NUMBER THEORY (10/25/23)

Warm-up

1. What is the last digit of the 2023-rd Fibonacci number? (The Fibonacci sequence is defined by $a_1 = a_2 = 1$, and then $a_{k+2} = a_k + a_{k+1}$.)

2. The last 2023 digits of an integer a are the same as the last 2023 digits of a^2. How many possibilities are there for these 2023 digits?

Actual competition problems

3. (2010-A1) Given a positive integer n, what is the largest k such that the numbers $1, 2, \ldots, n$ can be put into k boxes so that the sum of the numbers in each box is the same? [When $n = 8$, the example $\{1, 2, 3, 6\}, \{4, 8\}, \{5, 7\}$ shows that the largest k is *at least* 3.]

4. (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.

5. (2009-B1) Show that every positive rational number can be written as a quotient of products of factorials of (not necessarily distinct) primes. For example,

$$\frac{10}{9} = \frac{2! \cdot 5!}{3! \cdot 3! \cdot 3!}$$

6. (2008-A3) Start with a finite sequence $a_1, a_2, \ldots, a_n$ of integers. If possible, choose two indices $j < k$ such that a_j does not divide a_k, and replace a_j and a_k by $\gcd(a_j, a_k)$ and $\operatorname{lcm}(a_j, a_k)$ respectively. Prove that if this process is repeated, it must eventually stop and the final sequence does not depend on the choices made. (Note: gcd means greatest common divisor and lcm means least common multiple.)

7. (2009-B3) Call a subset S of $\{1, 2, ..., n\}$ *mediocre* if it has the following property: Whenever a and b are elements of S whose average is an integer, that average is also an element of S. Let $A(n)$ be the number of mediocre subsets of $\{1, 2, ..., n\}$. [For instance, every subset of $\{1, 2, 3\}$ except $\{1, 3\}$ is mediocre, so $A(3) = 7$.] Find all positive integers n such that

$$A(n + 2) - 2A(n + 1) + A(n) = 1.$$

8. (2008-B4) Let p be a prime number. Let $h(x)$ be a polynomial with integer coefficients such that $h(0), h(1), ..., h(p^2 - 1)$ are distinct modulo p^2. Show that $h(0), h(1), ..., h(p^3 - 1)$ are distinct modulo p^3.

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).

The Chinese Remainder Theorem. If m and n are coprime, then for any a and b there exists a number x such that

$$\begin{cases} x \equiv a \mod m \\ x \equiv b \mod n, \end{cases}$$

moreover, x is unique modulo mn.

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.

If $p(x)$ is a polynomial with integer coefficients, then for any integers a and b, $(b-a)|(p(b)-p(a))$.

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.

Hints (by problem)

1. The sequence of last digits will be periodic.

2. Solve the congruence $a^2 \cong a \mod 10^{2023}$; the Chinese Remained Theorem helps.

3. Just try to make the sum in each box as small as possible.

4. Consider the sequence modulo 2006 and show that it is periodic. Then look back in time.

5. Think in terms of the prime factorization, and eliminate primes one by one.

6. Somewhat similar to the previous problem: what happens to the factorization of the numbers?

7. The left-hand side looks oddly specific. What is its meaning?

8. Note that $h(k)$ and $h(k+p)$ are the same modulo p. When are they distinct modulo p^2? (It may be easier to start with $k=0$.)

9. Mostly, this is Euler's Theorem, but you have to be careful with the details.