MATH 8: HANDOUT 25

Summary of previous

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.

Chinese Remainder Theorem

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

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

has a unique solution mod ab, i.e. there exists exactly one integer x such that $0 \leq x < ab$ and x satisfies both the above congruences.

Proof. Let $x = k + ta$ for some integer t. Then x satisfies the first congruence, and our goal will be to find t such that x satisfies the second congruence.

To do this, write $k + ta \equiv l \mod b$, which gives $ta \equiv l - k \mod b$. Notice now that because a, b are relatively prime, a has an inverse $h \mod b$ such that $ah \equiv 1 \mod b$. Therefore $t \equiv h(l - k) \mod b$, and $x = k + ah(l - k)$ is a solution to both the congruences.

To see uniqueness, suppose x and x' are both solutions to both congruences such that $0 \leq x, x' < ab$. Then we have

$$x - x' \equiv k - k \equiv 0 \mod a$$
$$x - x' \equiv l - l \equiv 0 \mod b$$

Thus $x - x'$ is a multiple of both a and b; because a, b are relatively prime, this implies that $x - x'$ is a multiple of ab, but if this is the case then x and x' cannot both be positive and less than ab unless they are in fact equal.

□

Homework

1. Is it possible for a multiple of 3 to be congruent to $5 \mod 12$?

2. (a) Find inverse of 7 mod 11.

(b) Find all solutions of the equation

$$7x \equiv 5 \mod 11$$

3. Solve the following systems of congruences

(a)

$$x \equiv 1 \mod 3$$
$$x \equiv 1 \mod 5$$

(b)

$$z \equiv 1 \mod 5$$
$$z \equiv 6 \mod 7$$

4. (a) Find the remainder upon division of 23^{2019} by 7.

(b) Find the remainder upon division of 23^{2019} by 70. [Hint: use $70 = 7 \cdot 10$ and Chinese Remainder Theorem.]

5. (a) Find the remainder upon division of 24^{46} by 100.

(b) Determine all integers k such that $10^k - 1$ is divisible by 99.

6. In a calendar of some ancient race, the year consists of 12 months, each 30 days long. They also use 7 day weeks, same as we do.

If first day of the year was a Monday, will it ever happen that 13th day of some month is a Friday? If so, when will be the first time it happens, and how often will it repeat afterwards?

[Hint: this can be rewritten as a system of congruences: $n \equiv 5 \mod 7$, $n \equiv 13 \mod 30$.]

7. Al and Barb start their new jobs on the same day. Al's schedule is 3 work-days followed by 1 rest day. Barb's schedule is 7 workdays followed by 3 rest days. On how many of their first 1000 days do both have rest days on the same day? (AMC)

8. Solve system of linear congruences:

$$x \equiv 1 \mod 3$$
$$x \equiv 2 \mod 4$$
$$x \equiv 4 \mod 5$$