问题求解（三）第12周作业

黄奕诚161220049

November 21, 2017

TJ Chapter 2

13

Proof. (1) 首先由第二数学归纳法推第一数学归纳法：由第二数学归纳法知，对于某个整数n_0，若$S(n_0)$成立，且可以由$S(n_0), S(n_0+1), \cdots, S(k)$可推出$S(k+1)$，其中$k \geq n_0$，则对任意的$n \geq n_0$，$S(n)$都成立.因为$k$是任取的，当取到$n_0, n_0+1, \cdots$时，可以由$S(n_0)$推得$s(n_0+1)$，由$S(n_0), S(n_0+1)$推得$S(n_0+2)$，$\cdots$，将其中多余的条件删去，便有：$S(n_0) \rightarrow S(n_0+1), S(n_0+1) \rightarrow S(n_0+2),] \cdots$由此便推得第一数学归纳法.

(2) 其次由第一数学归纳法推第二数学归纳法：不妨以良序定理为中间结论，先由第一数学归纳法推良序定理，再由良序定理推第二数学归纳法。对于第一点，由Theorem 2.2已经推出，对于第二点，证明如下：
设集合S满足如下条件：$n_0 \in S$，若$n_0, n_1, \cdots, k \in S$，则$k+1 \in S$.假设$S$不等于$A = \{k | k \geq n_0\}$，则令$T$为其补集，且$T$非空.由良序定理知$T$中有最小值$m \in A$，并且$m \neq n_0$，由$T$的定义知$m-1 \in S$，由$S$的定义可推知$m \in S$，这与$m \in T$矛盾.因此可证得第二数学归纳法.

(3) 综上所述，第一与第二数学归纳法等价.

□

14

(1) 首先证明自然数的良序定理可以推知1是最小的自然数：

Proof. 因为自然数满足良序定理，所以存在最小数，而$N = \{n | n \geq 1\}$，有$1 \in N$，且对任意的$n_0 \in N$，都有$n_0 \geq 1$，因此1是最小的自然数. □

(2) 由良序定理证明数学归纳法与题13的第(2)部分相同，令上题的$n_0 = 1$，即可证明$S = \mathbb{N}$.

15

(a) 39=14*2+11, 14=11*1+3, 11=3*3+2, 3=2*1+1, 2=1*2+0
gcd(14,39)=1，且$r = 14, s = -5$

(b) 234=165*1+69, 165=69*2+27, 69=27*2+15, 27=15*1+12, 15=12*1+3, 12=3*4+0
gcd(234,165)=3，且$r = 12, s = -17$

(c) 9923=1739*5+1228, 1739=1228*1+511, 1228=511*2+206, 511=206*2+99, 206=99*2+8, 99=8*12+3, 8=3*2+2, 3=2*1+1, 2=1*2+0
gcd(1739,9923)=1，且$r = 3709, s = -650$

(d) 562=471*1+91, 471=91*5+16, 91=16*5+11, 16=11*1+5, 11=5*2+1, 5=1*5+0
gcd(471,562)=1，且$r = -105, s = 88$

(e) 23771=19945*1+3826, 19945=1826*10+1685, 1826=1685*1+141, 1685=141*11+134, 141=134*1+7, 134=7*19+1, 7=1*7+1
gcd(23771,19945)=1，且$r = 881, s = -1050$

(f) 4357=3754*1+603, 3754=603*6+136, 603=136*4+59, 136=59*2+18, 59=18*3+5, 18=5*3+3, 5=3*1+2, 3=2*1+1, 2=1*2+0
gcd(-4357,3754)=1，且$r = 1463, s = 1698$

16

Proof. 假设a,b不互质，设$\gcd(a,b)=m$，其中$m>1$且$m\in N$.可得$m|a$且$m|b$，因此$m|(ar+bs)$，故$m|1$，可得$m=1$，而$m>1$，矛盾.因此a,b互质. □

19

Proof. 因为xy是完全平方数，所以$xy=k^2$，其中$k\in\mathbb{Z}$.因为x,y互质，所以$\gcd(x,y)=1$.若$k=1$，则$x=y=1$满足条件，若$k>1$，由算数基本定理可知，$k=p_1p_2\cdots p_i$，其中$p_1p_2\cdots p_i$都是素数，于是$k^2=p_1^2p_2^2\cdots p_i^2$，也即$xy=p_1^2p_2^2\cdots p_i^2$.假设$x,y$中有不是完全平方数的数，则其必含有因数$p_t$(指数为1)，此时另一个数也会含有因数$p_t$，因此它们不互质，矛盾。从而$x,y$都是完全平方数. □

22

Proof. 对于$\mathbb{Z}$中的任意元素m，都可以表示为带余除法：$m=nq+r$，其中$0\le r\le n-1$，由此可知$m-r\equiv 0(\mod n)$，也即$m\equiv r(\mod n)$，所以任意整数都与集合$\{0,1,\cdots,n-1\}$中的某个元素关于n同余. □

28

Proof. 假设p是合数，则p可表示为$p=mn$，其中$2\le m,n<p$且$m,n\in\mathbb{N}$.由此有$2^p-1=2^{mn}-1=(2^m)^n-1$.设$s=2^m\ge 4$，则原式等于s^n-1，有$(s-1)|(s^n-1)$.又因为$s-1\ge 3>1$，所以s^n-1是合数，即2^p-1是合数，与其是素数矛盾，因此p是素数. □

29

Proof. 设自然数$p=p_1p_2p_3\cdots p_k\cdots+1$，$p_i$为素数，其中$p_1,p_2,\cdots,p_k$是其前$k$个素数，且$p_1=2,p_2=3$，由此有$p=6p_3p_4\cdots+1$.假设$p$不是素数，则存在$p_i(1\le i\le n)$使得$p_i|6p_3p_4\cdots$且$p_i|1$，后者显然不成立，因此$p=6p_3\cdots+1$是素数，结合Theorem 2.7知即形如$6n+1$的素数有无穷多个. □

30

Proof. 在上题中将$p_1=2,p_2=3$改为$p_1=p_2=2$，正1改为负1，其余同理可证. □

31

Proof. 假设存在整数p,q使得$p^2=2q^2$，则有$2|p^2$，因为2是素数，故$2|p$，p为偶数.设$p=2k$，得$q^2=2k^2$，可得q也为偶数.因为2是素数，原命题等价于p,q互质.而因为p,q都是偶数，显然不互质，所以矛盾.不存在整数p,q使得$p^2=2q^2$.另外，假设$\sqrt{2}$是有理数，即可以表示为$\frac{a}{b}(\gcd(a,b)=1)$.此时$a^2=2b^2$，又前面的证明可知并不存在这样的整数a,b.因此$\sqrt{2}$是无理数. □

P.E. 1

```
#include <stdio.h>
#include <stdlib.h>
#include <string.h>
#include <math.h>

bool isPrime[100000];
void Sieve(int n)
{
for (int i = 2; i <= sqrt(n); i++)
        if (isPrime[i])
        for (int j = i; j*i<= n; j++)
                isPrime[i*j] = false;
for (int k = 2; k <= n; k++)
        if (isPrime[k])
                printf("%d ", k);
printf("\n");
}
int main()
{
        int N;
        while (scanf("%d", &N) == 1) {
                memset(isPrime, true,
                  sizeof(isPrime));
                Sieve(N);
        }
        return 0;
}
```

当$N = 120$时，输出为2 3 5 7 11 13 17 19 23 29 31 37 41 43 47 53 59 61 67 71 73 79 83 89 97 101 103 107 109 113.

P.E. 3

```
#include <stdio.h>
int a,b,x,y;
int gcd()
{
        int d=a;
        if (b){
                d=gcd(b,a%b,y,x);
                y-=(a/b)*x;
        }
        else{
                x=1;
                y=0;
        }
        return d;
}
int main()
{
        while (scanf("%d%d",&a,&b)==2)
        {
                int ans=gcd();
                printf("gcd:%d x:%d y:
                %d\n",ans,x,y);
        }
        return 0;
}
```

CS 2.2

2

因为$a\cdot 133-2m\cdot 277=1$，所以$a\cdot 133=1+2m\cdot 277$，故可以保证a有一个模m的逆元，即133(mod m).

4

因为$\gcd(31,22)=1$，故存在a使得$a\cdot_{31}22=1$且只存在一个这样的a，当$a=24$
因为$\gcd(10,2)=2\neq 1$，故不存在a使得$a\cdot_{10}2=1$.

6

因为$a\cdot 133-m\cdot 277=1$，所以由Theorem 2.15可知a,m互质，由此它们只有唯一的公因数，即1.

8

由$k=jq+r$，所以$k=qj+r$，由欧几里得算法可知gcd(q,k)=gcd(r,q).

15

两者之间有关系：gcd(j,k)是gcd(r,k)的因数.当gcd$(r,k)=1$，即r,k互质时，有gcd(j,k)=gcd(r,k)=1.

16

由题意知，$m=-qn-r$且$m=q'n+r', r'=n-r$，因此可得$q'=-q-1$.因为r'满足$0\leq r'<n$，所以对于任意的整数(可以是非正整数)m，总存在整数q',r'使得$m=nq'+r'$，其中$0\leq r'<n$，由此便由Theorem 2.12推广到了Theorem 2.1

17

计算gcd(F_i,F_{i+1})时，在拓展GCD算法中，首先判断两者是否相等.因为斐波那契数列中，相等的元素只有F_1,F_2，若是它们则返回gcd=1,$x=1,y=0$.否则需要依次计算q_i,r_i,k_{i+1}以及j_{i+1}，并利用斐波那契数列$F_{i+2}=F_{i+1}+F_i$的性质进行替换.由于每一个F_i都可以表示为F_1,F_2的线性组合，所以GCD递归必有出口.最终运算结果为：$\gcd(F_i,F_{i+1})=1, x=(-1)^{i-1}F_i, y=(-1)^iF_{i-1}$.

19

$\gcd(x,y)*\mathrm{lcm}(x,y)=xy$.

Proof. 设$a=\gcd(x,y), b=$ x,y，则有$x=ma, y=na$，其中m,n互质.所以$b=mna$，此时$ab=mna^2=(ma)(na)=xy=\gcd(x,y)*\mathrm{lcm}(x,y)$，得证. □