4 CRT, RSA, and Polynomials

Computer Science Mentors 70

Sept 28 - Oct 2
Fall 2020

Prepared by: Aishani Sil, Austin Lei, Agnibho Roy, Debayan Bandyopadhyay, Abinav Routhu

1 CRT

1. Suppose we have a number v, which we do not know, but which satisfies the following system of modular equivalences. The numbers n, l, and m are coprime to each other.

$$\begin{aligned} v &\equiv a \mod \ell \\ v &\equiv b \mod m \\ v &\equiv c \mod n \end{aligned}$$

We want to use the numbers a, b, and c, which we do know, to reconstruct v.

Just for this worksheet, we will compactly write the system of modular equivalences as a tuple, for example, $v \equiv (a, b, c)$.

(a) Construct a number x' which is zero mod m and mod n, but is nonzero mod ℓ.

Solution: A number which is zero mod m and mod n must be a multiple of m and n. We can choose $x' = mn$. Because m and n share no factors with ℓ, $x' = mn$ is not a multiple of ℓ, so it is nonzero mod ℓ.

(b) Using x' from the previous part, construct a number x which is still zero mod m and mod n, but is now 1 mod ℓ. In other words, find $x \equiv (1, 0, 0)$.

Solution: Because m and n are coprime to ℓ, they have multiplicative inverses mod ℓ. If we multiply x' by their inverses, we can scale x' to be 1 mod ℓ. In symbols, $x = (m^{-1} \text{mod } \ell)(n^{-1} \text{mod } \ell)x' = m(m^{-1} \text{mod } \ell) \cdot n(n^{-1} \text{mod } \ell)$. Because it is still a multiple of m and of n, it will still be zero in those moduli.

(c) We want to do the same with the other two moduli. Find $y \equiv (0, 1, 0)$ and $z \equiv (0, 0, 1)$.

Solution: Following the same process, $y = \ell(\ell^{-1} \text{mod } m) \cdot n(n^{-1} \text{mod } m)$, and $z = \ell(\ell^{-1} \text{mod } n) \cdot m(m^{-1} \text{mod } n)$.

(d) Using the numbers x, y, and z above, construct a number v which satisfies our system of modular equivalences. Is this the only number v that satisfies this system of equivalences? Why or why not?

Solution: Consider $v = ax + by + cz$. We've scaled up the relevant bit in each modulus and added them together. The amount that we scale x has no effect on the equivalence mod m and mod n, for example, but allows us to match the condition $v \equiv a$ mod ℓ. This is not the only solution, as we can add multiples of ℓmn to our solution and still satisfy the above equivalences.

(e) If two numbers v and w both satisfy the system of modular equivalences, meaning $v \equiv (a, b, c) \equiv w$, show that $v \equiv w$ mod ℓmn.

Solution: Consider the number $u = v - w$. Because v and w are the same under the three different equivalences, subtracting them will just give zero under each modulus. Now we use the procedure above to reconstruct $u = (0, 0, 0)$. This gives $u = 0x + 0y + 0z = 0$. So $u = 0$ is a valid solution to this system of equivalences, but from our previous answer, we know that any multiple of ℓmn can be added to this. Thus, $u \equiv 0$ mod ℓmn, which implies that $v \equiv w$ mod ℓmn.

2. The supermarket has a lot of eggs, but the manager is not sure exactly how many he has. When he splits the eggs into groups of 5, there are exactly 3 left. When he splits the eggs into groups of 11, there are 6 left. What is the minimum number of eggs at the supermarket?

Solution: We have that $x \equiv 3 \mod 5$ and $x \equiv 6 \mod 11$. We can use the Chinese Remainder Theorem to solve for x.

Recall from the note on modular arithmetic, the solution to x is defined as $x = \sum_{i=1}^{k} a_i b_i \mod N$, where b_i are defined as $\left(\frac{N}{n_i}\right)\left(\frac{N}{n_i}\right)^{-1}_{\text{mod } n_i}$ and $N = n_1 \cdot n_2 ... \cdot n_k$.

In our case, $a_1 = 3$, $a_2 = 6$, $n_1 = 5$ and $n_2 = 11$.

$$b_1 = \left(\frac{55}{5}\right)\left(\frac{55}{5}\right)^{-1}_{\text{mod } 5} = 11 \cdot 11^{-1}_{\text{mod } 5} = 11 * 1 = 11$$

$$b_2 = \left(\frac{55}{11}\right)\left(\frac{55}{11}\right)^{-1}_{\text{mod } 11} = 5 \cdot 5^{-1}_{\text{mod } 11} = 5 * 9 = 45$$

Therefore, $x \equiv 3 \cdot 11 + 6 \cdot 45 (\mod 55) = 28$

You can quickly verify that 28 indeed satisfies both conditions.

3. The numbers 124, 125, 126 are special, because they form a sequence of three consecutive numbers which are all divisible by square numbers greater than 1 (124 is divisible by 4, 125 divisible by 25, and 126 divisible by 9). Show that there exists a sequence of 100 consecutive numbers, all of which are divisible by a square number greater than 1.

Solution: By Chinese remainder theorem, there exists a number n such that n is 0 mod 4, 1 mod 9, 2 mod 25, ..., (100-1) mod (100th prime number)^2 (Note that all the mod amounts are relatively prime). Then $n - 1$ is divisible by 9, $n - 2$ is divisible by 16, ..., $n - 99$ is divisible by $(100\text{th prime number})^2$. This forms a sequence of 100 consecutive numbers, all of which are divisible by a square number greater than 1.

2 RSA

Main idea: Given two large primes, p and q, and a message x (an integer), find an encryption function E and an decryption function D such that $D(E(x)) = x$. In other words, two people can encrypt and decrypt a message if they know E and D.
Mechanism:
N = pq
$E(x) = x^e$ mod N
$D(x) = x^d$ mod N, where $d = e^{-1}$ mod$(p-1)(q-1)$
The pair (N, e) is the recipient's **public key**, and d is the recipient's **private key**. The sender sends $E(x)$ to the recipient, and the recipient uses $D(x)$ to recover the original message. The security of RSA relies on the assumption that given N, there is no efficient algorithm to determine $(p-1)(q-1)$.

1. **RSA-BC123 [Practice Bank]**
Bob would like to receive messages from Alice via RSA.

(a) He chooses 2 primes, $p = 7$ and $q = 11$. What is N?

Solution: $N = pq = (7)(11) = 77$

(b) He chooses $e = 7$. To what number is e relatively prime?

Solution: e must be relatively prime to $(p-1)(q-1) = 60$.

(c) Calculate d.

Solution: $d = e^{-1} \bmod (p-1)(q-1) = 7^{-1} \bmod 60 = 13$

(d) Imagine Alice wants the send Bob a message $x = 30$. She applies her encryption function $E(x)$ to 30. What is the encrypted message?

Solution: $E(x) = x^e \bmod N \rightarrow 30^7 \bmod 77 = 2$

(e) What is the result of Bob applying his decryption function $D(x')$?

Solution: $D(x') = (x')^d \bmod 77 = 2^{43} \bmod 77 = 30$

2. **RSA T/F [Practice Bank]**

(a) Bob has to publish his key (N, e) to get encrypted messages from Alice.

Solution: True. This is the public key.

(b) Alice needs to know Bob's key d to send encrypted messages to Bob.

Solution: False. This is the private key. Anyone with this value can decrypt messages.

(c) The security of RSA relies on the "computation intractability" of determining x from $y = x^e$ even when y and e are known.

Solution: True. Factoring is hard.

(d) $E(x) = x^e \bmod N$ is a bijection on GF(N).

Solution: True.

3. **Prove the correctness of RSA.**
Hint: Proving RSA amounts to showing that given $d = e^{-1} \bmod (p-1)(q-1)$:

$$(x^e)^d = x \bmod N \qquad \forall x \in \{0, 1, 2, \ldots, N-1\}$$

Solution:

$$\begin{aligned}(x^e)^d &= x \bmod N \qquad \forall x \in \{0,1,2,\ldots,N-1\}\\ (x^e)^d - x &= x^{1+(p-1)(q-1)k} - x \bmod N\\ &= x(x^{(p-1)(q-1)k} - 1) \bmod N\end{aligned}$$

Now, we will show that the last expression is divisible by both p and q by FLT.

Case 1: $x \bmod p = 0$:

$$x(x^{(p-1)(q-1)k} - 1) = 0(0^{(p-1)(q-1)k} - 1) = 0 \bmod p$$

Case 2: $x \bmod p \neq 0$:

$$x(x^{(p-1)(q-1)k} - 1) = x((x^{(p-1)})^{(q-1)k} - 1) \bmod p$$
$$x(1-1) = 0 \bmod p$$

A symmetric argument works for q. If the expression is divisible by both p and q, then it is divisible by $pq = N$. Thus,

$$x(x^{(p-1)(q-1)k} - 1) = 0 \bmod N$$
$$(x^e)^d = x \bmod N$$

4. Alice wants to respond to a previous message that Bob has sent her with either "yes" or "no". She does not want to use the regular RSA scheme to encrypt her response in fear of Eve intercepting this communication.

(a) What is wrong with using the standard RSA procedure to send a "yes" or "no"?

Solution: Since there are only two options, Eve can just guess-and-check. Eve knows the public key that Bob will release in order to receive Alice's message, so now Eve can just encrypt both "yes" and "no" using e and see which one matches Alice's encrypted message, which she can publicly see.

(b) What modification to the procedure can be made so that Eve cannot easily guess the message? (Hint: try sending more information than just "yes" or "no".)

Solution: Following the hint, we will need incorporate Alice's response into a bigger message. We can create some random large secret number W and hide the "yes" or "no" into the k^{th} bit of W as 1 or 0. Then, Alice can use Bob's public key to encrypt two messages: W, and k. Bob can put this information together and find the "yes" or "no" in the indicated bit.

(c) Followup question to the provided solution for (b): will Eve be able to figure out if Alice wanted to say "yes" or "no" if k was NOT encrypted before sending through the channel (so Eve has access to k's value?

Solution: No. Eve will still need to know the decrypted value of W to locate the k^{th} bit of it, which she will not be have knowledge of without knowing Bob's private key.

3 Polynomials

There are two fundamental properties of polynomials:

A non-zero polynomial of degree d has at most d real roots.

$d + 1$ distinct points uniquely define a polynomial of degree at most d.

We can represent polynomials in multiple ways:

Coefficient Representation: This representation is probably what you've seen before. We could represent a polynomial of degree d like this:

$$p(x) = a_d x^d + a_{d-1}x^{d-1} + a_{d-2}x^{d-2} + \cdots + a_1 x + a_0$$

As you can see, we need $d + 1$ coefficients $(a_0, \ldots, a_d)$.

Value Representation: Using the second property of polynomials, if we have a collection of $d + 1$ distinct points

$$(x_0, y_0), (x_1, y_1), \ldots, (x_d, y_d)$$

we actually would have a unique polynomial of degree at most d.

Root representation: If we know all d roots $r_1, \ldots, r_d$ of our polynomial, we can represent our polynomial as follows:

$$a_d(x - r_1)(x - r_2)\cdots(x - r_d)$$

1. In this problem, consider all polynomials to be over GF(p), where $p > n$ for all the n defined in the problems.

(a) How many distinct degree n polynomials are there?

Solution: A degree n polynomial must be of the form $a_n x^n + a_n x^{n-1} \cdots + a_1 x + a_0$, where $a_n \neq 0$, and each a_i is taken from GF(p) (or in other words, from 0 to $p - 1$), and a polynomial is determined uniquely by its coefficients. Thus, we have $p - 1$ choices for a_n and p choices for $a_0, a_1, \ldots, a_{n-1}$, giving $\boxed{(p-1)p^n}$ such polynomials.

(b) How many distinct polynomials of degree at most n are there?

Solution: We follow the same solution as in part (a), but now there are p choices for a_n, since a_n can be 0. We thus get $\boxed{p^{n+1}}$ polynomials.

(c) How many distinct polynomials of degree at most n are there such that $p(0) = 1$ and $p(1) = 2$?

Solution: A polynomial of degree at most n is uniquely determined by the values of the polynomial at $n + 1$ points (for example, $p(0), p(1), \ldots, p(n-1), p(n)$). We have p choices for the values of $p(2), p(3), \ldots, p(n-1), p(n)$ (since they can taken on any value from 0 to $p - 1$), and these values combined with the $p(0)$ and $p(1)$ uniquely determine a polynomial, so there are $\boxed{p^{n-1}}$ such polynomials.

2. Let $n \geq 2$ be a positive integer, and let p be a prime greater than n. Find all polynomials $q(x)$ of degree at most n in GF(p) such that $(x - 2)q(x) = xq(x - 1)$.

Solution: First, we plug in $x = 0$, giving that $-2q(0) = 0$. Thus, $q(0) = 0$, so 0 is a root of $q(x)$. Then has a factor of x, so $q(x) = xq_1(x)$ for some polynomial q_1 in GF(p). Then we have that $(x - 2)xq_1(x) = x(x - 1)q_1(x - 1)$.

Next, we plug in $x = 1$. Then $-1q_1(1) = 0$, so $q_1(1) = 0$. Thus, q_1 has a factor of $x - 1$, so $q_1(x) = (x - 1)q_2(x)$. Then $(x - 2)x(x - 1)q_2(x) = x(x - 1)(x - 2)q_2(x - 1)$. Moreover, note that q_2 has degree at most $n - 2$.
Suppose that x is not equal to $0, 1$ or 2. Then $q_2(x) = q_2(x - 1)$. Thus, we conclude that $q_2(2) = q_2(3) = \cdots = q_2(n) = c$, where c is some constant. Note that we have that $n - 1$ values of the polynomial q_2, which has degree at most $n - 2$. Thus, there is a unique polynomial that satisfies these equations; specifically, the constant polynomial $q_2(x) = c$. Thus, we conclude that $q(x) = xq_1(x) = x(x - 1)q_2(x) = cx(x - 1)$ for some constant c in GF(p).