MATH 314 Spring 2018 - Class Notes

03/07/2019

Scribe: Olashupo Ajala

Summary: Continuation of Legendre symbols and Jacobi on how to determine if a number is a square of its modulo number.

Notes: From the previous class, Legendre symbols has four main properties on how to be implemented while determining a number is a square.

• Legendre Symbols

1. $(\frac{a}{p}) = \begin{cases} 0 \text{ if } p|a \\ 1 \text{ if } x^2 \equiv a \pmod{n} \text{ has a solution} \\ -1 \text{ otherwise} \end{cases}$

2. $(\frac{a}{p}) = 1$ if we can take a square root of $a \pmod{p}$

Rules for Legendre Symbols

1. $(\frac{a}{p}) = (\frac{b}{p})$ if $a \equiv b \pmod{p}$

2. $(\frac{a}{p}) = \begin{cases} (\frac{q}{p}) \text{ if not } p \equiv 3 \pmod{4} or \neq q \equiv 3 \pmod{4} \\ \\ -(\frac{q}{p}) \text{ if } p \equiv q \equiv 3 \pmod{4} \text{Provided p and q is odd and prime.} \end{cases}$

3. $(\frac{ab}{p}) = (\frac{a}{p})(\frac{b}{p})$

4. $(\frac{2}{p}) = \begin{cases} 1 \text{ if } p \equiv 1 \pmod{4}, 7 \pmod{8} \\ \\ -1 \text{ if } p \equiv 3, 5 \pmod{4} \end{cases}$

5. $(\frac{1}{p}) = 1$

   Note p has to be an odd prime

For further explanation, more complicated examples will be considered.
is 1001 a square $\pmod{9907}$?
Lets compute

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

$$(\frac{7 * 11 * 13}{9907}) = (\frac{7}{9907})(\frac{11}{9907})(\frac{13}{9907}) = (-1)(1)(1) = -1$$

Solve the equations individually

$$(\frac{7}{9907}) = (\frac{9907}{7}) \pmod{7} = -(\frac{2}{7}) = -1$$

$$(\frac{11}{9907}) = (\frac{9907}{11}) \pmod{11} = -(\frac{7}{11}) = -(-(\frac{11}{7})) = (\frac{4}{7}) = (\frac{2}{7})(\frac{2}{7}) = 1$$

$$(\frac{13}{9907}) = (\frac{9907}{13}) \pmod{13} = (\frac{1}{13}) = 1$$

Problem :
Factoring numbers is to use Legendre symbols if the number on top is composite, we have to factor it.

• Jacobi Symbols

$(\frac{a}{n})$ n has to be an odd number, (but doesn't have to br prime)
If n is prime then the Jacobi symbol $(\frac{a}{n})$ is equal to the legendre symbol.
If n is composite the jacobi symbol does not tell us if $x^2 \equiv \pmod{n}$ has a solution.

Rules for Jacobi Symbols
All the same rules as Legendre symbols
- Only factor out factor of 2 in the top
- Quadratic reciprocity works for any odd p,q
Example: is 15 a square mod 37? No

$$(\frac{15}{37}) \rightarrow jacobiandLegendresymbol = (\frac{37}{15}) \rightarrow jacobisymbol = (\frac{7}{15}) = -(\frac{15}{7}) = -1$$

How can we tell if a number is prime?
Primality tests : Proves that the number is composite should be called compositeness test

Fermat Primality Test
Fremat's little theorem if p is prime then $a^{p-1} \equiv 1 \pmod{p}$

Steps of Fermat primality test
Want to test if n is a prime Pick an a<n
compute $a^{n-1} \pmod{n}$
If we don't get 1, n has to be composite
If we do get 1 pick a new "a" and try again.
If we do get 1 a whole bunch of times then we return "Probably prime"

if $a^{n-1} \pmod{n}$ but n is not prime we call n a "pseudoprime"(base a)
Example: Test is n = 15 a prime?
Pick a = 4
Provided that a is not or >n
Compute

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

$$4^{14-1} \pmod{15}$$

$$14 = 8 + 4 + 2$$

$$4^2 \equiv 16 \equiv 1 \pmod{15}$$

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

$$4^8 \equiv 1^4 \equiv 1 \pmod{15}$$

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

15 is a base 4 - pseudoprime

pick a = 5 instead
Compute

$$5^{14} = 5^8 * 5^4 * 5^2 \equiv 10 * 10 * 10 \equiv 10 \pmod{15} \not\equiv 1$$

so we conclude that 15 is composite

$$5^2 \equiv 25 \equiv 10 \pmod{15}$$

$$5^4 \equiv 10^2 \equiv 100 \pmod{15}$$

$$5^8 \equiv 10 \pmod{15}$$

If we try enough a's, can we be certain that our number is prime? No, because there are numbers called Carmichael numbe

The only Carmichael number less than 1000 is 341

In 1994 it was proven that there are infinitely many Carmichael numbers

To fix this we will need a better approach of Primality test which will be introduced later in the class.