CS 70 FALL 2006 — DISCUSSION #3

D. GARMIRE, L. ORECCHIA & B. RUBINSTEIN

1. Administrivia

(1) Course Information
- The fourth homework is due September 22^{th} at 4pm in 283 Soda Hall. Look for the CS70 tag on the drop-box, as the box has changed.
- You should be receiving your graded homework #2. The average was 77 points, the standard deviation was 22 (large lower tail), the mode 82.

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 sequence of proposals made by each man is non-increasing in his preference list.
(iii) The sequence of men that a woman holds on a string is non-decreasing in the woman's preference list.
(iv) The algorithm terminates with a stable matching.
(v) The propose-reject algorithm terminates in at most n^2 days.
(vi) The propose-reject algorithm always produces a male-optimal stable matching.
(vii) 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: $a \equiv b \mod n$, $b \equiv c \mod n \implies a \equiv c \mod n$

Date: September 20, 2006.
The authors gratefully acknowledge Chris Crutchfield and Amir Kamil for the use of their previous notes, which form part of the basis for this handout.

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 $a - b$.

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 $2^{2^{2006}} \mod 3$?

4. Euclid's algorithm

In class you saw Euclid's algorithm, devised by Euclid to compute the greatest common divisor of two lengths (now numbers):

1	Euclid	(a, b)
2		if $(b = 0)$, return a;
3		return Euclid$(b, a \mod b)$;

[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*

The correctness of this theorem is based on the following theorem:

Theorem 2. *If x and y are positive integers with $x \geq y$, then* $\gcd(x, y) = \gcd(x - y, y)$.

The complexity of the algorithm was proved to be $O(n)$, where n is the number of bits of the maximum of a and b. Can you recall the proof of this fact?

Exercise 5. Use Euclid's algorithm to compute $\gcd(697, 969)$.

Exercise 6. Prove that for all $n > 0$, the gcd of two consecutive Fibonacci numbers $\gcd(F_n, F_{n+1})$ equals 1. (*N*ote: this should make you think about why Fibonacci is Euclid's worst enemy.)

5. Extended Euclid and Multiplicative Inverses

In class you should have seen how backtracking Euclid's algorithm gives a new algorithm, called Extended Euclid. On input a and b, Extended Euclid runs as Euclid to obtain $d = \gcd(a, b)$. Then, it backtracks through the recursion levels to get integers r, s such that $d = ra + sb$.

This can be used to certify that the d is the greatest among the divisors of a and b. Indeed, suppose a larger divisor $d' > d$ existed. This would mean $d'|ra$ and $d'|sb$, which in turn implies $d'|ra + sb$, i.e. $d'|d$. Hence $d' \leq d$, which is a contradiction.

This is useful, but not strictly necessary, as we already knew that Euclid was correct. The main purpose of Extended Euclid is, however, to perform division $\bmod N$. All we need to do this, is to find a procedure to compute multiplicative inverses[3]. Suppose we have a and N, such that $\gcd(a, N) = 1$. Then, we could use Extended Euclid to find r, s such that:

$$ra + sN = 1$$

Consider now the integer r given by Extended Euclid and notice that $ra = 1 \mod N$, that is r is the multiplicative inverse of $a \mod N$. This is how Extended Euclid helps us in finding inverses.

The next question is: what happens when $\gcd(a, N) = d \neq 1$? Can we find an inverse then? Well, if we were able to, then we could find integers p, q such that $pa + qN = 1$. But we just showed that this means $\gcd(a, N) = 1$. Hence the conclusion must be:

$$a \text{ has a (multiplicative) inverse } \mod N \iff \gcd(a, N) = 1$$

Now, let's put all of this into practice.

Exercise 7. Review Extended Euclid and run it on $(697, 969)$.

Exercise 8. Find the inverses, if they exist, of $(20 \mod 79)$, $(3 \mod 62)$, $(21 \mod 91)$, $(5 \mod 23)$.

Exercise 9. If a has an inverse $\mod b$, then b has an inverse $\mod a$. Prove true or false.

Exercise 10. If a has an inverse $\mod n$, then this inverse is unique.

[3]Recall the multiplicative inverse of $x \mod N$ is that number y such that $xy = 1 \mod N$