CS 70 SPRING 2008 — DISCUSSION #4

LUQMAN HODGKINSON, AARON KLEINMAN, MIN XU

1. Just Division

Exercise 1. After Alice, Bob, and Carol died, God decided to punish their gluttony by forcing them to divide and eat cakes for all eternity. So now, Alice, Bob, and Carol all hate cake and prefer to not have any of it but some may hate specific parts of the cake more than others. We call a division algorithm *just* for Alice if Alice will get $\leq 1/n$ of the cake by her measure, and the algorithm is just if just for everyone.

(1) For $n = 2$, is the cut-and-choose algorithm just?
(2) Is the moving knife algorithm just?
(3) Can you think of a simple way to modify the moving knife procedure so that it becomes just?

2. Modular Arithmetics

Exercise 2. (1) Suppose $x + 4 \equiv 2 \pmod{99}$. Find all possible values of x.
(2) Suppose $x + y \equiv 2 \pmod{2008}$ and $x + 2y \equiv 5 \pmod{2008}$. Find all possible values of (x, y).
(3) Suppose $x^2 + x + 1 \equiv 0 \pmod{3}$. Find all possible values of x.

Exercise 3. What is $(2008^{2007^{2006}})! \pmod{2007}$?

Exercise 4. What is $2008^{2007^{2006}} \pmod{2007}$?

Exercise 5. Prove that a number a is divisible by 4 if and only if the number formed by the last two digits of a is divisible by 4. For example, 1332 is divisible by 4 because 32 is divisible by 4.

Exercise 6. In class, you learned a method for quickly determining if a number is divisible by 9 (add up the digits of the number; the new number is divisible by 9 if and only if the original number is divisible by 9). Suppose you want to come up with a similar test for divisibility by 11. Let $a \in \mathbb{N}$ be a natural number, and define the *sign* of a to be the quantity formed by alternatively adding and subracting the digits of a. For example, if $a = 39250$ then the sign of a is $3 - 9 + 2 - 5 + 0 = -9$. Prove that a is divisible by 11 if and only if its sign is divisible by 11.

3. Asymptotic Running Time

Recall that we say $f(x) \in O(g(x))$ if $\exists N_0 \in \mathbb{N}.\exists C \geq 0.\forall x > N_0.f(x) \leq Cg(x)$.
Remember also from calculus that $\lim_{x\to\infty} f(x) = a$ is defined as $\forall \epsilon > 0.\exists N_0 \in \mathbb{N}.\forall x > N_0.a - \epsilon < f(x) < a + \epsilon$.

Exercise 7. Assume that $\forall x \in \mathbb{R}.f(x) > 0 \wedge g(x) > 0$. Also, assume that $\lim_{x\to\infty} \frac{f(x)}{g(x)}$ exists and is finite. Prove that $f(x) \in O(g(x))$.

4. Fermat's Little Theorem

Exercise 8. Suppose p is a prime number which does not divide the integer a. Prove that $a^{p-1} \equiv 1 \pmod{p}$. (A slightly more general version of this formula is the basis for RSA encryption).

Date: February 21, 2008.

The authors gratefully acknowledge the TA's of CS70 Past for the use of their previous notes: Assane Gueye, Vahab Pournaghshband, Alex Fabrikant, Chris Crutchfield, Amir Kamil, David Garmire, Lorenzo Orecchia, and Ben Rubinstein. Their notes form the basis for this handout.