Honors Homework 1

Discrete Structures, CS 173, Spring 2015

Released: Monday February 16, due: Monday March 2

Honors homework must be formatted using the LaTeX document formatting package. (Not just the equation mode found in Piazza and Moodle.) See the CS 173 honors web page for help getting started with LaTeX. Exception: you do not need to format supporting materials such as program source code, screenshots, and figures.

Your homework should be submitted as hardcopy in the CS 173 honors dropbox in the basement of Siebel. Please submit a hardcopy of your LaTeX document **both source code and formatted output** and hardcopies of any supporting materials.

The dropboxes are located just east of the lounge area with the big windows. If you get to the candy/soda machines, you've gone too far east.

Fermat's Little Theorem and the Chinese Remainder Theorem

1. *Warm-Up:* Can you find a solution for the equation $4x \equiv 1 \pmod 5$? How about $4x \equiv 1 \pmod 6$?

   Problem: Show that for any positive integer m, an element $a \in \mathbb{Z}_m$ has a multplicative inverse — i.e., $x \in \mathbb{Z}_m$ such that $ax = 1$ (where the multiplication is modulo m) — iff $\gcd(a, m) = 1$.

   When $a \in \mathbb{Z}_m$ has a multiplicative inverse, we may denote it by a^{-1}. In particular, if m is a prime, for all $a \in \{1, 2, \ldots, m-1\}$, a^{-1} exists modulo m.

2. **Fermat's Little Theorem** gives a formula for $a^{-1} \pmod p$, when p is a prime. It states that if $a \not\equiv 0 \pmod p$, then $a^{(p-2)} \equiv a^{-1} \pmod p$. (This is often stated as $a^p \equiv a \pmod p$. We will not prove this now; it can be shown using mathematical induction.)

   Problem: For $p = 11$, list the multiplicative inverse of each element in $\{1, \ldots, p-1\}$. (You may use brute-force to search for a^{-1}, or alternately use the above theorem.)

3. *Warm-Up:* See if you can find a solution for the system $x \equiv 1 \pmod 9$ *and* $x \equiv 2 \pmod 6$.

Problem: Suppose m, n, g are positive integers such that $\gcd(m, n) = g$. Then, show that if there is a number x satisfying $x \equiv a \pmod{m}$ and $x \equiv b \pmod{n}$, then $a \equiv b \pmod{g}$.

4. *Warm-Up:* See if you can find a solution for the system $x \equiv 2 \pmod{3}$ and $x \equiv 4 \pmod{5}$.

   Here's a way to do it: list all 15 numbers, in $\mathbb{Z}_{15}$, and for each one write down its congruence class modulo 3 and its congruence class modulo 5. Which all pairs $(a, b) \in \mathbb{Z}_3 \times \mathbb{Z}_5$ occur in this list? Does $(2, 4)$ occur?

   Problem: Suppose m, n are coprimes (aka relatively prime). Let m', n' be such that $mm' \equiv 1 \pmod{n}$, and $nn' \equiv 1 \pmod{m}$. For any a, b, show that for $x = bmm' + ann'$, $x \equiv a \pmod{m}$ and $x \equiv b \pmod{n}$.

5. **Problem:** For any positive integers m, n such that $\gcd(m, n) = 1$, and any non-negative integers a, b, argue that there is exactly one value of x such that $0 \leq x < mn$ and $x \equiv a \pmod{m}$ and $x \equiv b \pmod{n}$.

   [Hint: Use the previous problem. Use a counting argument to show uniqueness.]

   What you have proven above is (a basic version of) the **Chinese Remainder Theorem** (CRT). It states that there is a one-to-one correspondence between $\mathbb{Z}_{mn}$ and $\mathbb{Z}_m \times \mathbb{Z}_n$. That is, every $x \in \mathbb{Z}_{mn}$ can be *uniquely* represented by a pair $(a, b) \in \mathbb{Z}_m \times \mathbb{Z}_n$ such that $x \equiv a \pmod{m}$ and $x \equiv b \pmod{n}$.

6. *Warm up*: Calculate $17^3 \pmod{35}$ easily using CRT.

   Here's how you can go about it: Let $m = 5, n = 7$, so that $35 = mn$, and $\gcd(m, n) = 1$. With respect to this decomposition, the CRT representation of 17 is $(2, 3)$. Argue that the CRT representation of 17^3 is $(2^3, 3^3) \equiv (3, 6)$. (To complete the calculation, you can employ Fermat's Little Theorem from above to find $5^{-1} \pmod{7}$ and $7^{-1} \pmod{5}$, since $7, 5$ are prime.)

   Problem: Suppose m, n are prime numbers, and $\gcd(x, mn) = 1$. Then, derive a formula for $x^{-1} \pmod{mn}$ using CRT and Fermat's Little Theorem. Use it to calculate $22^{-1} \pmod{35}$.