MATH 8: HANDOUT 20
NUMBER THEORY 5: CONGRUENCES CONTINUED

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 the multiple of $\gcd(a, b)$.

Moreover, Euclid's algorithm gives us an explicit way to find x, y. Thus, it also gives us a way of solving congruences

$$ax \equiv m \mod b$$

As a corollary we get this:

Theorem. *Equation*

$$ax \equiv 1 \mod b$$

has a solution if and only if a, b are relatively prime, i.e. if $\gcd(a, b) = 1$.

Such an x is called inverse of a modulo b.

As another corollary, we see that in some situations we can divide both sides of a congruence by a number.

Theorem. *Assume that a, b are relatively prime. Then*

$$an \equiv 0 \mod b$$

if and only if $n \equiv 0 \mod b$.

Indeed, let h be inverse of a mod b. Then multiplying both sides of congruence by h, we get $han \equiv 0 \mod b$. SInce $ha \equiv 1 \mod b$, we get $n \equiv 0$.

Application: check digits

An interesting application of congruences is so-called check digits. They are used to detect (but not correct) errors appearing when manually copying or entering long strings of numbers such as bank account numbers, credit card numbers, and more. Here is one application; UPC codes.

A Universal Product Code (UPC) is a numeric code assigned to virtually all products sold in stores; you usually see it as a bar code, which you scan at the cash register. The UPC is a 12-digit numeric code $a_1 \dots a_{12}$; the 12 digits have to satisfy the condition below:

$$3a_1 + a_2 + 3a_3 + a_4 + \dots + a_{12} \equiv 0 \mod 10$$

The sum $3a_1 + a_2 + 3a_3 + a_4 + \dots + a_{12} \mod 10$ is called the *checksum*.

If the digits do not satisfy this condition, it can not be a valid UPC code — so probably there was an error when scanning the barcode and it needs to be re-scanned. For example, 380177-051136 is a valid UPC code (check!); however, if the first 3 was replaced by 8, this would change the checksum by $3 \times 5 = 15 \equiv 5 \mod 10$, so the new checksum woudln't be zero.

It is easy to show that the UPC code always detects an error in single digit (this uses that 3 is invertible mod 10). It can also detect some (but not all) digit transpositions: e.g. if we replaced 380... by 308..., it would change the checksum:

old: $3 \times 3 + 8 + 3 \times 0 + \dots = 17 + \dots \equiv 7 + \dots$

new: $3 \times 3 + 0 + 3 \times 8 + \dots = 33 + \dots \equiv 3 + \dots$

Homework

When doing this homework, be careful that you only used the material we had proved or discussed so far — in particular, please do not use the prime factorization. And I ask that you only use integer numbers — no fractions or real numbers.

1. Prove that $30^{2021} + 61^{2020}$ is divisible by 31.

2. Find the last two digits of $(2016)^{2021}$.

3. Prove that for any integer n, $n^9 - n$ is a multiple of 5. [Hint: can you prove it if you know $n \equiv 1 \mod 5$? or if $n \equiv 2 \mod 5$? or ...]

4. (a) Find the inverses of the following numbers modulo 14 (if they exist): 3; 9; 19; 21
(b) Of all the numbers 1–14, how many are invertible modulo 14?

5. (a) Find inverse of 3 modulo 28.
(b) Solve $3x \equiv 7 \mod 28$ [Hint: multiply both sides by inverse of 3...]

6. Prove that if a, b are relatively prime, and m divisible by a and also divisible by b, then m is divisible by ab. [Hint: $m = ax = by$, so $ax \equiv 0 \mod b$.] Deduce from this that the least common multiple of a, b is ab.

Is it true without the assumption that a, b are relatively prime?

7. Find **all** solutions of the following equations
(a) $5x \equiv 4 \mod 7$
(b) $7x \equiv 12 \mod 30$
(c) In a calendar of some ancient race, all months were exactly 30 days long; however, they used same weeks as we do. If in that calendar, first day of a certain month is Friday, how many weeks will pass before Friday will fall on the 13th day of a month? [Hint: this can be rewritten as some congruence of the form $7x \equiv \dots$, where x is the number of weeks.]

***8.** (a) Let p be a prime other than 2. Consider the remainders of numbers $2, 4, 6, \dots, 2(p-1)$ modulo p. Prove that they are all different and that every possible remainder from 1 to $p-1$ appears in this list exactly once. [Hint: if $2x \equiv 2y$, then $2(x-y) \equiv 0$.] Check it by writing this collection of remainders for $p = 7$.
(b) Use the previous part to show that

$$1 \cdot 2 \cdots (p-1) \equiv 2 \cdot 4 \cdots 2(p-1) \mod p$$

Deduce from it

$$2^{p-1} \equiv 1 \mod p$$

(c) Show that for any a which is not a multiple of p, we have

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