MATH 314 Fall 2019 - Class Notes

10/07/19

Scribe: Kenny Vu

Jacobi Symbol

- Any Legendre Symbol is also a Jacobi Symbol
- Remember: Legendre Symbols # on bottom is prime
- Jacobi Symbol - Allows the # on bottom to be an odd composite #
- If $(\frac{a}{n})$ is a Jacobi Symbol where n is composite the value of$(\frac{a}{n})$ does not tell us whether a is a quadratic residue or not.
- In Quadratic reciprocity the #'s don't need to be prime just odd.
- When working with Jacobi Symbols we don't completely factor the # on top just factor out 2's

Is 47 a square $\pmod{89}$? (Jacobi Symbol)

$$(\tfrac{47}{89}) = (\tfrac{89}{47}) = (\tfrac{42}{47}) \rightarrow (\tfrac{2}{47})(\tfrac{21}{47})$$

$$(\tfrac{2}{47}) = 1 \text{ because } 47 \equiv 7 \pmod{8}$$

$$(\tfrac{21}{47}) = (\tfrac{47}{21}) = (\tfrac{5}{21}) = (\tfrac{21}{5}) = (\tfrac{1}{5}) = 1$$

Fermat Primality Test

Recall Fermat's little theorem

If p is prime then $a^{p-1} = 1 \pmod{p}$

a is not divisible by p

Suppose we have some # n

Compute

$a^{n-1} \not\equiv 1 \pmod{n}$

This means n cannot be prime

Fermat Primality Test

1. pick a random integer a $1 < a < p - 1$
2. compute $a^{n-1} 1 \pmod{n}$

If it isn't 1 we are certain n is composite

If it is 1 then n is probably prime

Try this out

Take n = 9

Pick a random a $\rightarrow a = 2$

Compute

$2^{9-1} = 2^8 \pmod{9}$

$2^2 = 4$
$2^4 = (2^2)^2 = 4^2 = 16 \equiv 7 \pmod{9}$
$2^8 = (2^4)^2 = 7^2 = 49 \equiv \underline{\mathbf{4}} \pmod{9}$

This returned a 4. So 9 is a composite.

Another example

$n = 15$ check if 15 is prime

$a = 4$

Compute

$4^{15-1} = 4^{14} \pmod{15} = 4^{8+4+2}$

$4^2 = 16 = \underline{\mathbf{1}} \pmod{15}$
$4^4 = (4^2)^2 = 1^2 = \underline{\mathbf{1}} \pmod{15}$
$4^8 = (4^4)^2 = 1^2 = \underline{\mathbf{1}} \pmod{15}$

$(1)(1)(1) = 1 \pmod{15}$

Fermat's test says that it's "probably prime"

Try again

$n = 15$

$a = 7$

Compute

$7^{15-1} = 7^{14} \pmod{15} = 7^{8+4+2}$

$7^2 = 49 = \underline{\mathbf{4}} \pmod{15}$
$7^4 = (7^2)^2 = 4^2 = \underline{\mathbf{1}} \pmod{15}$
$7^8 = (7^4)^2 = 1^2 = \underline{\mathbf{1}} \pmod{15}$

$(4)(1)(1) = 4 \pmod{15}$

Fermat's test says that it's composite

- If $a^{n-1} \equiv 1 \pmod{n}$, but n is a composite. We say that n is a base - a pseudoprime
- Ex: 15 is a base 4 pseudoprime
- There exist number's called carmichael numbers which are composite but they are pseudoprime to every base
- Smallest Carmichael number is 561

Feistel Cipher

Operate on a sting of m bits

m- is the block length

m- is even (fixed by chiper)

A feistel cipher consists of multiple rounds of the following

-Break the block into 2 havles L,R $m/2$ bits each

Last half moves to the front

L_i	R_i
$\searrow$	$\swarrow$ $\downarrow$
	$f(R, K)$
	$\oplus$
	$\downarrow$
$L_{i+1} \equiv (R_i)$	R_{i+1}

To define a cipher using the feistel setup we need to

1. Pick a block size m
2. Pick a function f(R,K)
3. Pick a rule for choosing the key used in each round
4. Decide how many rounds we want.

Encryption: Follow the Feistel rule several times

Decryption: Swap left and right halves. Then do the same steps as encryption but in reverse.

$S \oplus S =$ all 0's

$\oplus \leftarrow$ also subtraction

$101 \oplus 101 = 000$

2 rounds of feistel cipher

$P = L_0, R_0$
$\downarrow$

$$
\begin{array}{llll}
L_0 & & & R_0 \\
 & \searrow & \swarrow & \downarrow \\
 & & & f(R_0, K_1) \\
 & & & \oplus \\
 & & & \downarrow \\
L_1 \equiv (R_0) & & & R_1 \equiv L_0 \oplus f(R_0, K_1) \\
 & \searrow & \swarrow & \downarrow \\
 & & & f(R_0, K_1) \\
 & & & \oplus \\
 & & & \downarrow \\
L_2 \equiv R_1 \equiv L_0 \oplus f(R_0, K_1) & & & R_2 \equiv R_0 \oplus f(R_1, K_2)
\end{array}
$$