MATH 8: ASSIGNMENT 26

APRIL 25, 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 $0 \leq x < ab$.

Homework

1. Find all solutions of the system

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

2. Find all solutions of the system

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

3. The theory of biorhythms suggests that one's emotional and physical state is subject to periodic changes: 23-day physical cycle and a 28-day emotional cycle. (This is a highly dubious theory, but for this problem, let us accept it.) Assuming that for a certain person January 1st, 2021 was the first day of both cycles, how many days will it take for him to achieve top condition on both cycles (which happens on 6th day of 23-day cycle and 7th day of 28-day cycle)? When will be the next time he achieves top condition in both cycles? (Note: first day is day 1, not day 0!)

4. (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, $a^{13} \equiv a^{25} \equiv a \mod 35$.

5. (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.