CS 6001 Homework 2

Michael Catanzaro, Jacob Fischer, Christian Storer

September 22, 2016

1 Find an x that satisfies the following linear congruences

$$x \equiv 2 \; mod \; 5$$
$$x \equiv 3 \; mod \; 7$$
$$x \equiv 8 \; mod \; 11$$

To do so, use Chinese Remainder Theorem

$$x \equiv a_i \ mod \ n_i$$

$$x = N_1 * b_1 * a_1 + N_2 * b_2 * a_2 + N_3 * b_3 * a_3$$

$$n = 5 * 7 * 11 = 385$$

$$\begin{aligned} a_1 &= 2 \\ n_1 &= 5 \\ N_1 &= n/n_1 = 77 \end{aligned}$$

$$\begin{aligned} a_2 &= 3 \\ n_2 &= 7 \\ N_2 &= n/n_2 = 55 \end{aligned}$$

$$\begin{aligned} a_3 &= 8 \\ n_3 &= 11 \\ N_3 &= n/n_3 = 35 \end{aligned}$$

$$N_i * b_i \equiv 1 \ mod \ n_i$$

$$\begin{aligned} N_1 * b_1 &\equiv 1 \ mod \ n_1 \\ 77 * b_1 &\equiv 1 \ mod \ 5 \\ b_1 &\equiv 3 \end{aligned}$$

$$\begin{aligned} 55 * b_2 &\equiv 1 \ mod \ 7 \\ b_2 &= 6 \end{aligned}$$

$$\begin{aligned} 35 * b_3 &\equiv 1 \ mod \ 11 \\ b_3 &= 6 \end{aligned}$$

$$\begin{aligned} x &= 77 * 3 * 2 + 55 * 6 * 3 + 35 * 6 * 8 \\ x &= 3132 \end{aligned}$$

2 Discuss some useful applications of the Chinese Remainder Theorem

CRT is useful for secret sharing. If you have some secret code x, and you want it to be shared among n people, however you also wish that any subset of the n people cannot decipher the code x without all n people. To do this, you give each member some function $f_i()$, which is one of congruence equations in Problem 1. To find the x that satisfies all the equations $f()$ you must have all the $f_i()$. Having only a subset does not spoil the secret, as they cannot calculate x.

3 Under the RSA encryption scheme, suppose p = 89 and q = 113.

Let e = 17, show how to derive the private key d.

$$\begin{aligned}\varphi(n) &= (p-1)(q-1)\\ &= (89-1)(113-1) = 9856\end{aligned}$$

$$GCD(e, \varphi(n)) = GCD(17, 9856) = 1$$

$$\begin{aligned}d * e \ mod \ \varphi(n) &= 1\\ d * 17 \ mod \ 9856 &= 1\end{aligned}$$

To find d from here, we can use Euclid's algorithm

$$17 * d = 1 \ (mod 9856)$$

$$\begin{aligned}9856 &= 17 * 579 + 13 \rightarrow 13 = 9856 - 17 * 579\\ 17 &= 13 * 1 + 4 \rightarrow 4 = 17 - 13 * 1\\ 13 &= 4 * 3 + 1 \rightarrow 1 = 13 - 4 * 3\\ 4 &= 1 * 4\end{aligned}$$

$$GCD(9856, 17) = 1$$

$$
\begin{aligned}
1 &= 13 - 4 * 3 \\
&= (9856 - 17 * 579) - (17 - 13) * 3 \\
&= 9856 - 17 * 579 - (17 - (9856 - 17 * 579)) * 3 \\
&= 9856 - 17 * 579 - (17 * 3 - (9856 * 3 - 17 * 579 * 3)) \\
&= 9856 - 17 * 579 - (17 * 3 - 9856 * 3 + 17 * 579 * 3) \\
&= 9856 - 17 * 579 - 17 * 3 + 9856 * 3 - 17 * 579 * 3 \\
&= 9856 * 4 - 17 * 2319 \\
d &= 9856 - 2319 \\
d &= 7537
\end{aligned}
$$

Given m = 65, compute the encryption of m and verify the encryption is correct by decrypting the encrypted value.

$$E(m) = m^e \ mod \ n$$

$$n = 89 * 113 = 10057$$

$$
\begin{aligned}
E(65) &= 65^17 \ mod \ 10057 \\
E(65) &= 6619 \\
e &= 6619
\end{aligned}
$$

$$
\begin{aligned}
D(e) &= e^d mod \ n \\
D(e) &= 6619^7 537 \ mod \ 10057 \\
D(e) &= 65
\end{aligned}
$$

4 Show $f_a(x) = ax \mod n$ is a permutation of Z_n^*

Because $f_a(x) : Z_n^* \mapsto Z_n^*$, $x \in Z_n^*$ must be true. By applying the closure property of multiplicative operators it is known that,

$$x, a \in Z_n^* \implies xa \in Z_n^*$$

For $f_a(x)$ to be a permutation of Z_n^*, it must be a one-to-one function such that

$$a_i x \mod n \neq a_j x \mod n : a_i \neq a_j \text{ and } a_i, a_j \in Z_n^*$$

To prove this assume $a_i x \mod n = a_j x \mod n$

$$
\begin{aligned}
a_i x \mod n = a_j x \mod n &\implies a_i x + kn = a_j x + k'n : k, k' \text{ are some integer} \\
&\implies a_i x - a_j x = n(k' - k) \\
&\implies a_i x \equiv a_j x \mod n
\end{aligned}
$$

However,

$$\begin{aligned}
x \in Z_n^* &\implies \gcd(x,n) = 1 \\
\gcd(x,n) = 1 &\implies xi \not\equiv xj \mod n : 0 \leq i < j < n \\
xi \not\equiv xj \mod n &\implies a_i x \not\equiv a_j x \mod n
\end{aligned}$$

Thus $f_{a_i}(x) \neq f_{a_j}(x)$ is one-to-one and since $\forall a, x \in Z_n^* \implies ax \in Z_n^*$ it can be said that $f_a(x)$ is a permutation of Z_n^*.

5 Show that if p is a prime and e is a positive integer, then $\phi(p^e) = p^{e-11}(p-1)$

Based on the definition of Euler's totient function, $\phi(p^e)$ is the number of positive integers $m \leq p^e$ such that $\gcd(m, p^e) = 1$. This can also be rewritten as the p^e minus the number positive integers $m \leq p^e$ such that $\gcd(m, p^e) \neq 1$.

Because p^e is $p * p * \ldots * p$, e times, only a multiple of p can divide p^e.

$$\begin{aligned}
\gcd(m, p^e) \neq 1 &\implies m = kp : k \in \mathbb{Z}^+ \\
m \leq p^e &\implies m = 1p, 2p, \ldots, p^{e-1}p \\
m = 1p, 2p, \ldots, p^{e-1}p &\implies k = 1, 2, \ldots, p^{e-1} \\
k = 1, 2, \ldots, p^{e-1} &\implies \exists p^{e-1} \text{ numbers}(m\text{'s}) : \gcd(m, p^e) \neq 1
\end{aligned}$$

$\therefore \phi(p^e) = p^e - p^{e-1} = p^{e-1}(p-1)$

6 Prove that Z_n^* is a group where the group operation is multiplication modulo n

For $a, b \in Z_n^*$ prove $a * b \in Z_n^*$

$$\begin{aligned}
a, b \in Z_n^* &\implies \gcd(a,n) = 1 \land \gcd(b,n) = 1 \\
\gcd(a,n) = 1 &\implies ap + nq = 1 : p, q \in \mathbb{Z} \\
\gcd(b,n) = 1 &\implies bp' + nq' = 1 : p', q' \in \mathbb{Z}
\end{aligned}$$

$$
\begin{aligned}
ap + nq &= 1 \\
1 - nq &= ap \\
&= ap(1) \\
&= ap(bp' + nq') \\
&= apbp' + apnq' \\
1 &= apbp' + apnq' + nq \\
&= abpp' + n(apq' + q) \\
&= abp'' + nq'' \\
1 = abp'' + nq'' &\implies \gcd(ab, n) = 1
\end{aligned}
$$

Since $\gcd(ab, n) = 1$ closure exists for the multiplication operation