MATH 8B: HANDOUT 26 [MAY 11, 2025]
NUMBER THEORY 7: CHINESE REMAINDER THEOREM (CONTINUED). FERMAT'S LITTLE THEOREM, WILSON'S THEOREM

SUMMARY OF PREVIOUS RESULTS

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

Theorem 1. *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 2 (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 $0 \leq x < ab$.

MORE ABOUT THE CHINESE REMAINDER THEOREM

Theorem 3. *Let a, b, c be integers such that a is relatively prime to b and to c. Then a is relatively prime to bc.*

Proof. This follows immediately from the fundamental theorem of arithmetic (unique prime factorization). There are no common primes dividing a and b, and similarly no common primes dividing a and c. So there is no prime dividing both a and bc. □

Therefore, we can extend the Chinese remainder theorem to multiple moduli, as long as they are relatively prime in pairs, as follows.

Theorem 4. *Let $a_1, \ldots, a_r$ be relatively prime in pairs, i.e., $(a_i, a_j) = 1$ for each $i \neq j$. Then for any choice of $k_1, \ldots, k_r$, the system of congruences*

$$x \equiv k_1 \mod a_1$$
$$\ldots$$
$$x \equiv k_r \mod a_r$$

has a unique solution mod $a_1 a_2 \ldots a_r$.

We won't go over the proof in detail, but it basically follows by mathematical induction. (First, solve the first two mod a_1a_2, then combine that solution with the next congruence to solve mod $a_1a_2a_3$, and so on, at each step using the Chinese remainder theorem.)

Typically, we use this generalized form of the Chinese remainder theorem to solve congruences modulo $n = p_1^{e_1}p_2^{e_2}\dots p_r^{e_r}$ by solving it modulo its prime power divisors $p_i^{e_i}$, which are all relatively prime in pairs.

Example: How many solutions are there to the congruence

$$x^2 \equiv 1 \mod 105$$

We can check that $x^2 \equiv 1 \mod p$ has exactly 2 solutions, where p is an odd prime. So the above congruence has 8 solutions, since $105 = 3 \cdot 5 \cdot 7$.

Fermat's Little Theorem

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

Theorem 5 (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.

Corollary 1. *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. Here is another.

Proof. Consider the numbers $1, 2, \dots, p-1$ modulo p; these are all distinct. Now multiply each of them by a, i.e. look at the numbers $a, 2a, \dots, (p-1)a$. We can see that these are all distinct modulo p, because if we had

$$ia \equiv ja \mod p$$

then because a is relatively prime to p, we can cancel it from both sides of the congruence to get $i \equiv j \mod p$. Similarly, all these numbers ia mod p are also not 0 modulo p. So they must be a permutation of the set $\{1, \dots, (p-1)\}$ modulo p. In particular, if we multiply them together, we get

$$a^p \cdot (p-1)! \equiv (p-1)! \mod p$$

Now because $(p-1)!$ is coprime to p, we can cancel it and get our theorem. □

Note that Fermat's little theorem is distinct from Fermat's big theorem (there are no solutions to $a^n + b^n = c^n$ with $n > 2$ and $abc \neq 0$), which was not really a theorem that Fermat proved ...

Now, you may wonder what the product $(p-1)!$ that showed up in the above proof is mod p.

Theorem 6 (Wilson's theorem)**.** *For any prime p, we have $(p-1)! \equiv -1 \mod p$.*

Proof. It is enough to prove it for odd primes (why?). Now, for an odd prime p, look at the set $\{1, \dots, p-1\}$ and pair up the numbers x mod p with x^{-1} mod p. The only numbers for which $x = x^{-1}$ are the solutions of $x^2 \equiv 1 \mod p$, namely ± 1. Let's call the pairs $a_1, a_1^{-1}, a_2, a_2^{-1}, \dots, a_k, a_k^{-1}$, where $k = (p-3)/2$. So we can rearrange the product $(p-1)!$ as

$$1 \dots (p-1) \equiv 1 \cdot (-1) \cdot (a_1 \cdot a_1^{-1}) \dots (a_k \cdot a_k^{-1}) \equiv 1 \cdot (-1) \equiv -1 \mod p.$$

□

CLASSWORK

Remember that for a natural number n, we define Euler's totient function $\phi(n)$ to be the number of elements of $\{1, \dots, n\}$ which are coprime to n. We saw earlier that $\phi(p) = p-1$ for a prime p, and more generally $\phi(p^e) = p^{e-1}(p-1)$. Show that $\phi(mn) = \phi(m)\phi(n)$ for m and n relatively prime, as follows:

- If $1 \le a \le mn$ is relatively prime to mn, then it is relatively prime to m and n. So considering its remainders mod m and mod n, we get two numbers b, c such that $1 \le b \le m$ and $1 \le c \le n$ and b is relatively prime to m, c is relatively prime to n.
- Conversely, if we have a b and c as above, one can find a unique a modulo mn (and therefore a unique a satisfying $1 \le a \le mn$) such that it is relatively prime to mn and its remainders mod m and mod n are b and c respectively. (Why?)

Calculate $\phi(n)$ for $n = p_1^{e_1} \dots p_r^{e_r}$.

HOMEWORK

1. 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!)

2. (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.

3. Find 5^{2021} modulo 11.

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

5. How many solutions are there to
(a) $x^2 \equiv -1 \mod 65$?
(b) $x^2 \equiv -1 \mod 69$?

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

7. Show that the number $111 \dots 1$ (16 ones) is divisible by 17. [Hint: can you prove the same about number $999 \dots 9$?]

8. 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} mod 31 and this gives him the original number a.

9. Let p be a prime number.

(a) Show that for any k, $1 \leq k \leq p-1$, the binomial coefficient $\binom{p}{k}$ 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: use induction on a and the previous part.]

***10.** Let p be a prime, and let $0 \leq b \leq a < p$. Then show

$$\binom{ap}{bp} \equiv \binom{a}{b} \mod p.$$