12 May 2021 Randomized Primality Testing

Announcements:

Today I'll initiate the survey to pick alternate final exam time.
Thinking of asking about May 20-25.

Final exam coverage: cumulative up to approximation algorithms. (Omitting randomized algorithms.)

Primality testing: given positive integer $n > 1$, decide if n is prime.
In cryptography one frequently needs to solve this for n with hundreds or thousands of digits.
Algorithms with running time $O(n)$ are way too slow.
We need $O(\text{polylog}(n))$ meaning $(\log(n))^{O(1)}$.
Miller-Rabin Primality Test (1980): a randomized algorithm widely used

for this problem. Runs in $O(\log^3(n))$.

If n is prime, MR always outputs "prime".
If n is composite, MR outputs "composite"
with probability at least $1/2$,
but could potentially output "prime".
(Probability of an error like that is $\leq \frac{1}{2}$.)

If we run MR primality test on n
twice using independent randomness,
$\Pr(\text{false positive}) \leq \frac{1}{4}$.
Run it k times, $\Pr(\text{false positive}) \leq \frac{1}{2^k}$.
E.g. run 7 times independently,
$\Pr(\text{false positive}) < 1\%$.

Some facts from number theory.

(1) If p is prime and a is any integer,
$$a^p \equiv a \pmod{p}.$$

Proof. $(a+b)^p = \sum_{i=0}^{p} \binom{p}{i} a^i b^{p-i}$

$\binom{p}{i}$ divisible by p except $i=0$, $i=p$.

$$\equiv a^p + b^p \pmod{p}.$$

$$\underbrace{(1+1+\cdots+1)^p}_{a \text{ times}} \equiv \underbrace{1^p + 1^p + \cdots + 1^p}_{a \text{ times.}} \pmod{p}$$

(2) Fermat's Little Theorem: If p prime and a not divisible by p, then

$$a^{p-1} \equiv 1 \pmod{p}.$$

Proof. $a \cdot \text{LHS} \equiv a \cdot \text{RHS}$ by Fact 1,
so $a \cdot (\text{LHS} - \text{RHS})$ is divisible by p.
But a not divisible by p, so
LHS − RHS must be div by p.

Fermat Test for Primality. Given n, sample
random $x \in \{1, \ldots, n-1\}$.
Calculate $x^{n-1} \pmod{n}$.
If $x^{n-1} \not\equiv 1 \pmod{n}$ output "composite".
Else output "prime".

Obs. 1. If n is prime, FLT says $x^{n-1} \equiv 1 \pmod{n}$
so we will definitely output "prime".
If n is composite it is possible to
output "prime" for example when $x = 1$.
So false positives happen with probability > 0.
How often do they happen?

Def. If n composite and $x^{n-1} \not\equiv 1 \pmod{n}$
we call x a "Fermat witness" for n.
If $x^{n-1} \equiv 1 \pmod{n}$ x is a "Fermat liar".

Lemma. Assume n has at least one x such that $\gcd(x,n)=1$ and $x^{n-1} \not\equiv 1 \pmod{n}$. Then the Fermat witnesses for n are at least as numerous as the Fermat liars.

"Either Fermat witnesses are quite easy to find by random sampling, or they're impossible to find."

Proof. Let $S = \{ ax + bn \mid a, b \in \mathbb{Z} \}$.

S is an additive subgroup of $\mathbb{Z}$, i.e. closed under addition and subtraction.

Claim $S = \mathbb{Z}$.

Note this is equivalent to claiming $1 \in S$.

Let $d \in S$ be an element with minimum absolute value. Every integer multiple of d belongs to S, by repeated addition and subtraction.

In the open interval from kd to $(k+1)d$ there can be no element $y \in S$ because $|y - kd| < d$ and d is the minimum abs value element of S.

$\therefore$ $S = \{$ integer multiples of $d \}$.

Note $x \in S$, $n \in S \Rightarrow$ x and n are both multiples of d.

Recall $\gcd(x,n) = 1 \Rightarrow d = \pm 1$, $1 \in S$.

This means we know $\exists\ a,b \in \mathbb{Z}$ s.t.

$$ax + bn = 1$$

$$ax \equiv 1 \pmod{n}.$$

Now we're trying to prove Fermat witnesses are at least as numerous as Fermat liars.

Let $W = \{\text{witnesses}\}$, $L = \{\text{liars}\}$.

Define $h: L \to W$ and show h is one-to-one.

$$h(y) = x \cdot y.$$

If $y \in L$ it means $y^{n-1} \equiv 1 \pmod{n}$.

Then

$$\begin{aligned} h(y)^{n-1} &= (xy)^{n-1} \\ &= x^{n-1} \cdot y^{n-1} \\ &\equiv x^{n-1} \cdot 1 \pmod{n} \\ &\not\equiv 1 \pmod{n} \end{aligned}$$

since $x^{n-1} \not\equiv 1 \pmod{n}$.

This shows $h(y) \in W$ when $y \in L$.

To show h is one-to-one, notice

$$xy \equiv xy' \pmod{n}$$

$$\Rightarrow\ a \cdot xy \equiv a \cdot xy' \pmod{n}$$

$$\Rightarrow\ (ax) \cdot y \equiv (ax) \cdot y' \pmod{n}$$

$$\Rightarrow\ y \equiv y' \pmod{n} \quad \text{since } ax \equiv 1.$$

Conclusion. If n has at least one Fermat witness x with $\gcd(x,n) = 1$ then Fermat test has $\leq \frac{1}{2}$ prob of false positive.

Def. n is a **Carmichael number** if n is composite and every x with $\gcd(x,n) = 1$ satisfies $x^{n-1} \equiv 1 \pmod{n}$.

When n is a Carmichael number, the Fermat test only succeeds when it samples x that has a common factor with n.

Implementing Fermat test in poly time.

How to compute $x^{n-1} \pmod{n}$ is poly $(\log n)$ time?

Use repeated squaring, e.g.

multiply these three.

$$x^{100} = x^{64} \cdot x^{32} \cdot x^{4}$$

Compute $x, x^2, (x^4), x^8, x^{16}, (x^{32}), (x^{64})$

More generally computing $x^k \pmod n$
requires $\log(k)$ squaring mod n ops
$\log(k)$ mult. mod n ops.

In total $x^{n-1} \pmod n$ requires
$O(\log n)$ mult-mod-n ops.
Each takes $O(\log n \log\log n)$.
So $O(\log^2 n \log\log n)$ running time for FT.

What's known about Carmichael numbers?

1. Infinitely many of them.
2. Smallest is 561.
3. Each of them factors as a product of at least three distinct primes.
4. Miller & Rabin found a randomized test to detect them by searching for a "fake square root of 1."

Lemma. If $\exists x$ s.t. $x^2 \equiv 1 \pmod n$
but $x \notin \{1, -1\} \pmod n$
then n is composite.

Proof. $x^2 - 1 = (x+1)(x-1)$.

So under the Lemma's hypotheses n is divisor of x^2-1 but it divides neither of $x+1, x-1$.

$x^k \pmod n$.

Write k in binary:

$$k = 2^{n_1} + 2^{n_2} + \cdots 2^{n_\ell}$$

where $\log k \geq n_1 > n_2 > \cdots > n_\ell \geq 0$.

Compute

$$x^1, x^2, x^4, \ldots, x^{2^{n_1}}$$

Compute

$$x^{2^{n_1}} \cdot x^{2^{n_2}} \cdots x^{2^{n_\ell}} = x^{2^{n_1}+\cdots+2^{n_\ell}} = x^k$$

Each of these factors is on this list.