MATH 314 Class Notes for 4/16/2018

Scribe: Daniel Pereira

Summary: We discussed a few strategies/tests to determine whether a large number is "composite" or "probably prime" in order to use them for RSA.

Notes:

-How do we find prime numbers p,q for RSA?

-Generally, it is good practice to pick p,q to have around 120 digits.

-How many prime numbers are there to choose from?

- $\pi(x)$ = number of prime numbers less than or equal to x

Examples: $\pi(10) = (2, 3, 5, 7) = 4$

$\pi(11) = (2, 3, 5, 7, 11) = 5 = \pi(12)$

-Prime Number Theorem: $\pi(x) = \frac{x}{ln(x)}$

-The number of prime numbers with 120 digits is:

$$\pi(10^{121}) - \pi(10^{120}) \approx \frac{10^{121}}{\ln(10^{121})} - \frac{10^{120}}{\ln(10^{120})} = \frac{10^{121}}{121\ln(10)} - \frac{10^{120}}{120\ln(10)}$$

-About 1 in every $121\ln(10) \approx 240$ numbers are prime.

Strategy to find prime numbers for RSA:

-Pick a random number with about 120 digits.

-Call this number i

-Check if i is prime.

-If it is, use it. Otherwise, repeat and try again.

-On average, this requires about 120 times/trials.

-Generally, we don't want p,q to be consecutive prime numbers.

-How do we check if i is prime?

-One option is to try dividing i by all of the numbers (odd), up to $\sqrt{i}$

-If i has 120 digits, $\sqrt{i}$ has 60 digits.

-Doing 10^{60} operations isn't possible, so this method isn't very useful.

-Recall: Fermat's Primality Test, and also recall that if p is prime, then $a^{p-1} \equiv 1 \pmod{p}$

Steps to Fermat's Primality Test for n:

Repeat the following 3 steps k times:

1) Pick a random a where $2 \leq a < n - 1$

2) Compute $a^{n-1} \pmod{n}$

3) If this is not 1, then return "composite". But if we get 1 every time, then return "probably prime".

-If $a^{n-1} \equiv 1 \pmod{n}$, but n is not prime, then n is called a *(base a) pseudoprime.*

-If n is composite and $a^{n-1} \not\equiv 1 \pmod{n}$, then a is called *a witness of the compositeness of n*.

-*Carmichael numbers* are pseudoprimes to every base, or composite numbers with no witness.

-Smallest example of a Carmichael number is 341

-We need p,q to be prime numbers, so Carmichael numbers aren't very useful.

Solovay-Strassen Primality Test:

-Recall: If p is prime, then the Jacobi symbol, $(\frac{a}{p}) = 1$ if $a \equiv x^2 \pmod{p}$, or $(\frac{a}{p}) = -1$ if $a \not\equiv x^2 \pmod{p}$

-If p is not prime, then the Jacobi symbol doesn't tell us if a is a square or not.

-Theorem: If p is prime, then for any a, we have the equation: $(\frac{a}{p}) \equiv a^{\frac{p-1}{2}} \pmod{p}$

-Note that this equation is only valid if p is a prime number.

Steps for the Solovay-Strassen Primality Test for n:

Repeat the following 3 steps k times:

1) Pick a random a where $2 \leq a < n-1$.

2) Compute $(\frac{a}{n})$ and $a^{\frac{n-1}{2}} \pmod{n}$

3) If $(\frac{a}{n}) \neq a^{\frac{n-1}{2}} \pmod{n}$, then return "composite". But if $(\frac{a}{n}) = a^{\frac{n-1}{2}} \pmod{n}$, every time, then return "probably prime".

-If $(\frac{a}{n}) \equiv a^{\frac{n-1}{2}} \pmod{n}$, but n is composite, then n is called a *(base a) Euler pseudoprime*.

-For any composite n, at least half of the possible a's are witnesses.

-If we repeat the Solovay-Strassen Test k times, and we got "probably prime" each of those times, then the probability that n is composite is at most $\frac{1}{2^k}$

-Refer to the Solovay-Strassen SAGE file in the Handouts section of CoCalc.

-Steps for the Miller-Rabin Primality Test (Improved Fermat Primality Test):

Repeat the following 3 steps k times:

1) Check if n is prime.

2) Pick a random a where $2 \leq a < n-1$.

3) Compute $a^{n-1} \pmod{n}$

-We break down the last step into the following 3 steps:

1) Write $n-1 = m * 2^k$, where m is odd.

-*Example*: For $n = 21$, we have that $n-1 = 20 = 5 * 2^2$, where $m = 5$ and $k = 2$, where k is the exponent 2.

2) Compute $b_0 \equiv a^m \pmod{n}$. If $b_0 \equiv \pm 1 \pmod{n}$, return "probably prime".

3) For i in 1,2,...,k-1, compute $b_i \equiv b_{i-1}^2 \pmod{n}$. If $b_i \equiv 1 \pmod{n}$, return "composite", but if $b_i \equiv -1 \pmod{n}$, return "probably prime". If the for loop finishes, and $b_{k-1} \not\equiv \pm 1 \pmod{n}$, return "composite".

-Note: Essentially, what we are computing in the Solovay-Strassen Test is $b_{k-1} \equiv a^{\frac{n-1}{2}} \pmod{n}$.

-If n is composite, then at least 3/4 of the possibilities for a are witnesses for the Miller-Rabin Test.

-If we repeat the Miller-Rabin Test k times and we get "probably prime" each time, the probability that n is composite is at most $(\frac{1}{4})^k$.

-There exists a test called the AKS Primality Test that can check for certain if a number is prime, in polynomial time. However, it is too slow for practical applications.