MATH 8: NUMBER THEORY 7: CHINESE REMAINDER THEOREM CONTINUED

MAY 2, 2021

Inverses in modular arithmetic

Recall that we say that t is inverse of a mod n if $at \equiv 1 \mod n$.

Theorem. *A number a has an inverse mod n if and only if a is relatively prime with n, i.e.* $\gcd(a, n) = 1$.

If a has an inverse mod n, then we can easily solve equations of the form

$$ax \equiv b \mod n$$

Namely, just multiply both sides by inverse of a.

Least common multiple

Theorem. *Let a, b be relatively prime. Then any common multiple of a, b is a multiple of ab; in particular, the least common multiple of a, b is ab.*

Chinese Remainder Theorem

Theorem (Chinese Remainder Theorem)**.** *Let a, b be relatively prime. Then, for any choice of k, l, the following system of congruences:*

$$x \equiv k \mod a$$
$$x \equiv l \mod b$$

has a unique solution mod ab, i.e. it has solutions and any two solutions differ by a multiple of ab. In particular, there exists exactly one solution x such that $0 \le x < ab$.

Homework

1. (a) Provide a list of integers x such that $x \equiv 1 \mod 5$. There are infinitely many such numbers, so explain what numbers will be on this list without writing out the entire list.

(b) Find all integer solutions to $x^2 \equiv 1 \mod 5$. Again, there are infinitely many solutions to this congruence, so explain what numbers are solutions without listing them all.

2. Find all integer solutions of the system

$$x \equiv 4 \mod 9$$
$$x \equiv 5 \mod 11$$

3. Find all integer solutions of the system

$$x \equiv 5 \mod 7$$
$$x \equiv 9 \mod 30$$

4. In the faraway land of Rainbowland, there is a town where, on the main street, the houses follow a color pattern. On the north side of the street, the houses cycle through 7 rainbow colors: red, orange, yellow, green, cyan, blue, violet. So, whenever there is a red house, the next neighbor to the east is an orange house, the neighbor after that to the east is a yellow hosue, etc. On the south side of the street, the houses cycle through 5 sunset colors: red, dark orange, light orange, amber, yellow. On both sides of the street, the houses are evenly spaced, 100m apart. On the far western end of the street, there is a red house across from a red house.

(a) How much distance do you have to walk from the western end of the street in order to find another pair of red houses that are across from each other?

(b) How far from the western end of the street will it take to find a pair of yellow houses that are across from each other?

(c) In the first 10km from the western end, how many times is there a house directly across from a house of the same color? Assume that rainbow red = sunset red, and rainbow yellow = sunset yellow, but dark orange $\neq$ light orange $\neq$ orange.

5. (a) Show that for any number a which is not divisible by 5, we have $a^4 \equiv 1 \mod 5$. [For now, you can just do it by testing all possible remainders mod 5; next time, we will learn how to do that without testing each possibility.]

(b) Show that for any number a which is not divisible by 7, we have $a^6 \equiv 1 \mod 7$.

(c) Show that for any number a which is not divisible by 5 or 7, we have $a^{12} \equiv 1 \mod 35$. [Hint: use Chinese remainder theorem!]

(d) Show that for any a, $a^{13} \equiv a^{25} \equiv a \mod 35$.

6. (a) Prove that for any integer x, we have $x^5 \equiv x \mod 30$

(b) Prove that if integers x, y, z are such that $x + y + z$ is divisible by 30, then $x^5 + y^5 + z^5$ is also divisible by 30.