Math55Hw6

Trustin Nguyen

October 2022

Chinese Remainder Theorem, Cryptography, and Review

Chapter 4.4

Exercise 20: Use the construction in the proof of the Chines remainder theorem to find all solutions to the system of congruences $x \equiv 2 \pmod 3$, $x \equiv 1 \pmod 4$, $x \equiv 3 \pmod 5$.

$x_1 \equiv 1 \pmod 3$	$x_1 \equiv 0 \pmod 4$	$x_1 \equiv 0 \pmod 5$
$x_2 \equiv 0 \pmod 3$	$x_2 \equiv 1 \pmod 4$	$x_2 \equiv 0 \pmod 5$
$x_3 \equiv 0 \pmod 3$	$x_3 \equiv 0 \pmod 4$	$x_3 \equiv 1 \pmod 5$

We have:

$$x_1 \equiv 20y_1 \equiv 1 \pmod 3,\ x_2 \equiv 15y_2 \equiv 1 \pmod 4\ ,\ x_3 \equiv 12y_3 \equiv 1 \pmod 5$$

Euclidean Algorithm:

$20 = 6(3) + 2$ $3 = 1(2) + 1$	$2 = 20 - 6(3)$ $1 = 3 - 1(2)$	So $1 = 3 - 20 + 6(3) = 7(3) - 20$.
$15 = 3(4) + 3$ $4 = 1(3) + 1$	$3 = 15 - 3(4)$ $1 = 4 - 1(3)$	So $1 = 4 - 1(15 - 3(4)) = 4(4) - 15$
$12 = 2(5) + 2$ $5 = 2(2) + 1$	$2 = 12 - 2(5)$ $1 = 5 - 2(2)$	So $1 = 5 - 2(12 - 2(5)) = 3(5) - 2(12)$

Results: $y_1 = -1$, $y_2 = -1$, $y_3 = -2$. Construction of x:

$$x = (2(20)(y_1) + 1(15)(y_2) + 3(12)(y_3)) \mod 60$$
$$x = (-40 - 15 - 72) \mod 60$$
$$x = (-127) \mod 60$$
$$\text{x}{=}180 - 127{=}\ \boxed{53}$$

Exercise 29: Let $m_1, m_2, ..., m_n$ be pairwise relatively prime integers greater than or equal to 2. Show that if $a \equiv b \pmod{m_i}$, for $i = 1, 2, ..., n$, then a $\equiv$ b (mod m) where $m = m_1m_2...m_n$.

Proof. Suppose $a \equiv b \pmod{m_i}$, for i = 1,2, ..., n. We have by definition:

$$\begin{gathered} m_1|(a-b) \\ m_2|(a-b) \\ \vdots \\ m_n|(a-b) \end{gathered}$$

Proposition: If j and k are relatively prime and j|n and k|n, then jk|n. We have

j(a)=n, k(b)=n

For some a,b $\in \mathbb{R}$, so j(a)=k(b) and j|kb.
By Euclid's Lemma, since j does not divide k, j divides b. We can conclude that

$$m_1 m_2 \ldots m_n|(a-b)$$

as desired. $\square$

Exercise 30: Complete the proof of the Chinese Remainder Theorem by showing that the simultaneous solution of a system of linear congruences modulo pairwise relatively prime moduli is unique modulo the product of these moduli.

Proof. Suppose x and y are two simultaneous solutions to a system of linear congruences modulo pairwise relatively prime moduli. They we have:

$$\begin{array}{c|c} x \equiv a_1 \pmod{m_1} & y \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} & y \equiv a_2 \pmod{m_2} \\ \vdots & \vdots \\ x \equiv a_n \pmod{m_n} & y \equiv a_n \pmod{m_n} \end{array}$$

Thus,

$$\begin{gathered} x \equiv y \pmod{m_1} \\ x \equiv y \pmod{m_2} \\ \vdots \\ x \equiv y \pmod{m_n} \end{gathered}$$

Or,

$$\begin{gathered} x-y \equiv 0 \pmod{m_1} \\ x-y \equiv 0 \pmod{m_2} \\ \vdots \\ x-y \equiv 0 \pmod{m_n} \end{gathered}$$

Since m_i divides $x-y$ for all $i = 1, 2, \ldots, n$, from Exercise 30, $m_1 m_2 \ldots m_n | x-y$. We have shown that x and y are congruent modulo $m_1 m_2 ... m_n$, so there is a unique solution in $\{1,\ 2,\ \ldots,\ m_1 m_2 \ldots m_n - 1\}$ as desired. $\square$

Chapter 4.6

Exercise 23: Show that we can easily factor n when we know that n is the product of two primes, p and q, and we know the value of $(p-1)(q-1)$.

Proof. Suppose we know $n = pq$ and the value of $(p-1)(q-1)$. Let the difference of n and $(p-1)(q-1)$ to be d. Observe that

$$\begin{aligned}
(p-1)(q-1) &= pq - p - q + 1 \\
n - (p-1)(q-1) &= p + q - 1 \\
d &= p + q - 1 \\
d + 1 &= p + q
\end{aligned}$$

Consider the polynomial with roots p, q:

$$(x-p)(x-q)$$

$$x^2 - (p+q)x + pq$$
$$x^2 - (d+1)x + n$$

Using the quadratic formula:

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

We can find p, q which are

$$\frac{(d+1) - \sqrt{(d+1)^2 - 4n}}{2}$$

and

$$\frac{(d+1) + \sqrt{(d+1)^2 - 4n}}{2}$$

as desired. $\square$

Exercise 26: What is the original message encrypted using the RSA system with $n = 53 \cdot 61$ and $e = 17$ if the encrypted message is 3185 2038 2460 2550?
Inverse of $e = 17$ modulo $52 \cdot 60$:
Euclidean Algorithm:

$$\begin{array}{c|c}
3120 = 183(17) + 9 & 9 = 3120 - 183(17) \\
17 = 1(9) + 8 & 8 = 17 - 1(9) \\
9 = 1(8) + 1 & 1 = 9 - 1(8)
\end{array}$$

$$1 = 9 - 1(17 - 1(9) = 2(9) - 17 = 2(3120 - 183(17)) - 17 = 2(3120) - 367(17)$$

$$e^{-1} \equiv -367 \equiv 2753 \pmod{3120}$$
$$\hat{M} = (3185^{2753} \mod 3233)\ (2038^{2753} \mod 3233)\ (2460^{3233} \mod 3233)$$
$$(2500^{3233} \mod 3233)$$

Exercise 28: Suppose that (n, e) is an RSA encryption key, with $n = pq$ where p and q are large primes and $gcd(e, (p-1)(q-1)) = 1$. Furthermore, suppose that d is the inverse of e modulo $(p-1)(q-1)$. Suppose that $C \equiv M^e \pmod{pq}$. In the text, we showed that RSA decryption, that is, the congruence $C^d \equiv M \pmod{pq}$ holds when $gcd(M, pq) = 1$. Show that this decryption congruence also holds when $gcd(M, pq) > 1$.

Proof. Consider the system of congruences:

$$\begin{aligned} x &\equiv M \pmod{p} \\ x &\equiv M \pmod{q} \end{aligned}$$

Observe that the system holds when $x = M$. But when $gcd(M, pq) > 1$, we have $p|M$, $q|M$, or $pq|M$. Consider one variable p. If p divides M, then

$$M^{ed} \equiv M \equiv 0 \pmod{p}$$

If p does not divide M, then we can use Fermat's Little Theorem:

$$M^{p-1} \equiv 1 \pmod{p}$$

We also know that:

$$\begin{aligned} ed &\equiv 1 \pmod{(p-1)(q-1)} \\ ed - 1 &= k(p-1)(q-1) \\ ed &= k(p-1)(q-1) + 1 \end{aligned}$$

So

$$M^{ed} \equiv M^{k(p-1)(q-1)} \cdot M \equiv 1 \cdot M \equiv M \pmod{p}$$

Since for all cases, $M^{ed} \equiv M \pmod{p}$ and $M^{ed} \equiv M \pmod{q}$, from Lesson 4.4 Exercise 29,

$$M^{ed} \equiv M \pmod{pq}$$

Therefore,

$$C^d \equiv M \pmod{pq}$$

as desired. □