Rabin-Miller Primality Test

**Lemma 0.1** Suppose $p$ is an odd prime. Let $p - 1 = 2^k m$ where $m$ is odd. Let $1 \leq a < p$. Either

i) $a^m \equiv 1 \pmod{p}$ or

ii) one of $a, a^2, a^4, a^8, \ldots, a^{2^{k-1}}m$ is congruent to $-1 \pmod{p}$.

**Proof** We know that

$$\left(a^{2^{k-1}m}\right)^2 = a^{p-1} \equiv 1 \pmod{n}.$$ 

Thus $a^{2^{k-1}m} \equiv \pm 1 \pmod{p}$. If $a^{2^{k-1}m} \equiv -1 \pmod{p}$ we are done. Otherwise we proceed by induction.

If each of $a^{2^{i+1}m}, \ldots, a^{2^{k-1}m}$ is congruent to 1, then $a^{2^i}m \equiv \pm 1$. It follows that if ii) fails, we must have $a^m \equiv 1 \pmod{p}$.

Suppose we are given an odd number $n$ and want to know if it prime. We could pick $1 \leq a < n$ and calculate

$a, a^2, a^4, a^8, \ldots, a^{2^{k-1}}m \pmod{n}$. If neither i) nor ii) holds then we would know $n$ is composite. In this case we say $a$ is a witness that $n$ is composite.

If $a$ is not a witness, this does not tell us that $n$ is prime, but it gives us some evidence that $n$ might be prime.

If $n$ is composite, most $1 < a < n$ will witness that it is composite.

**Theorem 0.2** If $n$ is composite, then at least 75% of numbers $1 < a < n$ witness that $n$ is composite.

This gives rise to a probabilistic algorithm for testing primality.

**Rabin-Miller Algorithm**

- Randomly pick $a_1, \ldots, a_k$ independent elements $1 < a < n$.
- For each $a_i$ do the test described above.
• If any \( a_i \) is a witness that \( n \) is composite, you know \( n \) is composite
• If no \( a_i \) is a witness, guess that \( n \) is prime.

If you decide that \( n \) is composite, you will know that this is the correct answer. If you guess that \( n \) is prime, there is some chance that you were just unlucky. But if you guess that \( n \) is prime, the chance that you are wrong is less that \( (.25)^k \). If we took \( k = 100 \), then \( (.25)^{100} < 10^{-60} \). Taking \( k \) larger will increase our level of certainty further.

Fermat Test–A Flawed Attempt

One might try a simpler version of the Rabin-Miller test. If we want to know if \( n \) is prime, pick \( 1 < a_1, \ldots, a_k < n \) and test if \( a_i^n \equiv a_i \pmod{n} \). If this fails for any \( i \), then we know \( n \) is composite, while if it is always true we might guess \( n \) is prime. For most numbers \( n \) we are very likely to get the right answer, but there are some composite numbers that would always pass this test.

Definition 0.3 We say \( n \) is a *Carmichael number* if \( a^n \equiv a \pmod{n} \) for all \( n \).

\[ 561 = (3)(11)(17). \] But for any \( a \),
\[ a^{561} = (a^2)^{280}(a) \equiv a \pmod{3} \]
\[ a^{561} = (a^{10})^{56}(a) \equiv a \pmod{11} \]
\[ a^{561} = (a^{16})^{35}(a) \equiv a \pmod{17}. \]

Thus \( a^{561} \equiv a \pmod{561} \). Thus 561 is a Carmichael number.

There are infinitely many Carmichael numbers.