FERMAT'S COMPOSITENESS TEST

KEITH CONRAD

The most naive method of seeing if an integer $m > 1$ is composite is *trial division* up to $\sqrt{m}$. This method will only prove m is composite if we find a divisor of m. A slight improvement on trial division is the following: pick a random a with $1 \leq a \leq m-1$ and compute (a, m) by Euclid's algorithm. If $(a, m) > 1$ then m is certifiably composite, and in fact (a, m) will be a nontrivial factor of m. If $(a, m) = 1$, pick another a at random and try again. We call this the *gcd test* for compositeness.

Example 1. Let $m = 1387$. It turns out that 1387 has just 2 proper factors (not including 1 and 1387), while the number of $a \leq 1386$ with $(a, 1387) > 1$ is 90. There is greater chance of randomly stumbling onto an integer sharing a common factor with m than there is of randomly picking an actual factor of m itself. Still, the odds are not that great for the gcd test to work by trying only a few random choices of a: $90/1386 \approx 6.5\%$.

A real improvement on the gcd test can be described using the conclusion of Fermat's little theorem, which says for prime p that $a^{p-1} \equiv 1 \bmod p$ for *all* a not divisible by p. Even though Fermat's little theorem is about prime moduli, the congruence in the theorem is something that we can think about for any modulus. That is, we want to discuss the validity of

$$a^{m-1} \equiv 1 \bmod m.$$

Let's call this "Fermat's little congruence."[1] *It may or may not be true as a varies.* When m is prime, Fermat's little congruence is true for all $a \not\equiv 0 \bmod m$. What if m is composite? In practice, Fermat's little congruence will often have a lot of counterexamples.

Example 2. Let $m = 1387$. Among the numbers from 1 to 1386, the number of a with $a^{1386} \not\equiv 1 \bmod 1387$ is 1062, and $1062/1386 \approx 77\%$.

Our interest in counterexamples to Fermat's little congruence comes from the following, which is called *Fermat's compositness test*:

$$\text{if } a^{m-1} \not\equiv 1 \bmod m \text{ for at least one } a \not\equiv 0 \bmod m, \text{ then } m \text{ is composite.}$$

Indeed, if m were prime then Fermat's little theorem says $a^{m-1} \equiv 1 \bmod m$ for *all* $a \not\equiv 0 \bmod m$. So when this breaks down even once, m must be composite.

An integer less than m which proves m is composite is called a witness to the compositeness of m. For instance, 3 is a *trial division witness* for 15, since it reveals the compositness of 15 through trial division. We call 10 a *gcd witness* for 15 since $(10, 15) > 1$ (and that proves 15 is composite). Since $2^{14} \not\equiv 1 \bmod 15$, 2 is a counterexample for Fermat's little congruence mod 15 and therefore is called a *Fermat witness* for 15.

Example 3. Let $m = 477703$. Since $2^{477702} \equiv 122500 \bmod 477703$, 477703 must be composite and 2 is a Fermat witness. Notice we have proved 477703 is composite without factoring the number.

[1] This terminology is convenient, but not standard; I made it up.

Example 4. Let $m = 1387$. Since $2^{1386} \equiv 1 \bmod 1387$, we don't learn anything. (Maybe 1387 is actually prime, so this congruence with 2 is just an instance of Fermat's little theorem.) However, $3^{1386} \equiv 875 \bmod 1387$, so 3 is a Fermat witness proving 1387 is composite.

Example 5. Let $m = 2^{32}+1 = 4294967297$. (This is the fifth Fermat number, which Fermat mistakenly thought was prime.) We have $2^{m-1} \equiv 1 \bmod m$ but $3^{m-1} \equiv 3029026160 \not\equiv 1 \bmod m$, so 3 is a Fermat witness and proves that m is composite.

Remark 6. In practice, 2 is often a Fermat witness. That is, when $m > 1$ is composite we usually find that $2^{m-1} \not\equiv 1 \bmod m$, so just one application of the Fermat test is needed. There are only three composite numbers less than 1000 for which 2 is not a Fermat witness: 341, 561, and 1105, and up to 10000 there are only twenty-two such composite numbers.

Any composite number up to 10000 has either 2, 3, 5, or 7 as a Fermat witness, and all but seven of those numbers have 2 or 3 as a Fermat witness (they are 1105, 1729, 2465, 2701, 2821, 6601, and 8911). Using Fermat's little congruence sure beats trial division to determine compositeness!

The Fermat compositeness test (finding a between 1 and m such that $a^{m-1} \not\equiv 1 \bmod m$) has some interesting features:

- when it works, this test proves a number is composite without factoring it,
- each application of the test runs quickly since $a^{m-1} \bmod m$ can be computed very rapidly on a computer, which raises to powers using repeated squaring,
- if the test doesn't work with one a, we just pick another value for a at random and try again (finding only one Fermat witness is enough to prove compositeness). In practice, when the modulus is composite only a handful of a need to be tested before a Fermat witness is found.

It is the last point that we want to understand better. When m is composite, will there always be a Fermat witness, and how many are there? The evidence in Example 2 is compelling: 77% of numbers from 1 to 1386 are Fermat witnesses for 1387's compositeness.

Since the condition $a^{m-1} \equiv 1 \bmod m$ implies $(a, m) = 1$, if $(a, m) > 1$ (*e.g.*, a is a nontrivial factor of m) then $a^{m-1} \not\equiv 1 \bmod m$, so any gcd witness is a Fermat witness. The interesting potential about the Fermat test over the gcd test is that there are usually a lot more a satisfying $a^{m-1} \not\equiv 1 \bmod m$ than $(a, m) > 1$. The next result quantifies this.

Theorem 7. *If $m > 1$ is composite and some unit modulo m is a Fermat witness for m, over half the integers modulo m are Fermat witnesses: $\#\{a \bmod m : a^{m-1} \not\equiv 1 \bmod m\} > m/2$.*

Proof. Set

$$A = \left\{a \in \mathbf{Z}/(m) : a^{m-1} \equiv 1 \bmod m\right\},$$

$$B = \left\{a \in \mathbf{Z}/(m) : a \text{ is a unit mod } m \text{ and } a^{m-1} \not\equiv 1 \bmod m\right\},$$

and

$$C = \{a \in \mathbf{Z}/(m) : (a, m) \neq 1\}.$$

The sets A, B, and C are disjoint (any element of A is a unit modulo m and no element of C can have a power equal to 1). Every element of $\mathbf{Z}/(m)$ is in one of the three sets and the Fermat witnesses are the elements of B and C. We want to show: if $B \neq \emptyset$ then $\#B + \#C \geq m/2$.

We are assuming there is some $b_0 \in B$. Then the set $Ab_0 = \{ab_0 : a \in A\}$ belongs to B. Indeed, for any $a \in A$, the product ab_0 is a unit modulo m, so $ab_0 \in A$ or $ab_0 \in B$. To show

$ab_0 \in B$ we argue by contradiction: if $ab_0 \in A$ then $(ab_0)^{m-1} \equiv 1 \bmod m$. Then

$$1 \equiv (ab_0)^{m-1} \equiv a^{m-1}b_0^{m-1} \equiv b_0^{m-1} \bmod m,$$

so $b_0 \in A$, a contradiction. Therefore $ab_0 \notin A$ for all $a \in A$, so $Ab_0 \subset B$.

Because the number of elements in Ab_0 is $\#A$, from $Ab_0 \subset B$ we have $\#A = \#(Ab_0) \leq \#B$. Therefore

$$m = \#A + \#B + \#C \geq \#A + \#A + 1 > 2\#A,$$

so $\#A < m/2$. Hence

$$\#B + \#C = m - \#A > m - \frac{m}{2} = \frac{m}{2}.$$

□

Remark 8. A reader who knows about cosets in group theory will recognize the use of a coset Ab_0 in the computation above. The argument we gave can be recast in terms of group theory, as follows. The units modulo m are a group under multiplication, and the set A of solutions to Fermat's little congruence $a^{m-1} \equiv 1 \bmod m$ is a subgroup of the units modulo m. If there is a counterexample to Fermat's little congruence among the units, *i.e.*, $B \neq \emptyset$, then A is a proper subgroup of the units mod m and therefore has index at least 2 in the units mod m, which means the size of A is *at most* half the size of the group of units modulo m. Then the counterexamples to $a^{m-1} \equiv 1 \bmod m$ include *at least* half the units modulo m and certainly *all* the non-units modulo m, which adds up to more than half the numbers modulo m. Again, this all follows from the hypothesis that $B \neq \emptyset$.

So as long as *at least one* unit modulo m does not satisfy $a^{m-1} \equiv 1 \bmod m$, more than half the numbers a mod m don't satisfy this congruence, so 50% of the numbers mod m are Fermat witnesses for m. This provides us with a *probabilistic* test for primality: pick lots of values of a less than m at random and check for each of them if Fermat's little congruence breaks down. Naively, if there is at least a 50% "probability" of a randomly chosen number modulo m being a Fermat witness for m, finding $a^{m-1} \equiv 1 \bmod m$ for 10 random values of a is like flipping a coin and getting the same side 10 times in a row: pretty unlikely! In fact, the probability of that happening is $1/2^{10} \approx .000976$. So we might say that m appears to be prime with "probability" $1 - 1/2^{10} \approx .99902$. The "probability" of a number being prime if we don't find any Fermat witnesses for it after 20 random trials of Fermat's little congruence is even closer to 1: $1 - 1/2^{20} \approx .999999046$.

Unfortunately, the basis for our use of Fermat's little theorem as a probabilistic primality test is undermined by the italicized part of the first sentence in the previous paragraph: we need to know that $a^{m-1} \not\equiv 1 \bmod m$ for at least one unit a to get the 50% lower bound on the proportion of Fermat witnesses in Theorem 7. It turns out that there are composite m for which $a^{m-1} \not\equiv 1 \bmod m$ *only* for the non-units mod m, or equivalently for which $a^{m-1} \equiv 1 \bmod m$ whenever $(a, m) = 1$.

Example 9. Let $m = 294409$. It turns out that $a^{294408} \equiv 1 \bmod 294409$ when $(a, m) = 1$, so any Fermat witness satisfies $(a, m) > 1$. Thus a Fermat witness is the same as a gcd witness in this case. To find a Fermat witness we have to find a nonunit modulo m. The number of those is 14472, and $14472/294408 \approx 4.9\%$, so around 95% of the numbers modulo m are *not* Fermat witnesses. This is a striking contrast to Theorem 7, but it is not a counterexample to Theorem 7 because the hypothesis of the theorem is not satisfied for this m.

Composite m for which $a^{m-1} \equiv 1 \bmod m$ whenever $(a, m) = 1$ are called *Carmichael* numbers. This honors R. D. Carmichael, who found the first examples in 1910. The first

five Carmichael numbers are 561, 1105, 1729, 2465, and 2821. The number 294409 from Example 9 is the 25th Carmichael number. (About ten years before Carmichael's work, Korselt proved a few theorems about such numbers without providing a single example. If he had found any then surely we would speak of Korselt numbers instead of Carmichael numbers.) It is known [1] that there are infinitely many Carmichael numbers, and there is no simple algorithm for determining if a general number is Carmichael, so the Fermat compositeness test *can't* be considered a true probabilistic primality test: if we find that $a^{m-1} \equiv 1 \bmod m$ for a lot of values of a, maybe m is a Carmichael number rather than a prime.

References

[1] W. R. Alford, A. Granville, C. Pomerance, *There are infinitely many Carmichael numbers*, Ann. of Math. **139** (1994), 703–722.