Number Theory 1

Ilqar Ramazanli

January 28, 2018

Definition

A *complete set of residue classes in mod m* is a set of numbers $\{a_0, a_1, \ldots, a_{m-1}\}$ such that for all $i = 0, 1, \ldots, m-1$ we have $a_i \equiv i \pmod{m}$.

Problems

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

1. Find a positive integer n such that the 1000 integers in $\{n, n+1, n+2, \ldots, n+999\}$ are all composite.
2. Prove that there are infinitely many prime numbers.
3. Prove that for positive integers m and n, there exist integers x and y such that $mx+ny = \gcd(m,n)$.
4. Compute the probability that a randomly chosen positive divisor of 10^{99} is an integer multiple of 10^{88}.
5. Determine the product of distinct positive integer divisors of $n = 420^4$
6. Prove that for any positive integer n, $\tau(n) \leq 2\sqrt{n}$ where τn represents number of divisors of n.
7. Find the sum of even positive divisors of 10000.
8. Let a be an odd integer. Prove that $a^{2^n} + 2^{2^n}$ and $a^{2^m} + 2^{2^m}$ are relatively prime for all positive integers n and m with $n \neq m$.
9. Let m be a positive integer, and let a and b be integers relatively prime to m. If x and y are integers such that $a^x \equiv b^x$ (mod m) and $a^y \equiv b^y$ (mod m), then $a^{\gcd(x,y)} \equiv b^{\gcd(x,y)}$ (mod m).
10. Let m be an even positive integer. Assume that $\{a_1, a_2, ..., a_m\}$ and $\{b_1, b_2, ..., b_m\}$ are two complete sets of residue classes modulo m. Prove that $\{a_1+b_1, a_2+b_2, ..., a_m+b_m\}$ is not a complete set of residue classes.
11. Let a be a positive integer. Determine all the positive integers m such that $\{1 \cdot a, 2 \cdot a, 3 \cdot a, ..., m \cdot a\}$ is a set of complete residue classes modulo m.
12. Let m be a positive integer. Let a be an integer relatively prime to m, and let b be an integer. Assume that S is a complete set of residue classes modulo m. Prove that the set

$$T := aS + b := \{as + b | s \in S\}$$

is also a complete set of residue classes modulo n.

13. (Wilson?s Theorem) Prove that for any prime p, $(p-1)! \equiv -1$ (mod p).
14. (IMO 2005) Let $a_1, a_2, \cdots$ be a sequence of integers with infinitely many positive and negative terms. Suppose that for every positive integer n the numbers $a_1, a_2, \cdots, a_n$ leave n different remainders upon division by n. Prove that every integer occurs exactly once in the sequence $a_1, a_2, \cdots$

Solutions

1. Let $m = 1001!$. Then $k \mid m + k$ for $k = 2, 3, \ldots, 1001$, so we can take $n = m + 2 = 1001! + 2$.

2. For a few different proofs, look at the Wikipedia page for "Euclid's Theorem".

3. Look at the wikipedia page for "Bezout's Identity".

4. $10^{99} = 2^{99}5^{99}$, so 10^{99} has $(99+1)(99+1) = 10000$ divisors. If n is a divisor of 10^{99} which is also a multiple of 10^{88}, we can write $n = 10^{88}k$ where k is a divisor of $\frac{10^{99}}{10^{88}} = 10^{11}$. So the number of n is the number of divisors of $10^{11} = 2^{11}5^{11}$, which is $(11+1)(11+1) = 144$. The probability is $\frac{144}{10000} = \frac{9}{625}$.

5. The product of distinct positive integer divisors of n, in general, is $n^{k/2}$, where k is the number of divisors of n. Since $n = 420^4 = 2^8 3^4 5^4 7^4$, its number of positive integer divisors are $(8+1)(4+1)(4+1)(4+1) = 9 \cdot 5 \cdot 5 \cdot 5 = 1125$. So our answer is $420^{4 \cdot 1125/2} = 420^{2250}$.

6. We note that for every pair of numbers that multiply to n, one of them must be less than $\sqrt{n}$ and one must be greater than $\sqrt{n}$. There are exactly $\sqrt{n}$ numbers that are less than $\sqrt{n}$, and each of them can pair up with at most one other number to multiply to n. So the total number of positive divisors must be less than $\sqrt{n} + \sqrt{n} = 2\sqrt{n}$.

7. Each even divisor of 10000 can be written as $2k$ where k is a divisor of 5000. The sum of the divisors of $5000 = 2^3 5^4$ is $(1+2+4+8)(1+5+25+125+625) = 11715$. Thus the sum of the even divisors of 10000 is $2 \cdot 11715 = 23430$.

8.

9.

10. We look at the total sum of $\{a_1, ..., a_m\}$ and show that it is not congruent to the sum of $\{a_1 + b_1, ..., a_m + b_m\}$ (mod m). Since $\{a_1, ..., a_m\}$ is a complete set of residue classes, it has the numbers $\{0, 1, ..., m-1\}$. Adding all of these up gives $(m^2 - m)/2$. Looking at $\{a_1 + b_1, ..., a_m + b_m\}$, this yields $(m^2 - m)$. We note that since m is even, we can write $m = 2k$ for some positive integer k. So we now look at their difference, which is just $(m^2 - m)/2 = 2k^2 - k$. Taking this (mod 2k), we find that their difference is k (mod 2k), which means that $\{a_1 + b_1, ..., a_m + b_m\}$ cannot be a complete set.

11.

12.

13. Look up Wilson's Theorem.

14. Look at http://www.georgmohr.dk/imo/imo05sol.pdf