MATH 465 NUMBER THEORY, SPRING TERM 2025, SOLUTIONS 1

1. Let $a, b, c \in \mathbb{Z}$. Prove each of the following.
(i) If $a|b$ and $b|c$, then $a|c$. (ii) If $a|b$, then $ac|bc$. (iii) If $ac|bc$ and $c \neq 0$, then $a|b$. (iv) If $a|b$ and $a|c$, then $a|bx + cy$ for all $x, y \in \mathbb{Z}$.

(i) We have $b = am$, $c = bn$. By substitution, $c = bn = a(mn)$. (ii) We have $b = am$. Hence $bc = acm$. (iii) We have $bc = acm$. Since $c \neq 0$ it can be cancelled. (iv) We have $b = am$, $c = an$. Therefore $bx + cy = amx + any = a(mx + ny)$.

2. Define the integer sequence a_n, $n \in \mathbb{N}$ by $a_1 = 1 = a_2 = 1$ and

$$a_{n+2} = 3a_{n+1} - a_n.$$

Prove that if $m|a_{n+1}$ and $m|a_n$ for some $n \in \mathbb{N}$, then $m = 1$.

Proof by induction on n. First suppose that $n = 1$. We have $m|a_1 = 1$ so $m = 1$. Now assume that for a given n if $m|a_n$ and $m|a_{n+1}$, then $m = 1$. If $m|a_{n+1}$ and $m|a_{n+2}$, then $m|(a_{n+2} - 3a_{n+1}) = a_n$. Hence $m|a_n$ and $m|a_{n+1}$, so on the inductive hypothesis $m = 1$.

3. Prove that for every $n \in \mathbb{Z}$ we have $3|n^3 - n$.

Proof. By the division algorithm $n = 3q + r$ with $r = 0, 1$ or 2. Thus $n^3 - n = (3q + r)^3 - 3q - r = 3(9q^3 + 9q^2r + 3qr^2 - q) + r^3 - r$. Morever $r^3 - r = 0, 0, 6$ accoridng as $r = 0, 1, 2$ and so is also a multiple of 3.

4. (i) Show that if $4|m - 1$ and $4|n - 1$, then $4|mn - 1$.
(ii) Show that if $m, n \in \mathbb{N}$, and $4|mn + 1$, then either $4|m + 1$ or $4|n + 1$.
(iii) Show that if $4|n + 1$, then there is a prime number p with $p|n$ and $4|p + 1$.
(iv) Show that there are infinitely many primes p such that $4|p + 1$.

(i) We have $m - 1 = 4k$, $n - 1 = 4l$ for some integers k, l, and $mn = (4k + 1)(4l + 1) = 16kl + 4k + 4l + 1 = 4(4kl + k + l) + 1$. (ii) m, n must be odd so are of the form $4k \pm 1$. If both are of the form $4k + 1$, then by (i) their product cannot be of the form $4k - 1$. (iii) All the prime factors of $4k - 1$ are odd, and so of the form $4k \pm 1$. If they were all of the form $4k + 1$, then by repeated use of (i), as in (ii), it would follow that their product is of wrong form. Hence at least one of them must be of the form $4k - 1$. (iv) Suppose that there are only a finite number of primes of the form $4k - 1$, say $p_1, p_2, \ldots, p_r$. Let $n = 4p_1 \ldots p_r - 1$. Obviously $n > 1$ and so by (iii) will have at least one prime factor p of the form $4k - 1$. But then $p|p_1 \ldots p_r$. Hence $p|4p_1 \ldots p_r - n = 1$ which is impossible.