Weekly Puzzle
Number Theory

Thomas Winrow-Campbell

17/11/2024 - 24/12/2024

What you need to know:

We shall use the notation $a|b$ to mean a is a divisor of b. The definition of $x \equiv y\,(mod\,m)$ is that $m|(x-y)$.

Questions:

Modular arithmetic:

1. (a) What is the set of all x satisfying $x \equiv 2\,(mod\,5)$?

   (b) Prove that if $a_1 \equiv b_1\,(mod\,m)$ and $a_2 \equiv b_2\,(mod\,m)$, then $a_1 + a_2 \equiv b_1 + b_2\,(mod\,m)$.

   (c) Prove that if $a \equiv b\,(mod\,m)$ then $ka \equiv kb\,(mod\,m)$.

   (d) Prove that if $a \equiv b\,(mod\,m)$ then $a^k \equiv b^k\,(mod\,m)$.

   One can calculate the last digit of an integer, n, by calculating what $n\,(mod\,10)$ is.

   (e) $11 \equiv 1\,(mod\,10)$, so what is the last digit of 11^{1000}?

   (f) What is the last digit of 12^{1000}?

   (g) Prove that a number is divisible by 9 if and only if the sum of its digits is also divisible by 9.

Irrationality:

2. (a) Prove that $\log_2 3$ is irrational. (Hint: proof by contradiction.)

   (b) Prove that $\sqrt{2}$ is irrational.

   (c) Why does a similar proof not work for $\sqrt{4}$?

Prime numbers:

3. (a) Prove there is no largest prime number.

   Fermat's little theorem states that if p is a prime number, then for any integer x, $x^p \equiv x\,mod\,p$.

(b) Prove Fermat's little theorem. (Hint: proof by induction.)

When massive primes are found, they are often Mersenne numbers, which are integers of the form $2^n - 1$, where n is an integer. A Mersenne prime is a number with is both a Mersenne number and a prime number.

(c) Suppose a and p are positive integers. Prove that if $a^p - 1$ is prime, then either $a = 2$ or $p = 1$.

(d) Prove that if $2^p - 1$ is prime, then p is prime. (Hint: contrapositive.)

©2024 Thomas Winrow-Campbell