underGraduate Homework In Mathematics

NumberTheory

白永乐

202011150087

202011150087@mail.bnu.edu.cn

北京师范大学数学科学学院

General fire extinguisher

PROBLEM I Prove that $\forall n \in \mathbb{Z}, 3 \mid n(n+1)(2n+1)$.

SOLUTION. If $n \equiv 0 \mod 3$ then $3 \mid n$. If $n \equiv 1 \mod 3$ then $3 \mid 2n+1$. So no matter what is n mod 3, we can obtain $3 \mid n(n+1)(2n+1)$. $\square$

PROBLEM II Let $a, b \in \mathbb{Z}$ and $b \neq 0$. Prove that there exists a pair of $s, t \in \mathbb{Z}$ such that $a = sb + t \wedge |t| \leq \frac{|b|}{2}$. And if b is odd, then the pair s, t is unique. What if b is even?

SOLUTION. Let $A := \{x \in \mathbb{Z} : \exists y \in \mathbb{Z}, a = yb + x\}$. Since $a = 0b + a$ we know $a \in A$, so $A \neq \emptyset$. By the definition of m we know $\exists s, t \in \mathbb{Z}, |t| = m, a = sb+t$. Then $a = (s-1)b+(t+b), a = (s+1)b+(t-b)$. So by the definition of A we get $t \pm b \in A$. Thus, by the definition of m we get $|t \pm b| \geq |t|$. So we get $||t| - |b|| \geq |t|$. Easily $|t| - |b| < |t|$ since $b \neq 0$, so we get $|b| - |t| \geq |t|$, i.e., $|t| \leq \frac{|b|}{2}$.

Now take $2 \nmid b$, we will prove the uniqueness. Assume there are two pairs $s_1, t_1; s_2, t_2$ satisfy the given condition, then $a = s_1 b + t_1 = s_2 b + t_2$. Then we get $b \mid s_1 b - s_2 b = t_2 - t_1$. Since $(s_1, t_1) \neq (s_2, t_2)$ we easily get $t_1 \neq t_2$. So $|b| \leq |t_1 - t_2|$. Noting $|t_1 - t_2| \leq |t_1| + |t_2| \leq \frac{|b|}{2} + \frac{|b|}{2} = |b|$, we obtain $|t_1| = |t_2| = \frac{|b|}{2}$. But $2 \nmid b$, so $\frac{|b|}{2} \notin \mathbb{Z}$, contradiction!

Now we consider b is even. Take $a \equiv \frac{b}{2} \mod b$, then $a = kb + \frac{b}{2}$ for some $k \in \mathbb{Z}$, and $a = (k+1)b - \frac{b}{2}$. So there is exactly two pairs of (s, t) satisfy the condition. When $a \not\equiv \frac{b}{2} \mod b$, obviously (s, t) is unique. $\square$

PROBLEM III Use Problem II to prove the existence of the greatest common factor of any pair $(x, y) \in \mathbb{Z} \wedge (x, y) \neq (0, 0)$, and find an algorithm to get $\gcd(x, y)$, and find $\gcd(76501, 9719)$ by your algorithm and Euckidean algorithm respectively.

SOLUTION. Without loss of generality assume $|x| \leq |y|$. If $x = 0$ then easily $\gcd(x, y) = |y|$. Now assume $|y| \geq |x| > 0$. Now we prove $\gcd(x, y)$ exists by contradiction, assume for some $x, y \in \mathbb{Z}, |x| \leq |y|$ there is $\gcd(x, y)$ not exists. Let $A := \{x \in \mathbb{Z} : \exists y \in \mathbb{Z}, |y| \geq |x|, \gcd(x, y) \text{not exists}\}$. Then $A \neq \emptyset$. Let $t = \min\{|x| : x \in A\}$. Then by the definition of A we know $\exists s \in \mathbb{Z} \wedge |s| \geq |t|$ such that $\gcd(s, t)$ doesn't exist. Since we have proved $\gcd(0, y)$ exists, we get $t \neq 0$. From Problem II we know there exists $x, y \in \mathbb{Z}$ such that $s = xt + y, |y| \leq \frac{|t|}{2}$. Consider the pair (t, y), we know $|y| < |t|$, so by the definition of t we get $\gcd(t, y)$ exists. So $\gcd(t, y) = \gcd(t, xt + y) = \gcd(s, t)$. Contradict to that $\gcd(s, t)$ doesn't exist. So we get $\forall (x, y) \in \mathbb{Z}^2 \wedge (x, y) \neq (0, 0), \gcd(x, y)$ exists.

From above, we can get following algorithm to get $\gcd(x, y)$:

```c
#include<stdio.h>
int abs(int x){
  return x>0?x:-x;
}
int min_abs_remainder(int y,int x){
  if(x==0){
    return y;
  }
  int r = (y % abs(x) + abs(x)) % abs(x);
  if(r>abs(x)/2){
    return r-abs(x);
  }
  return r;
}
```

```c
//this function is to get the greatest commom factor of two integer.
int gcd(int x,int y){
  if(abs(x)>abs(y)){
//the function int abs(int a) returns the absolute value of a.
    int temp = x;
    x = y;
    y = temp;
  }
  if(x == 0){
    return abs(y);
  }
  int r=min_abs_remainder(y,x);
  int k=(y-r)/x;
  printf("%d &= %d &\\times %d &+ %d\n",y,k,x,r);
  return gcd(x,min_abs_remainder(y,x));
//the return value of function min_abs_remainder is the least-abs remainder of x divide y, which we have proved is less or equal to abs(x)
}
int main(){
  printf("%d",gcd(76501,9719));
  return 0;
}
```

Now we use Euckidean algorithm to get $\gcd(76501, 9719)$.

$$\begin{aligned}
76501 &= 7 &\times 9719 &+ 8468 \\
9719 &= 1 &\times 8468 &+ 1251 \\
8468 &= 6 &\times 1251 &+ 962 \\
1251 &= 1 &\times 962 &+ 289 \\
962 &= 3 &\times 289 &+ 95 \\
289 &= 3 &\times 95 &+ 4 \\
95 &= 23 &\times 4 &+ 3 \\
4 &= 1 &\times 3 &+ 1 \\
3 &= 3 &\times 1 &+ 0
\end{aligned}$$

So $\gcd(76501, 9719) = 1$.

Now we use the new algorithm to get $\gcd(76501, 9719)$.

$$\begin{aligned}
76501 &= & 8 \times 9719 & -1251 \\
9719 &= & (-8) \times (-1251) & -289 \\
-1251 &= & 4 \times (-289) & -95 \\
-289 &= & 3 \times (-95) & -4 \\
-95 &= & 24 \times (-4) & +1 \\
-4 &= & (-4) \times 1 & +0
\end{aligned}$$

So $\gcd(76501, 9719) = 1$. $\square$

PROBLEM IV Assume $f(x) = \sum_{k=0}^{n} a_k x^k \in \mathbb{Z}[x]$ and $a_0, a_n \neq 0$. Prove that if a rational number $\frac{p}{q}, \gcd(p,q) = 1$ is root of f, then $p \mid a_0, q \mid a_n$. Thus, $\sqrt{2} \notin \mathbb{Q}$.

SOLUTION. Since $\frac{p}{q}$ is a root of f, we get $f(\frac{p}{q}) = 0$. So $\sum_{k=0}^{n} a_k (\frac{p}{q})^k = 0$. Multiple q^n, we get $\sum_{k=0}^{n} a_k p^k q^{n-k} = 0$. Mod p, we get $p \mid 0 = \sum_{k=0}^{n} a_k p^k q^{n-k}$. For $k > 0$ we have $p \mid a_k p^k q^{n-k}$, so $p \mid \sum_{k=1}^{n} a_k p^k q^{n-k}$. So $p \mid \sum_{k=0}^{n} a_k p^k q^{n-k} - \sum_{k=1}^{n} a_k p^k q^{n-k} = a_0 q^n$. Since $\gcd(p,q) = 1$, easily $p \mid a_0 q^n \iff p \mid a_0$. So we get $p \mid a_0$. For the same reason easy to get $q \mid a_n$.

Consider $f(x) = x^2 - 2 \in \mathbb{Z}[x]$. Easily $f(\sqrt{2}) = 0$. So if $\sqrt{2} = \frac{p}{q}, \gcd(p,q) = 1$, then we get $p \mid 2, q \mid 1$. Without loss of generality assume $q > 0$, then $q = 1$. Then $\sqrt{2} = \pm 1, \pm 2$. But none of them is root of f, contradiction! $\square$