CS 70 SPRING 2007 — DISCUSSION #3

VAHAB POURNAGHSHBAND

1. Administrivia

(1) Course Information
- The second homework is due February 6th at 2:30pm in 283 Soda Hall.
- Please write down your section's time on the homework.
- Web-page for this section: `http://inst-eecs.berkeley.edu/~vahab/cs70`

2. The Stable Marriage Problem

Recall from class the Stable Marriage Problem, and the associated propose and reject (a.k.a. the Traditional Marriage) algorithm. The following facts can be proven about the correctness of this algorithm:

Facts 1. *For the case when men propose and women accept/reject:*

(i) No man can be rejected by all women.
(ii) The algorithm terminates with a stable matching.
(iii) The propose-reject algorithm terminates in at most n^2 days.
(iv) The propose-reject algorithm always produces a male-optimal stable matching.
(v) A male-optimal stable matching is a female-pessimal stable matching.

Exercise 1. Try to recall the proof of each of these facts.

3. Modular Arithmetic

In modular arithmetic, we concern ourselves with the notion of *congruences*. Much like equalities in normal arithmetic, congruences form a so-called *equivalence relation*. That is, they satisfy the following three properties:

(1) Reflexive: $a \equiv a \mod n$
(2) Symmetric: $a \equiv b \mod n \implies b \equiv a \mod n$
(3) Transitive: $a \equiv b \mod n, b \equiv c \mod n \implies a \equiv c \mod n$

Recall that when we're looking at numbers *modulo* n, (sometimes denoted as $\mathbb{Z}/n\mathbb{Z}$ and more succinctly as $\mathbb{Z}_n$),

$$a \equiv b \mod n \iff n|(a-b)$$

Why is this true? Recall that if $a \equiv b \mod n$, then this means that $a = b + nk$ for some $k \in \mathbb{Z}$. Then clearly we have $nk = a - b$, from which it follows that n must divide $a - b$.

Date: February 1, 2007.

The author gratefully acknowledge the TA's of CS70 past for the use of their previous notes: Chris Crutchfield, Amir Kamil, David Garmire, Lorenzo Orecchia, and Ben Rubunstein. Their notes form the basis for this handout.

Equivalently, if you consider the C-like % (remainder) operator, then

$$a \equiv b \mod n \iff a\%n = b\%n.$$

Addition and multiplication in $\mathbb{Z}_n$ work the same as they do in $\mathbb{Z}$. The following rules hold:

(1) $a \equiv b \mod n \implies a + c \equiv b + c \mod n$
(2) $a \equiv b \mod n \implies a \cdot c \equiv b \cdot c \mod n$

But what about subtraction and division? Well, subtraction is easy, since additive inverses always exist in $\mathbb{Z}_n$. For example, if you consider $a - b$ in $\mathbb{Z}/n\mathbb{Z}$, the quantity $-b$ is congruent to $n - b, 2n - b, 3n - b, \ldots$. So you can always turn subtraction into addition[1]. Division, though, is not so easy. It turns out that you can't always divide by a number in modular arithmetic. Let's consider what it means when you want to solve for x in the equation

$$2x \equiv 6 \mod 8.$$

Well, clearly $x \equiv 3 \mod 8$ is a solution. But $x \equiv 7 \mod 8$ is also a solution! So, in a sense, division by 2 in $\mathbb{Z}/8\mathbb{Z}$ is not well-defined (how can x be congruent to both 3 and 7?)

However, if we try and solve for x in the problem

$$3x \equiv 6 \mod 8,$$

the only solution is $x \equiv 2 \mod 8$ (try it out!) Can you guess when you're allowed to divide and when you aren't?

Now let's move on to exercises[2]:

Exercise 2. Show that if a is an odd integer, then $a^2 \equiv 1 \mod 8$.

Exercise 3. Show that if $n \equiv 3 \mod 4$, then n cannot be the sum of the squares of two integers.

Exercise 4. What is $2^{2^{2006}} \mod 3$?

Exercise 5. We saw in class that the following statement can be proven by induction.

$$\forall n \in \mathbb{N}, if \quad a \equiv b \mod m, \ then \quad a^n \equiv b^n \mod m \tag{3.1}$$

Complete this proof.

Exercise 6. Show that if $2^n - 1$ is prime, then n is prime.

[1]This is somewhat imprecise language, but if you think of it in the following way it might be helpful: When you subtract, you're really just adding the additive inverse. So $a - b$ becomes $a + (-b)$.

[2]Exercises are from Rosen's *Elementary Number Theory* and Dasgupta, Papadimitriou and Vazirani's *Algorithms*