MA/CSSE 473 Day 08

Randomized Primality Testing

Carmichael Numbers

Miller-Rabin test

MA/CSSE 473 Day 09

- Student questions
- Primality Testing
- Implications of Fermat's Little Theorem
  - What we can show and what we can't
- Frequency of "non-Fermat" numbers
- Carmichael numbers
- Randomized Primality Testing.

Why a certain math prof who sometimes teaches this course does not like the Levitin textbook…

Recap: Fermat's Little Theorem

- **Formulation 1:** If p is prime, then for every number a with $1 \le a < p$, $a^{p-1} \equiv 1 \pmod{p}$
- **Formulation 2:** If p is prime, then for every number a with $1 \le a < p$, $a^{p} \equiv a \pmod{p}$

Q4-5

Easy Primality Test?

"composite" means "not prime"

- Is N prime?
- Pick some **a** with 1 < **a** < N
- Is $\mathbf{a}^{N-1} \equiv 1 \pmod{N}$?
- If so, N is prime; if not, N is composite
- Nice try, but…
  - Fermat's Little Theorem is not an "if and only if" condition.
  - It doesn't say what happens when N is not prime.
  - 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** if $\mathbf{a}^{N-1} \equiv 1 \pmod{N}$
- We can hope that if N is composite, then many values of **a** will fail the test
- It turns out that this hope is well-founded
- 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.

How many “Fermat liars"?

- If N is composite, and we randomly pick an **a** such that $1 \le$ **a** $< N$, and gcd(a, N) = 1, how likely is it that **a**$^{N-1}$ is $\equiv 1 \pmod{n}$?
- If **a**$^{N-1} \not\equiv 1 \pmod{n}$ for *some* **a** that is relatively prime to N, then this must also be true for at least half of the choices of **a** < N.
  - Let b be some number (if any exist) that passes the Fermat test, i.e. $b^{N-1} \equiv 1 \pmod{N}$.
  - Then the number a·b fails the test:
    - $(ab)^{N-1} \equiv a^{N-1}b^{N-1} \equiv a^{N-1}$, which is not congruent to 1 mod N.
  - Diagram on whiteboard.
  - For a fixed **a**, f: b→ab is a one-to-one function on the set of b's that pass the Fermat test,
  - so there are at least as many numbers that fail the Fermat test as pass it.

Carmichael Numbers

- A Carmichael number is a composite number N such that
- $\forall$ a ∈ {1, ..N-1} (if gcd(a, N)=1 then **a**$^{N-1}$ **≡ 1** (mod N)) i.e. every possible **a** passes the Fermat test.
  - 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

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 $a<N$.
- $Pr(a^{N-1} \equiv 1 \pmod{N}$ if N is prime) = 1
  $Pr(a^{N-1} \equiv 1 \pmod{N}$ if N is composite) ≤ ½
- How to reduce the likelihood of error?

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

Does this work?

Note that this algorithm may produce a "false prime", but the probability is very low if k is large enough.

Miller-Rabin test

- A **Carmichael number** N is a composite number that passes the Fermat test for all **a** with $1 \le$ **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}(mod N), but do it this way:
  - Calculate a^u (mod N), then repeatedly square, to get the sequence
    a^u (mod N), a^{2u} (mod N), …, $a^{2^t u}$ (mod N) $\equiv a^{N-1}$ (mod N)
- Suppose that at some point, $a^{2^i u} \equiv 1$ (mod 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.

Example (first Carmichael number)

- N = 561. We might randomly select a = 101.
  - Then $560 = 2^4 \cdot 35$, so u=35, t=4
  - $a^u \equiv 101^{35} \equiv 560$ (mod 561) which is -1 (mod 561) (we can stop here)
  - $a^{2u} \equiv 101^{70} \equiv 1$ (mod 561)
  - …
  - $a^{16u} \equiv 101^{560} \equiv 1$ (mod 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
  - $a^u \equiv 83^{35} \equiv 230$ (mod 561)
  - $a^{2u} \equiv 83^{70} \equiv 166$ (mod 561)
  - $a^{4u} \equiv 83^{140} \equiv 67$ (mod 561)
  - $a^{8u} \equiv 83^{280} \equiv 1$ (mod 561)
  - So 83 is a witness that 561 is composite, because 67 is a non-trivial square root of 1 (mod 561).