Weekly Puzzle - Solutions

Number Theory

Thomas Winrow-Campbell

17/11/2024 - 24/12/2024

Questions:

Modular arithmetic:

1. (a) $\{x \mid x = 5n + 2, n \in \mathbb{Z}\}$.

   (b) This means $a_1 = b_1 + k_1 m$ and $a_2 = b_2 + k_2 m$, where $k_1, k_2 \in \mathbb{Z}$. Therefore, $a_1 + a_2 = b_1 + k_1 m + b_2 + k_2 m = b_1 + b_2 + (k_1 + k_2)m$. Let $k = k_1 + k_2$, so $k \in \mathbb{Z}$. Then $a_1 + a_2 = b_1 + b_2 + km$, so $a_1 + a_2 \equiv b_1 + b_2 \,(mod\, m)$.

   (c) $a \equiv b \,(mod\, m)$ means $a = b + cm$, where $c \in \mathbb{Z}$. Then, $ka = kb + kcm$. As $kc \in \mathbb{Z}$, therefore $ka \equiv kb \,(mod\, m)$.

   (d) $a = b + cm$, then $a^k = (b + cm)^k$.
   Using the binomial theorem, then $a^k = \sum_{i=0}^{k} \binom{k}{i} b^{k-i} (cm)^i$.
   The only term where $\binom{k}{i} b^{k-i} (cm)^i$ would not necessarily be divisible by cm is when $i = 0$, and so this term would be b^k. So, $a^k = b^k + dm$, where $d \in \mathbb{Z}$, so $a^k \equiv b^k \,(mod\, m)$.

   (e) From the previous part, $a \equiv b \,(mod\, m)$ implies $a^k \equiv b^k \,(mod\, m)$, where $k \in \mathbb{Z}^+$. So as $11 \equiv 1 \,(mod\, 10)$, then $11^{1000} \equiv 1^{1000} \,(mod\, 10)$, so $11^{1000} \equiv 1 \,(mod\, 10)$, so the last digit is 1.

   (f) From part (d), $12^{1000} \equiv 2^{1000} \,(mod\, m)$.
   We notice that by increasing the power of 2^i, where $i \in \mathbb{Z}^+$, we seem to have a repeating pattern of $2, 4, 8, 6$.
   However, this is not a proof, so we can use induction to show that the final digit of 2^{4i} is 6, where $i \in \mathbb{Z}^+$.
   However, this can be made simpler, $2^{4i} \equiv 16^i \equiv 6^i \,(mod\, 10)$.
   Base case: $6^1 \equiv 6 \,(mod\, 10)$, so this is correct.
   If it is true for $i = k$, then $6^k \equiv 6 \,(mod\, 10)$, so $6^{k+1} \equiv 36 \equiv 6 \,(mod\, 10)$, so it is true for $i = k + 1$.
   Therefore, by mathematical induction, the statement that $6^i \equiv 6 \,(mod\, 10)$ is true for all $i \in \mathbb{Z}^+$. As $4 \mid 1000$, then the last digit of 2^{1000} is 6.

   (g) We can represent an integer as a series of digits, from the least significant digit to the most significant digit as the digits a_i, starting from $i = 0$ where the number has n digits.
   This means the number 123 would have $a_0 = 3$, $a_1 = 2$, $a_2 = 1$ and $n = 3$.
   A number in this format is equal to $\sum_{i=0}^{n-1} a_i \times 10^i$. From part (d), when $i \geq 1$, then
   $10^i \equiv 1^i \equiv 1 \,(mod\, 9)$. So then $\sum_{i=0}^{n-1} a_i \times 10^i \equiv \sum_{i=0}^{n-1} a_i \,(mod\, 9)$. We have therefore proven it.

Irrationality:

2. (a) Suppose $\log_2 3$ is rational, so $\log_2 3 = \frac{a}{b}$, where $a, b \in \mathbb{Z}$ and $b \neq 0$.
Then, $2^{\frac{a}{b}} = 3$, so $2^a = 3^b$. As $3 > 1$, we know that $\log_2 3$ is positive, so we can say both $a, b \in \mathbb{Z}^+$. Therefore, 2^a is even, and 3^b is odd. However, as an even number cannot equal an odd number, then $2^a \neq 3^b$, so we have a contradiction, so our original assumption was wrong and so $\log_2 3$ is irrational.

   (b) Suppose $\sqrt{2}$ is rational, so $\sqrt{2} = \frac{a}{b}$, where $a, b \in \mathbb{Z}$ and $b \neq 0$, and we shall say that $\frac{a}{b}$ is in its lowest form. So $\frac{a^2}{b^2} = 2$. Therefore $a^2 = 2b^2$. So, a^2 is even, and therefore a is even. If a is even, then $a = 2c$. So $4c^2 = 2b^2$, so $b^2 = 2c^2$, so b is even. However, as $\frac{a}{b}$ is in its lowest form, then both a and b cannot be even, so we have a contradiction. So $\sqrt{2}$ is irrational.

   (c) If $a^2 = 4b^2$, this does not imply that a is a multiple of 4. For example, $2^2 = 4 \times 1^2$, but 2 is not a multiple of 4.

Prime numbers:

3. (a) Suppose there is a largest prime number. Then we can write the finite set of prime numbers with elements p_i. But, then the number $1 + \prod_i p_i$ is not divisible by any p_i, so this is a new largest prime number. So, there is no largest prime number.

   (b) As we need to prove it for all integers x, we need to use induction twice, one with an ascending inductive step, and one with a descending inductive step.

   If $x = 0$, then $x^p = 0 = x \,(mod\, p)$, so the statement is true for $x = 0$.

   If it is true for $x = k$, then $k^p \equiv k \,(mod\, p)$.
   Let a be an integer.
   $(k + a)^p = \sum_{i=0}^{p} \binom{p}{i} k^i \times a^{p-i}$
   If $1 \leq i \leq n-1$, then $\binom{p}{i} = \frac{p!}{i!(p-i)!}$. As p is prime, it divides the numerator but not the denominator, so the only two terms left in the sum are k^p and a^p, so $(k + a)^p \equiv k^p + a^p \equiv k + a^p \,(mod\, p)$.

   If $a = 1$, then $(k + 1)^p \equiv k + 1^p \equiv k + 1 \,(mod\, p)$, so the statement is true for $x = k + 1$. If $a = -1$, then $(k - 1)^p \equiv k + (-1)^p \,(mod\, p)$.
   If p is odd, then $(k - 1)^p \equiv k + (-1)^p \equiv k - 1 \,(mod\, p)$. If p is even, then p is 2, so $(k - 1)^p \equiv k + (-1)^2 \equiv k + 1 \equiv k - 1 \,(mod\, p)$, so the statement is true for $x = k - 1$.

   As the statement is true for $x = 0$, and if it is true for $x = k$, then it is true for $x = k + 1$ and $x = k - 1$, then by mathematical induction the statement is true for all $x \in \mathbb{Z}$.

   (c) $a^p - 1 = (a - 1)(a^{p-1} + a^{p-2} + \cdots + a + 1)$. If $a^p - 1$ is prime, then the only two factors are 1 and $a^p - 1$. So $a - 1 = 1$ or $a - 1 = a^p - 1$. So $a = 2$ or $a = a^p$. As $a \neq 0$ and $a \neq 1$, otherwise $a^p - 1$ is not prime, then for $a = a^p$ to be true, $p = 1$. So either $a = 2$ or $p = 1$.

   (d) The contrapositive of the statement is that if p is not prime, then $2^p - 1$ is not prime. Suppose $p = ab$, where a and b are factors which are not 1. Then $2^p - 1 = 2^{ab} - 1$. As $x - y \mid x^n - y^n$, then $2^a - 1 \mid 2^{ab} - 1$ and $2^b - 1 \mid 2^{ab} - 1$, so as $a \neq 1$ and $b \neq 1$, then $2^a - 1 \neq 1$ and $2^b - 1 \neq 1$, so $2^p - 1$ is not prime. Therefore, by the law of contrapositives, if $2^p - 1$ is prime, then p is prime.