Problem Solving: Homework 3.12

Name: Chen Shaoyuan Student ID: 161240004

November 21, 2017

1 [TJ] Exercise 2-13

The First Principle of Mathematical Induction is a special case of the second one, so we only have to prove that the first one implies the second one.

Let $S'(n)$ denote the statement that for every integer $k(n_0 \le k \le n)$, $S(k)$ holds. The basis of the second one says that $S(n_0)$ holds, hence $S'(n_0)$ holds. Assume that $S'(n)$ holds, i.e. $S(n_0), S(n_0+1), \cdots, S(n)$ hold. By the induction of the second one, $S(n+1)$ holds, so $S'(n+1)$ holds. By the First Principle of Mathematical Induction, $S'(n)$ holds for all $n \ge n_0$, i.e. the Second Principle of Mathematical Induction is true.

2 [TJ] Exercise 2-14

Assume, to the contrary that 1 is not the smallest natural number. Let $S \neq \varnothing$ denote the set of natural numbers that are less than 1. By the Principle of Well-Ordering, S must contain a smallest number, say x. Since $x \neq 1$, by the definition of natural number, it must have a predecessor $x-1$, such that $x-1 < x < 1$, so $x-1 \in S$. This means that x is not the smallest integer of S, which leads to contradiction. Therefore, 1 is the smallest natural number.

Assume, to the contrary that $S \neq \mathbb{N}$, then $\mathbb{N} \setminus S \neq \varnothing$. By the Principle of Well-Ordering, S has a smallest number, say x. If $x = 1$, it contradicts the basis of the mathematical induction. If $x \neq 1$, by the contrapositive of the induction, $x-1 \notin \mathbb{N} \setminus S$, which means x is not the smallest number of $\mathbb{N} \setminus S$. The contradiction must occur whatever the value of x is. This means $\mathbb{N} \setminus S \neq \varnothing$, also we have $S \subset \mathbb{N}$, so $S = \mathbb{N}$. Hence the Principle of Mathematical Induction is true.

3 [TJ] Exercise 2-15

(a)

$$\begin{aligned}
39 &= 14 \cdot 2 + 11 \\
14 &= 11 \cdot 1 + 3 \\
11 &= 3 \cdot 3 + 2 \\
3 &= 2 \cdot 1 + 1 \\
2 &= 1 \cdot 2 + 0
\end{aligned}$$

$$\begin{aligned}
1 &= 3 + (-1) \cdot 2 \\
&= 3 + (-1) \cdot (11 - 3 \cdot 3) \\
&= 4 \cdot (14 - 1 \cdot 11) + (-1) \cdot 11 \\
&= 4 \cdot 14 + (-5) \cdot (39 + (-2) \cdot 14) \\
&= 14 \cdot 14 + (-5) \cdot 39
\end{aligned}$$

$$\gcd(14, 39) = 1 = 14 \cdot 14 + (-5) \cdot 39$$

(b)

$$\begin{aligned}
562 &= 471 \cdot 1 + 91 \\
471 &= 91 \cdot 5 + 16 \\
91 &= 16 \cdot 5 + 11 \\
16 &= 11 \cdot 1 + 5 \\
11 &= 5 \cdot 2 + 1 \\
5 &= 1 \cdot 5 + 0
\end{aligned}$$

$$\begin{aligned}
1 &= 11 + (-2) \cdot 5 \\
&= 11 + (-2) \cdot (16 + (-1) \cdot 11) \\
&= 3 \cdot (91 + (-5) \cdot 16) + (-2) \cdot 16 \\
&= 3 \cdot 91 + (-17) \cdot (471 + (-5) \cdot 91) \\
&= 88 \cdot (562 + (-1) \cdot 471) + (-17) \cdot 471 \\
&= 88 \cdot 562 + (-105) \cdot 471
\end{aligned}$$

$$\gcd(471, 562) = 1 = (-105) \cdot 471 + 88 \cdot 562$$

(c)

$$\begin{aligned}
234 &= 165 \cdot 1 + 69 \\
165 &= 69 \cdot 2 + 27 \\
69 &= 27 \cdot 2 + 15 \\
27 &= 15 \cdot 1 + 12 \\
15 &= 12 \cdot 1 + 3 \\
12 &= 3 \cdot 4 + 0
\end{aligned}$$

$$3 = 15 + (-1) \cdot 12$$

$$
\begin{aligned}
&= 15+(-1)\cdot(27+(-1)\cdot 15)\\
&= 2\cdot(69+(-2)\cdot 27)+(-1)\cdot 27\\
&= 2\cdot 69+(-5)\cdot(165+(-2)\cdot 69)\\
&= 12\cdot(234+(-1)\cdot 165)+(-5)\cdot 165\\
&= 12\cdot 234+(-17)\cdot 165
\end{aligned}
$$

$$\gcd(234,165)=3=12\cdot 234+(-17)\cdot 165$$

(d)

$$
\begin{aligned}
23771 &= 19945\cdot 1+3826\\
19945 &= 3826\cdot 5+815\\
3826 &= 815\cdot 4+566\\
815 &= 566\cdot 1+249\\
566 &= 249\cdot 2+68\\
249 &= 68\cdot 3+45\\
68 &= 45\cdot 1+23\\
45 &= 23\cdot 1+22\\
23 &= 22\cdot 1+1\\
22 &= 1\cdot 22+1
\end{aligned}
$$

$$
\begin{aligned}
1 &= 23+(-1)\cdot 22\\
&= 23+(-1)\cdot(45+(-1)\cdot 23)\\
&= 2\cdot(68+(-1)\cdot 45)+(-1)\cdot 45\\
&= 2\cdot 68+(-3)\cdot(249+(-3)\cdot 68)\\
&= 11\cdot(566+(-2)\cdot 249)+(-3)\cdot 249\\
&= 11\cdot 566+(-25)\cdot(815+(-1)\cdot 566)\\
&= 36\cdot(3826+(-4)\cdot 815)+(-25)\cdot 815\\
&= 36\cdot 3826+(-169)\cdot(19945+(-5)\cdot 3826)\\
&= 881\cdot(23771+(-1)\cdot 19945)+(-169)\cdot 19945\\
&= 881\cdot 23771+(-1050)\cdot 19945
\end{aligned}
$$

$$\gcd(23771,19945)=1=881\cdot 23771+(-1050)\cdot 19945$$

(e)

$$
\begin{aligned}
9923 &= 1739\cdot 5+1228\\
1739 &= 1228\cdot 1+511\\
1228 &= 511\cdot 2+206\\
511 &= 206\cdot 2+99\\
206 &= 99\cdot 2+8\\
99 &= 8\cdot 12+3\\
12 &= 3\cdot 4+0
\end{aligned}
$$

$$
\begin{aligned}
3 &= 99+(-12)\cdot 8\\
&= 99+(-12)\cdot(206+(-2)\cdot 99)\\
&= 25\cdot(511+(-2)\cdot 206)+(-12)\cdot 206\\
&= 25\cdot 511+(-62)\cdot(1228+(-2)\cdot 511)\\
&= 149\cdot(1739+(-1)\cdot 1228)+(-62)\cdot 1228\\
&= 149\cdot 1739+(-211)\cdot(9923+(-5)\cdot 1739)\\
&= 1204\cdot 1739+(-211)\cdot 9923
\end{aligned}
$$

$$\gcd(1739,9923)=3=1204\cdot 1739+(-211)\cdot 9923$$

(f)

$$
\begin{aligned}
-4357 &= 3754\cdot(-2)+3151\\
3754 &= 3151\cdot 1+603\\
3151 &= 603\cdot 5+136\\
603 &= 136\cdot 4+59\\
136 &= 59\cdot 2+18\\
59 &= 18\cdot 3+5\\
18 &= 5\cdot 3+3\\
5 &= 3\cdot 1+2\\
3 &= 2\cdot 1+1\\
2 &= 1\cdot 2+0
\end{aligned}
$$

$$
\begin{aligned}
1 &= 3+(-1)\cdot 2\\
&= 3+(-1)\cdot(5+(-1)\cdot 3)\\
&= 2\cdot(18+(-3)\cdot 5)+(-1)\cdot 5\\
&= 2\cdot 18+(-7)\cdot(59+(-3)\cdot 18)\\
&= 23\cdot(136+(-2)\cdot 59)+(-7)\cdot 59\\
&= 23\cdot 136+(-53)\cdot(603+(-4)\cdot 136)\\
&= 235\cdot(3151+(-5)\cdot 603)+(-53)\cdot 603\\
&= 235\cdot 3151+(-1228)\cdot(3754+(-1)\cdot 3151)\\
&= 1463\cdot(-4357+(-2)\cdot 3754)+(-1228)\cdot 3754\\
&= 1463\cdot(-4357)+1698\cdot 3754
\end{aligned}
$$

$$\gcd(-4357,3754)=1=1463\cdot(-4357)+1698\cdot 3754$$

4 [TJ] Exercise 2-16

Suppose that a and b are not relatively prime. Let $g=\gcd(a,b)>1$, then $a=pg$, $b=qg$, where p and q are integers. Hence $pgr+qgs=g(pr+qs)=1$. The lhs of the equation is a multiple of g, while the rhs is not, which leads to contradiction. Therefore a and b are relatively prime.

5 [TJ] Exercise 2-19

Let $xy=q^2$. By the Fundamental Theorem of Arithmetic, x,y can be written as

$$x=\prod_{i=1}^{k}{p_i}^{m_i},\qquad y=\prod_{i=1}^{k}{p_i}^{n_i},\qquad q=\prod_{i=1}^{k}{p_i}^{s_i}$$

where p_i is the ith prime, m_i, n_i, s_i are nonnegative integers.

$xy = q^2$ implies $2s_i = m_i + n_i$. Since x and y are relatively prime, we have $m_i n_i = 0$. Hence m_i, n_i are even, which means x and y are perfect squares.

6 [TJ] Exercise 2-22

For every integer m, by the division algorithm, there exists unique integers q and $t (0 \le t < n)$, such that $m = nq + t$. So every integer is congruent mod n to precisely one of the integers $0, 1, \cdots, 1$. This means that if r is an integer, there exists unique $s \in \mathbb{Z}$ such that $0 \le s < n$ and $[r] = [s]$. The union of $[0], [1], \cdots, [n-1]$ is $\mathbb{Z}$, and any two of them are disjoint. So the integers are partitioned by congruence mod n.

7 [TJ] Exercise 2-28

Note that $2^p - 1 = 1 + 2 + 4 + \cdots + 2^{p-1}$. If p is not prime, i.e. $p = qr$, where $q, r \ge 2$, then

$$\begin{aligned}
2^p - 1 =& 1 + 2 + \cdots + 2^{q-1} + \\
& 2^q + 2^{q+1} + \cdots + 2^{2q-1} + \\
& \cdots \\
& 2^{q(r-1)} + 2^{q(r-1)+1} + \cdots + 2^{qr-1} \\
=& (1 + 2^q + \cdots + 2^{q(r-1)})(1 + 2 + \cdots + 2^{q-1})
\end{aligned}$$

is not a prime, which leads to contradiction.

8 [TJ] Exercise 2-29

Assume, to the contrary that there are finitely many primes of the form $6n+5$, and let $p_1, p_2, \cdots, p_k$ denote them. Every odd prime is either of the form $6n+1$ or $6n+5$. Consider the number $P = p_1 p_2 \cdots p_k + 6$, which is congruent to 5 modulo 6. P is not a multiple of any p_i because P is congruent to 6 modulo p_i, while 6 can't be a multiple of p_i. This means, P is the product of several primes of the form $6n+1$, but this means that P is congruent to 1 modulo 6, which leads to contradiction. Therefore, there are an infinite number of primes of the form $6n+5$.

9 [TJ] Exercise 2-30

Assume, to the contrary that there are finitely many primes of the form $4n-1$, and let $p_1 = 3, p_2, \cdots, p_k$ denote them. Every odd prime is either of the form $4n+1$ or $4n-1$. Consider the number $P = 4p_2 p_3 \cdots p_k + 3$, which is congruent to 3 modulo 4. P is not a multiple of any p_i because P is congruent to 3 if $i \ne 1$ or $4p_2 p_3 \cdots p_k$ if $i = 1$, which can't be a multiple of p_i. This means, P is the product of several primes of the form $4n+1$, but this means that P is congruent to 1 modulo 4, which leads to contradiction. Therefore, there are an infinite number of primes of the form $4n-1$.

10 [TJ] Exercise 2-30

Suppose to the contrary that there exists integers p, q such that $p^2 = 2q^2$. By the Fundamental Theorem of arithmetic, p^2 and q^2 can be written as

$$p^2 = \prod_{i=1}^{k} P_i^{2m_i}, \qquad q^2 = \prod_{i=1}^{k} P_i^{2n_i}$$

where P_i is the ith prime, m_i, n_i are nonnegative integers. Since $p^2 = 2q^2$, we have $2m_1 = 2n_1 + 1$, which leads to contradiction. Hence there do not exist such integers p, q.

By rewriting $p^2 = 2q^2$, we know that $\sqrt{2} = p/q$. However, we have proved that there do not exists such integers p, q, so $\sqrt{2}$ is not a rational number.