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.

(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 $x \equiv (1, 0, 0)$.

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

(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?

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

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?

$40^{-1} \bmod 51$ — don't care

$40(\ ) + 51(\ ) = 1$

$40(0) + 51(1) = 51$

$40(1) + 51(0) = 40$

$40(-1) + 51(1) = 11$

$40(2) + 51(-1) = 29$

$40(3) + 51(-2) = 18$

$40(4) + 51(-3) = 7 \leftarrow$

$40(5) + 51(-4) = 4 \leftarrow$

$40(-1) + 51(-1) = 3$

$40(\ ) + 51(\ ) = 1$

$17^{-1} \bmod 19$

$\rightarrow 17(-3) + 19(3) = 6$

$17(-5) + 19(5) = 10$

$17(-1) + 19(1) = 2$

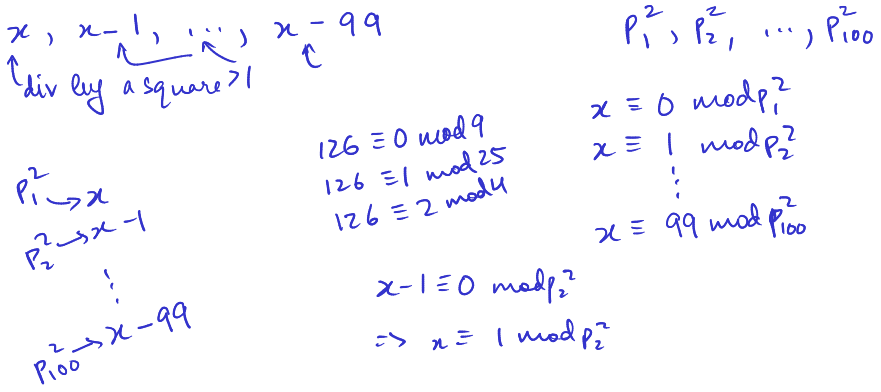
$\rightarrow 17(6) + 19(-5) = 7$

$$\begin{array}{r} 204 \\ 200 \\ \hline 4 \end{array}$$

$$\begin{array}{r} 160 \\ 153 \\ \hline 7 \end{array}$$

$$\gcd(a+b, b)$$
$$= \gcd(b, (a+b) \bmod b)$$
$$= \gcd(b, a \bmod b)$$
$$= \gcd(a, b)$$

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.



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
$E(x) = x^e \bmod N$
$D(x) = x^d \bmod N$, where $d = e^{-1} \bmod (p-1)(q-1)$
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?

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

   (c) Calculate d.

(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?

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

2. **RSA T/F [Practice Bank]** public key (p, q, d)

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

(b) Alice needs to know Bob's key d to send encrypted messages to Bob. No

$m^e \bmod N$

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

(d) $E(x) = x^e \bmod N$ is a bijection on ~~$\mathbb{Z}_N$~~ set of ints mod N $\{0, 1, \ldots, N-1\}$ True
$D(y) = y^d$ $(x^e)^d \equiv x \bmod N$

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

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

$x^{k(p-1)(q-1)+1} \equiv x \bmod p$

FLT $x^{p-1} \equiv 1 \bmod p$ $1^k \equiv 1 \bmod \_\_$

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

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

$(x^e)^d$ BAD $x^{(1 \bmod (p-1)(q-1))} \equiv x$

$d = e^{-1} \bmod (p-1)(q-1)$
$\Rightarrow ed \equiv 1 \bmod (p-1)(q-1)$

WTS: $x^{k(p-1)(q-1)+1} \equiv x \bmod pq$ $ed = k(p-1)(q-1) + 1$

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

$\Rightarrow x^{k(p-1)(q-1)} \equiv 1 \bmod pq$

$\Rightarrow x^{k(p-1)(q-1)+1} \equiv x \bmod pq$ ∎

$x \equiv 0 \bmod m_1$
$x \equiv 0 \bmod m_2$
$x \equiv 0 b_1 + 0 b_2 \equiv 0 \bmod m_1, m_2$

$31 \mid x$ $4 \mid x$
$10 \mid x$ $8 \mid x$
$310 \mid x$ $16 \nmid x$

$x^{(p-1)(q-1)} \equiv 1^{(q-1)} \equiv 1 \bmod p$

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"?

   00
   10
   11
   01

   1
   0

   (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".)

   ↳ $k = 6$

   10111010 0101000011011111

   Need to decrypt first!

   (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?

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?

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

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

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 $(x-2)q(x) = xq(x-1)$.