MATH 314 Spring 2018 - Class Notes

3/6/2018

Scribe: Scott Swatling

Summary: We finished Jacobi symbols by doing an example, learned how to conduct a Fermat Primality Test, and started covering Modern Cryptography and the Feistal Cipher.

Notes:

Jacobi symbols example: Is 1001 a square (mod 9907)

$(\frac{1001}{9907})$

Rule 4:

$(\frac{9907}{1001})$

Rule 1:

$(\frac{898}{1001})$

Rule 3:

$(\frac{2}{1001})(\frac{449}{1001})$

Rule 5:

$(1)(\frac{449}{1001})$

$(\frac{449}{1001})$

Rule 4:

$(\frac{1001}{449})$

Rule 1:

$(\frac{103}{449})$

Rule 4:

$(\frac{449}{103})$

Rule 1:

$(\frac{37}{103})$

Rule 4:

$(\frac{103}{37})$

Rule 1:

$(\frac{29}{37})$

Rule 4:

$(\frac{37}{29})$

Rule 1:

$(\frac{8}{29})$

Rule 3 (done twice):

$(\frac{2}{29})(\frac{2}{29})(\frac{2}{29})$

Rule 5:

$(-1)(-1)(-1)$

(-1)

1001 is not a square (mod 9907)

Fermat Primality Test

- Tests whether a number is composite
- Lets assume that we have some large number, N, that we think might be prime

Steps:

1. Pick some random integer A
2. Use A to calculate: $A^{N-1} \pmod{N}$

If N is a prime number then, $A^{N-1} \equiv 1 \pmod{N}$, otherwise, N is composite.

Unfortunately, there are some "false Positives" when using this test.

There exists bases A, such that $A^{N-1} \equiv 1 \pmod{N}$ even though N is composite.

In this case N is considered a Base-A pseudoprime.

To overcome these false positives, we simply redo the test with a different A value.

Examples:

Is 15 a prime?

Lets have $A = 4$

$4^{15-1} \pmod{15}$

$4^{14} \pmod{15}$

We can use Modular Exponentiation to solve this:

$14 = 8 + 4 + 2$

$4^1 = 4 \pmod{15}$

$4^2 = 1 \pmod{15}$

$4^4 = 4^{2^2} = 1^2 = 1 \pmod{15}$

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

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

So we can concule that 15 <u>might</u> be a prime

Lets try it again with another A value

This time let $a = 2$

$2^{15-1} \pmod{15}$

$2^{14} \pmod{15}$

$14 = 8 + 4 + 2$

$2^1 = 2 \pmod{15}$

$2^2 = 4 \pmod{15}$

$2^4 = 2^{2^2} = 4^2 = 1 \pmod{15}$

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

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

Because we did not get 1 when $A = 2$, Fermats Primality Test says that 15 is a composite number

Unfortunetaly, there are composite numbers which are psuedoprime to every possible A value (341 is the smallest), These numbers are known as **Carmicheal Numbers**. There are infinitely many carmicheal numbers, but they are still rarer than primes.

Modern Cryptography

With the advent of computers, there is no longer a need to use (mod 26) cryptosystems. Messages, images, video, and pretty much any form of data can be translated into binary in some way. As a result, almost anything can be encrypted using binary.

Lets say we have two bit strings A, and B, of the same length.

$A \oplus B$ is the bitwise sum of A and B (mod 2 without carries), also known as "XOR"

Example:

Let A be the bit string "0110101"

Let B be the bit string "1110000"

$A \oplus B = 0110101 \oplus 1110000$
To calculate this we compare the two bit strings and follow this logic,

- if both bits are "1" or both bits are "0" the resulting bit is "0"
- Otherwise the resulting bit is "1"

So, In our example $0110101 \oplus 1110000 = 1000101$

$A \oplus A$ will always result in an all "0" string, so, $(B \oplus A) \oplus A = B$

This is the bit version of the one time pad

We can pick some key, K, that is a bit string the same length as our message, and use it to encode our message.

The encryption and decryption functions would be the exact same, that is to say,

- $Encrypt_k(M) = M \oplus K$
- $Decrypt_k(M) = M \oplus K$

Feistal Cipher (Early 1970's)

Consists of multiple "rounds"

Inside of a round:

- Break the plaintext into two equal length bit strings $Left_i$ and $Right_i$
- Define $Left_{i+1} = Right_i$
- Define $Right_{i+1} = F(Right_i, K) \oplus Left_i$, where $F(Righti, K)$ can be any function

Note: Some functions $F(Righti, K)$ will be more secure than others