NUMBER THEORY (11/16/22)

Warm-up

If these are too easy, try thinking about possible other approaches to the problems.

1. Let (x, y, z) be a solution to $x^2 + y^2 = z^2$. Show that one of the three numbers is divisible (a) by 3 (b) by 4 (c) by 5.

2. The next to last digit of 3^n is even.

3. Show that for every n, n does not divide $2^n - 1$.

4. For any n, 2^n does not divide $n!$. (Extra question: can you find all n such that 2^{n-1} divides $n!$)

Actual competition problems

5. (2006-A3) Let $1, 2, 3, \ldots, 2005, 2006, 2007, 2009, 2012, 2016, \ldots$ be a sequence defined by $x_k = k$ for $k = 1, \ldots, 2006$ and $x_{k+1} = x_k + x_{k-2005}$ for $k \geq 2006$. Show that the sequence has 2005 consecutive terms each divisible by 2006.

6. (2005-A1) Show that every positive integer n is a sum of one or more numbers of the form $2^r 3^s$, where r and s are non-negative integers and no summand divides another. (For example, $23 = 9 + 8 + 6$.)

7. (2014-B3) Let A be an $m \times n$ matrix with rational entries. Suppose that there are at least $m + n$ distinct prime numbers among the absolute values of the entries of A. Show that the rank of A is at least 2.

8. (2013-A2) Let S be the set of all positive integers that are not perfect squares. For n in S, consider choices of integers $a_1, a_2, \ldots, a_r$ such that

$$n < a_1 < a_2 < \cdots < a_r$$

and $n \cdot a_1 \cdot a_2 \cdots a_r$ is a perfect square, and let $f(n)$ be the minimum of a_r over all such choices. For example, $2 \cdot 3 \cdot 6$ is a perfect square, while $2 \cdot 3$, $2 \cdot 4$, $2 \cdot 5$, $2 \cdot 3 \cdot 4$, $2 \cdot 3 \cdot 5$, $2 \cdot 4 \cdot 5$, and $2 \cdot 3 \cdot 4 \cdot 5$ are not, and so $f(2) = 6$. Show that the function f from S onto the integers is one-one (injective).

9. (1997-B5) Define $d(n)$ for $n \geq 0$ recursively by $d(0) = 1$, $d(n) = 2^{d(n-1)}$. Show that for every $n \geq 2$,

$$d(n) \equiv d(n-1) \mod n.$$

A few important facts from number theory

Standard Conventions. $a|b$ means 'a divides b', $a \equiv b \mod n$ means 'a is congruent to b modulo n, that is, $n|(a-b)$ (or equivalently, a and b have the same remainder when divided by n).

Fermat's Little Theorem. If a is not divisible by a prime p, then $a^{p-1} \equiv 1 \mod p$. (Version: for any a and any prime p, $a^p \equiv a \mod p$.)

Euler's Theorem. For any number n, let $\phi(n)$ be the number of integers between 1 and n that are coprime to n. Then for any a that is coprime to n, $a^{\phi}(n) \equiv 1 \mod n$.

Suppose a rational number b/c is a solution of the polynomial equation $a_n x^n + \cdots + a_0 = 0$ whose coefficients are integers. Then $b|a_0$ and $c|a_n$, assuming b/c is reduced.

A number $n \geq 1$ can be written as a sum of two squares if and only if every prime p of the form $4k+3$ appears in the prime factorization of n an even number of times.