Sketch of Lecture 15

Mon, 2/11/2019

Review. If N is composite, then a residue a is a Fermat liar modulo N if $a^{N-1} \equiv 1 \pmod{N}$.

Example 89. Somewhat suprisingly, there exist composite numbers n with the following disturbing property: every residue a is a Fermat liar or $\gcd(a, n) > 1$.

This means that the Fermat primality test is unable to distinguish n from a prime, unless the randomly picked number a happens to reveal a factor (namely, $\gcd(a, n)$) of n (which is exceedingly unlikely for large numbers). [Recall that, for large numbers, we do not know how to find factors even if that was our primary goal.]

Such numbers are called **absolute pseudoprimes** or Carmichael numbers.

The first few are $561, 1105, 1729, 2465, \ldots$ (it was only shown in 1994 that there are infinitely many of them). These are very rare, however: there are 43 absolute pseudoprimes less than 10^6. (Versus $78, 498$ primes.)

Example 90. Show that 561 is an absolute pseudoprime.

Solution. We need to show that $a^{560} \equiv 1 \pmod{561}$ for all invertible residues modulo 561.

Since $561 = 3 \cdot 11 \cdot 17$, $a^{560} \equiv 1 \pmod{561}$ is eqivalent to $a^{560} \equiv 1 \pmod{p}$ for all of $p = 3, 11, 17$.

By Fermat's little theorem, we have $a^2 \equiv 1 \pmod{3}$, $a^{10} \equiv 1 \pmod{11}$, $a^{16} \equiv 1 \pmod{17}$. Since $2, 10, 16$ all divide 560, it follows that indeed $a^{560} \equiv 1 \pmod{p}$ for $p = 3, 11, 17$.

Comment. Korselt's criterion (1899) states that what we just observed in fact characterizes absolute pseudoprimes. Namely, a composite number n is an absolute pseudoprime if and only if n is square-free, and for all primes p dividing n, we also have $p - 1 | n - 1$.

Theorem 91. (Korselt's Criterion) Let n be positive and composite. Then $a^n \equiv a \pmod{n}$ holds for any integer a if and only if n is squarefree and $(p-1)|(n-1)$ for any prime divisor p of n.

[if and only if $a^{n-1} \equiv 1 \pmod{n}$ holds for any integer a with $\gcd(a, n) = 1$]

Proof. Here, we will only the "if" part (the "only if" part is also not hard to show but the typical proof requires a little more insight into primitive roots than we currently have). In other words, assume that n is **squarefree** and $(p-1)|(n-1)$ for any prime divisor p of n. Let a be any integer. We will show that $a^n \equiv a \pmod{n}$.

n being squarefree means that its prime factorization is of the form $n = p_1 \cdot p_2 \cdots p_d$ for distinct primes p_i (this is equivalent to saying that there is no integer $m > 1$ such that $m^2 | n$). By Fermat's little theorem $a^{p_i - 1} \equiv 1 \pmod{p_i}$ and, since $(p_i - 1)|(n-1)$, $a^{n-1} \equiv 1 \pmod{p_i}$. But, wait! This is only true if $\gcd(a, p_i) = 1$, that is, $a \not\equiv 0 \pmod{p_i}$. However, in either case (that is, for all a), we get $a^n \equiv a \pmod{p_i}$. It then follows by the Chinese remainder theorem that $a^n \equiv a \pmod{n}$. □

The Miller–Rabin primality test

The Fermat primality test picks a and checks whether $a^{n-1} \equiv 1 \pmod{n}$.

- If $a^{n-1} \not\equiv 1 \pmod{n}$, then we are done because n is definitely not a prime.
- If $a^{n-1} \equiv 1 \pmod{n}$, then either n is prime or a is a Fermat liar.
  But instead of leaving off here, we can dig a little deeper:
  Note that $a^{(n-1)/2}$ satisfies $x^2 \equiv 1 \pmod{n}$. If n is prime, then $a^{(n-1)/2} \equiv \pm 1 \pmod{n}$.
  [Recall that, if n is composite (and odd), then $x^2 \equiv 1 \pmod{n}$ has additional solutions!]
  - Hence, if $a^{(n-1)/2} \not\equiv \pm 1 \pmod{n}$, then we again know for sure that n is not a prime.
    Advanced comment. In fact, we can now factor n! See bonus challenge below.
  - If $a^{(n-1)/2} \equiv 1 \pmod{n}$ and $\frac{n-1}{2}$ is divisible by 2, we continue and look at $a^{(n-1)/4} \pmod{n}$.
    - If $a^{(n-1)/4} \not\equiv \pm 1 \pmod{n}$, then n is not a prime.
    - If $a^{(n-1)/4} \equiv 1 \pmod{n}$ and $\frac{n-1}{4}$ is divisible by 2, we continue...

Write $n - 1 = 2^s \cdot m$ with m odd. In conclusion, if n is a prime, then

$$a^m \equiv 1 \quad \text{or, for some } r = 0, 1, \ldots, s - 1, \quad a^{2^r m} \equiv -1 \quad \pmod{n}.$$

In other words, if n is a prime, then the values $a^m, a^{2m}, \ldots, a^{2^s m}$ must be of the form $1, 1, \ldots, 1$ or $\ldots, -1, 1, 1, \ldots, 1$. If the values are of this form even though n is composite, then a is a **strong liar** modulo n.

This gives rise to the following improved primality test:

Miller–Rabin primality test

Input: number n and parameter k indicating the number of tests to run

Output: "not prime" or "likely prime"

Algorithm:

```
Write $n - 1 = 2^s \cdot m$ with $m$ odd.
Repeat $k$ times:
    Pick a random number $a$ from $\{2, 3, \ldots, n - 2\}$.
    If $a^m \not\equiv 1 \pmod{n}$ and $a^{2^r m} \not\equiv -1 \pmod{n}$ for all $r = 0, 1, \ldots, s - 1$, then
        stop and output "not prime".
Output "likely prime".
```

Comment. If n is composite, then less than a quarter of the values for a could possibly be strong liars. In other words, for any composite number, the odds that the Miller–Rabin test returns "likely prime" are less than 4^{-k}.

Comment. Note that, though it looks more involved, the Miller–Rabin test is essentially as fast as the Fermat primality test (recall that, to compute a^{n-1}, we proceed using binary exponentiation).

Advanced comments. This is usually implemented as a probabilistic test. However, assuming GRH (the generalized Riemann hypothesis), it becomes a deterministic algorithm if we check $a = 2, 3, \ldots, \lfloor 2(\log n)^2 \rfloor$. This is mostly of interest for theoretical applications. For instance, this then becomes a polynomial time algorithm for checking whether a number is prime.

More recently, in 2002, the AKS primality test was devised. This test is polynomial time (without relying on outstanding conjectures like GRH).

Example 92. Suppose we want to determine whether $n = 221$ is a prime. Simulate the Miller–Rabin primality test for the choices $a = 24$, $a = 38$ and $a = 47$.

Solution. $n - 1 = 4 \cdot 55 = 2^s \cdot m$ with $s = 2$ and $m = 55$.

- For $a = 24$, we compute $a^m = 24^{55} \equiv 80 \not\equiv \pm 1 \pmod{221}$. We continue with $a^{2m} \equiv 80^2 \equiv 212 \not\equiv -1$, and conclude that n is not a prime.

  Note. We do not actually need to compute that $a^{n-1} = a^{4m} \equiv 81$, which features in the Fermat test and which would also lead us to conclude that n is not prime.

- For $a = 38$, we compute $a^m = 38^{55} \equiv 64 \not\equiv \pm 1 \pmod{221}$. We continue with $a^{2m} \equiv 64^2 \equiv 118 \not\equiv -1$ and conclude that n is not a prime.

  Note. This case is somewhat different from the previous in that 38 is a Fermat liar. Indeed, $a^{4m} \equiv 118^2 \equiv 1 \pmod{221}$. This means that we have found a nontrivial sqareroot of 1. In this case, the Fermat test would have failed us while the Miller–Rabin test would have succeeded.

- For $a = 47$, we compute $a^m = 47^{55} \equiv 174 \not\equiv \pm 1 \pmod{221}$. We continue with $a^{2m} \equiv 174^2 \equiv -1$. We conclude that n is a prime or a is a strong liar. In other words, we are not sure but are (incorrectly) leaning towards thinking that 221 was a prime.

Comment. In this example, only 4 of the 218 residues $2, 3, \ldots, 219$ are strong liars (namely $21, 47, 174, 200$). For comparison, there are 14 Fermat liars (namely $18, 21, 38, 47, 64, 86, 103, 118, 135, 157, 174, 183, 200, 203$).

Example 93. (bonus challenge) If $a^{n-1} \equiv 1 \pmod{n}$ but $a^{(n-1)/2} \not\equiv \pm 1 \pmod{n}$, then we can find a factor of n! How?!

Comment. However, note that this only happens if a is a Fermat liar modulo n, and these are typically very rare. So, unfortunately, we have not discovered an efficient factorization algorithm.

But we have run into an idea, which is used for some of the best known factorization algorithms. If time permits, more on that later...

Send in a solution by Feb 24 for a bonus point!