CS 70 SPRING 2008 — DISCUSSION #5

LUQMAN HODGKINSON, AARON KLEINMAN, MIN XU

1. Buckets

Exercise 1. Upon hearing that our CS70 class has found a way to consistently defuse their bombs, the villains in Die Hard decided to make their puzzles harder to crack by adding more buckets. So now, you have a 6-gallon bucket, a 10-gallon bucket, and a 15-gallon bucket and the villains order you to get precisely 13 gallons of water in one bucket. But before we tackle this problem, let's do some number theory:

(1) Show that given $(6, 10, 15)$, the gcd of any pair of numbers is greater than 1. Now, find the greatest common divisor of all three numbers, what is it?
(2) Describe mathematically all possible values of the expression $6x + 10y$ where x, y are integers.
(3) Now, describe mathematically all possible values of the expression $6x + 10y + 15z$.
(4) Use the idea of the two buckets algorithm developed in class to devise a new one to get 13 gallons of water from the 3 buckets (it doesn't have to be efficient!)
(5) Describe informally how you might generalize this algorithm to solve problems involving any number of buckets?

2. Algorithmic Complexity of Modular Arithmetic with a Guest Appearance by Induction

Exercise 2. Modding is in general an $O(n^2)$ operation, but in some cases it can be faster. Prove that if a, b are integers, then $2^a - 1 \mod 2^b - 1 = 2^{(a \mod b)} - 1$. Suppose that $x = 2^a - 1, y = 2^b - 1$, what is the running time of $x \mod y$ if $\max(x, y)$ is an n-bit number.

Exercise 3. Now use the previous exercise and Euclid's algorithm to prove that $\gcd(2^a - 1, 2^b - 1) = 2^{\gcd(a,b)} - 1$.

3. Multiplicative Inverses

Exercise 4. Find the multiplicative inverse of 10 modulo 743.

Date: February 28, 2008.

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