

MATH 8: HANDOUT 19
NUMBER THEORY 4: CONGRUENCES

REMINDER: EUCLID'S ALGORITHM

Recall that as a corollary of Euclid's algorithm we have the following result:

Theorem. *An integer m can be written in the form*

$$m = ax + by$$

if and only if m is a multiple of $\gcd(a, b)$.

For example, if $a = 18$ and $b = 33$, then the numbers that can be written in the form $18x + 33y$ are exactly the multiples of 3.

To find the values of x, y , one can use Euclid's algorithm; for small a, b , one can just use guess-and-check.

CONGRUENCES

In many situation, we are mostly interested in remainder upon division of different numbers by same integer n . For example, in questions related to the last digit of a number k , we are really looking at remainder upon division of k by 10.

This motivates the following definition: we will write

$$a \equiv b \pmod{m}$$

(reads: a is congruent to b modulo m) if a, b have the same remainder upon division by m (or, equivalently, if $a - b$ is a multiple of m).

Congruences can be added and multiplied in the same way as equalities: if

$$\begin{aligned} a &\equiv a' \pmod{m} \\ b &\equiv b' \pmod{m} \end{aligned}$$

then

$$\begin{aligned} a + b &\equiv a' + b' \pmod{m} \\ ab &\equiv a'b' \pmod{m} \end{aligned}$$

Here are some examples:

$$2 \equiv 9 \equiv 23 \equiv -5 \equiv -12 \pmod{7}$$

$$10 \equiv 100 \equiv 28 \equiv -8 \equiv 1 \pmod{9}$$

Note: we will occasionally write $a \pmod{m}$ for remainder of a upon division by m .

Since $23 \equiv 2 \pmod{7}$, we have

$$23^3 \equiv 2^3 \equiv 8 \equiv 1 \pmod{7}$$

And because $10 \equiv 1 \pmod{9}$, we have

$$10^4 \equiv 1^4 \equiv 1 \pmod{9}$$

One important difference is that in general, one can not divide both sides of an equivalence by a number: for example, $5a \equiv 0 \pmod{m}$ does not necessarily mean that $a \equiv 0 \pmod{m}$ (see problem 3b below).

PROBLEMS

1. (a) Use $10 \equiv -1 \pmod{11}$ to compute $100 \pmod{11}$; $100,000,000 \pmod{11}$. Can you derive the general formula for $10^n \pmod{11}$?
 (b) Without doing long division, compute $1375400 \pmod{11}$. [Hint: $1375400 = 10^6 + 3 \cdot 10^5 + 7 \cdot 10^4 \dots$]
2. (a) Compute remainders modulo 12 of 5, 5^2 , 5^3 , \dots . Find the pattern and use it to compute $5^{1000} \pmod{12}$
 (b) Prove that for any a, m , the following sequence of remainders mod m :
 $a \pmod{m}, a^2 \pmod{m}, \dots$
 sooner or later starts repeating periodically (we will find the period later). [Hint: have you heard of pigeonhole principle?]
 (c) Find the last digit of 7^{2021}
3. (a) For of the following equations, find at least one integer solution (if exists; if not, explain why)

$$5x \equiv 1 \pmod{19}$$

$$9x \equiv 1 \pmod{24}$$

$$9x \equiv 6 \pmod{24}$$

[Hint: $5x \equiv 1 \pmod{19}$ is the same as $5x = 1 + 19y$ for some integer y .]

 (b) Give an example of a, m such that $5a \equiv 0 \pmod{m}$ but $a \not\equiv 0 \pmod{m}$
4. (a) Show that the equation $ax \equiv 1 \pmod{m}$ has a solution if and only if $\gcd(a, m) = 1$. Such an x is called the *inverse* of a modulo m . [Hint: Euclid's algorithm!]
 (b) Find the following inverses
 inverse of 2 mod 5
 inverse of 5 mod 7
 inverse of 7 mod 11
 Inverse of 11 mod 41
5. (a) Find $\gcd(48, 39)$
 (b) Solve $48x + 39y = 3$
 (c) Find inverse of 39 mod 48.
6. (a) Integers a, b are such that $a^2 + b^2$ is divisible by 3. Show that then $a^2 + b^2$ is divisible by 9.
 (b) Integers a, b are such that $a^2 + b^2$ is divisible by 21. Show that then $a^2 + b^2$ is divisible by 441.
- *7. Prove that no positive integer solutions exist for the following equations.
 (a) $x^3 = x + 10^n$ [Hint: see if you can prove that $x^3 \equiv x \pmod{3}$]
 (b) $x^3 + y^3 = x + y + 10^n$
8. For a positive number n , let $\sigma(n)$ (this is Greek letter "sigma") be the sum of all divisors of n (including 1 and n itself).
 Compute
 $\sigma(10)$
 $\sigma(77)$
 $\sigma(p^a)$, where p is prime (the answer, of course, depends on p, a)
 $\sigma(p^a q^b)$, where p, q are different primes
 $\sigma(10000)$
 $\sigma(p_1^{a_1} p_2^{a_2} \dots p_k^{a_k})$, where p_i are distinct primes.