MA/CSSE 473 Day 10

Primality Testing

MA/CSSE 473 Day 10

- **A place to read about modular arithmetic**, including exponentiation and inverse: Weiss Sections 7.4-7.4.4
- **In-class exam:** Tuesday, October 5
  - You may bring your textbook, plus a two-sided 8.5x11 inch piece of paper containing anything that you can read unaided or with normal eyeglasses.
- **Student Questions**
- Primality Testing, Carmichael numbers

Recap: Easy Primality Test?

- Is N prime?
- Pick some **a** with $1 < \mathbf{a} < N$
- Is $\mathbf{a}^{N-1} \equiv 1 \pmod{N}$? If not, N is composite.
- But, it is possible that N may not be prime, but we might just happen to pick an **a** for which $\mathbf{a}^{N-1} \equiv 1 \pmod{N}$
  - **Example:** 341 is not prime (it is 11·31), but $\mathbf{2}^{340} \equiv 1 \pmod{341}$
- **Definition:** We say that a number **a passes the Fermat test** iff $\mathbf{a}^{N-1} \equiv 1 \pmod{N}$
- If any integer that is relatively prime to N fails the test, then at least half of the numbers **a** such that $1 \le a < N$ also fail it.

"composite" means "not prime"

Q1

Where are we now?

- For a moment, we pretend that Carmichael numbers do not exist.
- If N is prime, $a^{N-1} \equiv 1 \pmod{N}$ for all $0 < a < N$
- If N is not prime, then $a^{N-1} \equiv 1 \pmod{N}$ for at most half of the values of $a<N$.
- Pr(algorithm returns **true** if N is prime) = 1
  Pr(algorithm returns **true** if N is composite) ≤ ½
- How to reduce the likelihood of error?

Q2

Carmichael Numbers

- A Carmichael N number is a composite number that passes the Fermat test for all **a** with $1 \le \mathbf{a} < N$ and gcd(a, N)=1.
  - The smallest Carmichael number is 561
  - We'll see later how to deal with those
  - How rare are they? Let C(X) = number of Carmichael numbers that are less than X.

n	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
$C(10^n)$	1	7	16	43	105	255	646	1547	3605	8241	19279	44706	105212	246683	585355	1401644	3381806	8220777

  - For now, we pretend that we live in a Carmichael-free world

Q3

The algorithm (modified)

- To test N for primality
  - Pick positive integers $a_1, a_2, \ldots, a_k < N$ at random
  - For each a_i, check for $a_i^{N-1} \equiv 1 \pmod N$
    - Use the Miller-Rabin approach, (next slides) so that Carmichael numbers are unlikely to thwart us.
    - If a_i^{N-1} is not congruent to 1 (mod N), or Miller-Rabin test produces a non-trivial square root of 1 (mod N)
      - return false
  - return true

Miller-Rabin test

- A Carmichael N number is a composite number that passes the Fermat test for all **a** with $1 \le \mathbf{a} < N$ and gcd(a, N)=1.
- **A way around the problem (Rabin and Miller):** Note that for some t and u (u is odd), $N-1 = 2^t u$.
- As before, compute $a^{N-1} \pmod N$, but do it this way:
  - Calculate $a^u \pmod N$, then repeatedly square, to get the sequence
    $a^u \pmod N$, $a^{2u} \pmod N$, …, $a^{2^t u} \pmod N \equiv a^{N-1} \pmod N$
- Suppose that at some point, $a^{2^i u} \equiv 1 \pmod N$, but $a^{2^{i-1} u}$ is not congruent to 1 or to N-1 (mod N)
  - then we have found a nontrivial square root of 1 (mod N).
  - We will show that if 1 has a nontrivial square root (mod N), then N cannot be prime.

Q4,5

Example (first Carmichael number)

- N = 561. We might randomly select a = 101.
  - Then $560 = 2^4 \cdot 35$, so u=35, t=4
  - $a^u \equiv 101^{35} \equiv 560 \pmod{561}$ which is -1 (mod 561) (we can stop here)
  - $a^{2u} \equiv 101^{70} \equiv 1 \pmod{561}$
  - …
  - $a^{16u} \equiv 101^{560} \equiv 1 \pmod{561}$
  - So 101 is not a witness that 561 is composite (we say that 101 is a *liar for 561,* if indeed 561 is composite)
- Try a = 83
  - $a^u \equiv 83^{35} \equiv 230 \pmod{561}$
  - $a^{2u} \equiv 83^{70} \equiv 166 \pmod{561}$
  - $a^{4u} \equiv 83^{140} \equiv 67 \pmod{561}$
  - $a^{8u} \equiv 83^{280} \equiv 1 \pmod{561}$
  - So 83 is a witness that 561 is composite, because 67 is a non-trivial square root of 1 (mod 561).

Q5,6

Lemma: Modular Square Roots of 1

- If s is neither 1 or -1 (mod N), but $s^2 \equiv 1 \pmod{N}$, then N is not prime
- **Proof** (by contrapositive)**:**
  - Suppose that N is prime and $s^2 \equiv 1 \pmod{N}$
  - $s^2-1 \equiv 0 \pmod{N}$ [subtract 1 from both sides]
  - $(s - 1)(s + 1) \equiv 0 \pmod{N}$ [factor]
  - So N divides (s - 1) (s + 1) [def of congruence]
  - Since N is prime, N divides (s - 1) or N divides (s + 1) [def of prime]
  - S is congruent to either 1 or -1 (mod N) [def of congruence]
- This proves the lemma, which validates the Miller-Rabin test

Q7

Accuracy of the Primality Test

- Rabin* showed that if N is composite, this test will demonstrate its non-primality for at least ¾ of the numbers **a** that are in the range 1…N-1, even if **a** is a Carmichael number.
- Note that 3/4 is the worst case; randomly-chosen composite numbers have a much higher percentage of witnesses to their non-primeness.
- If we test several values of **a**, we have a very low chance of flagging a composite number as prime.

*Journal of Number Theory 12 (1980) no. 1, pp 128-138

Efficiency of the Test

- Testing an n-bit number is $\Theta(n^3)$
- If we use the fastest-known integer multiplication techniques (based on Fast Fourier Transforms), this can be pushed to $\Theta(n^2 * \log n * \log \log n)$

Testing "small" numbers

- **Wikipedia article on the Miller-Rabin primality test:**
- When the number N we want to test is small, smaller fixed sets of potential witnesses are known to suffice. For example, Jaeschke has verified that
  - if N < 9,080,191, it is sufficient to test a = 31 and 73
  - if N < 4,759,123,141, it is sufficient to test a = 2, 7, and 61
  - if N < 2,152,302,898,747, it is sufficient to test a = 2, 3, 5, 7, 11
  - if N < 3,474,749,660,383, it is sufficient to test a = 2, 3, 5, 7, 11, 13
  - if N < 341,550,071,728,321, it is sufficient to test a = 2, 3, 5, 7, 11, 13, 17.

Generating Random Primes

- For cryptography, we want to be able to quickly generate random prime numbers with a large number of bits
- Are prime numbers abundant among all integers? Fortunately, yes
- Lagrange's prime number theorem
  - Let $\pi(N)$ be the number of primes that are $\leq N$, then $\pi(N) \approx N / \ln N$.
  - Thus the probability that an n-bit number is prime is approximately $(2^n / \ln (2^n)) / 2^n \approx 1.44 / n$

Q8

Random Prime Algorithm

- To generate a random n-bit prime:
  - Pick a random n-bit number N
  - Run a primality test on N
  - If it passes, output N
  - Else repeat the process
  - Expected number of iterations is $\Theta(n)$

Q9-1