underGraduate Homework In Mathematics

NumberTheory

王胤雅

201911010205

201911010205@mail.bnu.edu.cn

Beijing Normal University

General fire extinguisher

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

SOLUTION. 1. If $n = 3k, k \in \mathbb{Z}$, then $3|n(n+1)(2n+1)$.

2. If $n = 3k+1, k \in \mathbb{Z}$, then $2n+1 = 2(3k+1)+1 = 6k+3 = 3(2k+1)$, then $3 \mid n(n+1)(2n+1)$.

3. If $n = 3k+2, k \in \mathbb{Z}$, then $n+1 = 3k+3 = 3(k+1)$, then $3 \mid n(n+1)(2n+1)$.

□

PROBLEM II If $a, b \in \mathbb{Z}$, $b \neq 0$, prove: $\exists s, t \in \mathbb{Z}$ s.t.

$$a = bs + t, |t| \leq \frac{|b|}{2}$$

and when b is odd, s, t are unique, how about that b is even?

SOLUTION. First of all, when $b \geq 0$, by Euclidean division, $\exists u, v \in \mathbb{Z}$, s.t. $a = bu + v, 0 \leq v < b$. If $|v| \leq \frac{|b|}{2}$, then $s = u, t = v$. If $\frac{|b|}{2} < v < |b|$, then $s = u+1, t = v-b$, where $|t| \leq \frac{|b|}{2}$. So when $b < 0$, only need to consider $a, -b > 0$, then $\exists p, q \in \mathbb{Z}$, s.t. $a = (-b)p + q = b(-p) + q$, let $s = -p, t = q$.

When b is odd, if $a = bs_1 + t_1 = bs_2 + t_2$, where $|t_1|, |t_2| \leq \frac{|b|}{2}$. Then $|t_1|, |t_2| \leq \frac{|b|-1}{2} < \frac{|b|}{2}$. So $b(s_1 - s_2) = t_2 - t_1$, then $|b| \mid |t_2 - t_1|$. And $|t_1 - t_2| \leq |t_1| + |t_2| < |b|$, then $|t_1 - t_2| = 0$. Thus, $s_1 = s_2, t_1 = t_2$.

When b is even, consider $a = bx + \frac{b}{2} \exists x \in \mathbb{Z}$, then $a = b(x+1) - \frac{b}{2}$. For $a \notin \{bx + \frac{b}{2} : x \in \mathbb{Z}\}$, then $a = bm + n$, where $|n| \leq \frac{|b|}{2}$. Then by the same reason in the situation when b is odd, we can get $\exists \mid s, t$ s.t. $a = bs + t$, where $|t| \leq \frac{|b|}{2}$. □

PROBLEM III Use Problem II to prove $\forall a, b \in \mathbb{Z}, b \neq 0, \exists \gcd(a,b)$, and show its argorithm. Use the argorithm and Euclidean algorithm to compute $\gcd(76501, 9719)$.

SOLUTION. 1. If $a = 0$, then $\gcd(a,b) = b$. If $a \neq 0$, since $\gcd(a,b) = \gcd(|a|,|b|)$, we only need to consider $a, b \in \mathbb{N}^+$. Without loss of generality, assume $a \geq b > 0$, then by Problem II, then $\exists s, t \in \mathbb{Z}$ s.t. $a = bs + t$, where $|t| \leq \frac{b}{2}$. If $t = 0$, then $\gcd(a,b) = b$. If $|t| > 0$, then by $\gcd(a,b) = \gcd(b,|t|)$ and Problem II again, we get $\exists s_1, t_1 \in \mathbb{Z}, |t_1| \leq \frac{|t|}{2}$ such that $b = |t|s_1 + t_1$. Repeat the process above, until it appers that the remainder becomes 0. That is because $t_0 := t$ is finite, and the remainder $t_{k+1} = \frac{t_k}{2}, k \geq 0$. So we will get these equations:

$$\begin{aligned}
&a = bs + t_0, 0 < |t_0| < \frac{|b|}{2},\\
&b = |t_0|s_1 + t_1, 0 < |t_1| < \frac{|t_0|}{2},\\
&|t_0| = |t_1|s_2 + t_2, 0 < |t_2| < \frac{|t_1|}{2},\\
&\cdots\cdots\\
&|t_{n-1}| = |t_n|s_{n+1} + t_{n+1}, 0 < |t_{n+1}| < \frac{|t_n|}{2},\\
&|t_n| = |t_{n+1}|s_{n+2}.
\end{aligned} \tag{1}$$

So we can get $\gcd(a, b) = \gcd(b, |t_0|) = \cdots = \gcd(|t_n|, |t_{n+1}|) = |t_{n+1}|$

2. The argorithm of 1:

```lua
--This function is to find the remainder of two integers x,y, where y is not 0.
--Input: x,y : two integers
--Output: the absoute value of remainder of x,y, whose absoute value is smaller than half of absoute value of y.
local remainder_half = function(x, y)
  if x % y == 0 then
    return 0
  elseif y % 2 ~= 0 then
    if math.abs(x % y) <= math.abs(y) / 2 then
      return math.abs(x % y)
    else
      return math.abs(x % y - y)
    end
  else
    if math.abs(x % y) == math.abs(y) / 2 then
      return math.abs(x % y)
    else
      if math.abs(x % y) < math.abs(y / 2) then
        return math.abs(x % y)
      else
        return math.abs(x % y - y)
      end
    end
  end
end
--This function is to find the maximum common factor of two integels x,y, where x is not 0 or y is not 0.
--Input: x,y: two integels
--Output: gcd(x,y): the maximum common factor of x,y
local function gcd(x, y)
  if math.abs(x) > math.abs(y) then
    local a = x
    x = y
    y = a
  end
  if x == 0 then
    return math.abs(y)
  else
    return gcd(remainder_half(y, x), x)
  end
end
```

3. Two ways to compute the $\gcd(76501, 9719)$:

(a) Use the argorithm in 1

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

(b) Use Euclidean algorithm:

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

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

□

PROBLEM IV Let $F(x) = \sum_{k=0}^{n} a_k x^n \in \mathbb{Z}[x]$, where $a_0, a_n \neq 0$. Then reasonable root $\frac{p}{q}$ of $F(x)$ must satisfiy that $p|a_0, q|a_n, \gcd(p,q) = 1$. Therefore, $\sqrt{2}$ is not reasonable.

SOLUTION. Since $F(\frac{p}{q}) = \sum_{k=0}^{n} a_k (\frac{p}{q})^k = 0$, then $\sum_{k=0}^{n} a_k p^k q^{n-k} = 0$. Then $-a_n p^n = \sum_{k=0}^{n-1} a_k p^k q^{n-k} = p(\sum_{k=1}^{n-1} a_k p^{k-1} q^{n-k}) + a_0 q^n = q(\sum_{k=0}^{n-1} a_k q^{n-k-1} p^k)$. Since $\gcd(p,q) = 1$, then $q \mid a_n, p \mid a_0$. Since $F(x) = x^2 - 2$ s.t. $F(\sqrt{2}) = 0$. If $\sqrt{2}$ is reasonable, then $\sqrt{2} = \frac{p}{q}$. Thus, $p \mid 2, q \mid 1$, so $\sqrt{2} = 2, 1$, which is contradict with the define of $\sqrt{2}$! □