Putnam Club. Fall 2020

Problem session for September 30. Number theory-1.

Here are some general number theory problems that I want to discuss on our next meeting on Sep 30. They are of the different level of difficulty and on the different ideas, so enjoy!

1. Prove that equation $m^2 = n^5 - 4$ has no integer solutions.
2. Solve equation in the positive integers: $x^x = y^{3y}$.
3. We have a deck of $2n$ cards. Each shuffling changes the order from $a_1, a_2, \ldots, a_n, b_1, b_2, \ldots, b_n$ to $a_1, b_1, a_2, b_2, \ldots, a_n, b_n$. Determine all even numbers $2n$ such that after shuffling the deck 8 times the original order is restored.
4. Let p, q be relatively prime positive integers. Prove that
$$\sum_{k=0}^{pq-1} (-1)^{\left\lfloor \frac{k}{p} \right\rfloor + \left\lfloor \frac{k}{q} \right\rfloor} = \begin{cases} 0 & \text{if } pq \text{ is even} \\ 1 & \text{if } pq \text{ odd} \end{cases}$$
5. Let $P(x)$ be a polynomial with integer coefficients. Assume that the equation $P(x) = x$ does not have any integer roots. Prove that then the equation $P(P(P(x))) = x$ does not have any integer roots either.
6. Let p be a prime number. Call a positive integer n interesting if
$$x^n - 1 = (x^p - x + 1)f(x) + pg(x)$$
for some polynomials f and g with integer coefficients.
   a) Prove that the number $p^p - 1$ is interesting.
   b) For which p is $p^p - 1$ the minimal interesting number?

A few important facts from number theory

Standard Conventions. $a|b$ means 'a divides b', $a \equiv b \pmod{n}$ 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). 'gcd(a,b)' is a greater common divider of a and b ; a and b are coprime if $gcd(a, b) = 1$.

The Chinese Remainder Theorem. If m and n are coprime, then for any a and b there exists a number x such that
$$\begin{cases} x \equiv a \pmod{m} \\ x \equiv b \pmod{n} \end{cases}$$
moreover, x is unique modulo mn.

Wilson's Theorem. If p is a prime, then $p|(p-1)! + 1$

Fermat's Little Theorem. For any a and any prime p, $a^p \equiv a \pmod{p}$.

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, $a^{\phi(n)} \equiv 1 \pmod{n}$.

Suppose a rational number b/c is a solution of the polynomial equation $a_n x^n + \ldots + a_0 = 0$ 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.