CS 70 SPRING 2007 — DISCUSSION #4

ALEX FABRIKANT

1. Administrivia

(1) Course Information
- Next homework is **due February 13th** at 2:30pm in 283 Soda Hall; please put your section time on your homework.
- Homework 1 stats: mean 27.4/35, standard deviation 7.2, median 29.5
- Midterm 1 will be on Tuesday, March 6th, in class. All exam dates are now posted on the course website.

2. Modular Arithmetic Warmup

Exercise 1. What is $2^{2^{2006}} \bmod 3$?

3. ISBNs

Books are[1] identified by an **International Standard Book Number (ISBN)**, a 10-digit code $x_1 x_2 \ldots x_{10}$ assigned by the publisher. These 10 digits consist of blocks identifying the language, the publisher, the number assigned to the book by its publishing company, and finally, the last digit is a "check digit" that is either a digit or the letter X (used to represent the number 10). This check digit is selected so that $\sum_{i=1}^{10} i \cdot x_i \equiv 0 \pmod{11}$.[2]

Exercise 2. The ISBN for the original 1970 *Anarchist's Cookbook* starts with "0-9623032-0-". The dashes in ISBN are meaningless — they're only inserted for readability. What is the last digit?

Exercise 3. Wikipedia says that you can get the check digit by computing $\sum_{i=1}^{9} i \cdot x_i \bmod 11$. Show that Wikipedia's description is equivalent to Rosen's description (the one quoted above).

Exercise 4. Prove that changing any single digit of the ISBN will render the ISBN invalid. That is, the check digit allows you to *detect* a single-digit substitution error.

Exercise 5. Can you *switch* any two digits in an ISBN and still have it be a valid ISBN? (E.g., could both 01**2**34**5**678X and 01**5**34**2**678X both be valid ISBNs?

Exercise 6. Canada decides to change its ISBN system by doing the check digit computation modulo 12 rather than modulo 11 (if the check digit needs to be "11", they'll use "Y"). That is, the digits now have to satisfy $\sum_{i=1}^{10} i \cdot x_i \equiv 0 \pmod{11}$. Shall we blame Canada for reducing the error-detecting capabilities of the check digit?

Date: February 12, 2007.

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

[1] Technically, were, until 5 weeks ago. As of Jan 1st, 2007, the international standard is now ISBN 13, a 13-digit extension of the original 1970 ISBN 10 standard.

[2] Description reproduced from Rosen, *Discrete Mathematics*, 5th ed.

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):

```
Euclid $(a, b)$
    if $(b = 0)$, return a;
    return Euclid$(b, a \bmod b)$;
```

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

Theorem 7. *If x and y are positive integers with $x \geq y$, then* $\gcd(x, y) = \gcd(x - y, y)$.

Exercise 8. Use Euclid's algorithm to compute $\gcd(697, 969)$.

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 $ra = 1 \bmod N$, that is r is the multiplicative inverse of $a \bmod N$. 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:

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

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

Exercise 9. Review Extended Euclid and run it on $(697, 969)$.

Exercise 10. Find the inverses, if they exist, of $(20 \bmod 79)$, $(3 \bmod 62)$, $(21 \bmod 91)$, $(5 \bmod 23)$.

Exercise 11. If a has an inverse $\bmod b$, then b has an inverse $\bmod a$. Prove true or false.

Exercise 12. If a has an inverse $\bmod n$, then this inverse is unique.

6. Challenge problem

Exercise 13. Prove that, if p is a prime, then $(p-1)! \equiv -1 \pmod{p}$.

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