Contents

Chapter 1

初等数论

问题 1.0.1

求所有的多项式$f(x)$, 满足$f(x^2+1)=f^2(x)+1$, 且$f(0)=0$.

解. 求导并让$x=0$. □

解. 定义数列$\{x_n\}$为$x_0=0$, $x_{n+1}=x_n^2+1$, 则$f(x)-x=0$有无穷多个根$\{x_n\}$. □

问题 1.0.2

设$f(x)\in\mathbb{R}[x]$, 如果对任意实数x有$f(x)\geq 0$, 则$f(x)$是两个实系数多项式的平方和.

解. 由于$f=\prod_{b,c}\left[(x-b)^2+c\right]$和$(x^2+y^2)(z^2+w^2)=(xz-yw)^2+(xw+yz)^2$. □

问题 1.0.3

证明多项式$x^{2n}-2x^{2n-1}+3x^{2n-2}-\cdots-2nx+(2n+1)$没有实根.

解. 当$x\leq 0$时, $f(x)=x^{2n}-2x^{2n-1}+3x^{2n-2}-\cdots-2nx+(2n+1)>0$; 若$x>0$, $(1+x)f(x)=f(x)+xf(x)=x\frac{x^{2n+1}+1}{x+1}+2n+1>0$, 所以对$x>0$时亦有$f(x)>0$. □

问题 1.0.4

设$f(x)$是一个整系数多项式, 首项系数为1, 且$f(0)\neq 0$. 若$f(x)$仅有一个单根α使得$|\alpha|\geq 1$, 则$f(x)$在$\mathbb{Z}$上不可约.

解. 反证, $f=gh$, 设$h(\alpha)=0$, 则$|g(0)|\geq 1$是其根的模之积, 又小于1, 矛盾. □

问题 1.0.5

设$a_1,\cdots,a_n$是互不相同的整数, 证明: 多项式

$$(x-a_1)\cdots(x-a_n)-1$$

在$\mathbb{Z}$上不可约.

解. 反证, $f=gh$, 因$f(a_i)=-1$, 知$g(a_i)+h(a_i)=0$, 由次数限制而导致矛盾. □

问题 1.0.6

给定$2n$个互不相同的复数$a_1,\cdots,a_n,b_1,\cdots,b_n$, 将其按下列规则填入$n\times n$方格中: 第$i$行第$j$列相交处方格内填$a_i+b_j$, $(i,j=1,\cdots,n)$, 证明: 若各列数乘积相等, 则各行数的积也相等.

解. 设各列的积都为c, 则$f(x)=(x+a_1)\cdots(x+a_n)-c$, 有$n$个根$b_1,\cdots,b_n$. 所以$f(x)=\prod_j(x-b_j)$, 所以$f(-a_i)=(-1)^n\prod_j(a_i+b_j)=-c$, 即$\prod_j(a_i+b_j)=(-1)^{n+1}c$, $(\forall i)$. □

问题 1.0.7

设a,b,c为整数, $abc\neq 0$, 求证:

$$[(a,b),(b,c),(c,a)]=([a,b],[b,c],[c,a]).$$

问题 1.0.8

设$\{F_n\}$是符合$F_1=F_2=1$的裴波那契数列, 若$(m,n)=d$, 则$(F_m,F_n)=F_d$; 反之, 若$(F_m,F_n)=F_d$, 则$d=(m,n)$或$d=1$, $(m,n)=2$或$d=2$, $(m,n)=1$.

解. 先证$F_q=F_kF_{q-k+1}+F_{k-1}F_{q-k}$, 后证$m=nq+r$, $q\geq 0$, $1\leq r\leq n-1$时, $(F_m,F_n)=(F_n,F_r)$, 即$(F_m,F_n)=F_{(m,n)}$, 于是$F_d=F_{(m,n)}$的解即为结论的三种情况. □

问题 1.0.9

当a,b满足什么条件时, $3\mid n(an+1)(bn+1)$对任意n成立.

解. 根据同余理论, 只需让n分别取$1,2,3$分别代入上式, 可得$3\mid ab+1$, 即$ab\equiv 2\pmod 3$ □

问题 1.0.10

a,b正整数, $d=(a,b)$, 证$S=\{ma+nb\}$, $(m,n$遍历正整数$)$包含d的大于ab的所有倍数.

解. 设$t>ab$是d的倍数且$ax+by=t$, 由Bézout等式, 左式有解$x=x_0+br$, $y=y_0-ar$, 调整r使$0<x<b$, 得$-\frac{x_0}{b}<r<\frac{b-x_0}{b}$, 于是$y=y_0-ar>y_0-a\frac{b-x_0}{b}=\frac{t-ab}{b}>0$. □

问题 1.0.11

$4k-1$形素数无穷.

解. 反证: $p_1,p_2,\cdots,p_r$为r个有限$4k-1$形素数, 考虑$p_1^2p_2^2\cdots p_r^2-1$的因子中必有$4k-1$形素因子. 另外也可考虑$4p_1p_2\cdots p_r-1$. □

问题 1.0.12

$6k-1$形素数无穷.

解. 想法同上, 考虑$6p_1p_2\cdots p_r-1$中必有$6k-1$形素数, 却不是$p_1,p_2,\cdots p_r$中的一个. □

问题 1.0.13

$4k+1$形素数无穷.

解. $4(p_1p_2\cdots p_r)^2+1$的素因子均可写成$4k+1$形素数, 但不是$p_1,\cdots,p_r$中的任一个. □

问题 1.0.14

假设自然数N有形如$4n-1$的因子, 则N必有形如$4n-1$的素因子.

问题 1.0.15

对每个素数$p=4n-1$和整数a, p^2不可能整除a^2+1.

解. 反证, 若$p^2\mid a^2+1$, $a^2\equiv -1 \pmod{p^2}$, 说明a的阶等于4. a可以看成群$\mathbb{Z}_{p^2}^*$中的元素, 由Euler定理, 群$\mathbb{Z}_{p^2}^*$的阶为$p(p-1)=2(4n-1)(2n-1)$. 在由Cauchy定理, 群中元素的阶必整除群的阶, 所以有$4\mid 2(4n-1)(2n-1)$. 矛盾. □

问题 1.0.16

证明a^2+1没有$4n-1$的因子, a,n是任何正整数.

解. 假设自然数$N=a^2+1$有形如$4n-1$形因子, 则由问题1.0.14知N必有形如$4n-1$的素因子, 记为p. 而N可以写成两个整数的平方和($N=a^2+1^2$), 所以由问题**??**知N的素因子分解中p出现次数为偶数. 从而必有p^2整除$N=a^2+1$, 与问题1.0.15矛盾. 所以N不可能有形如$4n-1$的因子. □

问题 1.0.17

a,b正整数, $a+b=57$, $[a,b]=680$, 求a,b.

解. 用$(a,b)[a,b]=ab=(a+b,b)[a,b]$, 所以$(57,b)\cdot 680=ab$, 然后$57=3\times 19$, 分四种情况讨论$(57,b)$的值, 并计算出$ab$的值联合$a+b$的值用Vieta定理. □

问题 1.0.18

$a,b,c,d\in\mathbb{Z}$, $a-c\mid ab+cd$, 则$a-c\mid ad+bc$.

问题 1.0.19

$a,b\in\mathbb{Z}$且$\frac{b+1}{a}+\frac{a+1}{b}\in\mathbb{Z}$, 则$(a,b)\le\sqrt{a+b}$.

问题 1.0.20

a,b为大于1的正整数, $(a,b)=1$, 则有唯一一对整数r,s使得$ar-bs=1$, 且$0<r<b$, $0<s<a$.

问题 1.0.21

q-进表示n中. $n=\sum_{i=0}^k a_iq^i$, 有$a_i=\left[\frac{n}{q^i}\right]-q\left[\frac{n}{q^{i+1}}\right]$.

问题 1.0.22

$p^{\alpha_p}\| n!$, 则$\alpha_p=\sum_{i=1}^\infty\left[\frac{n}{p^i}\right]$, 设$n=\sum_{i=0}^k a_iq^i$, 则$a_i=\left[\frac{n}{q^i}\right]-q\left[\frac{n}{q^{i+1}}\right]$. 而$S_p(n)=\sum_{i=0}^\infty a_i=(n+\alpha_p)-q\alpha_p$, 所以$\alpha_p=\sum_{i=1}^\infty\left[\frac{n}{p^i}\right]=\frac{n-S_p(n)}{p-1}$. 其中$S_p(n)$为$n$的$p$-进展开的各个数字值之和.

问题 1.0.23

若2^m+1是素数, 则m是2的幂, 从而是Fermat数F_n.
$a,m>1$, a^m-1是素数, 则$a=2$且m是素数. 从而是梅森Mersenne数.

问题 1.0.24: 偶完全数

$\sigma(n)=2n$则称n是完全数, 证明偶完全数形如$2^k(2^{k+1}-1)$.

解. σ是积性函数, 设$n=2^p\cdot q$, 则$(2^{p+1}-1)\sigma(q)=2^{p+1}q$, 即$\frac{q}{\sigma(q)}=\frac{2^{p+1}-1}{2^{p+1}}$且$2^{p+1}-1\mid q$. 设$q=(2^{p+1}-1)k$.
(1). 若$2^{p+1}-1$是合数, q的最小质因子$p_1<2^{p+1}-1$, 所以$q=p_1^{\alpha_1}w$. 这与$\frac{q}{\sigma(q)}=\frac{p_1^{\alpha_1}w}{\sum_i p^i f(w)}<\frac{p_1}{p_1+1}<\frac{2^{p+1}-1}{2^{p+1}}$.
(2). 若$2^{p+1}-1$是素数, 若$k=1$, 命题显然成立. 否则$q=(2^{p+1}-1)^\alpha w$.

- 若$w=1$, $\alpha>1$, $\frac{q}{\sigma(q)}=\frac{(2^{p+1}-1)^\alpha}{\sum_i(2^{p+1}-1)^i}<\frac{2^{p+1}-1}{2^{p+1}}$. 这导致矛盾.
- 若$w>1$, 则$\frac{q}{\sigma(q)}=\frac{(2^{p+1}-1)^\alpha}{\sum_i(2^{p+1}-1)^i}\frac{w}{\sigma(w)}<\frac{2^{p+1}-1}{2^{p+1}}$, 又矛盾.

故$w=1$, $\alpha=1$. □

问题 1.0.25

若$m>2$, 则$\varphi(m)$是偶数.

解. 由Euler公式, $(-1)^{\varphi(m)}\equiv 1 \pmod m$. □

解. 若i与m互素, 则$m-i$与m也互素, 所以与m互素的数总是成对出现. 若有$i=m-i$, 这表明m是i的倍数, 则i不可能是与m互素的$\varphi(m)$个数的任一个. □

问题 1.0.26

设$a,b\in\mathbb{Z}$, 且p为素数, 若$a^p\equiv b^p \pmod p$, 则$a^p\equiv b^p \pmod{p^2}$.

解. Fermat定理$a\equiv b \pmod{()p}$, 所以$a\equiv b \pmod p$, 于是可设$a=b+mp$, 并用二项式定理证得. □

问题 1.0.27

设p是素数, $k\in\mathbb{N}_+$, 则

- $p|\binom{p}{k}$, $k=1,\cdots,p-1$.
- $\binom{p-1}{k}\equiv(-1)^k \pmod p$, $k=0,\cdots,p-1$.
- $\binom{k}{p}\equiv\left[\frac{k}{p}\right] \pmod p$.

解.

- $p|k\binom{p}{k}=p\binom{p-1}{k-1}$, $(k,p)=1$.
- $\binom{p}{k}-\binom{p-1}{k}=\binom{p-1}{k-1}\implies\binom{p-1}{k}\equiv-\binom{p-1}{k-1} \pmod p$, 用归纳法.
- $\binom{k}{p}=\frac{k(k-1)\cdots(k-p+1)}{p!}$, $k,k-1,\cdots,k-p+1$中必有p的倍数, 设为$k-i$,
  则$\binom{k}{p}=\frac{k-i}{p}\cdot\frac{k(k-1)\cdots(k-p+1)}{(k-i)(p-1)!}=\left[\frac{k}{p}\right]\frac{k(k-1)\cdots(k-p+1)}{k-i}\cdot\frac{1}{(p-1)!}\equiv\left[\frac{k}{p}\right]\frac{-1}{-1} \pmod p$.
  最后一步用Wilson公式.

□

问题 1.0.28

素数$p \geq 5$, 则$\frac{1}{1^2}+\frac{1}{2^2}+\cdots+\frac{1}{(p-1)^2} \equiv 0 \pmod p$.

解. $1,2,\cdots,p-1$是模p的缩系. 所以$\frac{1}{1},\frac{1}{2},\cdots,\frac{1}{p-1}$也是模$p$的缩系. 故对$p \geq 5$有

$$\sum_{k=1}^{p-1}\left(\frac{1}{k}\right)^2 \equiv \sum_{k=1}^{p-1}k^2=\frac{(p-1)p(2p-1)}{6} \equiv 0 \pmod p.$$

□

解. $\frac{1}{1},\frac{1}{2},\cdots,\frac{1}{p-1}$是模$p$的缩系, 对任意$a$, $p \nmid a$, $\frac{a}{1},\frac{a}{2},\cdots,\frac{a}{p-1}$也是模$p$的缩系. 故

$$\sum_{k=1}^{p-1}\left(a\cdot\frac{1}{k}\right)^2 \equiv \sum_{k=1}^{p-1}\left(\frac{1}{k}\right)^2 \pmod p \Longrightarrow (a^2-1)\sum_{k=1}^{p-1}\left(\frac{1}{k}\right)^2 \equiv 0 \pmod p.$$

对$p \geq 5$可取a满足$p \nmid a$且$p \nmid a^2-1$即得. □

问题 1.0.29

若 $p>3$, 证明

$$p^2 \mid (p-1)!\left(1+\frac{1}{2}+\cdots+\frac{1}{p-1}\right).$$

解. 用1.0.28, 知

$$\sum_{i=1}^{p-1}\frac{1}{i(p-i)} \equiv \sum_{i=1}^{\frac{p-1}{2}}\frac{2}{i(p-i)} \equiv 0 \pmod p.$$

从而

$$(p-1)!\sum_{i=1}^{p-1}\frac{1}{i} \equiv (p-1)!\sum_{i=1}^{\frac{p-1}{2}}\frac{p}{(p-i)i} \equiv 0 \pmod{p^2}.$$

□

解. 设

$$(x-1)(x-2)\cdots(x-p+1)=x^{p-1}-s_1x^{p-2}+\cdots+s_{p-1}, \tag{1.1}$$

其中 $s_{p-1}=(p-1)!$, $s_{p-2}=(p-1)!\left(1+\frac{1}{2}+\cdots+\frac{1}{p-1}\right)$. 因

$$s_1x^{p-2}+\cdots+s_{p-2}x=(x-1)(x-2)\cdots(x-p+1)-x^{p-1}+1 \equiv 0 \pmod p$$

有 $p-1$ 个根, 所以 $s_1,\cdots,s_{p-2}$ 都是 p 的倍数. 对1.1中取 $x=p$ 有

$$p^{p-2}-s_1p^{p-3}+\cdots+s_{p-3}p-s_{p-2}=0.$$

所以 $p^2 \mid s_{p-2}$. □

问题 1.0.30

n是偶数, $a_1,\cdots,a_n$与$b_1,\cdots,b_n$都是模n的完系, 证$a_1+b_1,\cdots,a_n+b_n$不是模n的完系.

解. 反证法, $\sum a_i \equiv \frac{n(n-1)}{2} \equiv \sum b_i \pmod n$, 若$a_1+b_1,\cdots,a_n+b_n$是模$n$的完系. 则$\sum(a_i+b_i) \equiv \frac{n(n-1)}{2}$, 于是$n(n-1) \equiv \frac{n(n-1)}{2} \pmod n$, 由于$n(n-1) \equiv 0 \pmod n$, 故$\frac{n(n-1)}{2} \equiv 0 \pmod n$, 即$n|\frac{n(n-1)}{2}$, 但$(n,n-1)=1$, 所以$n|\frac{n}{2}$不可能. □

问题 1.0.31

设a,b为正整数, n是正整数, 证明

$$n! \mid b^{n-1}a(a+b)\cdots(a+(n-1)b).$$

解. 只需证对任意的素数p, 若$p^{\alpha}\| n!$, 则$p^{\alpha} \mid b^{n-1}a(a+b)\cdots(a+(n-1)b)$.

(1). 若$p\mid b$, 则由于$\alpha=\sum_{i\geq 1}\left[\frac{n}{p^i}\right]<\frac{n}{p-1}\leq n$, 所以$p^{\alpha}|b^{n-1}$.

(2). 若$p\nmid b$, 则$(p,b)=1$, 从而有$b_1 b\equiv 1 \pmod p$, 于是

$$b_1^n a(a+b)\cdots(a+(n-1)b)\equiv ab_1(ab_1+1)\cdots(ab_1+n-1) \pmod p.$$

由于$n!\mid ab_1(ab_1+1)\cdots(ab_1+n-1)$, 所以$p^{\alpha}\mid ab_1(ab_1+1)\cdots(ab_1+n-1)$. □

问题 1.0.32

设p是一个奇素数, 证明

- $1^2\cdot 3^2\cdots(p-2)^2\equiv(-1)^{\frac{p+1}{2}} \pmod p$;
- $2^2\cdot 4^2\cdots(p-1)^2\equiv(-1)^{\frac{p+1}{2}} \pmod p$.

解. 用Wilson公式, 注意到$k\equiv -(p-k) \pmod p$. □

问题 1.0.33

求所有有理数k, 使得$0\leq k\leq\frac{1}{2}$, 且$\cos k\pi$是有理数.

解. k有三个值, $0,\frac{1}{3},\frac{1}{2}$使$\cos k\pi$为有理数, 设$\cos\theta=\frac{p}{q}$, $q\geq 3$, $p<q$, 且p与q互素, 那么$\cos 2\theta=\frac{2p^2-q^2}{q^2}$, 其分子分母的公因子必整除$2p^2$及$q^2$, 故$2p^2-q^2$与$q^2$的最大公因数是1或2. 于是当$\frac{2p^2-q^2}{q^2}$写成最简形式时, 其分母至少是$\frac{q^2}{2}>q$, 因此$\cos 2\theta\neq\cos\theta$. 且$\cos 2\theta$, $\cos 4\theta$, ... 都是有理数, 且其分母组成一个递增序列. 设$\theta=2^i\left(\frac{u}{v}\right)\pi$, u,v是互素奇数, 由v是奇数, 存在正整数$w>|i|$, 使$v\mid(2^w-1)$, 故$2^{2w-i+1}\theta-2^{w-i+1}\theta=\frac{2^w-1}{v}2^w u\,(2\pi)$, 从而$\cos\left(2^{2w-i+1}\theta\right)=\cos\left(2^{w-i+1}\theta\right)$. 由前面所证得, 当$\theta=2^i\left(\frac{u}{v}\right)\pi$时, $\cos\theta$不能是分母超过2的有理数. □

问题 1.0.34

证明: 不存在正整数a,b,c, 使得$a^2+b^2+c^2=a^2b^2$.

解. 模4下讨论奇偶性, 无穷递降法. □

问题 1.0.35: 21届IMO

$\frac{m}{n}=1-\frac{1}{2}+\frac{1}{3}-\frac{1}{4}+\cdots-\frac{1}{1318}+\frac{1}{1319}$, 其中$m,n$都是正整数, 证明: $1979\mid m$.

解.

$$\frac{m}{n}=\frac{1}{660}+\frac{1}{661}+\cdots+\frac{1}{1319}=1979\times\left(\frac{1}{600\times 1319}+\cdots+\frac{1}{661\times 1318}+\cdots+\frac{1}{989\times 990}\right)=\frac{1979k}{660\times\cdots\times 1319}.$$

其中k是整数, 1979是素数. □

问题 1.0.36: 39届IMO, T4

已知a,b是正整数, 且$\left(ab^2+b+7\right)\mid\left(a^2b+a+b\right)$, 求$a,b$.

解. $\left(ab^2+b+7\right) \mid a\left(ab^2+b+7\right)-b\left(a^2b+a+b\right)=7a-b^2$.

(1) 若$7a=b^2$, $(a,b)=\left(7k^2,7k\right)$, $(k\in\mathbb{N})$.

(2) 若$7a>b^2$, 则$7a-b^2\geq ab^2+b+7$, 所以$7>b^2$,..., $(a,b)=(11,1)$, $(49,1)$.

(3) $7a<b^2$, 则$b^2-7a\geq ab^2+b+7>b^2$... □

问题 1.0.37

若$n^2+15n+42$是一完全平方数, 求n.

解. $n\geq 8$时, $(n+7)^2<n^2+15n+42<(n+8)^2$, $n<-22$时, $(n+8)^2<n^2+15n+42<(n+7)^2$. $n=-13$, -22, -2, 7. □

问题 1.0.38

求不定方程

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

的所有正整数解.

问题 1.0.39

设a, b, c, d为正整数, $ab = cd$. 证明: $a^4 + b^4 + c^4 + d^4$不是素数.

解. 由$ab = cd$, 不妨设$a = us, b = vt, c = vs, d = ut$, 则

$$a^4 + b^4 + c^4 + d^4 = (u^4 + v^4)(s^4 + t^4)$$

不是素数. $\square$

问题 1.0.40

设$n > 1$是奇数, 若n的分解$n = uv$, 其中$0 < u - v \leq 4\sqrt[4]{n}$, 证明: n的这种分解是唯一的.

Chapter 2

语录

在我年轻的时候，我听从建议去读庞加莱，希尔伯特，克莱因以及胡尔维茨等的著作，并从中获益．而我自己对布拉须凯，嘉当和霍普夫的著作更为熟悉，其实这也是中国的传统：在中国我们被教导要读孔夫子，韩愈的散文以及杜甫的诗歌，我真诚地希望这套全集不要成为书架上的摆设，而是在年轻数学家的手里被翻烂掉．

有人主张依靠直观去进行数学教学，我却认为再没有比这种数学教学方法更为荒谬和更为有害的了，每一个数学教师都应当不遗余力地教会学生去思考而不依赖于直观感觉．
--柯勒里吉

数学不是规律的发现者，因为它不是归纳．数学也不是理论的缔造者，因为他不是假说．但数学却是规律和理论的裁判和主宰者．因为规律和假说都要向数学表明自己的主张，然后等待数学的裁判．如果没有数学上的认可，则规律不能起作用，理论也不能解释．
--Peirce，Benjamin