

## CS 70 SPRING 2008 — DISCUSSION #5

LUQMAN HODGKINSON, AARON KLEINMAN, MIN XU

### 1. MORE BUCKETS

**Exercise 1.** Upon hearing that our CS70 class has found a way to consistently defuse their bombs, the terrorists 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?

#### Solutions:

- (1)  $\gcd(6, 10) = 2, \gcd(6, 15) = 3, \gcd(10, 15) = 5$ , but  $\gcd(6, 10, 15) = 1$ .
- (2) Since  $\gcd(6, 10) = 2$ , the answer is  $\{2k | k \in \mathbb{Z}\}$ .
- (3) Since the sets  $\{6x + 10y | x, y \in \mathbb{Z}\} = \{2k | k \in \mathbb{Z}\}$ , we know that  $\{6x + 10y + 15z | x, y, z \in \mathbb{Z}\} = \{2k + 15z | k, z \in \mathbb{Z}\}$ . And because  $\gcd(2, 15) = 1$ , the expression  $6x + 10y + 15z$  can evaluate to any integer given the appropriate  $x, y, z$ .
- (4) Using the reasoning of the above step, we can treat the 6-gallon bucket and the 10-gallon bucket collectively as a 2-gallon bucket. In order to fill this new "2-gallon bucket", we would perform Prof. Wagner's algorithm. And then, we can use the same algorithm to get 13 gallons from the "2-gallon bucket" and the 15 gallon bucket. Alternatively, we can just consider the 6-gallon and 10-gallon bucket as a "16-gallon" bucket and since  $\gcd(16, 15) = 1$ , we can create 13 gallons of water.
- (5) We just recursively repeat Prof. Wagner's algorithm, provided that the gcd of the capacity of the buckets actually allows us to solve the problem of course.

### 2. POTPOURRI

**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 positive integers, then  $2^a - 1 \bmod 2^b - 1 = 2^{(a \bmod b)} - 1$ . Suppose that  $x = 2^a - 1, y = 2^b - 1$ , what is the running time of  $x \bmod y$  if  $\max(x, y)$  is an  $n$ -bit number.

#### Solutions:

For the first part, we observe that  $2^{(a \bmod b)} - 1 \equiv 2^{b \lfloor a/b \rfloor} (2^{(a \bmod b)} - 1) \equiv 2^a - 1 \pmod{2^b - 1}$ . We know that to calculate  $x \bmod y$ , we need only calculate  $a \bmod b$  and then flip about  $n$  bits. Since  $x, y$  are both at most  $n$ -bits, we know that  $a, b$  are at most  $n$  and thus each have at most  $\log n$  bits. Hence,  $a \bmod b$  is about  $O((\log n)^2)$ . In order to actually create the number, we have to allocate about  $O(a \bmod b)$  bits and then set them all to "1", and since  $(a \bmod b) \in O(n)$ , the running time is  $O(n)$ .

*Date:* February 26, 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.

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

**Solutions:**

We use proof by induction over  $\min(a, b)$ . Without loss of generality, suppose that  $b \leq a$ . Base case:  $b = 1$ , then the claim is clearly true since  $2^b - 1 = 1$ . Now,  $\gcd(2^a - 1, 2^b - 1) = \gcd(2^b - 1, 2^a - 1 \pmod{2^b - 1}) = \gcd(2^b - 1, 2^{(a \pmod b)} - 1)$ . Since  $(a \pmod b) < b$ , by inductive hypothesis, we know that  $\gcd(2^b - 1, 2^{(a \pmod b)} - 1) = 2^{\gcd(b, a \pmod b)} - 1$ . Thus, we conclude that  $\gcd(2^a - 1, 2^b - 1) = 2^{\gcd(b, a \pmod b)} - 1 = 2^{\gcd(a,b)} - 1$  by another application of Euclid's Algorithm.

### 3. MULTIPLICATIVE INVERSES

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

**Solutions:**

We can use the iterative extended-gcd algorithm:

$$\begin{aligned} 1 \cdot 743 + 0 \cdot 10 &= 743 \\ 0 \cdot 743 + 1 \cdot 10 &= 10 \\ 1 \cdot 743 - 74 \cdot 10 &= 3 \\ -3 \cdot 743 + 223 \cdot 10 &= 1 \end{aligned}$$

Where we get equation  $(n)$  from subtracting equation  $(n-1)$  multiplied by a constant from equation  $(n-2)$ . This constant is the floor of the RHS of equation  $(n-2)$  divided by the RHS of equation  $(n-1)$ .

We can also use the extended-gcd algorithm.

```
e-gcd(743,10)
  e-gcd(10,3)
    e-gcd(3,1)
      e-gcd(1,0)
        return (1,1,0)
      return (1,0,1)
    return (1,1,-3)
  return (1,-3,223)
```

Since the gcd of 743 and 10 is 1, we know that 10 has a multiplicative inverse modulo 743. We know from the return values that  $1 = (-3)(743) + (223)(10)$ . Modulo 743, this is equivalent to  $1 = (223)(10)$ , telling us that 223 is the multiplicative inverse of 10 modulo 743.

- Exercise 5.**
- (1) What is  $4! \pmod 5$  ?
  - (2) What is  $6! \pmod 7$  ?
  - (3) What is  $10! \pmod 11$  ?
  - (4) Can you make a conjecture about the value of  $(p-1)! \pmod p$  when  $p$  is prime? Prove it.

**Solutions:**

We will prove that  $(p-1)! \equiv -1 \pmod p$ .

Since we are working in  $(\pmod p)$ , every number has a multiplicative inverse. Suppose that  $x^2 \equiv 1 \pmod p$  where we assume  $0 \leq x < p$ , then by definition of modular arithmetics, it has to be that  $p \mid x^2 - 1 \Rightarrow p \mid (x-1)(x+1)$ . Since  $p$  is prime, this can only happened when  $x-1 = 0$  or  $x+1 = p$ . Thus, we see that if  $x \neq 1$  and  $x \neq p-1$ , then inverse of  $x$  is not  $x$  itself. Thus, in  $(p-1)! \equiv 1 * (p-1) \equiv -1 \pmod p$ .

### 4. A CHALLENGE

**Exercise 6.** Prove or find counterexample: if  $\gcd(m, n) = 1$ , then  $\gcd(m+n, mn) = 1$ .

**Solutions:**

Suppose  $\gcd(m, n) = 1$ , then it must be that  $\gcd(m^2, n^2) = 1$  by Fundamental Theorem of Arithmetics (wikipedia this if you don't know it). Suppose  $d|m+n$  and  $d|mn$ , then  $d|m(n+m)$  and hence  $d|mn+m^2$ . Since we assume that  $d|mn$ , we conclude that  $d|m^2$ . We know also that  $d|n(n+m)$ , and hence  $d|mn+n^2$  and thus  $d|n^2$ . Since  $\gcd(n^2, m^2) = 1$ , it must be that  $d = 1$ .