1)$当且仅当$(n-1)\mid k$.

(ii)$(n-1)^3 \mid (n^k-1)$当且仅当$2(n-1)^2 \mid k(2+(k-1)(n-1))$.

证明

将n^k-1改写成$(n-1+1)^k-1$,利用二项式展开有$(n-1+1)^k-1=(n-1)^k+\binom{k}{1}(n-1)^{k-1}+\cdots+\binom{k}{k-1}(n-1)$.

(i)若$(n-1)^2 \mid (n^k-1)$,那么有上述的二项式展开式,我们知道$n-1 \mid \frac{n^k-1}{n-1}=(n-1)^{k-1}+\binom{k}{1}(n-1)^{k-2}+\cdots+\binom{k}{k-1}$, 注意到除$\binom{k}{k-1}=k$这一项之外均被$n-1$整除,所以由$(n-1)^2 \mid (n^k-1)$,知道必须有$n-1 \mid k$.

反之若$n-1 \mid k$,那么有$k=t(n-1)$成立,对某个正整数t成立,从而$n^k-1=(n-1)^2((n-1)^{k-2}+\binom{k}{1}(n-1)^{k-3}+\cdots+t)$,故而$(n-1)^2 \mid (n^k-1)$.

(ii)类似上一问,$(n-1)^3 \mid (n^k-1)$成立与否等价于$(n-1)^3$是否整除$k(n-1)+\binom{k}{2}(n-1)^2$, 简单的变形可知,$(n-1)^3 \mid k(n-1)+\binom{k}{2}(n-1)^2$等价于$2(n-1)^2 \mid k(2+(k-1)(n-1))$.命题得证. □

(29)证明对任意正整数m,n,我们有$\gcd(2^m-1,2^n-1)=2^{\gcd(m,n)}-1$.

证明

我们先证明这样一个结论,如果$t_1=q_1t_2+r_1$,那么我们有

$$\gcd(\sum_{i=0}^{t_1-1}2^{di},\sum_{i=0}^{t_2-1}2^{di})=\gcd(\sum_{i=0}^{r_1-1}2^{di},\sum_{i=0}^{t_2-1}2^{di})$$

.

特别的,如果t_1,t_2互素,那么我们就有$\gcd(\sum\limits_{i=0}^{t_1-1}2^{di},\sum\limits_{i=0}^{t_2-1}2^{di})=1$.

$\gcd(\sum\limits_{i=0}^{t_1-1}2^{di},\sum\limits_{i=0}^{t_2-1}2^{di})=\gcd(\sum\limits_{i=0}^{t_1-1}2^{di}-(\sum\limits_{i=0}^{q_1-1}2^{t_2di})(\sum\limits_{i=0}^{t_2-1}2^{di}),\sum\limits_{i=0}^{t_2-1}2^{di})$.

即$\gcd(2^{q_1t_2}\sum\limits_{i=0}^{r_1-1}2^{di},\sum\limits_{i=0}^{t_2-1}2^{di})$,由于2与$\sum\limits_{i=0}^{t_2-1}2^{di}$互素,所以

$$\gcd(2^{q_1t_2}\sum_{i=0}^{r_1-1}2^{di},\sum_{i=0}^{t_2-1}2^{di})=\gcd(\sum_{i=0}^{r_1-1}2^{di},\sum_{i=0}^{t_2-1}2^{di}).$$

结论得证.

设$\gcd(m,n)=d$,所以$m=t_1d$,$n=t_2d$,t_1,t_2互素.那么我们有$\gcd(2^m-1,2^n-1)=\gcd(2^{t_1d}-1,2^{t_2d}-1)=\gcd((2^d-1)(\sum\limits_{i=0}^{t_1-1}2^{di}),(2^d-1)(\sum\limits_{i=0}^{t_2-1}2^{di}))=(2^d-1)\gcd(\sum\limits_{i=0}^{t_1-1}2^{di},\sum\limits_{i=0}^{t_2-1}2^{di})=2^d-1=2^{\gcd(m,n)}-1$. 最后一步使用了证明的结论. □

(31)令m,n,a,b分别为正整数,并且$a>b$且满足$(a,b)=1$.证明$(a^m-b^m,a^n-b^n)=a^{(m,n)}-b^{(m,n)}$.

证明

与29题类似,我们先证明如果$t_1=q_1t_2+r_1$,那么我们有

$$\gcd(\sum_{i=0}^{t_1-1}a^{di}b^{d(t_1-1-i)},\sum_{i=0}^{t_2-1}a^{di}b^{d(t_1-1-i)})=\gcd(\sum_{i=0}^{r_1-1}a^{di}b^{d(t_1-1-i)},\sum_{i=0}^{t_2-1}a^{di}b^{d(t_2-1-i)})$$

特别的,如果t_1,t_2 互素,a,b 互素,那么我们就有

$$\gcd(\sum_{i=0}^{t_1-1}a^{di}b^{d(t_1-1-i)},\sum_{i=0}^{t_2-1}a^{di}b^{d(t_1-1-i)})=1.$$

具体证明与上题类似,这里就省略了.最后利用该结论,就可以得到待证的式子. □

(33)证明$n^{4l^4}+4l^4$在$n>1$或者$l>1$时均为复合数.

证明　先考虑分解式$n^{4l^4}+4l^4=(n^{2l^4}+2ln^{l^4}+2l^2)(n^{2l^4}-2ln^{l^4}+2l^2)$.当$n\neq 1$,$l\neq 1$时,这两个因子均不为1,(第一个因子显然大于1,只需要考虑第二个因子即可),从而为复合数. □

(35)令$1\leq a_1<a_2<\cdots<a_{2010n+1}\leq 2011n$.证明存在$1\leq i\leq j\leq 2010n+1$,使得$a_i\mid a_j$.

证明　首先注意到2011是一个素数.所以由算术基本定理可知,对每一个整数a_i,我们均可以写成$a_i=2011^{j_i}b_{j_i}$, 其中b_{j_i}是一个和2011互素的数. 所以,对每一个a_i,我们有一个b_{j_i}相对应.由于$1\leq a_1<a_2<\cdots<a_{2010n+1}\leq 2011n$,所以共有$2010n+1$个这样的$b_{j_i}$,而在$1,\cdots,2011n$之间,不被2011整除的数,只有$2010n$个.

所以由抽屉原理,必有某个$i<k$,b_{j_i}=b_{j_k}.再由$a_i<a_k$,以及$a_i=2011^{j_i}b_{j_i}<2011^{j_k}b_{j_i}=a_k$,知$j_i<j_k$.即$a_i\mid a_k$,对某些$a_i,a_k$满足$1\leq i\leq k\leq 2010n+1$成立. □

(37)令n为任意的正整数.令p为一个满足$n<p<2n$.则p整除$\binom{2n}{n}$

证明　事实上,我们还能证明p恰好整除$\binom{2n}{n}$.我们计算$v_p(\binom{2n}{n})$,注意到$\binom{2n}{n}=\frac{(2n)!}{(n!)^2}$,所以我们有$v_p(\binom{2n}{n})=v_p((2n)!)-2v_p(n!)$,由于$p>n$,所以$v_p(k)=0$,对所

有$1 \leq k \leq p-1$成立,所以$v_p(n!)=0$.另一方面$n<p<2n$,所以$p \mid v_p((2n)!)$. 但是$2p>2n$,所以$p^2 \nmid (2n)!$,从而$v_p((2n!))=1$.故p恰好整除$\binom{2n}{n}$. □

(39)设a,b为两个互素的两个整数.证明如果$a+b$为奇数,则$(a+b,a-b)=1$.

证明 由辗转相除法,我们有$(a+b,a-b)=(2a,a+b)$.注意到$(2,a+b)=1$,所以$(2a,a+b)=(a,a+b)=(a,b)$,由题设,a,b互素,故$(a,b)=1$,即$(a+b,a-b)=(a,b)=1$. □

(41)令m,n为整数,并且m为奇数.证明如果a为偶数时,(a^m-1,a^n+1)等于1;

a为奇数时,(a^m-1,a^n+1)等于2.

证明 令$(a^m-1,a^n-1)=d$,那么存在整数K,T使得$a^m-1=Kd,a^n+1=Td$,即$a^m=Kd+1,a^n=Td-1$.由上式,我们有$a^{mn}=(a^m)^n=(Kd+1)^n=(a^n)^m=(Td-1)^m$.

对上式使用二项式定理并注意到m是奇数,我们有$1+Sd=-1+Rd$.其中R,S为两个整数.从而我们有$2=(R-S)d$,从而$d \mid 2$,所以d只能为2. 再注意到a为偶数时,a^m-1,a^n+1均为奇数,所以此时$(a^m-1,a^n+1)=2$; a为奇数时,a^m-1,a^n+1 均为偶数,所以此时$(a^m-1,a^n+1)=1$. □

(43)令p为一个奇素数,且令$(a,b)=1$,并且$a+b \neq 0$.证明$(a+b,\frac{a^p+b^p}{a+b})$等于1或者$p$.

证明 令$a+b=t$,所以$b=t-a$,所以$\frac{a^p+b^p}{a+b}=t^{p-1}+\binom{p}{1}(-a)t^{p-2}+\cdots+\binom{p}{p-1}(-a)^{p-1}$,注意到,上式除开最后一项以外,其余项均被$t$整除,所以$(\frac{a^p+b^p}{a+b},a+b)=(pa^{p-1},a+b)$.又因为$(a,b)=1$,所以$(a^{p-1},a+b)=(a,a+b)=(a,b)=1$,所以$(pa^{p-1},a+b)=(p,a+b)$.

注意$a+b \neq 0$,所以当$p \mid a+b$,$(a+b,\frac{a^p+b^p}{a+b})=p$,当$p \nmid a+b$,$(a+b,\frac{a^p+b^p}{a+b})=1$. □

(45)令$n \geq 1$为一个整数.计算$\gcd(\binom{2n}{1},\binom{2n}{3},\cdots,\binom{2n}{2n-1})$

解 注意到$\binom{2n}{1}=2n$,记$d=\gcd(\binom{2n}{1},\binom{2n}{3},\cdots,\binom{2n}{2n-1})$,所以$d \mid 2n$. 对每个素数$p \mid 2n$我们计算$v_p(d)$,这样就可以求出$d$的值了.

当$p=2$时,显然$v_2(d) \neq v_2(2n)=v_2(n)+1$.另一方面,对任意的$0 \leq k \leq n-1$,$\binom{2n}{2k+1}=\frac{(2n)!}{(2k+1)!(2n-2k-1)!}=\frac{2n}{2n-2k-1}\cdot\binom{2n-1}{2k+1}$,所以$v_2(\binom{2n}{2k+1})=v_2(2n)-v_2(2n-2k-1)+v_2(\binom{2n-1}{2k+1}) \geq v_2(2n)=v_2(n)+1$.所以$v_2(d)=v_2(n)+1$.

当$p \neq 2$时,记$v_p(n) = r$,显然p^r属于集合$\{1, 3, \cdots, 2n-1\}$.设$2n$的p-adic展开式为$2n = a_0 p^r + a_1 p^{r+1} + \cdots + a_l p^{r+l}$.记$\sigma(n)$为$n$的$p$-adic展开的数字和.考虑$v_p(\binom{2n}{p^r}) = \frac{\sigma(2n-p^r)+\sigma(p^r)-\sigma(2n)}{p-1} = \sum_{i=1}^{l} a_i + a_0 - 1 + 1 - \sum_{i=0}^{l} a_i = 0$. 所以当$p \neq 2$时,我们有$v_p(\binom{2n}{p^r}) = 0$,所以$p \nmid d$.

综上$d = 2^{v_2(n)+1}$. □

(47)(i)如果$(a, b) = 1$,则对每个$n > ab$,存在正的x和y,使得$n = ax + by$. (ii)如果$(a, b) = 1$,则不存在正数x和y,使得$ab = ax + by$.

证明 (i) 令$x_0 = x - 1, y_0 = y - 1$,所以$n = ax + by = ax_0 + by_0 + a + b$.所以立得$n - a - b = ax_0 + by_0$,从而只要证明存在非负整数$x_0, y_0$可以表出$n - a - b$. 由于$(a, b) = 1$,直接计算$G(a, b) = (a-1)(b-1) = ab - a - b + 1 \leq n - a - b$,即$n - a - b \geq G(a, b)$,从而可以被表示出来.故这样的$x, y$是存在的.

(ii) 如果存在x和y,使得$ab = ax + by$,那么,则存在非负整数x_0, y_0,使得方程$ab - a - b = ax_0 + by_0$有解.但是由(i)知,$ab - a - b$恰好小于$G(a, b)$.由$G(a, b)$的定义可知,这样的非负的x_0, y_0是不存在的.所以这样的正的x和y也是不存在的.

□

(49)若$m \neq n$,根据a的取值计算$\gcd(a^{2^m} + 1, a^{2^n} + 1)$

解 设$\gcd(a^{2^m} + 1, a^{2^n} + 1) = d$,因为$m \neq n$,所以不妨设$m > n$.

由$\gcd(a^{2^m} + 1, a^{2^n} + 1) = d$,我们有$a^{2^m} + 1 = k_1 d, a^{2^n} + 1 = k_2 d$,于是$a^{2^m} = k_1 d - 1, a^{2^n} = k_2 d - 1$.

又因为$m > n$,故我们有$a^{2^m} = (a^{2^n})^{2^{m-n}}$,从而由上式立得$k_1 d - 1 = (k_2 d - 1)^{2^{m-n}} = 1 + \binom{2^{m-n}}{1} k_2 d (-1)^{2^{m-n}-1} + \cdots + (k_2 d)^{2^{m-n}}$,即$k_2 d - 1 = 1 + dU$,其中$U$为某一个整数.

所以有$(k_1 - U)d = 2$,这样有$d = 1$或者$d = 2$. 注意到当a为偶数时,$2 \nmid a^{2^n} + 1$,此时$d = 1$; 注意到当a为奇数时,$2 \mid a^{2^n} + 1$,此时$d = 2$.

(51)令$m > 0$,且a, b为整数,满足$(a, b) = 1$.证明算术级数$\{a + bi\}_{i=0}^{\infty}$存在无穷多个整数与$m$互素.

证明 先证明存在一个n_0使得$\gcd(a + bn_0, m) = 1$.

设m所有的素因子为$p_1, \cdots, p_k$.设满足$p_i \nmid ab$构成的集合为S. 令n_0为S中元素的乘积.那么我们断言$\gcd(a + bn_0, m) = 1$.

对m的任何一个素因子p_i,若$p_i \in S$,我们有$p_i \mid bn_0$,但$p_i \nmid a$,所以$p_i \nmid a+bn_0$.

若$p_i \notin S$,由于$\gcd(a,b)=1$,所以p_i仅整除a,b中的一个,且$p_i \nmid n_0$,从而$p_i \nmid a+bn_0$. 这表明$\gcd(a+bn_0,m)=1$.

注意到$\gcd(a+b(n_0+im),m)=\gcd(a+bn_0,m)$,令$i$取遍所有非负整数就得到无穷大个$i$满足与$m$互素. □

(53)令$n \geq 1$为一个整数,且令$S_n=\sum_{k=1}^{n}(k^5+k^7)$.找出$S_n$与$S_{3n}$的最大公因子.

解 用数学归纳法,我们可以证明$\sum_{k=1}^{n} k^5+k^7=\frac{n^4(n+1)^4}{8}$.

分n为奇数和偶数讨论.

若n为奇数时,不妨设$n=2t+1$,$\gcd(S_n,S_{3n})=\gcd(2[(2t+1)(t+1)]^4,2[3(2t+1)(3t+2)]^4)=2(2t+1)\gcd(3^4,(t+1)^4)$.

所以若$3 \mid t+1$时,$\gcd(S_n,S_{3n})=162n^4$;

若$3 \nmid t+1$时,$\gcd(S_n,S_{3n})=2n^4$.

类似的,当$n=2t$时,若$t=3l+1$时,$\gcd(S_n,S_{3n})=\frac{81n^4}{8}$;

若$t \neq 3l+1$时,$\gcd(S_n,S_{3n})=\frac{n^4}{8}$.

□

(55)证明任何一个包含$mn+1$个不同整数序列中要么包含一个长度大于m的递增序列,要么包含一个长度大于n的递减序列.

证明 设这$mn+1$个整数分别为$a_1,a_2,\cdots,a_{mn+1}$,我们对这$mn+1$个数做一个到$\mathbb{Z}^+ \times \mathbb{Z}^+$的映射$\phi$.其中第一个分量为以这个数结尾的在这个整数序列中最长的递增数列的长度,第二个分量为以这个数开头的在这个整数序列中最长的递减数列的长度.

例如,序列为$3,5,2,1,4,6,7$,$\phi(4)=(2,1)$,$\phi(5)=(2,3)$.

我们先证明这个映射是一个单射.任取$a_i,a_j,i \neq j$,不妨设a_i排在a_j前方.

若$a_i > a_j$,则a_i的第二个分量大于a_j的第二个分量;若$a_i < a_j$,则a_i的第一个分量小于a_j的第一个分量;故映射ϕ一定为一个单射.

而第一个分量不超过m有m种取法,第二个分量不超过n有n种取法,从而共有mn种取法.

然而序列中共有$mn+1$个数,由抽屉原理,要么两个数是同一种取法,要么有一个数在这mn种取法之外,但是ϕ是一个单射,这就表明有一个数在这mn种取法之外. 即要么包含一个长度大于m的递增序列,要么包含一个长度大于n的递减序列.

□

(57)令$d_1,\cdots,d_n$为正整数,对所有的$1\leq i\leq n$,令$u_i=(d_i,\frac{d_1\cdots d_n}{d_i})$.证明对所有的$1\leq i\leq n$,我们有$u_i=(u_i,\frac{u_1\cdots u_n}{u_i})$.

证明 我们证明,对任意的素数p,我们均有$v_p(u_i)\leq v_p(\frac{u_1\cdots u_n}{u_i})$.从而$u_i\mid\frac{u_1\cdots u_n}{u_i}$.

这就表明$u_i=(u_i,\frac{u_1\cdots u_n}{u_i})$.

设d_i的p-adic赋值分别为k_i.由$u_i=(d_i,\frac{d_1\cdots d_n}{d_i})$,我们有$v_p(u_i)=\min(k_i,\sum\limits_{j\neq i}^{n}k_j)$.

而$I:=v_p(\frac{u_1\cdots d_n}{u_i})=\sum\limits_{j\neq i}^{n}v_p(u_j)=\sum\limits_{j\neq i}^{n}\min(k_j,\sum\limits_{l\neq j}^{n}k_l)$.

若对任意的j均有$k_j\leq\sum\limits_{l\neq j}^{n}k_l$,则$I\geq\sum\limits_{j\neq i}^{n}k_j\geq\min(k_i,\sum\limits_{j\neq i}^{n}k_j)$. 若存在$j$使得$k_j>\sum\limits_{l\neq j}^{n}k_l$,由于$j\neq i$,$I\geq\sum\limits_{l\neq j}^{n}k_l=k_i+\sum\limits_{l\neq i,j}^{n}k_l\geq k_i\geq\min(k_i,\sum\limits_{j\neq i}^{n}k_j)$.

□

(59)令p为一个奇素数.证明p和$p+2$同时为素数的充要条件是$4(p-1)!+4\equiv -p\pmod{p(p+2)}$.

证明 充分性：由Wilson定理,我们有$(p-1)!\equiv -1\pmod p$,且$(p+1)!\equiv -1\pmod{p+2}$.由第一式,我们有$(p-1)!=Kp-1$对某个整数$p$成立,将其带入第二式,并注意到$p\equiv -2\pmod{p+2}$,$p+1\equiv -1\pmod{p+2}$,所以我们有$-4k-2\equiv -1\pmod{p+2}$, 从而,我们有$4(p-1)!+4\equiv 4Kp\equiv -p\pmod{p(p+2)}$.

必要性：反证法,若$p+2$不为素数,则一定有$1<d\leq d'<p$使得$dd'=p+2$.由$4(p-1)!+4\equiv -p\pmod{p(p+2)}$,我们有$4p!+4p\equiv -p^2\pmod{p(p+2)}$成立,由$1<d\leq d'<p$成立,我们可知$4p!\equiv 0\pmod{p(p+2)}$. 于是有$4p+p^2\equiv 0\pmod{p(p+2)}$,即$2p\equiv 0\pmod{p(p+2)}$.注意到$0<2p<p^2$,所以上式一定不成立,即为矛盾,故$p+2$为素数. □

第二章　同余式

(1)证明每一个整数模11同余于一个唯一的整数r,其中$-5 \leq r \leq 5$.

证明　由欧几里得算法,对任意的整数a,$a \equiv r_0 \pmod{11}$,其中$0 \leq r_0 \leq 10$,注意到对任意的r_0,$0 \leq r_0 \leq 10$,存在唯一的r,$-5 \leq r \leq 5$,使得$r_0 \equiv r \pmod{11}$. 故每一个整数模11同余于一个唯一的整数r,其中$-5 \leq r \leq 5$. □

(2)证明$a^4 \equiv 1 \pmod{5}$,如果$a \in \mathbb{Z}$且$5 \nmid a$.

证明　逐一列举a模5的剩余类或由费马小定理立得. □

(3)设$x_1, \cdots, x_m$为一个m个整数的序列,不必互不相同,证明存在整数 $1 \leq k \leq l \leq m$ 使得$\sum_{i=k}^{l} x_i \equiv 0 \pmod{m}$.

证明　考虑$x_1, x_1 + x_2, \cdots, \sum_{i=1}^{m} x_i$这$m$个数,若存在$t$,使得$\sum_{i=1}^{t} x_i = 0$,则令$k = 1, l = t$即可. 若这样的$t$不存在,那么这$m$个数中,必有两个数模$m$同余.不妨设$\sum_{i=1}^{m_1} x_i$与 $\sum_{i=1}^{m_2} x_i$ 模m同余,那么$\sum_{i=1}^{m_1} x_i \equiv \sum_{i=1}^{m_2} x_i \pmod{m}$, 即 $\sum_{i=m_1+1}^{m_2} x_i \equiv 0 \pmod{m}$,即令$k = m_1 + 1, l = m_2$即可. □

(4)证明对任意的正整数n,$n \equiv 3 \pmod{4}$不能写成两个数的平方和.

证明　假设$n = x^2 + y^2$,由于$x^2 \equiv 0, 1 \pmod{4}$,$y^2 \equiv 0, 1 \pmod{4}$,从而$x^2 + y^2 \equiv 0, 1, 2 \pmod{4}$,$n \equiv 3 \pmod{4}$不能写成两个数的平方和. □

(5)令p为素数,$m \geq 1$并且$0 \leq k \leq p-1$,证明

$$\binom{mp+k}{p} \equiv m \pmod{p}$$

证明　证明一:由Lucas同余式立得.

证明二：按照组合数定义,考虑

$$(p-1)!\binom{mp+k}{p} \equiv m(mp+k)\cdots(mp-p+k+1) \equiv (p-1)!m \pmod{p}.$$

所以$\binom{mp+k}{p} \equiv m \pmod{p}$. □

(6)找到下列同余式的解. (i).$5x \equiv 9 \pmod{11}$; (ii).$18x \equiv 3 \pmod{51}$; (iii).$28x \equiv 45 \pmod{70}$.

解 (i)$\gcd(5,11) \mid 9$,所以方程有解.且为唯一解,解出来可知$x = 4$;

(ii)$\gcd(18,51) \mid 3$,所以方程有解.由于$gcd(18,51) = 3$所以方程有3个解,解出来可知$x = 3, x = 20, x = 37$;

(iii)$\gcd(28,70) \nmid 45$,所以方程无解.

(7)证明$(m-1)! \equiv 0 \pmod{m}$对任意的合数$m \neq 4$.

证明 考虑m的任何一个非平凡因子d,令d'为它的共轭因子.若$d \neq d'$, 那么$d, d' \in \{1, 2, \cdots, m-1\}$,所以$(m-1)! \equiv 0 \pmod{m}$. 若$d = d'$,所以$m = d^2$,由于$m \neq 4$,所以$d \neq 2$,所以$d, 2d \in \{1, 2, \cdots, m-1\}$,所以$(m-1)! = d^2K \equiv 0 \pmod{d}^2$. □

(8)证明当素数$p \geq 5$,则$6(p-4)! \equiv 1 \pmod{p}$.

证明 因为$6 \equiv -(p-1)(p-2)(p-3) \pmod{p}$,再由Wilson定理,立得待证的结论. □

(10)我们说一个整数a是模m的幂零元,如果存在整数k使得$a^k \equiv 0 \pmod{m}$. 证明a是一个模m的幂零元当且仅当$a \equiv 0 \pmod{\text{rad(m)}}$.

证明 充分性：任取$p \mid m$,因为$a^k \equiv 0 \pmod{m}$,所以$p \mid a^k$.从而$p \mid a$,所以$\text{rad(m)} \mid a$.

必要性：不妨设$m = \prod_{i=1}^{l} p_i^{e_i}$.令$k = \max_{1 \leq i \leq l}\{e_i\}$,由于$a \equiv 0 \pmod{\text{rad(m)}}$,所以$v_{p_i}(a) \geq 1$,从而$v_{p_i}(a^k) \geq e_i$,即$a^k \equiv 0 \pmod{m}$. □

(12)计算$\varphi(2006)$和$\varphi(6993)$.

解 $2006 = 2 \cdot 17 \cdot 59$,所以$\varphi(2006) = \varphi(2) \cdot \varphi(17) \cdot \varphi(59) = 16 \cdot 58 = 928$.
$6993 = 7 \cdot 3^3 \cdot 37$,所以$\varphi(6993) = \varphi(7) \cdot \varphi(3^3) \cdot \varphi(37) = 6 \cdot 18 \cdot 36 = 3888$.

(14)证明$\varphi(m^k) = m^{k-1}\varphi(m)$对所有正整数$m$和$k$成立.

证明 注意到$\varphi(n)$是乘性函数,又因为$\varphi(p^k) = p^{k-1}\varphi(p)$,原命题得证. □

(16)证明$\varphi(m) = \varphi(2m)$当且仅当m是一个奇数.

证明 充分性:将m写作$m = 2^k m'$,其中m'为一个奇数,$\varphi(m) = \varphi(2^k)\varphi(m') = 2^{\max\{k-1,0\}}\varphi(m')$,$\varphi(2m) = \varphi(2^{k+1})\varphi(m') = 2^{\max\{k,0\}}\varphi(m')$, 又$\varphi(m) = \varphi(2m)$,所以$\max\{k-1, 0\} = \max\{k, 0\}$,即$k = 0$,所以$m$是一个奇数.

必要性：m是一个奇数,所以$\varphi(2m)=\varphi(2)\varphi(m)=\varphi(m)$. □

(18)找到所有满足$\varphi(5n)=5\varphi(n)$的正整数n.

解 考虑n的标准分解,$n=5^{e_0}\prod_{i=1}^{n}p_i^{e_i}$.

直接计算有$\varphi(5n)=\varphi(5^{e_0+1})\varphi(\prod_{i=1}^{n}p_i^{e_i})$,另一方面$5\varphi(n)=5\varphi(5^{e_0})\varphi(\prod_{i=1}^{n}p_i^{e_i})$. 所以我们有$\varphi(5^{e_0+1})=5\varphi(5^{e_0})$,这个式子在$e_0\geq 1$时成立,所以这些正整数$n$ 为所有5的倍数即可.

(20)找到下列同余式的所有解：

(i).$6x^3+27x^2+17x+24\equiv 0 \pmod{30}$.

(ii).$5x^3-93\equiv 0 \pmod{231}$.

解 (i).$6x^3+27x^2+17x+24\equiv 0 \pmod{30}$成立,所以

$$6x^3+27x^2+17x+24\equiv 0 \pmod{2};$$

$$6x^3+27x^2+17x+24\equiv 0 \pmod{3};$$

$$6x^3+27x^2+17x+24\equiv 0 \pmod{5}.$$

也成立.

解上述同余式,我们有$x\equiv 0 \pmod{3}; x\equiv 3 \pmod{5}$. 所以我们可以得出$x\equiv 3 \pmod{15}$为这个同余式的所有解.

(ii).解法与(i)类似,结果为$x\equiv 45 \pmod{231}$或$x\equiv 12 \pmod{231}$或$x\equiv 111 \pmod{231}$.

(22)找到线性同余式系统的所有解：

$2x+3y\equiv 5 \pmod{7}, x+5y\equiv 6 \pmod{7}$.

解 注意到这两个同余式在模7的意义下是一样的,所以只需求第一个式子的所有解就可以了.

让x跑遍模7的剩余类,所有解为$(0,4),(1,1),(2,5),(3,2),(4,6),(5,3),(6,0)$.

(24)下列线性同余式多少个不同余的解？

$2x+y+z\equiv 1\pmod 5, x+2y+z\equiv 1\pmod 5, x+y+2z\equiv 1\pmod 5.$

解 原式等于在5元有限域上求解如下方程

$$\begin{pmatrix}2&1&1\\1&2&1\\1&1&2\end{pmatrix}x=\begin{pmatrix}1\\1\\1\end{pmatrix}$$

由于在矩阵的行列式在5元有限域上不为零,所以方程有唯一解.

该解为$(4,4,4)$.

(25)找到7^{51}除以144的余数.

解 $\varphi(144)=48$,所以$7^{51}\equiv 7^3\equiv 55\pmod 1)44$.

(26)证明如果$n\geq 2$,则2^n-1不被n整除.

证明 反证法：假设存在$n\geq 2$, $n\mid 2^n-1$, 显然n不为偶数, 以下均假设n为奇数. 设$p\geq 3$为n最小的素因子.由费马小定理$2^{p-1}\equiv 1\pmod p$, 而$n\mid 2^n-1$, 所以$2^n\equiv 1\pmod p$. 而2模p的阶为$p-1$的因子,$2^n\equiv 1\pmod p$,这表明$p-1\mid n$, 但p已经是n最小的素因子,所以必然$p-1\nmid n$.故2^n-1不被n整除. □

(28)令p为奇素数.则由费马小定理,如果$(a,p)=1$,则$f_p(a)=\frac{a^{p-1}-1}{p}\in\mathbb{Z}$.证明如果$(ab,p)=1$,则$f_p(ab)\equiv f_p(a)+f_p(b)\pmod p$.

证明 $f_p(ab)=\frac{(ab)^{p-1}-1}{p}=\frac{(ab)^{p-1}-a^{p-1}+a^{p-1}-1}{p}=\frac{a^{p-1}(b^{p-1}-1)}{p}+\frac{a^{p-1}}{p}$. 注意到$\frac{a^{p-1}(b^{p-1}-1)}{p}\equiv\frac{b^{p-1}-1}{p}\pmod p$,所以我们有$f_p(ab)\equiv f_p(a)+f_p(b)\pmod p$. □

(30)证明6601是一个Carmichael数.

证明 $6601=7\times 23\times 41$.因为$6\mid 6600, 22\mid 6600, 40\mid 6600$由书上定理知6601为Carmichael 数. □

(32)找出下面线性同余式组的解：

1.$x+2y-23\equiv 0\pmod{209}, 4x-7y+88\equiv 0\pmod{209}$.

2.$x+4y-29\equiv 0\pmod{143}, 2x-9y+84\equiv 0\pmod{143}$.

解 利用Guass消元法可以解出结果为

1.$(x,y)\equiv(208,12)\pmod{209}$ 2.$(x,y)\equiv(4,42)\pmod{143}$

(34)证明对任意的整数x和y,$3x+2y \equiv 0 \pmod{17}$当且仅当$10x+y \equiv 0 \pmod{17}$.

证明 $\gcd(9,17)=1$,所以$(3x+2y)9 \equiv 27x+18y \equiv 10x+y \pmod{17}$. 所以$3x+2y \equiv 0 \pmod{17}$当且仅当$10x+y \equiv 0 \pmod{17}$. □

(35)令a和b为整数,p为一个奇素数.证明$a^p+b^p \equiv 0 \pmod{p}$,则$a^p+b^p \equiv 0 \pmod{p^2}$.

证明 首先$a^p \equiv a \pmod{p}$, $b^p \equiv b \pmod{p}$.所以$a^p+b^p \equiv a+b \equiv 0 \pmod{p}$.由第一章习题43.$\frac{a^p+b^p}{a+b} \equiv 0 \pmod{p}$.即$a^p+b^p \equiv 0 \pmod{p^2}$. □

(36)证明$(m-1)! \equiv 0 \pmod{m}$对任意的合数$m \neq 4$.

证明 考虑m的任何一个非平凡因子d,令d'为它的共轭因子.若$d \neq d'$, 那么$d, d' \in \{1,2,\cdots,m-1\}$,所以$(m-1)! \equiv 0 \pmod{m}$. 若$d=d'$,所以$m=d^2$,由于$m \neq 4$,所以$d \neq 2$,所以$d, 2d \in \{1,2,\cdots,m-1\}$,所以$(m-1)! = d^2K \equiv 0 \pmod{d}^2$. □

(38)证明$61!+1 \equiv 0 \pmod{71}$.

证明 注意到$(-1)\cdot(-2)\cdots(-9) \equiv 1 \pmod{71}$,再由Wilson定理,$70! \equiv -1 \pmod{71}$,故有$61!+1 \equiv 0 \pmod{71}$. □

(40)令p为一个奇素数并且$l=\frac{p-1}{2}$.证明$(l!)^2+(-1)^l \equiv 0 \pmod{p}$.

证明 因为

$$(l+1)(l+2)\cdots 2l \equiv -(p-(l+1))-(p-(l+2))\cdots-(p-(2l)) \equiv (-1)^l! \pmod{p}.$$

所以$(-1)^l(l!)^2 \equiv (p-1)! \equiv -1 \pmod{p}$. 从而$(l!)^2+(-1)^l \equiv 0 \pmod{p}$. □

(42)令p为一个素数且m为一个大于等于1的整数,证明下列式子成立：

1.$\binom{m}{p} \equiv [\frac{m}{p}] \pmod{p}$; 2.如果整数$l>0$且$p^l \mid [\frac{m}{p}]$,则$p^l \mid \binom{m}{p}$.

证明 1.由Lucas同余式立得. 2.$p^l \mid [\frac{m}{p}]$,所以$m=a_0+a_1p^{l+1}+\cdots+a_kp^{l+k}$,再由$\binom{m}{p}=\frac{(m-1)(m-2)(m-p+1)}{(p-1)!}$立得待证结论. □

(44)设$f(x) \in \mathbb{Z}[x]$ 且$m>0$, s和t为满足$s \equiv t \pmod{m}$的整数.证明$f(s) \equiv f(t) \pmod{m}$.

证明 只需证明$s^k \equiv t^k \pmod{m}$即可,其中k为任意给定的正整数.

注意到$s^k - t^k = (s-t)(s^{k-1} + ts^{k-2} + \cdots + t^{k-2}s + t^{k-1})$,所以由$s \equiv t \pmod m$, 我们可知$s^k \equiv t^k \pmod m$. □

(46)找到最小的整数x,使得$\frac{x}{2}$为一个平方数,$\frac{x}{3}$为一个立方数,$\frac{x}{5}$为一个数的5次方.

解 设$x = 2^{e_1}3^{e_2}5^{e_3}$,由题设

$$e_1 \equiv 1 \pmod 2; e_1 \equiv 0 \pmod 3; e_1 \equiv 0 \pmod 5;$$

$$e_2 \equiv 0 \pmod 2; e_2 \equiv 1 \pmod 3; e_2 \equiv 0 \pmod 5;$$

$$e_3 \equiv 0 \pmod 2; e_3 \equiv 0 \pmod 3; e_3 \equiv 1 \pmod 5;$$

解得$e_1 = 15; e_2 = 10; e_3 = 6$,所以$x = 2^{15}3^{10}5^6$;

(48)设p为一个素数,$p \geq 5$,并且若$1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{p} = \frac{r}{ps}$.证明$p^3 \mid (r-s)$.

证明 首先$1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{p-1} = \frac{r}{ps} - \frac{1}{p}$,所以$\frac{r-s}{ps} = \sum\limits_{k=1}^{p-1} \frac{1}{k}$.于是$\frac{r-s}{ps}(p-1)! = \sum\limits_{k=1}^{p-1} \frac{(p-1)!}{k}$.由Wolstenholme定理可知$\frac{r-s}{ps}(p-1)! = Kp^2$,注意到$\frac{r-s}{ps}(p-1)!$的分子被$p^3$整除,而$p \nmid (p-1)!$,所以$p^3 \mid (r-s)$. □

(49)令a, b以及x_0为正整数,且对所有的$n = 1, 2, \cdots$定义$x_n = ax_n - 1 + b$,证明不可能所有的x_n都是素数.

证明

先证明一个引理,设p为一个奇素数,a和p互素,则

$$\begin{cases} 1 + a + \cdots + a^{p-2} \equiv 0 \pmod p & a \not\equiv 1 \pmod p \\ 1 + a + \cdots + a^{p-2} + a^{p-1} \equiv 0 \pmod p & a \equiv 1 \pmod p \end{cases}$$

$a \equiv 1 \pmod p$的情况是显然的,下面证明$a \not\equiv 1 \pmod p$的情形.令$S = 1 + a + \cdots + a^{p-2}$,因为$a^{p-1} \equiv 1 \pmod p$ 则$aS \equiv S \pmod p$,又$a \not\equiv 1 \pmod p$,所以只能$S \equiv 0 \pmod p$.

下面选取一个$x_k = q$,q为一个奇素数且与a互素.从而$x_{k+1} \equiv b \pmod q$,由归纳法可证$x_{k+i} \equiv (a^{i-1} + a^{i-2} + \cdots + 1)b \pmod q$.

当$a \equiv 1 \pmod q$时,取$i = q$,则$x_{k+q} \equiv 0 \pmod q$,所以x_{k+q}不为素数.

当$a \not\equiv 1 \pmod q$ 时,取$i = q-1$,则$x_{k+q-1} \equiv 0 \pmod q$,所以$x_{k+q-1}$不为素数. □

(50)令a, b, n为正整数,且满足n整除$a^n - b^n$.证明n也整除$\frac{a^n-b^n}{a-b}$.

证明 设$p \mid n$,我们设$v_p(n) = r$,从而$p^r \parallel n$.我们证明对任意的p,$p^r \mid \frac{a^n-b^n}{a-b}$.令$a - b = t$

情形一:$p \nmid t$,由于$p^r \parallel n$,从而$p^r \mid t\frac{a^n-b^n}{t}$从而$p^r \mid \frac{a^n-b^n}{t}$.

情形二:$p \mid t$,这时我们考虑二项式展开$\frac{a^n-b^n}{t} = \sum_{i=1}^{n} \binom{n}{i} b^{n-i}t^{i-1}$. 我们计算每个单项的$p$进制赋值.

$v_p(\binom{n}{i}b^{n-i}t^{i-1}) \geq i - 1 + v_p(\binom{n}{i})$.而$\binom{n}{i} = \frac{n}{i}\binom{n-1}{i-1}$. 所以

$$v_p(\binom{n}{i}b^{n-i}t^{i-1}) \geq v_p(n) - v_p(i) + i - 1 = m - v_p(i) + i - 1.$$

注意到对任意的p,$i \geq v_p(i) + 1$.所以$v_p(\binom{n}{i}b^{n-i}t^{i-1}) \geq m$.故$p^r \parallel \frac{a^n-b^n}{t}$. 注意到这对所有的整除$n$的素因子都成立,所以$n$也整除$\frac{a^n-b^n}{a-b}$. □

(52)令n为一个大于1的奇数.证明集合$\{2-1, 2^2-1, 2^3-1, \cdots, 2^{n-1}-1\}$中至少有一个元素可以被$n$整除.

证明 由于n为奇数,所以$(2, n) = 1$,故$\{2, 2^2, \cdots, 2^{\varphi(n)}\}$构成模$n$的一个缩系.

而$\{2, 2^2, \cdots, 2^{\varphi(n)}\} \subset \{2, 2^2, 2^3, \cdots, 2^{n-1}\}$,所以存在$k$,使得$2^k \equiv 1 \pmod n$.

即集合$\{2-1, 2^2-1, 2^3-1, \cdots, 2^{n-1}-1\}$中至少有一个元素可以被$n$整除. □

(54)找到最小的整数n,使得$\frac{n}{2}$为一个平方数,$\frac{n}{3}$为一个立方数,$\frac{n}{5}$为一个数的5次方.

解 设$n = 2^{e_1}3^{e_2}5^{e_3}$,由题设

$$e_1 \equiv 1 \pmod 2; e_1 \equiv 0 \pmod 3; e_1 \equiv 0 \pmod 5;$$

$$e_2 \equiv 0 \pmod 2; e_2 \equiv 1 \pmod 3; e_2 \equiv 0 \pmod 5;$$

$$e_3 \equiv 0 \pmod 2; e_3 \equiv 0 \pmod 3; e_3 \equiv 1 \pmod 5;$$

解得$e_1 = 15; e_2 = 10; e_3 = 6$,所以$n = 2^{15}3^{10}5^6$;

(56)令p为一个素数,k为一个满足$0 \leq k \leq p-1$的整数.证明同余式$\frac{(kp)!}{k!p^k} \equiv (-1)^k \pmod{p}$成立.

证明 首先$\frac{(kp)!}{k!p^k} = (p-1)!(p+1)\cdots(2p-1)\cdots(tp+1)\cdots(tp+p-1)\cdots(kp-p+1)\cdots(kp+p-1)$. 注意到$(tp+1)\cdots(tp+p-1) \equiv (p-1)! \equiv -1 \pmod{p}$,从而同余式$\frac{(kp)!}{k!p^k} \equiv (-1)^k \pmod{p}$成立.

□

(58)令p为$F_m = 2^{2^m}+1$.证明$p^2 \mid F_m$当且仅当$2^{p-1} \equiv 1 \pmod{p^2}$.

证明 充分性:因为$p^2 \mid F_m$.所以$2^{2^m} \equiv -1 \pmod{p^2}$.又因为$F_m(F_m-2) = 2^{2^{m+1}}-1$. 所以$2^{2^{m+1}} \equiv 1 \pmod{p}$. 对比$2^{2^m} \equiv -1 \pmod{p^2}$,$2^{2^{m+1}} \equiv 1 \pmod{p}$. 两式,我们断言$2^{m+1}$为使得$2^n \equiv 1 \pmod{p}$成立的最小的$n$.

若存在$n_0 < 2^{m+1}$,那么$n_0 \mid 2^{m+1}$,所以n_0是2的方幂,但是$2^{2^m} \equiv -1 \pmod{p}$. 从而这样的$n_0$不可能存在.故$2^{m+1}$为使得$2^n \equiv 1 \pmod{p}$成立的最小的$n$. 由费马小定理$2^{p-1} \equiv 1 \pmod{p}$,所以$2^{m+1} \mid p-1$但因为$p^2 \mid F_m$,所以$2^{2^{m+1}} \equiv 1 \pmod{p^2}$,自然就有$2^{p-1} \equiv 1 \pmod{p^2}$.

必要性：令$2^{2^{m+1}} = u$,由充分性的讨论,我们知道$p-1 = k2^{m+1}$.故而$2^{p-1} \equiv 1 \pmod{p^2}$ 从而$p^2 \mid u^k - 1$.注意到$u \equiv 1 \pmod{p}$,所以$u^{k-1}+u^{k-2}+\cdots+u+1 \equiv k \pmod{p}$.因为$k<p$,所以这表明$p \nmid u^{k-1}+u^{k-2}+\cdots+u+1$,所以$p^2 \mid u-1$.又显然$p^2 \nmid 2^{2^m}-1$,于是$p^2 \mid F_m$.

□

(59)证明存在无穷多个整数$k \geq 1$,使得序列中$\{k2^n+1\}_{n=1}^{\infty}$中没有复合数.

证明 先把正整数进行如下划分$\mathbb{Z}_+ = (2\mathbb{Z}_{\geq 0}+1)\bigcup(4\mathbb{Z}_{\geq 0}+2)\bigcup(8\mathbb{Z}_{\geq 0}+4)\bigcup(16\mathbb{Z}_{\geq 0}+8)\bigcup(32\mathbb{Z}_{\geq 0}+16)\bigcup(64\mathbb{Z}_{\geq 0}+32)\bigcup(64\mathbb{Z}_{\geq 0})$

其中$a\mathbb{Z}_{\geq 0}+b = \{az+b|z \geq 0\}$.$\mathbb{Z}_+$表示所有正整数. 从而上述划分是成立的.

对任意的$n \in (2\mathbb{Z}_{\geq 0}+1)$,若$k_0 \equiv 1 \pmod{3}$,则$k \cdot 2^n + 1 \equiv 2k_0+1 \equiv 0 \pmod{3}$.

对任意的$n \in (4\mathbb{Z}_{\geq 0}+2)$,若$k_0 \equiv 1 \pmod{5}$,则$k \cdot 2^n + 1 \equiv 4k_0+1 \equiv 0 \pmod{5}$.

对任意的$n \in (8\mathbb{Z}_{\geq 0}+4)$,若$k_0 \equiv 1 \pmod{17}$,则$k \cdot 2^n + 1 \equiv 8k_0 + 1 \equiv 0 \pmod{17}$.

对任意的$n \in (16\mathbb{Z}_{\geq 0}+8)$,若$k_0 \equiv 1 \pmod{257}$,则$k \cdot 2^n + 1 \equiv 256k_0 + 1 \equiv 0 \pmod{257}$.

对任意的$n \in (32\mathbb{Z}_{\geq 0}+16)$,若$k_0 \equiv 1 \pmod{65537}$,则$k \cdot 2^n + 1 \equiv 65536k_0 + 1 \equiv 0 \pmod{65537}$.

对任意的$n \in (64\mathbb{Z}_{\geq 0}+32)$,若$k_0 \equiv 1 \pmod{641}$,则$k \cdot 2^n + 1 \equiv 640k_0 + 1 \equiv 0 \pmod{641}$.

对任意的$n \in (64\mathbb{Z}_{\geq 0})$,若$k_0 \equiv 1 \pmod{6700417}$,则$k \cdot 2^n + 1 \equiv -k_0 + 1 \equiv 0 \pmod{6700417}$.

由中国剩余定理在模$3 \cdot 5 \cdot 17 \cdot 257 \cdot 65537 \cdot 641 \cdot 6700417$意义下这样的正整数$k_0$ 有无限多个.再由刚才对$\mathbb{Z}$划分,我们可知序列$\{k2^n + 1\}_{n=1}^{\infty}$中没有复合数.

□

(60)令$k \geq 1$为任意给定整数.证明存在无穷多整数对(m, n),其中$m > 1$且$n > 1$,使得$n \mid m$且$n^k \mid \varphi(m)$.

证明　任取素数p,令$n = p^a$,令$m = p^{ak+1}$,显然$n \mid m$.另一方面$\varphi(m) = (p-1)p^{ak}$,从而$n^k \mid \varphi(m)$.令a跑遍所有正整数,这样我们就构造出无穷多对整数(n, m).
□

第三章　算术函数及其均值

(1).对所有整数 n ,用 $1(n)=1$ 定义算术函数 $1(n)$.证明 $(1*1)(n)=d(n)$.

证明 由定义 $d(n)=\sum_{d|n}1=(1*1)(n)$. □

(3).令 $\mathcal{A}$ 为复值函数所定义的算术函数构成的环.一个算术函数 f 称为环 $\mathcal{A}$ 的一个单位如果存在一个算术函数 g 使得 $f*g=\delta$.证明$f\in\mathcal{A}$ 是一个单位当且仅当$f(1)\neq 0$.

证明 充分性: 由 f 为一个单位,则存在 g ,使得 $f*g=\delta$,特别的 $f(1)g(1)=1$,从而必有 $f(1)\neq 0$.

必要性: $f(1)\neq 0$,令 $f(1)=a$,则 $g(1)=\frac{1}{a}$,对固定的 n ,不妨设对所有的小于 n 的因子 d 处的值已经给定.定义

$$g(n)=-\frac{1}{f(1)}(-\sum_{\substack{d|n\\ d\neq n}}f(d)g(\frac{n}{d}))$$

直接验算有 $f*g=\delta$,所以 $f\in\mathcal{A}$ 为一个单位. □

(5).对算术函数 f 和 g ,定义 $f\star g$ 为

$$(f\star g)(n)=\sum_{k=1}^{n-1}f(k)g(n-k).$$

这个乘积交换吗?时可结合的吗? $f\star\delta$ 是什么?

证明 交换性容易验证.

下面验证结合性:

$$\begin{aligned}
f\star g\star h(n)&=\sum_{2\leq n\leq k-1}(f\star g)(k)h(n-k)=\sum_{\substack{k+m=n\\ k\geq 2,m\geq 1}}(f\star g)(k)h(m)\\
&=\sum_{\substack{k+m=n\\ k\geq 2,m\geq 1}}\sum_{\substack{d+l=k\\ d\geq 1,l\geq 1}}f(d)g(l)h(m)=\sum_{\substack{d+l+m=n\\ d\geq 1,l\geq 1,m\geq 1}}f(d)g(l)h(m)\\
&=\sum_{\substack{d+s=n\\ d\geq 1,s\geq 2}}f(d)\sum_{\substack{l+m=s\\ l\geq 1,m\geq 1}}g(l)h(m)=\sum_{\substack{d+s=n\\ s\geq 2,d\geq 1}}f(d)(g\star h)(s)\\
&=f\star(g\star h)(n)
\end{aligned}$$

由定义,$f \star \delta = f(n-1)$. □

(7).对$0 < a < 1$, let $\gamma(a) = \frac{a}{1-a} + a\int_1^\infty \frac{\{t\}}{t^{a+1}}dt$.证明

$$\sum_{n\le x} \frac{1}{n^a} = \frac{x^{1-a}}{1-a} - \gamma(a) + O\left(x^{-a}\right).$$

证明 令 $f(1) = 1$, $g(n) = \frac{1}{n^a}$,则 $F[x] = \sum\limits_{n\le x} f(n) = [x]$. 利用部分求和公式

$$\begin{aligned}
\sum_{n\le x} \frac{1}{n^a} &= \frac{[x]}{x^a} + \int_1^x \frac{a[t]}{t^{1+a}}dt \\
&= \frac{x}{x^a} - \frac{\{x\}}{x^a} + \int_1^x \frac{at}{t^{1+a}}dt - \int_1^x \frac{a\{t\}}{t^{1+a}}dt \\
&= \frac{1}{x^{1-a}} + a\int_1^x \frac{1}{t^a}dt + \int_x^{+\infty} \frac{a\{t\}}{t^{1+a}}dt - \int_1^{+\infty} \frac{a\{t\}}{t^{1+a}}dt \\
&= \frac{x^{1-a}}{1-a} - \gamma(a) + \int_x^{+\infty} \frac{a\{t\}}{t^{1+a}}dt
\end{aligned}$$

注意到$\{t\} \le 1$,所以简单计算有$\int_x^{+\infty} \frac{a\{t\}}{t^{1+a}}dt = O(x^{-a})$. 这就完成了证明. □

(9).令 $1 \le a < b$ 和 $k \ge 2$ 为整数.证明

$$\sum_{n=a}^{b} \frac{1}{n^k} = \frac{-1}{k-1}\left(\frac{1}{b^{k-1}} - \frac{1}{a^{k-1}}\right) + O\left(\frac{1}{a^k}\right).$$

证明 利用(7)的结论,我们有

$$\sum_{n\le b} \frac{1}{n^k} = \frac{b^{1-k}}{1-k} - \gamma(k) + O\left(b^{-k}\right).$$

$$\sum_{n\le a} \frac{1}{n^k} = \frac{a^{1-k}}{1-k} - \gamma(k) + O\left(a^{-k}\right).$$

上面两式相减即有

$$\sum_{n=a}^{b} \frac{-1}{n^k} = \frac{1}{k-1}\left(\frac{1}{b^{k-1}} - \frac{1}{a^{k-1}}\right) + O\left(\frac{1}{a^k}\right).$$

对于误差项,只需注意到 $1 \le a < b$,所以$b^{-k} < a^{-k}$. □

(11).令 $d(n)$ 为除数函数.对每个正整数,我们有$\sum\limits_{k|n} d(k)\mu\left(\frac{n}{k}\right)=1$

证明 注意到 $d(n)=1*1(n)$,所以 $d*\mu(n)=1*1*\mu(n)=1*\delta(n)=1(n)$. □

(13).令 f 为一个乘性函数.证明如果 $f(1)=0$,则 f 恒等于 0 ,即对所有的 n ,都有 $f(n)=0$.证明如果 f 不是恒等于 0 ,则 $f(1)=1$.

证明 对所有的 n ,因为$(1,n)=1$,所以 $f(n)=f(1)f(n)=0$.

因为 $f(1)=f(1)f(1)$,又因为 f 不恒为 0 ,从而必有 $f(1)=1$. □

(15).令 $\sigma(n)$ 为 n 的所有正因子之和,即是,$\sigma(n)=\sum\limits_{d|n} d$.证明对所有正整数 n ,我们有$\sum\limits_{d|n}\sigma(d)\mu(n/d)=n.$

证明 令 $I(n)=n$,从而 $\sigma(n)=I(n)*1$,所以$\sum\limits_{d|n}\sigma(d)\mu(n/d)=I*1*\mu=I(n)=n.$ □

(16).证明对每个$\delta>0$,我们有 $\lim\limits_{n\to\infty}\frac{\varphi(n)}{n^{1-\delta}}=\infty.$

证明 令 $g(n)=\frac{n^{1-\delta}}{\varphi(n)}$, $f(n)=\frac{1}{g(n)}$. 不难验证, $g(n)$ 和 $f(n)$ 都是乘性函数.

考虑 $g(n)$ 在素数幂处的取值,则

$$g(p^k)=\frac{p^{k(1-\delta)}}{\varphi(p^k)}=\frac{p^k}{p^k(1-\frac{1}{p})p^{k\delta}}=\frac{1}{(1-\frac{1}{p})p^{k\delta}}$$

由于$1-\frac{1}{p}\geq\frac{1}{2}$,所以$g(p^k)\leq\frac{2}{p^{k\delta}}$.但是显然$g(n)>0$对所有 n 均成立.所以

$$\lim_{p^k\to\infty} g(p^k)=0.$$

由定理3.3.3可知, $\lim\limits_{n\to\infty} g(n)=0.$ 从而

$$\lim_{n\to\infty}\frac{\varphi(n)}{n^{1-\delta}}=f(n)=\frac{1}{g(n)}=\infty.$$

□

(17).证明

$$\prod_{p|n}\left(1-\frac{1}{p^2}\right)\geq\prod_{k=2}^{n}\left(1-\frac{1}{k^2}\right)>\frac{1}{2}.$$

证明 对任意的 $l \geq 1$,显然 $1-\frac{1}{l^2}<1$.从而

$$\prod_{k=2}^{n}\left(1-\frac{1}{k^2}\right) \leq \prod_{d|n}\left(1-\frac{1}{d^2}\right) \leq \prod_{p|n}\left(1-\frac{1}{p^2}\right)$$

注意到

$$\prod_{k=2}^{n}\left(1-\frac{1}{k^2}\right)=\frac{1}{2}\cdot\frac{2}{3}\cdot\frac{3}{2}\cdots\frac{n-1}{n}\cdot\frac{n+1}{n}=\frac{1}{2}\cdot\frac{n+1}{n}>\frac{1}{2}$$

□

(18).证明 $\frac{1}{2}<\frac{\varphi(n)\sigma(n)}{n^2}<1$

证明 首先注意到 $\varphi(n),\sigma(n),n^2$都是乘性函数.所以先考察$\frac{\varphi(n)\sigma(n)}{n^2}$在素数幂处的取值.

对任意素数幂 p^k ,我们有

$$\frac{\varphi(p^k)\sigma(p^k)}{p^{2k}}=\frac{(p-1)p^{k-1}\cdot\frac{p^{k+1}}{p-1}}{p^{2k}}=1-\frac{1}{p^{2k}}$$

故而由乘性,我们知道对任意的 n ,$\frac{\varphi(n)\sigma(n)}{n^2}<1$.

另一方面$\prod_{p|n}\left(1-\frac{1}{p^{2k}}\right)>\prod_{p|n}\left(1-\frac{1}{p^2}\right)$, 由17 题的结论,我们有 $\frac{\varphi(n)\sigma(n)}{n^2}>\frac{1}{2}$. 这就完成了证明. □

(19).证明对任意的 $\delta>0$, $n>1$,我们有$n<\sigma(n)\ll n^{1+\delta}$.

证明 由定义$\sigma(n)=\sum_{d|n}d$,显然 1 和 n 都是 n 的因子,所以自然有 $\sigma(n)\geq 1+n>n$. 令 $f(n)=\frac{\sigma(n)}{n^{1+\delta}}$.

由18题可知.$\frac{\varphi(n)\delta(n)}{n^2}<1$. 故 $f(n)<\frac{n^{1-\delta}}{\varphi(n)}$,又由16题可知：$\lim_{n\to\infty}\frac{n^{1-\delta}}{\varphi(n)}=0$. 所以$\lim_{n\to\infty}f(n)\leq 0$.另一方面, $f(n)\geq 0$,故$\lim_{n\to\infty}f(n)=0$.

从而对任意的 n ,$f(n)$是有界量,综上,我们有$n<\sigma(n)\ll n^{1+\delta}$. □

(21).证明$\limsup_{n\to\infty}\frac{\varphi(n)}{n}=1$.

证明 首先对任意的整数 n ,由 $\varphi(n)$ 的定义,我们有 $n<\varphi(n)$.又因为对于素数 p ,我们有 $\varphi(p)=p-1$,所以在自然数序列中,我们取子列 $\{p_n\}_{n=1}^{\infty}$,其中 p_n 代表第 n 个素数. 从而$\limsup_{n\to\infty}\frac{\varphi(n)}{n}=\lim_{n\to\infty}\frac{p_n-1}{p_n}=1$ □

(22).(Smith's 行列式,1875)令 f 为一个算术函数并且 $(f(\gcd(i,j)))$ 表示一个$n\times n$阶矩阵,其中i行,j列元素为 f 在$\gcd(i.j)$处的取值,其中$1\leq i,j\leq n$.证明$\det(f(\gcd(i,j)))=\prod\limits_{k=1}^{n}(f*\mu)(k)$.

证明 令$C_n=(c_{ij})_{n\times n}$,其中 $c_{ij}=\begin{cases}1, & j\mid i\\ 0, & j\nmid i\end{cases}$.

$B_n=\operatorname{diag}(f*\mu(1),\ldots,f*\mu(n))$.

设 $A=C_nB_nC_n^T$,则

$$\begin{aligned}a_{ij}&=\sum_{k=1}^{n}c_{ik}f*\mu(k)c_{jk}=\sum_{k|i,k|j}f*\mu(k)\\&=\sum_{k|\gcd(i,j)}f*\mu(k)=f*\mu*1(\gcd(i.j))\\&=f(\gcd(i,j))\end{aligned}$$

所以$A=(f(\gcd(i,j)))$,从而

$$\det(f(\gcd(i,j)))=\det(B_n)\det(C_n)^2=\prod_{k=1}^{n}(f*\mu)(k).$$

□

(23).(Smith's 行列式,1875)令 f 为一个乘性的算术函数并且 $(f(\operatorname{lcm}(i,j)))$ 表示一个$n\times n$阶矩阵,其中i行,j列元素为 f 在$\operatorname{lcm}(i.j)$处的取值,其中$1\leq i,j\leq n$.证明$\det(f(\operatorname{lcm}(i,j)))=\prod\limits_{k=1}^{n}f^2(k)\left(\frac{1}{f}*\mu\right)(k)$.

证明 注意到 f 是乘性的,所以我们有 $f(\operatorname{lcm}(i,j))=\frac{f(i)f(j)}{f(\gcd(i,j))}$.

令$C_n=(c_{ij})_{n\times n}$,其中 $c_{ij}=\begin{cases}f(i), & j\mid i\\ 0, & j\nmid i\end{cases}$.

$B_n=\operatorname{diag}(\frac{1}{f}*\mu(1),\ldots,\frac{1}{f}*\mu(n))$.

设 $A=C_nB_nC_n^T$,则

$$\begin{aligned}a_{ij}&=\sum_{k=1}^{n}c_{ik}f*\mu(k)c_{jk}=f(i)f(j)\sum_{k|i,k|j}\frac{1}{f}*\mu(k)\\&=f(i)f(j)\sum_{k|\gcd(i,j)}\frac{1}{f}*\mu(k)=f(i)f(j)\frac{1}{f}*\mu*1(\gcd(i.j))\\&=f(i)f(j)\frac{1}{f}(\gcd(i,j))=f(\mathrm{lcm}(i,j))\end{aligned}$$

所以$A=(f(\mathrm{lcm}(i,j)))$,从而

$$\det(f(\mathrm{lcm}(i,j)))=\det(B_n)\det(C_n)^2=\prod_{k=1}^{n}f^2(k)\left(\frac{1}{f}*\mu\right)(k).$$

□

(25).定义算术函数$\tilde{\mu}$为如下:

$$\tilde{\mu}(n)=\begin{cases}\mu(\sqrt{n}), & \text{如果}n\text{ 为一个平方数;}\\0, & \text{其它情形.}\end{cases}$$

证明$\tilde{\mu}$为乘性函数.

证明 这是(27)题的特殊情形. □

(27).令 $d\geq 1$ 为一个整数.定义算术函数$\tilde{\mu}_d$为如下:

$$\tilde{\mu}_d(n)=\begin{cases}\mu(\sqrt[d]{n}), & \text{如果}n\text{ 为一个}d\text{次方;}\\0, & \text{其它情形.}\end{cases}$$

证明$\mu(\sqrt[d]{n})$为乘性函数.

证明 取 m,n 互素,若 mn 为 d 次方,由 m,n 互素,那么我们可以推出 m 和 n 均为 d 次方,所以在这种情形下.不妨设 $m=a^d,n=b^d$ 我们有

$$\tilde{\mu}_d(mn)=\mu(\sqrt[d]{mn})=\mu(ab)=\mu(a)\mu(b)=\tilde{\mu}_d(n)\tilde{\mu}_d(m)$$

若 mn 不为 d 次方,则 m 和 n 中至少由一个不为 d 次方,此时也有

$$\tilde{\mu}_d(mn)=\tilde{\mu}_d(n)\tilde{\mu}_d(m)$$

所以它是乘性函数. □

(29).令 f 为一个算术函数并且 r 为一个给定的实数.对任意的正整数 n 定义算术函数 f^r 为$f^r(n) := f(n)^r$.证明如果 f 是乘性的,则 f^r 也是乘性的.

证明 对任意的 $(m,n) = 1$,若 f 是乘性的,则 $f(mn) = f(m)f(n)$,所以 $f^r(m)f^r(n) = f(m)^r f(n)^r = [f(m)f(n)]^r = f(mn)^r = f^r(mn)$. 从而 f^r 也是乘性的. □

(31).令$f(x) = x - [x] - \frac{1}{2}$.证明如下等式成立:

(i). $\sum_{k=0}^{n-1} f\left(x + \frac{k}{n}\right) = f(nx)$.

(ii). 如果 $m \geq 1$ 为一个整数并且 x 为一个实数,则$\left|\sum_{n=1}^{m} f\left(2^n x + \frac{1}{2}\right)\right| \leq 1$.

证明 (i)首先

$$\begin{aligned}\sum_{k=0}^{n-1} f\left(x + \frac{k}{n}\right) &= \sum_{k=0}^{n-1}\left(x + \frac{k}{n}\right) - \left[x + \frac{k}{n}\right] - \frac{1}{2} \\ &= nx + \frac{n-1}{2} - \sum_{k=0}^{n-1}\left[x + \frac{k}{n}\right] - \frac{n}{2} \\ &= nx - \sum_{k=0}^{n-1}\left[x + \frac{k}{n}\right] - \frac{1}{2}\end{aligned}$$

不妨设$[x] + \frac{i}{n} \leq x < [x] + \frac{i+1}{n}$,其中$0 \leq i \leq n-1$. 所以我们有$n[x] + i \leq nx < n[x] + i + 1$,即$[nx] = n[x] + i$

另一方面,我们有$[x] + \frac{i+k}{n} \leq x + \frac{k}{n} < [x] + \frac{i+k+1}{n}$,所以当 $k \geq n - i$ 时,均有$\left[x + \frac{k}{n}\right] = [x]+1$.即是$\sum_{k=0}^{n-1}\left[x + \frac{k}{n}\right] = n[x]+i$. 这就证明了$\sum_{k=0}^{n-1} f\left(x + \frac{k}{n}\right) = f(nx)$.

(ii).首先我们有$\left|\sum_{n=1}^{m} f\left(2x + \frac{1}{2}\right)\right| = \left|\sum_{n=1}^{m} 2x - \sum_{n=1}^{m}\left[2^n x + \frac{1}{2}\right]\right|$.

注意到$[nx] = [x] + \cdots + \left[x + \frac{n-1}{n}\right]$,将 $2^n x$ 带入这个式子,则我们有$[2^{n+1}x] = [2^{n+1}x] + \left[2^n x + \frac{1}{2}\right]$. 从而我们有$\sum_{n=1}^{m}\left[2^n x + \frac{1}{2}\right] = \sum_{n=1}^{m}[2^{n+1}x] - \sum_{n=1}^{m}[2x]$,带

入最开始的式子,我们有

$$\begin{aligned}&\left|\sum_{n=1}^{m}2x-\sum_{n=1}^{m}\left[2^nx+\frac{1}{2}\right]\right|\\=&\left|2^{m+1}x-2x-\left[2^{m+1}x\right]+[2x]\right|\\=&\left|\left(2^{m+1}x-\left[2^{m+1}x\right]\right)-(2x-[2x])\right|\\\leq&1\end{aligned}$$

其中最后一步是因为 a , b 如果满足$0\leq a<1$,$0\leq b<1$,那么$|a-b|\leq 1$以及$0\leq x-[x]<1$. □

(32).令 $a_1,a_2,\ldots,a_n$ 及 $b_1,b_2,\ldots,b_n$ 为任意 $2n$ 个正整数.证明如果对任意的$1\leq i_1<\ldots<i_t\leq n$,我们有$\gcd(a_{i_1},\ldots,a_{i_t})=\gcd(b_{i_1},\ldots,b_{i_t})$,则

$$\begin{aligned}&\frac{a_1a_2\cdots a_n}{\operatorname{lcm}(a_1,a_2,\ldots,a_n)}\cdot\prod_{r=2}^{t-1}\prod_{1\leq i_1<\ldots<i_r\leq n}\left(\gcd(a_{i_1},\ldots,a_{i_r})\right)^{(-1)^{r-1}}\\=&\frac{b_1b_2\cdots b_n}{\operatorname{lcm}(b_1,b_2,\ldots,b_n)}\cdot\prod_{r=2}^{t-1}\prod_{1\leq i_1<\ldots<i_r\leq n}\left(\gcd(b_{i_1},\ldots,b_{i_r})\right)^{(-1)^{r-1}}\end{aligned}$$

证明 先证明对任意的 k 满足 $t\leq k\leq n$,有$\gcd(a_{i_1},\ldots,a_{i_k})=\gcd(b_{i_1},\ldots,b_{i_k})$.

首先对固定的素数 p ,不妨设 $v_p(a_i)=r_i,v_p(b_i)=s_i$.由于对任意的$1\leq i_1<\ldots<i_t\leq n$,我们有$\gcd(a_{i_1},\ldots,a_{i_t})=\gcd(b_{i_1},\ldots,b_{i_t})$,所以由于对任意的$1\leq i_1<\ldots<i_t\leq n$, $\min\{r_{j_1},\ldots,r_{j_t}\}=\min\{s_{j_1},\ldots,s_{j_t}\}$.

从而$v_p(\gcd(a_{i_1},\ldots,a_{i_k}))=\min\limits_{1\leq i\leq k}\{r_{i_l}\}=\min\limits_{\substack{j_1<j_2<\ldots<j_t\\ j_1,\ldots,j_t\in\{i_1,i_2,\ldots,i_k\}}}\{r_{j_1},\ldots,r_{j_t}\}$.

由刚才的论证

$$\begin{aligned}&\min\limits_{\substack{j_1<j_2<\ldots<j_t\\ j_1,\ldots,j_t\in\{i_1,i_2,\ldots,i_k\}}}\{r_{j_1},\ldots,r_{j_t}\}\\=&\min\limits_{\substack{j_1<j_2<\ldots<j_t\\ j_1,\ldots,j_t\in\{i_1,i_2,\ldots,i_k\}}}\{s_{j_1},\ldots,s_{j_t}\}\\=&\min\limits_{1\leq i\leq k}\{s_{i_l}\}=v_p(\gcd(b_{i_1},\ldots,b_{i_k}))\end{aligned}$$

由于对任意素数 p 均成立,所以$\gcd(a_{i_1},\ldots,a_{i_k})=\gcd(b_{i_1},\ldots,b_{i_k})$.

再由定理3.6.4

$$\operatorname{lcm}(a_1,a_2,\ldots,a_n)=a_1a_2\ldots a_n\cdot\prod_{r=2}^{n}\prod_{1\le i_1<\ldots<i_r\le n}\left(\gcd(a_{i_1},\ldots,a_{i_r})\right)^{(-1)^{r-1}}$$

所以

$$\begin{aligned}&\frac{a_1a_2\cdots a_n}{\operatorname{lcm}(a_1,a_2,\ldots,a_n)}\cdot\prod_{r=2}^{t-1}\prod_{1\le i_1<\ldots<i_r\le n}\left(\gcd(a_{i_1},\ldots,a_{i_r})\right)^{(-1)^{r-1}}\\&=\prod_{r=t}^{n}\prod_{1\le i_1<\ldots<i_r\le n}\left(\gcd(a_{i_1},\ldots,a_{i_r})\right)^{(-1)^{r}}\\&=\prod_{r=t}^{n}\prod_{1\le i_1<\ldots<i_r\le n}\left(\gcd(b_{i_1},\ldots,b_{i_r})\right)^{(-1)^{r}}\\&=\frac{b_1b_2\cdots b_n}{\operatorname{lcm}(b_1,b_2,\ldots,b_n)}\cdot\prod_{r=2}^{t-1}\prod_{1\le i_1<\ldots<i_r\le n}\left(\gcd(b_{i_1},\ldots,b_{i_r})\right)^{(-1)^{r-1}}.\end{aligned}$$

这就完成了证明. □

(33).令 $a_1,a_2,\ldots,a_n$ 及 $b_1,b_2,\ldots,b_n$ 为任意 $2n$ 个正整数.证明如果对任意的$1\le i_1<i_2<i_3\le n$,我们有$\gcd(a_{i_1},a_{i_2},a_{i_3})=\gcd(b_{i_1},b_{i_2},b_{i_3})$,则

$$\frac{1}{\prod\limits_{1\le i<j\le n}\gcd(a_i,a_j)}\cdot\frac{a_1a_2\cdots a_n}{\operatorname{lcm}(a_1,a_2,\ldots,a_n)}=\frac{1}{\prod\limits_{1\le i<j\le n}\gcd(b_i,b_j)}\cdot\frac{b_1b_2\cdots b_n}{\operatorname{lcm}(b_1,b_2,\ldots,b_n)}.$$

证明 这是 32 题$t=3$的特殊情形. □

(34).令 $a_1,a_2,\ldots,a_n$ 及 $b_1,b_2,\ldots,b_n$ 为任意 $2n$ 个正整数.证明对任意的$1\le i<j\le n$,如果 $\gcd(a_i,a_j)=\gcd(b_i,b_j)$,则我们有

$$\frac{a_1a_2\cdots a_n}{\operatorname{lcm}(a_1,a_2,\ldots,a_n)}=\frac{b_1b_2\cdots b_n}{\operatorname{lcm}(b_1,b_2,\ldots,b_n)}$$

证明 由 32 题的证明中,可知对任意的$1\le i_1<i_2<i_3\le n$,

$$\gcd(a_{i_1},a_{i_2},a_{i_3})=\gcd(b_{i_1},b_{i_2},b_{i_3}),$$

利用 33 题的结论及任意的$1\le i<j\le n$,有 $\gcd(a_i,a_j)=\gcd(b_i,b_j)$ 立得待证式. □

(35). 令 $a_1, a_2, \ldots, a_n$ 及 $b_1, b_2, \ldots, b_n$ 为任意 $2n$ 个正整数.证明如果对任意的$1 \leq i_1 < \ldots < i_t \leq n$,我们有$\operatorname{lcm}(a_{i_1}, \ldots, a_{i_t}) = \operatorname{lcm}(b_{i_1}, \ldots, b_{i_t})$,则

$$\frac{a_1 a_2 \cdots a_n}{\gcd(a_1, a_2, \ldots, a_n)} \cdot \prod_{r=2}^{t-1} \prod_{1 \leq i_1 < \ldots < i_r \leq n} (\operatorname{lcm}(a_{i_1}, \ldots, a_{i_r}))^{(-1)^{r-1}}$$
$$= \frac{b_1 b_2 \cdots b_n}{\gcd(b_1, b_2, \ldots, b_n)} \cdot \prod_{r=2}^{t-1} \prod_{1 \leq i_1 < \ldots < i_r \leq n} (\operatorname{lcm}(b_{i_1}, \ldots, b_{i_r}))^{(-1)^{r-1}}$$

证明 与 32 题做法类似,运用定理3.6.6及

$$\max_{1 \leq i \leq k} \{r_{i_l}\} = \max \max_{\substack{j_1 < j_2 < \cdots < j_t \\ j_1, \ldots, j_t \in \{i_1, i_2, \ldots, i_k\}}} \{r_{j_1}, \ldots, r_{j_t}\}.$$

□

(36).令 $a_1, a_2, \ldots, a_n$ 及 $b_1, b_2, \ldots, b_n$ 为任意 $2n$ 个正整数.证明如果对任意的$1 \leq i_1 < i_2 < i_3 \leq n$,我们有$\operatorname{lcm}(a_{i_1}, a_{i_2}, a_{i_3}) = \operatorname{lcm}(b_{i_1}, b_{i_2}, b_{i_3})$,则

$$\frac{1}{\prod_{1 \leq i < j \leq n} \operatorname{lcm}(a_i, a_j)} \cdot \frac{a_1 a_2 \cdots a_n}{\gcd(a_1, a_2, \ldots, a_n)} = \frac{1}{\prod_{1 \leq i < j \leq n} \operatorname{lcm}(b_i, b_j)} \cdot \frac{b_1 b_2 \cdots b_n}{\gcd(b_1, b_2, \ldots, b_n)}.$$

证明 这是 35 题$t = 3$的特殊情形. □

(37).令 $a_1, a_2, \ldots, a_n$ 及 $b_1, b_2, \ldots, b_n$ 为任意 $2n$ 个正整数.证明对任意的$1 \leq i < j \leq n$,如果 $\operatorname{lcm}(a_i, a_j) = \operatorname{lcm}(b_i, b_j)$,则我们有

$$\frac{a_1 a_2 \cdots a_n}{\gcd(a_1, a_2, \ldots, a_n)} = \frac{b_1 b_2 \cdots b_n}{\gcd(b_1, b_2, \ldots, b_n)}$$

证明 与34题做法类似. □

(38).令$f(n) = [\sqrt{n}] - [\sqrt{n-1}]$为一个算术函数.证明 f 是乘性函数但不是完全乘性函数.

证明 这是40题的特殊情况. □

(39).令$f(n) = [\sqrt[3]{n}] - [\sqrt[3]{n-1}]$为一个算术函数.证明 f 是乘性函数但不是完全乘性函数.

证明 这是40题的特殊情况. □

(40).令$f(n)=[\sqrt[d]{n}]-[\sqrt[d]{n-1}]$为一个算术函数.证明 f 是乘性函数但不是完全乘性函数.

证明 首先我们注意到 $f(n)=\begin{cases}1, & \text{如果}n=l^d\\ 0, & \text{如果}n\neq l^d\end{cases}$.

这是因为如果 n 不为某个整数的 d 次方,则 n 必在两个 k^d 与 $(k+1)^d$ 之间,所以可以推出上面的结果.

取 m,n 互素,如果它们均不为某个整数的 d 次方,则它们的乘积也不会是某个整数的 d 次方,所以在这种情形下 $f(mn)=f(m)f(n)$;

如果它们均为某个整数的 d 次方,则它们的乘积也是某个整数的 d 次方,所以在这种情形下也有 $f(mn)=f(m)f(n)$.

综上, m,n 互素的情形下,必有 $f(mn)=f(m)f(n)$.即 f 是乘性的.

取$n=2,m=2^{d-1}$,则$f(2)=0$,$f(2^{d-1})=0$,但是 $f(2^d)=1\neq f(2)f(2^{d-1})=0$.所以它不是完全乘法函数. □

(41).令 f 为一个乘性函数.证明:

(i). 对每个无平方因子的整数 n ,$f^{-1}(n)=\mu(n)f(n)$.

(ii). 对每个素数 p ,$f^{-1}(p^2)=f(p)^2-f(p^2)$.

证明 (i).只需证明 $f*f^{-1}=\delta$. 注意到 $f*f^{-1}=\sum\limits_{d|n}\mu(d)f(d)f(\frac{n}{d})$. 因为 n 为无平方因子整数,所以$(d,\frac{n}{d})=1$.又因为 f 为乘性的,所以 $f(d)f(\frac{n}{d})=f(n)$,故

$$\begin{aligned}f*f^{-1}&=\sum_{d|n}\mu(d)f(d)f(\frac{n}{d})\\&=f(n)\sum_{d|n}\mu(d)\\&=\begin{cases}f(1)=1, & \text{如果}n=1\\ 0, & \text{如果}n>1\end{cases}\end{aligned}$$

这就证明了(i).

(ii). 注意到 $f*f^{-1}(p^2)=0$,即

$$f(p^2)f^{-1}(1)+f(p)f^{-1}(p)+f(1)f^{-1}(p^2)=0$$

由(i),$f^{-1}(p)=-f(p)$.代入整理后就有$f^{-1}(p^2)=f(p)^2-f(p^2)$. □