Math 300.2 Homework 5

Paul Hacking

February 29, 2012

Reading: Gilbert and Vanstone, Chapter 3.

(1) Recall that we say "a is congruent to b modulo m" and write $a \equiv b \bmod m$ if $m \mid (a-b)$. Thus $a \equiv r \bmod m$ where r is the remainder on dividing a by m (i.e. $a = qm + r$ where $q, r \in \mathbb{Z}$ and $0 \leq r < m$). [And r is the only integer in $\{0, 1, 2 \ldots, m-1\}$ which is congruent to a modulo m]. Use the congruence notation to compute the remainders of the following divisions by hand.

   (a) $68 \cdot 87$ divided by 7.
   (b) 2^9 divided by 13.
   (c) 2011^{100} divided by 2012.

(2) Suppose $n \in \mathbb{N}$ is a perfect square, i.e., $n = m^2$ for some $m \in \mathbb{N}$. Show that the last digit of n is one of the following numbers: $1, 4, 5, 6, 9, 0$. [Hint: The last digit of n is the remainder when we divide n by 10.]

(3) Let $a, b \in \mathbb{Z}$ and $m, n \in \mathbb{N}$. Show that

$$a \equiv b \bmod mn \Rightarrow a \equiv b \bmod m.$$

(4) Let $a, b \in \mathbb{Z}$ and $m, n \in \mathbb{N}$. Show that

$$an \equiv bn \mod mn \iff a \equiv b \mod m.$$

(5) Let $m \in \mathbb{N}$ and $a, b \in \mathbb{Z}$. Prove or give a counterexample to the following statement: If $ab \equiv 0 \bmod m$ then $a \equiv 0 \bmod m$ or $b \equiv 0 \bmod m$.

(6) Recall Fermat's little theorem: If p is a prime and a is an integer such that p does not divide a, then $a^{p-1} \equiv 1 \bmod p$. The proof of Fermat's little theorem given in class used the following observation: the numbers $1 \cdot a, 2 \cdot a, \ldots, (p-1) \cdot a$ are congruent modulo p to $1, 2, \ldots, p-1$ in some order. Check this for $a = 3$ and $p = 11$.

(7) Solve the following linear congruences or prove that no solutions exist.

  (a) $2x \equiv 7 \bmod 11$.

  (b) $15x \equiv 4 \bmod 18$.

  (c) $33x \equiv 22 \bmod 55$.

(8) Find all solutions of the following pairs of congruences or prove that no solutions exist.

  (a) $x \equiv 2 \bmod 5$, $x \equiv 3 \bmod 7$.

  (b) $x \equiv 6 \bmod 10$, $x \equiv 3 \bmod 14$.

(9) Recall the Chinese remainder theorem: Let $a, b \in \mathbb{Z}$ and $m, n \in \mathbb{N}$. Suppose $\gcd(m, n) = 1$. Then the pair of congruences

$$x \equiv a \bmod m, \quad x \equiv b \bmod n$$

are equivalent to the congruence $x \equiv c \mod mn$ for some $c \in \mathbb{Z}$. (In other words, the pair of congruences have a unique solution modulo mn.) In this question we will describe a way to compute the solution c for all pairs a, b fairly quickly.

  (a) By Euclid's algorithm we can find $u, v \in \mathbb{Z}$ such that $mu + nv = 1$. Show that $c \equiv anv + bmu \mod mn$. [Hint: Just check $x = c$ satsifies the pair of congruences above.]

  (b) Use part (a) to compile a table of solutions c for $m = 3, n = 5$, and $0 \leq a \leq m-1$, $0 \leq b \leq n-1$, like the one we wrote down in class for $m = 5$ and $n = 8$.

(10) Let p be a prime.

  (a) Show that if $ab \equiv 0 \bmod p$ then $a \equiv 0 \bmod p$ or $b \equiv 0 \bmod p$.

(b) Show that if $a \not\equiv 0 \bmod p$ then there is a $b \in \mathbb{Z}$ such that $ab \equiv 1 \bmod p$, and b is uniquely determined $\bmod p$. We sometimes write $b = a^{-1} \bmod p$.

(c) Now consider the finite set $S = \{0, 1, 2, \ldots, p-1\}$. Given $a, b \in S$ we can define $a \oplus b \in S$ and $a \otimes b \in S$ by $a \oplus b \equiv a + b \bmod p$ and $a \otimes b \equiv ab \bmod p$. Using the results of part (a) and (b) we see that this set S has analogues of all the usual arithmetic operations for real numbers (addition, subtraction, multiplication, division). It is called "the finite field with p elements" and often denoted $\mathbb{F}_p$. Write down the addition and multiplication tables for $p = 3$.