Number Theory 2

Ilqar Ramazanli
February 11, 2018

Definitions

We say that a has order d modulo m, denoted by $ord_m(a) = d$, if d is the smallest positive integer such that $a^d \equiv 1$ (mod m).

Problems

These problems are from "104 Number Theory Problems" by D. Andrica, T. Andreescu, Z. Feng.

1. Let p be a prime with $p > 5$. Prove that $p^8 \equiv 1$ mod 240.

2. (Fermat?s Little Theorem) Let a be a positive integer and let p be a prime. Prove that $a^p \equiv$ a mod p.

3. (Euler's Theorem) Let a and m be relatively prime positive integers. Then $a^{\phi(m)} \equiv 1 \pmod{m}$.

4. Let p be a prime. Prove that p divides $ab^p - ba^p$ for all integers a and b.

5. Let $p \geq 7$ be a prime. Prove that the number $11 \cdots 1$ (p-1 times 1) is divisible by p

6. Prove that for any even positive integer n, $n^2 - 1$ divides $2^{n!} - 1$.

7. (IMO 2005) Consider the sequence $a_1, a_2, ...$ defined by $a_n = 2^n + 3^n + 6^n - 1$ for all positive integers n. Determine all positive integers that are relatively prime to every term of the sequence.

8. (IMO 2003 shortlist) Determine the smallest positive integer k such that there exist integers $x_1, x_2, \ldots, x_k$ with ${x_1}^3 + {x_2}^3 + \cdots + {x_k}^3 = 2002^{2002}$.

9. A positive integer x is such that $a^x \equiv 1$ mod m if and only if x is a multiple of the order of a modulo m.

Solutions

1. Equivalently, we can show that $p^8 - 1$ is a multiple of 16, 3, and 5. Factor
$$p^8 - 1 = (p-1)(p+1)(p^2+1)(p^4+1).$$
Since p is odd, each term is even, so $16 \mid p^8 - 1$. Since $p \equiv \pm 1 \pmod 3$, one of the first two terms is a multiple of 3. If $p \equiv \pm 1 \pmod 5$ then one of the first two terms is a multiple of 5. Otherwise, $p^2 + 1$ is a multiple of 5.

   Note: by being more careful, we can even show that $p^4 - 1$ is a multiple of 240. Do you see how?

2. Google it.

3. Google it.

4. $ab^p - ba^p = ab(b^{p-1} - a^{p-1})$. If a or b is a multiple of p, we are done. Otherwise, b^{p-1} and a^{p-1} are both congruent to 1 (mod p), so $b^{p-1} - a^{p-1}$ is a multiple of p.

5. $11 \cdots 1 = \frac{1}{9} 99 \cdots 9 = \frac{10^{p-1}-1}{9}$. Since 10 is relatively prime to p, by Fermat's little theorem, $10^{p-1} \equiv 1 \pmod{p}$. Thus the numerator is a multiple of p, and 9 is relatively prime to p, so the whole number is a multiple of p.

6. Since n is even, $n+1$ and $n-1$ are relatively prime. Since $n^2-1=(n+1)(n-1)$, we need to show that each of them divides $2^{n!}-1$. Equivalently, we need to show that $2^{n!} \equiv 1 \pmod{n-1}$ and $2^{n!} \equiv 1 \pmod{n+1}$.

   Note that $\phi(n+1) \leq n$, so $\phi(n+1) \mid n!$. By Euler's theorem $2^{\phi(n+1)} \equiv 1 \pmod{n+1}$. Furthermore, $2^{n!}$ is a perfect power of $2^{\phi(n+1)}$, so also $2^{n!} \equiv 1 \pmod{n+1}$.

   The proof for $n-1$ is similar.

7. We have
$$6a_n = 6 \cdot 2^n + 6 \cdot 3^n + 6 \cdot 6^n - 6 = 3 \cdot 2^{n+1} + 2 \cdot 3^{n+1} + 6^{n+1} - 6$$
   For any prime p, let $n = p-2$ so that $n+1 = p-1$. By Fermat's little theorem, we have
$$2^{n+1} \equiv 3^{n+1} \equiv 6^{n+1} \equiv 1 \pmod{p},$$
   so we have $p \mid 6a_n$. If $p \neq 2, 3$ we have $p \mid a_n$. Note also that $a_2 = 48$ which is a multiple of 2 and 3, so every prime divides some term of the sequence. Thus any number with any prime factor cannot be relatively prime to each number in the sequence, so the only remaining positive integer is 1.

8. Let $M = 2002^{2002}$. Cubes are $0, 1, 8$ or $9 \pmod{16}$, and $M \equiv 0 \pmod{8}$. If $k < 4$, then equating the two sides mod 16 we see that all the a_i are even. Thus we can divide both sides by 16, and we have that $\frac{M}{8}$ is a a sum of k perfect cubes. Repeating this 499 more times, we have that $\frac{M}{2^{2000}} = 4 \cdot 1001^{2002}$ is a sum of k cubes. We have $1001^2 \equiv 1 \pmod{9}$ so $1001^{2002} \equiv 1 \pmod{16}$. Thus $\frac{M}{2^{2000}} \equiv 4 \pmod{16}$, but this is impossible if M is a sum of fewer than 4 cubes.

   We can solve this with $k = 4$, for example with $a_1 = a_2 = 10 \cdot 2002^{667}$ and $a_3 = a_4 = 2002^{667}$.

9. Omitted.