MATH 8
ASSIGNMENT 23: CONGRUENCES AND CHECK DIGITS

MARCH 29TH, 2020

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 $\gcd(a, b)$.

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 $\gcd(a, b) = 1$.

This also gave us a way of solving equations of the form $ax \equiv k \mod b$: multiply both sides by inverse of a (i.e., by x such that $ax \equiv 1$).

Problems

When doing this homework, be careful that you only use 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 $30^{2011} + 61^{2012}$ is divisible by 31.

2. Solve the following congruences:

$$\text{(a) } 17x \equiv 3 \mod 26 \quad \text{(b) } 22x \equiv 4 \mod 26 \quad \text{(c) } 28x \equiv 9 \mod 31$$

3. (a) Write the remainders of $10, 10^2, 10^3, \dots$ mod 7. Describe the pattern.

(b) Write first several digits of 1/7 (as a decimal). Do not use a calculator — do it the old-fashioned way, using long division. Describe the pattern. (Pay attention to the remainders you are getting).

(c) Is there a relation between part (a) and part (b)?

4. An interesting practical application of congruences are so-called check digits. Here is one example. Every book published anywhere in the world has so-called International Standard Book Number (ISBN). It is usually printed on the back of the book and looks something like this: ISBN 0-471-13934-3. In general, it is a ten-digit number $A_1A_2A_3A_4A_5A_6A_7A_8A_9A_{10}$ (frequently separated by dashes). The first nine digits encode information about the book; the last one is the "check digit". It carries no new information — instead, it is there for control purposes. Namely, it chosen so that the following congruence holds

$$A_{10} \equiv A_1 + 2A_2 + 3A_3 + 4A_4 + 5A_5 + 6A_6 + 7A_7 + 8A_8 + 9A_9 \mod 11 \tag{1}$$

(If the right-hand side gives remainder 10, then they write symbol X for the last digit, instead of 10 — to keep the ISBN always 10-digit long)

Thus, if this congruence does not hold, it is a signal that the ISBN is invalid. This way, it is easy to detect when one makes an error while copying ISBNs.

(a) Take any two books at home and check that congruence (1) holds.

(b) Someone spilled coffee on a book order form, making one of the digits of the ISBN illegible. Can you recover this digit if the rest of the ISBN is 0-590-5#880-9 (# stands for the illegible digit)

(c) Suppose that someone is copying an ISBN and makes an error, copying one of the digits incorrectly (this is by far the most common error). Show that it will necessarily give an invalid ISBN (i.e., congruence (1) will fail), making this error easy to detect. (Hint: how would right-hand side of (1) change if ISBN has digit $A_2 = 7$, and it is incorrectly copied as 1? More generally, if a digit A_2 is replaced by another digit A_2'?)

(d) Suppose that someone is copying an ISBN and makes an error, interchanging two adjacent digits (e.g., writing 57 instead of 75) — this is the second most common kind of error when copying. Show that it will necessarily give an invalid ISBN, making this error easy to detect. (Hint: how would right-hand side of (1) change if we interchanged A_1 and A_2?)