MATH 8: HANDOUT 22
NUMBER THEORY 7: CHINESE REMAINDER THEOREM CONTINUED.
FERMAT'S LITTLE THEOREM.

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 $0 \leq x < ab$.

FERMAT'S LITTLE THEOREM

The following two results are frequently useful in doing number theory problems:

Theorem (Fermat's Little theorem)**.** *For any prime p and any number a not divisible by p, we have $a^{p-1} - 1$ is divisible by p, i.e.*

$$a^{p-1} \equiv 1 \mod p.$$

This shows that remainders of a^k mod p will be repeating periodically with period $p-1$ (or smaller). Note that this only works for prime p.

As a corollary, we get that for any a (including those divisible by p) we have

$$a^p \equiv a \mod p$$

More generally, $a^{k(p-1)+1} \equiv a \mod p$.

Note that the condition that p be prime is important: notice, for example, that $3^{(8-1)} \mod 8$ is congruent to 3, not 1.

There are many proofs of Fermat's little theorem; one of them is given in problem 11 below.

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) 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.

5. Find 5^{2021} modulo 11.

6. Prove that $2019^{3000} - 1$ is divisible by 1001. [Hint: you can use Chinese remainder theorem and equality $1001 = 7 * 11 * 13$.]

7. Find the last two digits of 7^{1000}. [Hint: first find what it is mod 2^2 and mod 5^2.]

8. Show that for any integer a, the number $a^{11} - a$ is a multiple of 66

9. Show that the number $111\ldots1$ (16 ones) is divisible by 17. [Hint: can you prove the same about number $999\ldots9$?]

10. Alice decided to encrypt a text by first replacing every letter by a number a between 1–26, and then replacing each such number a by $b = a^7 \mod 31$.

Show that then Bob can decrypt the message as follows: after receiving a number b, he computes b^{13} and this gives him original number a.

11. Let p be a prime number.

(a) Show that for any k, $1 \le k \le p-1$, the binomial coefficient ${}_pC_k$ is divisible by p.

(b) Without using Fermat's little theorem, deduce from the previous part and the binomial theorem that for any a, b we have $(a+b)^p \equiv a^p + b^p \mod p$

(c) Prove that for any a, we have $a^p \equiv a \mod p$. [Hint: $a^p = (1 + 1 + \cdots + 1)^p$]