Lecture 14
10/28/2021

Last Time:

- We looked at solving linear congruences and discussed how to solve systems of linear congruences using the CRT. We gave some intuition behind why it worked and gave a proof of the result.

- We introduced Fermat's Little Theorem

  For $a \in \mathbb{N}$, $a \geq 2$, p prime with $p \nmid a$, $a^{p-1} \equiv 1 \bmod p$

  looked at some examples, and gave two proofs. The first was straightforward and the second was a geometric proof via an analogy with a word problem involving counting necklaces and strings considering rotations and cycles.

In our second proof, we never explicitly used the fact that p was prime

$\Rightarrow 9 = p,\ 4 = a$, does 9 divide $4^9 - 4$?

(4^9 is 262,144 and 9 does not divide 262,140)

If a number $m \nmid a^m - a$ then m not prime

Recall two ways of writing Fermat's Little Thm

$a^{p-1} \equiv 1 \bmod p \Rightarrow p \mid a^{p-1} - 1 \Rightarrow \exists z \text{ s.t. } pz = a^{p-1} - 1$

$a^p \equiv a \bmod p \Rightarrow p \mid a^p - a \Rightarrow \exists k \text{ s.t. } pk = a^p - a = a(a^{p-1} - 1$

Idea: to test whether a number M is prime, can pick some $a \geq 2$, $a \in \mathbb{N}$, where $M \nmid a$ and check:

Does $M \mid a^M - a$?

We know $M \nmid a^M - a \rightarrow M$ is not prime
(if M does not divide $a^M - a$ then M is not prime)

However, ~~do we know that~~ -

if $M \mid a^M - a$ do we know that M is prime?

$(M \mid a^M - a \rightarrow M$ prime$)$?

Ex: $M = 4$, $a = 4$ $\Rightarrow$ $4 \mid 4^4 - 4$ but 4 is not prime

$\Rightarrow$ Unfortunately no, ~~if~~ if $M \mid a^M - a$ then M is prime ~~"}$ is not true

the statement

This suggests an experiment.

How many numbers in $\{M \mid 2 \leq M \leq 1000, M \nmid a\}$ satisfy $M \mid a^M - a$ that are nonprime?

$\Rightarrow$ let's take $a = 2$ to keep the exponent small

Ex:

```
def checkPrimeCandidates(a):
    candidates = []
    for M in range(2,1000):
        if (a%M!=0) and ((a**M-a)%M==0):
            candidates.append(M)
    return M
```

when $a=2 \Rightarrow$ all non primes fail divisibility test up to $M=341$ is returned / passes our test but is composite

However, only 3 such numbers that pass our test that are composite

$M = 341 = 11 \cdot 31$ and $341 \mid 2^{341} - 2$

$M = 561 = 3 \times 11 \times 17$ and $561 \mid 2^{561} - 2$

$M = 645 = 3 \times 5 \times 43$ and $645 \mid 2^{645} - 2$

When $a = 3 \Rightarrow$

$M = 341 = 11 \times 31$ but $341 \nmid 3^{341} - 2$

$M = 561 = 3 \times 11 \times 17$ ~~and~~ $561 \mid 2^{561} - 2$

$M = 645 = 3 \times 5 \times 43$ but $645 \nmid 3^{645} - 3$

$\Rightarrow$ only one number fails w/ $a=3$ $(M=561)$

what if we take $a = 4, 5, \ldots$?

~~None of our tests all show that~~ $561 \mid a^{561} - a$ Always

~~for any element~~

Def Numbers that FLT cannot distinguish from prime are called Fermat Pseudoprimes or Carmichael numbers

These numbers are rare, for the first billion integers, there are 50 million primes, but only 646 Carmichael numbers.

Ex 561.

Still, it was proven in 1994 that there are infinitely many Carmichael numbers.

We can use the fact that these numbers are relatively rare. We will see that being able to easily generate large prime numbers (1000 digits) is important in cryptography and encryption algorithms.

We can build primality tests using FLT

Q: How would we prove that a number is a carmichael number? (i.e. we need to check infinitely many choices of a)?

⟹ proved that if you know the prime factorization

$561 = 3 \times 11 \times 17$ and subtract 1 from each side

$(3-1)(11-1)(17-1)$ ~~560~~

560 2, 10, 17

The number is a carmichael number iff the numbers on the right are different and they all divide the number on the ~~right~~ left

2|560 i.e. none of the factors repeat

10|560 and all the prime factors -1 divide

16|560 the number -1.

Euler's Totient Function

Def $\varphi(n)$ is the number of integers between 1 and n whose gcd with n is 1

$$\varphi(n) = |\{x : 1 \le x \le n, \gcd(n,x) = 1\}|$$

Ex $\varphi(6)$:

	1,	2,	3,	4,	5,	6
$\gcd(n,6)$	1	2,	3,	2,	1	6

Results for only two numbers whose $\gcd(n,6) = 1$ (1 and 5)

Checking $\varphi(p)$

1. if p prime, $\varphi(p) = p - 1$

   Ex: $\varphi(41) = 40$, $\varphi(7) = 6$

   b/c a prime number only has two divisors, 1 and itself,

   so the one $p-1$ numbers coprime to p

2. if $a = p^n$ is a prime power then $\varphi(p^n) = p^n - p^{n-1}$

   p^{n-1} is the number of nos p^n is divisible by p

   so we subtract this from the actual number we want to work out

   Ex $\varphi(32) \Rightarrow 32 = 2^5 \Rightarrow \varphi(32) = 2^5 - 2^4 = 16$

3. if $\gcd(m,n) = 1$ then $\varphi(mn) = \varphi(m)\varphi(n)$

   Ex $\varphi(35) = \varphi(7)\varphi(5) = 6 \times 4 = 24$

$$\varphi(600) = \varphi(2^3 \times 3 \times 5^2)$$
$$= \varphi(2^3) \times \varphi(3) \times \varphi(5^2)$$
$$= (2^3 - 2^2) \times (2) \times (25 - 5)$$
$$= 160$$

Def Suppose the prime divisors of n are $p_1 \cdots p_k$

then $\varphi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_k}\right)$

Thm $a^{\varphi(n)} \equiv 1 \bmod n$ for $n > 0$ and $a > 0$ with $\gcd(a, n) = 1$

Ex $n = 10$, $a =$ ~~1,2,4,5,6,8~~ $1, 3, 7, 9$

$\varphi(10) = \varphi(2)\varphi(5) = 1 \times 4 = 4$

$\Rightarrow a^4 \equiv 1 \bmod 10 \Rightarrow$

$1^4 \equiv 1 \bmod 10$

$3^4 = 81 \equiv 1 \bmod 10$

$7^4 = 2401 \equiv 1 \bmod 10$ ✓

$9^4 = 6561 \equiv 1 \bmod 10$

Ex Calculate $7^{133} \bmod 26$ $\quad 7^{133}$ in $\mathbb{Z}_{26}$

A few ways to handle modular exponentiation

$\Rightarrow \gcd(7, 26) = 1 \Rightarrow$ Can use Euler

$\varphi(26) = \varphi(2)\varphi(13) = 1 \times 12 = 12$

$\Rightarrow 7^{12} \equiv 1 \bmod 26 \Rightarrow$ How can we express 7^{133} as a function of 7^{12}?

$\Rightarrow 133 = 12 \times 11 \Rightarrow 7^{133} \equiv 7^{132} \times 7 \equiv \left(7^{12}\right)^{11} \times 7 \equiv 1^{11} \times 7 \equiv 1 \times 7 \equiv 7 \bmod$

$7^{12} \equiv 1 \bmod 26$ by Euler $\Rightarrow 7 \equiv$

Proof Sketch Euler

$a^{\varphi(n)} \equiv 1 \bmod n \Rightarrow$ when n prime $\varphi(n) = n-1$

$\Rightarrow a^{n-1} \equiv 1 \bmod n$ since $\gcd(n,n)=1$

$\Rightarrow n \times n$

Idea: look at Set of all #s rel prime to n $\quad S = \{1 \le x \le n \mid \gcd(x,n)=1\}$

$\Rightarrow |S| = \varphi(n)$ elmnts $\{x_1, \dots x_{\varphi(n)}\}$

Make new set by multplying each elmnt in S by a

$\Rightarrow aS = \{ax_1, \dots, ax_{\varphi(n)}\}$

$\Rightarrow |aS| = \varphi(n)$ elmnts

Will prove that S and aS each contain same residues mod n

$\Rightarrow (ax_1)(ax_2)\cdots(ax_{\varphi(n)}) \equiv x_1 \times x_2 \times \cdots x_{\varphi(n)} \pmod n$

Let $X = \prod_{i=1}^{n} x_i$, note $\gcd(n,X)=1$

$\Rightarrow a^{\varphi(n)} X \equiv X \bmod n \Rightarrow$ since $\gcd(n,X)=1$

X has unique inverse mod n

$\Rightarrow$ Multply both sides by X^{-1}

$\Rightarrow a^{\varphi(n)} \equiv 1 \bmod n$ $\square$

Thm Prof

$\varphi(n) = |\{1 \le m \le n \mid \gcd(m,n)=1\}|$, Format: For p prime $a \in \mathbb{Z}$ s.t. $p \nmid a$

$a^{p-1} \equiv 1 \bmod p$

Eulers Thm

For $n \in \mathbb{N}$, $a \in \mathbb{Z}$ s.t. $\gcd(a,n)=1$

$a^{\varphi(n)} \equiv 1 \bmod n \Rightarrow$ when n is prime, $\varphi(n) = n-1$ and this collapses to FLT. ($\gcd(m,n)=1 \iff m \nmid n$)

Proof: Consider $S = \{1 \le x \le n \mid \gcd(x,n)=1\}$ set of all #s relatively prime to n

$\Rightarrow |S| = \varphi(n)$ elements $\Rightarrow \{x_1, x_2, \dots x_{\varphi(n)}\}$

help build a new set off of S that are all

$aS = \{ax_1, ax_2, \dots, ax_{\varphi(n)}\}$ by multiplying each element in S by a

$\Rightarrow$ the set aS has $\varphi(n)$ elements, as residues mod n it also has $\varphi(n)$ elements (we will prove this by showing every elmt in aS is rel prime to n and all n congruent to each other).

Claim 1) $\gcd(ax_i, n) = 1$, otherwise there would be a prime p s.t. $p \mid ax_i$ and $p \mid n$

(if gcd $\neq 1$, gcd is some number divisible by a prime $\Rightarrow$ by def that prime must divide ax_i and n)

$p \mid ax_i \Rightarrow p \mid a$ or $p \mid x_i$

if $p \mid a$ then $p \mid \gcd(a,n)$

if $p \mid x_i$ then $p \mid \gcd(x_i, n)$

but $\gcd(x_i,n)$ and $\gcd(a,n)$ are both 1

so this contradicts $\gcd(a,n) = 1 = \gcd(x_i,n)$

2) No two elmts of aS are congruent mod n

Sps $ax_i \equiv ax_j \pmod{n}$

$\Rightarrow a(x_i - x_j) \equiv 0 \pmod{n}$

$\Rightarrow n \mid a(x_i - x_j)$ but we know $n \nmid a$ since n, a rel prm

$\gcd(n, a) = 1$

$\Rightarrow n \mid (x_i - x_j) \Rightarrow \exists k$ s.t. $nk = (x_i - x_j)$

However since x_i and x_j both smaller than n, no way for this to be a multiple of n except for the 0^{th} multiple

$\Rightarrow x_i - x_j = 0$

$\Rightarrow x_i = x_j$

We started w/ two elmts congruent mod n and showed that they are the same elmt.

$\Rightarrow$ It follows from ① and ②, so I says...

① aS completely made of numbers rel prime to n

② none of them are congruent mod n, so they form a same residues mod n (possibly in a different order) (in other words)

$\Rightarrow aS \equiv S \bmod n$

$S = \{x_1, \ldots, x_{\varphi(n)}\}$ and $aS = \{ax_1, \ldots ax_{\varphi(n)}\}$

each contain the same residues mod n

Proof $S = \{x_1, \dots, x_{\varphi(n)}\}$, $aS = \{ax_1, \dots, ax_{\varphi(n)}\}$

each contain the same residues mod n

$$\Rightarrow (ax_1)(ax_2)\cdots(ax_{\varphi(n)}) \equiv x_1 \times \cdots \times x_{\varphi(n)} \pmod{n}$$

Set $\bar{X} = x_1 \cdots x_n = \prod_{i=1}^{\hat{n}} x_i$, and note $\gcd(n, \bar{X}) = 1$

$$\Rightarrow a^{\varphi(n)}\bar{X} \equiv \bar{X} \pmod{n}$$

Since $\gcd(\bar{X}, n) = 1$, $\bar{X}$ has unique inverse mod n

$\Rightarrow$ Multiply both sides by $\bar{X}^{-1}$

$$\Rightarrow a^{\varphi(n)} \equiv 1 \bmod n$$

□

To appreciate why the RSA algorithm works, lets say something about algorithms

Def An algorithm is a finite seq of precise instructions for ~~performing~~ with inputs and outputs for performing a computation or solving a problem.

Al Khowarizmi solving quadratic eqns by completing the square

Al jabr

Interested in studying how long an algorithm takes to run as a function of its input.

⇒ Notation used to estimate # of operations an algorithm uses as input grows.

⇒ Lets say input size is n, we can compare two algorithms

(i) $100n^2+17n+4$ operations vs n^3 operations.

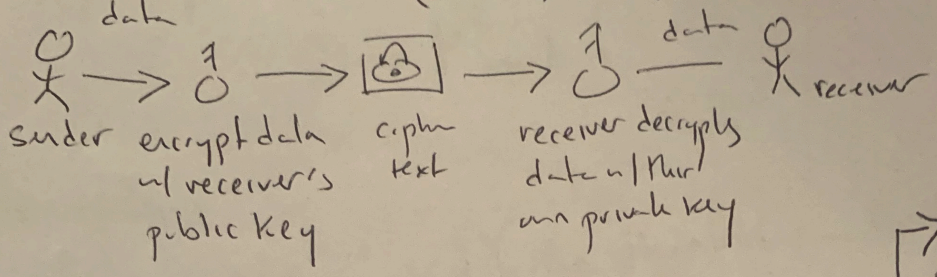
when n is small, (i) uses more operations, but when n large (ii) uses more

Let $f, g : \mathbb{Z} \to \mathbb{R}$ or $\mathbb{R} \to \mathbb{R}$, $f(x)$ is $O(g(x))$ if $\exists\ C, k$ s.t. $|f(x)| \leq C|g(x)|$ whenever $x > k$

We say $f(x)$ is Order of $g(x)$. ⇒ $f(x)$ grows

RSA Algorithm (Rivest, Shamir, Adleman)

- Algorithm uses two keys a public key and a private key
  (shared publically) (not shared w/ anyone)



1. Generating Keys
   1) Select two large prime numbers x and y
      (need to be large so difficult to figure out)
   2) Calculate $n = x \times y$
   3) Calculate the totient function $\varphi(n) = \varphi(x)\varphi(y) = (x-1)(y-1)$
   4) Select $e \in \mathbb{Z}$ s.t. e is coprime to $\varphi(n)$ ($\gcd(e, \varphi(n)) = 1$) and $1 < e < \varphi(n)$. The pair of numbers (n, e) make up the public key
   5) Calculate d s.t. $de \equiv 1 \pmod{n}$
      d can be found using EEA, the pair (n, d)
      Make up the private key.

n is a number you can factor but is large enough no one else can factor

Known factorization algorithms depend on relative size of e^{and} (largest prime factor)

Given public exponent e, only you can determine private exponent d.

Known as RSA problem

The hardness of performing private key op, d mod n $M \equiv C$ mod n given only public key e, n

proven as hard as factoring modulus.

2. Encryption

Given a plaintext P represented as a number,

the Ciphertext is calculated as

$$C = P^e \bmod n$$

3. Decryption

Using private key (n, d) the plaintext can be found

using $P = C^d \bmod n$