Number Theory Homework IV

RDB

August 17, 2021

This homework is on Week 3 stuff.
In general, assume that variables like n, m, and k are integers.

Exercise 1 Find the general solution to the following congruence systems.

(**a**)

$$\begin{aligned} 2x &= 0 \pmod 5 \\ x &= -1 \pmod 3 \end{aligned}$$

(**b**)

$$\begin{aligned} x &= 1 \pmod 3 \\ x &= 2 \pmod 5 \\ x &= 3 \pmod 7 \end{aligned}$$

Solution 1

Exercise 2

(**a**) Show that if $m_1, m_2, \ldots, m_n$ is any sequence of positive integers which are pairwise relatively prime, then there exist n consecutive positive integers x, $x+1$, $\ldots$, $x+n-1$ such that x is divisible by m_1, $x+1$ is divisible by m_2, and so on. [Hint: Chinese Remainder Theorem.]

(**b**) Let the primes be enumerated by $\{p_n\}_{n\geq 1}$. That is, $p_1 = 2$, $p_2 = 3$, $p_3 = 5$, and so on.

Prove that, for any n, there exist n conseuctive positive integers x, $x+1, \ldots, x+n-1$ such that the first is divisible by p_1, the second by p_2, the third by p_3, and so on. What is the *smallest* positive x when $n = 3$?

Solution 2

(**a**) This is equivalent to

$$\begin{aligned} x &\equiv 0 \pmod{m_1} \\ x &\equiv -1 \pmod{m_2} \\ &\vdots \\ x &\equiv -(n-1) \pmod{m_n}. \end{aligned}$$

By the CRT, this has a particular solution x_0, and all other solutions are of the form

$$x = x_0 + m_1 m_2 \cdots m_n t$$

for some integer t. In particular, we can get $x > 0$ by choosing a sufficiently large t.

(**b**) The existence of a solution is just the previous part with $m_k = p_k$.

Exercise 3 [Stolen from Section 5-3.]

A class in number theory was to divide itself into groups of equal sizes to study the Chinese Remainder Theorem. When the class was divided into groups of 3, two students were left out; when into groups of 4, one was left out. When it was divided into groups of five, the students found that if the professor was added to one of the groups, no one was left out. Since the professor had never really understood the Chinese Remainder Theorem when he was in college, the last arrangement worked out nicely. How many students were there in the class?

[Added: Assume that this is a small class.]

Exercise 4 Find three consecutive positive integers such that the first is divisible by the square of a prime, the second by the cube of a prime, and the third by the fourth power of a prime. [The prime does not have to be the same for each integer.]

Exercise 5 Fix relatively prime integers a and b. Use the Chinese Remainder theorem to show that every common multiple of a and b is divisible by ab. Deduce that $\operatorname{lcm}(a,b) = ab$ if $\gcd(a,b) = 1$, thereby circumventing one part of that horrible problem on last week's homework.

Exercise 6 If $x^2 \equiv a \pmod{m}$, then we say that x is a *square root* of a mod p.

(**a**) Prove that the square roots of 1 mod p are ± 1. That is, show that the equation $x^2 = 1 \pmod{p}$ has exactly two incongruent solutions, 1 and -1.

(**b**) Prove that $a \neq 0$ has either zero or two square roots mod p if $p \geq 3$ is prime. Prove that $a = 0$ has exactly one square root mod p.

(**c**) Show that 0 has more than two square roots mod 36.

Exercise 7 This exercise involves programming.

Say that a positive integer $n \geq k \geq 0$ is *k-divisible* if n is divisible by $n - k$.

(**a**) Prove that $k \leq n \leq 2k$ if n is k-divisible. [Hint: The smallest multiple of $n - k$ is $2(n - k)$.]

(**b**) Write a function `findDivisibles(k)` which takes an integer k and returns all n which are k-divisible. [Hint: You only need to look at $k \leq n \leq 2k$ by the previous part.]

(**c**) For $1 \leq k \leq 20$, compute D_k, the number of k-divisible integers n. Look the values of D_k up in the OEIS. What entry seems most likely? Does the OEIS contain this conjecture?