MATH 314 Spring 2022 - Class Notes

4/14/2022

Michael Fazio

Summary:
In class we covered ways of finding large prime numbers through Fermat's Primality Test and the Miller-Rabin Primality Test, in addition to learning a factoring trick to find composite numbers

Notes: Alice first picks a random large odd number, followed by either primality test.

Fermat's Primality Test: Key idea is to use Fermat's little theorem backwards, where it says "If p is prime then $a^{p-1} \equiv 1 \pmod{p}$". Fermat's little theorem backwards then is $a^{n-1} \not\equiv 1 \pmod{n}$, then n is not prime.

Ex. Test if n=33 is prime, using a where $2 < a < n-2$ to compute $a^{n-1} \pmod{n}$, if this does not equal 1, n is composite.

$a = 5, n = 33$

$$5^{32} \pmod{33} \equiv 5^{2*16} \pmod{33}$$
$$\equiv 25^{16} \pmod{33} \equiv -8^{2*8} \pmod{33} \equiv 64^{8} \pmod{33} \equiv 31^{8} \pmod{33}$$
$$\equiv -2^{2*4} \pmod{33} \equiv 4^{4} \pmod{33} \equiv 16^{2} \pmod{33} \equiv 256 \pmod{33} \equiv 25 \not\equiv 1$$

meaning 33 is composite

Ex 2. a=13, n=21

Compute $a^{n-1} \pmod{n}$ or $13^{20} \pmod{21}$

$$13^{20} \pmod{21} \equiv 13^{4+16} \pmod{21} 13^{2} \pmod{21} \equiv 169 \equiv 1$$
$$13^{4} \pmod{21} \equiv 1^{2} \equiv 113^{8} \pmod{21} \equiv 1^{4} \equiv 1$$
$$13^{16} \pmod{21} \equiv 1^{8} \equiv 113^{4} * 13^{16} \pmod{21} \equiv 1 * 1 \equiv 1$$

meaning 21 is probably prime, leading into step 2

Pick different base a, say a=2

$$2^{20} \pmod{21} \equiv 2^{4+16} \pmod{21} 2^2 \pmod{21} \equiv 4 \pmod{21}$$
$$2^4 \pmod{21} \equiv 4^2 \pmod{21} \equiv 16 \pmod{21}$$
$$2^8 \pmod{21} \equiv 16^2 \pmod{21} \equiv -5^2 \pmod{21} \equiv 24 \pmod{21} \equiv 4$$
$$2^{16} \pmod{21} \equiv 4^2 \equiv 16 2^4 * 2^{16} \equiv 16 * 16 \pmod{21} \equiv 4 \pmod{21}$$

meaning 21 isn't prime, it just has base 13 as a pseudoprime
Pseudoprimes that have

Miller-Rabin Primality Test: Key idea is similar to Fermat's Primality Test because you are testing to see if a number is composite or not.

Step 1: Pick a where $2 < a < n-2$ and compute $b_o \equiv a^m \pmod{n}, if b_o \equiv 1 \pmod{n} or -1 \pmod{m}$ return probably prime

Step 2: For i from 1 to k-1 where $n - 1 \equiv m * 2^k$: compute $b_i \equiv (b_{i-1})^2 \pmod{n}$ If $b_i \equiv 1 \pmod{n}$, return composite If $b_i \equiv 1 \pmod{n}$, return probably prime

Step 3: Else, return composite

Ex. $n = 21, a = 13$ (21 base 13 psuedoprime)

$$n - 1 = 20 = 2^2 * 5, k = 2, m = 5$$

Step 1: Compute $13^5 \pmod{21}$

$$13^5 \equiv 13^4 * 13^1$$
$$13^2 \equiv (-8)^2 \pmod{21} \equiv 64 \pmod{21} \equiv 1 \pmod{21}$$
$$13^4 \pmod{21} = 1^2 \pmod{21} \equiv 1 \pmod{21}$$

returns probably prime

Step 2: Compute $b_i = (b_o)^2$

$$(b_o)^2 \equiv 13^2 \pmod{21} \equiv 169 \pmod{21} \equiv 1 \pmod{21}$$

Return composite

Factoring Trick: If $a^2 \equiv b^2 \pmod{n}$ and $a \not\equiv b \pmod{n}$ and $a \not\equiv -b \pmod{n}$, then n is composite and gcd(n,b,-a) is a non-trivial factor of a.

Ex. $n = 77, a = 2, b = 9$

$$a^2 \equiv b^2 \pmod{77}$$
$$\equiv 2^2 \equiv 9^2 \pmod{77}$$
$$\equiv 4 \equiv 81 \pmod{77}$$
$$4 \equiv 4 \pmod{77}$$

$$a \not\equiv b \pmod{n}$$
$$4 \not\equiv 9 \pmod{77}$$

$$a \not\equiv -b \pmod{n}$$
$$4 \not\equiv -9 \pmod{77}$$

As all three checks are true, the factoring trick worked proving 77 is composite with 7 or a-b as a factor.