underGraduate Homework In Mathematics

NumberTheory 1

王胤雅

201911010205

201911010205@mail.bnu.edu.cn

2024 年 2 月 25 日

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 $3 \mid n(n+1)(2n+1)$.

$\square$

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 $|t| \leq \frac{|b|}{2}$. $\square$

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:

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