113 Class Problems: Integer Arithmetic

1. Does the cancellation law hold in $\mathbb{Z}/15\mathbb{Z}$? Does it hold in $\mathbb{Z}/7\mathbb{Z}$? Carefully justify your answers.

   Solution:

$[3], [5] \neq [0]$ in $\mathbb{Z}/15\mathbb{Z}$

$[3][5] = [15] = [0] = [3][0]$, however $[5] \neq [0]$

7 prime $\Rightarrow$ $\big([c] \neq [0] \Rightarrow \exists [u] \in \mathbb{Z}/7\mathbb{Z}$ such that $[u][c] = [1]\big)$

If $[a], [b], [c] \in \mathbb{Z}/7\mathbb{Z}$ such that $[c] \neq [0]$

$[a][c] = [b][c] \Rightarrow [a][c][u] = [b][c][u] \Rightarrow [a][1] = [b][1] \Rightarrow [a] = [b]$

2. Is the converse of Euclid's Lemma true? More precisely, if $p \in \mathbb{N}$ such that

$$\forall a, b \in \mathbb{Z},\ p|ab \Rightarrow p|a \text{ or } p|b,$$

   must it be true that p is prime? Carefully justify your answer.

   Solution:

Assume p is composite. Hence $\exists a, b \in \mathbb{N}$ such that $p = ab$, $p < a, p < b$

So p / ab , but $p \nmid a$ and $p \nmid b$.

Hence the converse of Euclid's Lemma is true

3. Why do we not define $1 \in \mathbb{N}$ to be prime?

   Solution:

1 is not a prime because the uniqueness of prime factorization would no longer hold.

4. Let $p \in \mathbb{N}$ be prime. Prove that $\sqrt[2]{p}$ is irrational. Is the same true for all $\sqrt[n]{p}$, where $n > 1$? Carefully justify your answers.

Solution:

Given $c \in \mathbb{N}$, Let $v_p(c) =$ number of times p divides c

For example $v_3(\underbrace{36}_{3^2 \cdot 2^2}) = 2$

Assume $\sqrt[2]{p} = \frac{a}{b}$ with $a, b \in \mathbb{N}$

$\Rightarrow \quad p = \frac{a^2}{b^2} \quad \Rightarrow \quad a^2 = p b^2$

$v_p(a^2) \equiv 0 \mod 2$, $v_p(pb^2) \equiv 1 \mod 2$

This contradicts the FTOA.

Assume $\sqrt[n]{p} = \frac{a}{b}$ with $a, b \in \mathbb{N}$

$\Rightarrow \quad p = \frac{a^n}{b^n} \quad \Rightarrow \quad a^n = p b^n$

$v_p(a^n) \equiv 0 \mod n$, $v_p(p b^n) \equiv 1 \mod n$

This contradicts the FTOA.