CS 70, Spring 2015 — Solutions to Homework 5

Due Monday February 23 at 12 noon

1. **Multiplicative Inverses**

   Assume $jamodn$ is not distinct for $j = 0, 1, 2, ..., n-1$. Meaning there exists j_i and j_k inside the element set j such that $j_i a \pmod{n} = j_k a \pmod{n}$.

   Therefore $a(j_i - j_k) \equiv_n 0$

   Then $\exists q \in \mathbb{Z}$ such that $nq = a(j_i - j_k)$. Note that $gcd(a, n) = 1$.

   Therefore $q = \pm a$ and $n = \pm(j_i - j_k)$

   This cannot be true because j can be at max $\pm(n-1)$ apart when $j_k = 0$ and $j_i = n-1$. This contradicts assumption.

   So all $ja \pmod{n}$ values are dinstact. Since we have n-values, starting at 0 to $n-1$. Number 1 has to be part of the set since it also has to be less than n. As a result, $a^{-1} \pmod{n}$ exists because one of the element in the set j, called j_x, will make it such that $j_x a \equiv_n 1$ by the definition of an inverse.

2. **Combining moduli**

(a) Given:

$$a \equiv 1 \mod 5$$
$$a \equiv 0 \mod 8$$

$a = 16$ because
$16 \equiv_5 1$ and $16 \equiv_8 0$

(b) Given:

$$b \equiv 0 \mod 5$$
$$b \equiv 1 \mod 8$$

$b = 25$ because
$25 \equiv_5 0$ and $25 \equiv_8 1$

(c) Given:

$$c \equiv 2 \mod 5$$
$$c \equiv 5 \mod 8$$

$c = 5b + 2a$ because
$5b + 2a = 157$
$157 \equiv_5 2$ and $157 \equiv_8 5$

(d) $d = 28$ because
$28 \equiv_5 3$ and $28 \equiv_8 4$
We find it by doing this:

$$\begin{aligned} d &\equiv_5 3 \\ d &= 5k + 3 \\ d &\equiv_8 4 \\ 5k + 3 &\equiv_8 4 \\ 5k &\equiv_8 1 \\ 5(5k) &\equiv_8 5 \\ k &\equiv_8 5 \\ k &= 8j + 5 \\ d &= 5(8j + 5) + 3 \\ d &= 40j + 28 \end{aligned}$$

Hence, the leftover is 28. Which is why we made $d = 28$

(e) $28 * 157 \equiv_4 04$
$c * d \equiv_5 2 * 3 \Rightarrow c * d \equiv_5 6 \Rightarrow c * d \equiv_5 1 \Rightarrow 4396 \equiv_5 1$. This statement is true.
$c * d \equiv_8 5 * 4 \Rightarrow c * d \equiv_8 20 \Rightarrow c * d \equiv_8 4 \Rightarrow 4396 \equiv_8 4$. This statement is true.

3. **CRT**

(a) i. I do this by constructive proof because I have no idea of how else to literally prove this. So the answer should be: $c = \frac{r_1 n_1 n_2}{n_1} * n_2^{-1} \pmod{n_1} + \frac{r_1 n_1 n_2}{n_2} * n^{-1} \pmod{n_2}$

ii. We attempt to simplify this by letting $e_2 \equiv_{n_1} n_2^{-1}$ and $e_1 \equiv_{n_2} n_1^{-1}$. Then our equation is now: $c = r_1 n_1 e_2 + r_2 n_1 e_1$.

iii. Note that $r_2 n_1 e_1$ remainder is 0 because we have n_1. So when we take (mod n_1), that side has a factor of n_1 and therefore will not have any remainders. So our only remainder comes from $r_1 n_1 e_2$.

iv. $c \equiv_{n_1} r_1 n_2 e_2$

v. We know that n_2 and e_2 will cancel out because of the definition of an inverse. Therefore the only thing left will be $c \equiv_{n_1} r_1$. Which is correct according to the first part of our given.

vi. To prove $c \equiv_{n_2} r_2$ is similar to how we proved $c \equiv_{n_1} r_1$.

vii. Now, $r_1 n_1 e_2$ has the remainder of 0 because there is a factor of n_2. Now our only remainder comes from $r_2 n_1 e_1$.

viii. $c \equiv_{n_2} r_2 n_1 e_1$

ix. Again, we know that n_1 and e_1 will cancel out by the definition of an inverse. Therefore the only thing left is $c \equiv_{n_2} r_2$. This proves the second part of what we are given.

x. Now we attempt to prove by contradiction that C is not unique. Meaning there exists a d such that $d \equiv_{n_1} r_1$ and $d \equiv_{n_2} r_2$ such that $c \equiv_{n_2} r_2$ and $c \equiv_{n_1} r_1$.

xi. This means that $d - c \equiv_{n_1} r_1 - r_1$ $d - c \equiv_{n_2} r_2 - r_2$.

xii. Similarly this means $d - c \equiv_{n_1} 0$ $d - c \equiv_{n_2} 0$. So this means the following: $n_1 \mid (d-c)$ and $n_2 \mid (d-c)$ and because $gdc(n_1, n_2) = 1$ it can be $n_1 n_2 \mid (d-c)$

xiii. Then you can rewrite it as $d - c = n_1 n_2 q, q \in \mathbb{Z} \Rightarrow d = n_1 n_2 q + c$

xiv. Now when we do $d \equiv_{n_1 n_2} c$ because the first part has both factors n_1 and n_2. So the only remainder would be c. Therefore it cannot be the same, and c has to be unique since it's the same.

(b) i. Similarly, I looked up equation which gave me: $c = \sum_{i=1}^{k} \left(\frac{r_i \prod_{j=1}^{k} n_j}{n_i} * \frac{n_j^{-1} (mod n_i)}{n_i^{-1} (mod n_i)} \right)$

ii. Consider for the i^{th} equation: $c_i \equiv_{n_i} r_i$

iii. Notice that only the i^{th} term will matter because all the other terms has its factors of n_i and therefore it will be divisible, and will not have a remainder.

iv. Therefore what we look at will be: i^{th} term $= r_i(n_1 * n_2 * n_3 * ... * n_{i-1} * n_{i+1} * ... * n_n) * (n_1^{-1} * n_2^{-1} * ... * n_{i-1}^{-1} * n_{i+1}^{-1} * ... * n_n^{-1})$

v. Notice that everything will cancel out such that we are left with r_i because it times its inverse will result in 1.

vi. This will work for all i's up to k, we just need to repeat the process.

vii. Now we will try to prove that c is unique by saying it is not unique and there exists another solution d that is the same. Therefore: $d \equiv_{n_i} r_i$ and $c \equiv_{n_i} r_i$

viii. $d - c \equiv_{n_i} r_i - r_i = 0$

ix. By definition $n_i \mid d - c$. And since all of n's are pairwise prime, we can write again: $n_1 * n_2 * ... * n_n \mid d - c$

x. Therefore we can rewrite as $d - c = n_1 * n_2 * n_3 * ... * n_n * q, q \in \mathbb{Z}$

xi. $d = n_1 * n_2 * ... * n_n + c$

xii. Therefore as before, we have the same answer because we see our only remainder can only be c in this situation. So our equation is now $d \equiv_n c$. Hence they are the same and c is unique

4. **Consecutive composites**

   Our numbers will be $(k+1)!+2, (k+1)!+3, (k+1)!+4, ..., (k+1)!+(k+1)$

   This works because the i^th term where $i \leq k$ will be divisible by $i+1$, therefore it is a list of composite numbers by the definition of a prime number. This works is because we are doing factorials of the one before it $(i+1)$. Therefore when we look at i, it has to exist since we use $(i+1)$ multiplied in there.

5. **Binary GCD**

(a) i. If m is even and n is even, $gcd(m, n) = 2gcd(\frac{m}{2}, \frac{n}{2})$.
The reason this is true because we can write m and n as the following because of the fundamental theorem of arithmetic:
$m = 2^{m_1} * 3^{m_2} * 5^{m_3} * ...$
$n = 2^{n_1} * 3^{n_2} * 5^{n_3} * ...$
Therefore we can rewrite: $gcd(m, n) = 2^{min(m_1,n_1)} * 3^{min(m_2,n_2)} * 5^{min(m_3,n_3)} * ...$
As a result, when we divide 2 out of m and n, our rewritten versions will look like this:
$\frac{m}{2} = 2^{m_1-1} * 3^{m_2} * 5^{m_3} * ...$
$\frac{n}{2} = 2^{n_1-1} * 3^{n_2} * 5^{n_3} * ...$
Now we can see that regardless, the $min(m_1 - 1, n_1 - 1) = min(m_1, n_1) - 1$.
As a result, our equation can now be rewritten as $2(2^{min(m_1-1,n_1-1)}*3^{min(m_2,n_2)}* 5^{min(m_3,n_3)} * ...)$
Which is equivalent to $2gcd(\frac{m}{2}, \frac{n}{2})$ since $gcd(\frac{m}{2}, \frac{n}{2}) = 2^{min(m_1-1,n_1-1)}*3^{min(m_2,n_2)}* 5^{min(m_3,n_3)} * ...$

ii. If m is even and n is odd, $gcd(m, n) = gcd(\frac{m/2}{2}, n)$.
Similarly we can rewrite m and n. Note that n is odd so our 2 will be 2^0
$n = 2^0 * 3^{n_2} * 5^{n_3} * ...$
$m = 2^{m_1} * 3^{m_2} * 5^{m_3} * ...$
Now we notice that the $min(0, m_1) = min(0, m_1 - 1) = 0$ when we do the minimum for 2 to the power. Therefore, when you pull out the 2 from m, it does not affect the minimum whatsoever, so our equation stays static. As a result, both side of the equation is equivalent.

iii. If m, n are both odd and $m \geq n$, $gcd(m, n) = gcd(\frac{(m-n)}{2}, n)$
First, state that $gcd(m, n) = b$. Then we can say that $m = ab$ and $n = cb$, where a, b, and c are all odd because n and m are odd.
Then we can say that $m - n = ab - cb = b(a - c)$. We also need to note that $(a - c) \Rightarrow even$ because $odd - odd \Rightarrow even$ and $odd * even \Rightarrow even$.
Now we can do $gcd(b(a - c), n)$, which should still be b because b was the greatest common factor in m and n. And since $m > b(a - c)$, the greatest common factor can only go down not up. And threfore $gcd(b(a - c), n) = b$
We substitute $x = b(a - c)$ and rewrite $gcd(\frac{x}{2}, n)$. We know from part 2, that it is equivalent to $gcd(x, n)$. Therefore, going backward, we know $gcd(x, n) = gcd(b(a - c), n) = gcd(m - n, n) = gcd(m, n)$. QED.

(b) Missing part:

If m is greater than or equal to n, return $gcd((m - n)/2, n)$

Else m is less than n, return $gcd((n - m)/2, m)$

Proof: we will follow down whatever repetition we need to go down. Up to a point, it will return either 1 or 2, which will eventually bring us down to either 1 or 2 as a GCD and we can eventually multiply it backwards to find the number we need to.

6. **Midterm 1**

```
Begin FindCoin(Coins C):
        divide C into 3 equal amounts called p_one, p_two, and p_three
        if p_one is heavier than p_two:
                if p_one has 1 coin:
                        return p_two
                return FindCoins(p_two)
        otherwise if p_one is lighter than p_two:
                if p_one has 1 coin:
                        return p_one
                return FindCoin(p_one)
        otherwise:
                if p_one has 1 coin:
                        return p_three
                return FindCoin(p_three)
End FindCoin
```

Proof: We will prove by induction on n, number of times we will need to weigh the coins.

Base Case: $n = 0$, there is only 1 coin. Therefore it is automatically the counterfeit since in every pile there exists a counterfeit. Our second base case can be $n = 1$. $3^1 = 3$, this means there are 3 coins, call it A, B, C. We can do this in one weighing because say we weigh A and B. There are three cases:

Case 1. A is heavier than B. Then B is the counterfeit coin.

Case 2. A is lighter than B. Then A is the counterfeit coin.

Case 3. A has the same weight as B. Then C is the counterfeit coin.

Hypothesis: $\exists k \in \mathbb{Z}$ such that $n = k$, which gives 3^k coins and we can find the counterfeit inside the 3^k in k-weighings.

Step: Say we have 3^{k+1} coins, that means within this, there are 3^k coins within this. That means we can weigh and eliminate 3^k coins from our pile of 3^{k+1} coins to a smaller pile that we will call x, such that $x = 3^{k+1} - 3^k$. From algebra, we know $3^{k+1} - 3^k = 3^{k-k+1} = 3^1$. So $x = 3^1$ means in this case $n = 1$. And from our basecase, we know that it takes 1 weighing. Therefore it will take $k + 1$ weighing. QED.

7. **Midterm 2**

   Number 6:

Proof: We will prove by induction on n, numbers of vertices.

Base Case: n = 2. v1 —— v2. We see that we can create a spanning tree with 1 edge, and whether we start at v1 or v2, it is still a tree. Both of these fit the description of a spanning tree and the graph in general is a complete graph.

Hypothesis: $\exists k \in \mathbb{Z}$ such that k is even and $n = k$ will create a spanning tree with $\frac{n}{2}$ edges.

Step: For $n = k + 2$, we know since it is a completed graph, there exists a completed subgraph of $n = k$. And by our hypothesis, we can find a spanning tree for $n = k$ vertices. This means that there exists a spanning tree with $\frac{k}{2}$ edges.

Let the set of vertices in the spanning tree for $n = k$ called V_s

Now we will choose a vertex, $v_x \in V_s$ and connect it it to vertex v' such that $v' \notin V_s$. The reason for this is v_x connects to another vertex within V_s, it will create a cycle and as a result, it will not be a tree at all. We also know that we can connect to another v' because this is a completed graph, therefore all vertices have edges connecting to all other vertices.

So by the definition, this covers the spanning tree definition that we wanted, such that there are $n/2$ edges. And there are no cycle because no vertices point back to each other. We know that this satisfy because for $n = k + 2$, the number of edges we should have is $k/2 + 1$, which is true in this case since we know for k it takes $k/2$ edges, and we included the additional edge in. QED.