FERMAT'S TEST

KEITH CONRAD

1. Introduction

Fermat's little theorem says for prime p that $a^{p-1} \equiv 1 \bmod p$ for all $a \not\equiv 0 \bmod p$. A naive extension of this to a composite modulus $n \geq 2$ would be: for all $a \not\equiv 0 \bmod n$,

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

Let's call the congruence "Fermat's little congruence."[1] *It may or may not be true.* For prime n it holds for all $a \not\equiv 0 \bmod n$. But for composite n it can have many counterexamples.

Example 1.1. When $n = 15$, the table below shows that for only four $a \not\equiv 0 \bmod 15$ do we have $a^{14} \equiv 1 \bmod 15$.

a	1	2	3	4	5	6	7	8	9	10	11	12	13	14
$a^{14} \bmod 15$	1	4	9	1	10	6	4	4	6	10	1	9	4	1

Example 1.2. Among all the numbers $a \not\equiv 0 \bmod 91$, 36 of them (less than half) satisfy $a^{90} \equiv 1 \bmod 91$. The situation for small a is shown below.

a	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	$\cdots$
$a^{90} \bmod 91$	1	64	1	1	64	64	77	64	1	1	64	1	78	14	64	$\cdots$

If Fermat's little congruence $a^{n-1} \equiv 1 \bmod n$ fails for even one $a \not\equiv 0 \bmod n$, then n isn't prime, so it's composite. For instance, from above $2^{14} \not\equiv 1 \bmod 15$ and $2^{90} \not\equiv 1 \bmod 91$, so 15 and 91 are composite. Of course 15 and 91 are small enough that their compositeness can be seen by direct factoring ($15 = 3 \cdot 5$ and $91 = 7 \cdot 13$). The real significance of breaking Fermat's little congruence is for much larger n, since it lets us prove a large number is composite without having to factor it. This is what we will explore here.

2. Three Tests

The simplest method of checking if an integer $n > 1$ is composite is *trial division* up to $\sqrt{n}$, which means testing integers a greater than 1 and less than or equal to $\sqrt{n}$ to see if $a \mid n$. If this ever happens then n is composite. If it never happens then n is prime. We only check up to $\sqrt{n}$ since if $n = ab$ where $a < n$ and $b < n$ then one of a or b is less than or equal to $\sqrt{n}$. Trial division only proves n is composite once we find a divisor of n.

Example 2.1. Let $n = 415693$. Then $\sqrt{n} \approx 644.74$. The only nontrivial proper factor of n less than $\sqrt{n}$ is 593. Since $593/\sqrt{n} \approx .92$, we have to go over 90% of the way to $\sqrt{n}$ before we have proved n is composite by trial division.

A slight improvement on trial division is using greatest common divisors with n: pick an integer a with $1 \leq a \leq n-1$ and compute (a, n) by Euclid's algorithm. Since $(a, n) \leq a < n$, if $(a, n) > 1$ then (a, n) is a nontrivial factor of n so n is composite. On the other hand, if

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

$(a, n) = 1$ then we learned nothing and pick another a at random from 1 to $n - 1$ and try again. We call this the *gcd test* for compositeness.

Example 2.2. Let $n = 415693$, as in the previous example. While n has only one nontrivial factor below $\sqrt{n}$, the number of a from 1 to $n - 1$ such that $(a, n) > 1$ is 1293, so there is a better chance of randomly picking an integer less than n that shares a common nontrivial factor with n than there is of picking an actual factor of n below $\sqrt{n}$. Still, the odds are quite small that the gcd test will work using a few random choices of a: $1293/(n-1) \approx .31\%$, which is less than $1/3$ of 1%.

A significant improvement on the gcd test comes from seeking to disprove Fermat's little congruence $a^{n-1} \equiv 1 \bmod n$ for some a with $1 \leq a \leq n - 1$.

Example 2.3. Let $n = 415693$ again. Then $2^{n-1} \equiv 58346 \not\equiv 1 \bmod n$, so after just one choice of a we proved n is composite!

Even better, the number of integers a from 1 to $n - 1$ that satisfy $a^{n-1} \not\equiv 1 \bmod n$ is 415677, and $415677/(n - 1)$ is over 99.99%. You'd have to be incredibly unlucky not to prove n is composite by picking an a from 1 to $n - 1$ at random to see if $a^{n-1} \not\equiv 1 \bmod n$.

Let us call the strategy we have introduced *Fermat's compositness test*:

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

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

An integer less than n that proves n is composite is called a witness to the compositeness of n. The type of witness depends on the type of test we use.

Definition 2.4. Let $1 \leq a \leq n - 1$. We call a a *trial division* witness for n if $a \mid n$.[2] We call a a *gcd witness* for n if $(a, n) > 1$. We call a a *Fermat witness* for n if $a^{n-1} \not\equiv 1 \bmod n$.

This terminology is reasonable: a trial division witness for n reveals compositeness of n through trial division of n by that number. A gcd witness for n reveals compositeness of n by computing its greatest common divisor with n. A Fermat witness reveals compositeness of n by testing it in Fermat's little congruence mod n.

For instance, 3 is a trial division witness for 15 and a gcd witness for 15, and 10 is a gcd witness for 15 but not a trial division witness for 15. What about Fermat witnesses for 15?

Example 2.5. Since $2^{14} \equiv 4 \not\equiv 1 \bmod 15$ (see the table in Example 1.1), 2 is a Fermat witness for 15, as is every number from 1 to 14 except 1, 4, 11, and 14.

Example 2.6. From Example 2.3, where $n = 415693$, since $2^{n-1} \not\equiv 1 \bmod n$ the number 2 is a Fermat witness for n, proving it is composite without having to factor n.

Example 2.7. Let $n = 1387$. Since $2^{1386} \equiv 1 \bmod 1387$, we don't learn anything. (Maybe 1387 is prime, so this congruence with 2 would just be an instance of Fermat's little theorem.) However, $3^{1386} \equiv 875 \not\equiv 1 \bmod 1387$, so 3 is a Fermat witness and 1387 is composite.

Example 2.8. Let $n = 2^{2^5} + 1 = 4294967297$. Fermat thought n is prime, but it is not: while $2^{n-1} \equiv 1 \bmod n$, it turns out that $3^{n-1} \equiv 3029026160 \not\equiv 1 \bmod n$, so 3 is a Fermat witness that proves n is composite without telling us a nontrivial factor of n. Euler discovered 641 is a factor of n about 100 years after Fermat mistakenly said n is prime.

[2]Strictly speaking, this term might be best limited to $a \leq \sqrt{n}$, since trial division is not done beyond $\sqrt{n}$. But as we allow $1 \leq a \leq n - 1$ in this definition, we use the term "trial division" witness that broadly.

Example 2.9. Let $n = 2^{2^{14}} + 1$. This number has 4933 digits. Although $2^{n-1} \equiv 1 \bmod n$, a computer calculation taking less than a minute shows $3^{n-1} \not\equiv 1 \bmod n$, so n is composite. Compositeness of n was first shown in 1961, but a nontrivial factor of n was found for the first time almost 50 years later, in 2010: the 54-digit number

$$116928085873074369829035993834596371340386703423373313.$$

Its complementary factor has 4880 digits and is composite (3 is a Fermat witness), but no factorization of the complementary factor into smaller parts is known.

For composite n the number 2 is often a Fermat witness. That is, often $2^{n-1} \not\equiv 1 \bmod n$, which immediately proves compositeness of n. There are only three $n < 1000$ that are composite and $2^{n-1} \equiv 1 \bmod n$: 341, 561, and 1105. Up to 10000 there are only twenty-two such composite numbers. If we look for multiple Fermat witnesses then even fewer composite numbers are "false positives" for primality: all but seven composite numbers up to 10000 have 2 or 3 as a Fermat witness (the exceptions are 1105, 1729, 2465, 2701, 2821, 6601, and 8911) and all composite numbers up to 10000 have 2, 3, 5, or 7 as a Fermat witness. Using Fermat's little congruence sure beats trial division or the gcd test to prove compositeness!

How are trial division witnesses, gcd witnesses, and Fermat witnesses of n related to each other? Since for $a > 1$

$$a^{n-1} \equiv 1 \bmod n \Longrightarrow (a, n) = 1 \Longrightarrow a \nmid n,$$

by passing to the contrapositive we have for $a > 1$ that

$$a \mid n \Longrightarrow (a, n) > 1 \Longrightarrow a^{n-1} \not\equiv 1 \bmod n,$$

so a trial division witness (that is, a proper factor greater than 1) is a gcd witness, and a gcd witness is a Fermat witness. What makes the Fermat witnesses so important is that there are usually *many* of them beyond the other two types of witnesses.

Example 2.10. We saw in Examples 2.1, 2.2, and 2.3 that for 415693 the proportion of trial division witnesses and gcd witnesses is less than 1% while the proportion of Fermat witnesses is over 99.99%.

Example 2.11. The number 1387 has 2 trial division witnesses, 91 gcd witnesses, and 1063 Fermat witnesses. The percentages of trial division witness and gcd witnesses for 1387 are both less than 1% while the percentage of Fermat witnesses for 1387 is around 77%. That is high enough that we should find a Fermat witness after just a few random guesses.

3. The Proportion of Fermat Witnesses

The next theorem gives a condition on a composite number n for the proportion of its Fermat witnesses to exceed 50%.

Theorem 3.1. *Let $n \geq 2$. If some integer b satisfies $b^{n-1} \not\equiv 1 \bmod n$ and $(b, n) = 1$ then*

$$|\{1 \leq a \leq n-1 : a^{n-1} \not\equiv 1 \bmod n\}| > \frac{n-1}{2}.$$

That is, if some Fermat witness for n is relatively prime to n then over half the positive integers less than n are Fermat witnesses for n.

Proof. Set

$$\begin{aligned} A &= \left\{1 \leq a \leq n-1 : a^{n-1} \equiv 1 \bmod n\right\}, \\ B &= \left\{1 \leq a \leq n-1 : (a,n) = 1 \text{ and } a^{n-1} \not\equiv 1 \bmod n\right\}, \\ C &= \{1 \leq a \leq n-1 : (a,n) > 1\}. \end{aligned}$$

The sets A, B, and C are disjoint (why?) and fill up all the integers from 1 to $n-1$. Together B and C are the Fermat witnesses for n and A is everything else between 1 and $n-1$.

The set A is not empty since $1 \in A$. Fermat witnesses are the elements of B and C. (Elements of C are the gcd witnesses, and every gcd witness is a Fermat witness.) By hypothesis $B \neq \emptyset$, so n is composite. The theorem asserts that if $B \neq \emptyset$ then $|B| + |C| > (n-1)/2$. To prove this we will use an idea from the proof of Fermat's little theorem: multiply every number in some set by a common number.

We are assuming there is some number in B, say b. The set $Ab = \{ab \bmod n : a \in A\}$ is inside B, where "$ab \bmod n$" means the remainder when we divide ab by n. Indeed, for any $a \in A$, the product ab is relatively prime to n and

$$(ab)^{n-1} \equiv a^{n-1}b^{n-1} \equiv b^{n-1} \not\equiv 1 \bmod n,$$

so $ab \bmod n \in B$. This holds for all $a \in A$, so $Ab \subset B$.

For a and a' in A, if $ab \equiv a'b \bmod n$ then we can cancel b and see $a \equiv a' \bmod n$, so $a = a'$ because numbers in A lie strictly between 0 and n. Thus the number of elements in Ab is $|A|$, so from $Ab \subset B$ we have $|A| = |Ab| \leq |B|$. Therefore

$$n - 1 = |A| + |B| + |C| \geq |A| + |A| + 1 > 2|A|,$$

so $|A| < (n-1)/2$, which means A is *less than half* of $\{1, 2, \ldots, n-1\}$, so its complement $B \cup C$ is *more than half* of $\{1, 2, \ldots, n-1\}$. Algebraically,

$$|B| + |C| = (n-1) - |A| > (n-1) - \frac{n-1}{2} = \frac{n-1}{2}.$$

□

Remark 3.2. A reader who knows about cosets in group theory will recognize the use of a coset Ab in the proof. Our proof can be recast in terms of group theory as follows. The invertible numbers modulo n are a group under multiplication, and the set A of solutions to Fermat's little congruence $a^{n-1} \equiv 1 \bmod n$ is a subgroup. If there is a counterexample to Fermat's little congruence among the invertible numbers, *i.e.*, if $B \neq \emptyset$, then A is a proper subgroup and therefore has index *at least* 2, so A is *at most half* the invertible numbers modulo n. Then the counterexamples to $a^{n-1} \equiv 1 \bmod n$ include *at least half* the invertible number modulo n and well as *all* the noninvertible numbers modulo n besides 0, which adds up to more than half the nonzero numbers modulo n.

Theorem 3.1 says that over half the nonzero numbers mod n are Fermat witnesses for n if some Fermat witness is relatively prime to n. The a satisfying $(a,n) > 1$ are automatically Fermat witnesses, so Theorem 3.1 says that if there is even one "non-obvious" Fermat witness (one that is not a gcd witness) then there must be many Fermat witnesses.

When the conclusion of Theorem 3.1 holds, we have a *probabilistic* test for primality: pick random positive integers less then n at random and check for each of them if Fermat's little congruence breaks down. If n is composite and over half the positive integers less than n are Fermat witnesses for n, then the probability of *not* finding a Fermat witness among, say, 10

random choices is smaller than the probability of flipping a fair coin and getting the same side 10 times in a row, and that is $1/2^{10} \approx .000976$, so we might say that n appears to be prime with "probability" at least $1 - 1/2^{10} \approx .99902$. We are putting the word probability in quotes because the primality of a number is not really a matter of probability. But there is a fundamental problem here: there are composite n for which Theorem 3.1 fails: every a with $(a, n) = 1$ has $a^{n-1} \equiv 1 \bmod n$. We address this issue in the next section.

Example 3.3. Let $n = 13079177569$. This number is composite and it turns out that $a^{n-1} \not\equiv 1 \bmod n$ only when $(a, n) > 1$, so a Fermat witness is the same as a gcd witness in this case. The number of gcd witnesses is 18483553, which seems large, but it has 8 digits while n has 11 digits. The proportion of Fermat (= gcd) witnesses for n is around .14%. (That is not a typo: we do mean .14% = .0014.) Using a random number generator to pick random numbers mod n, it took me 50 trials until I found a Fermat witness for n.

Example 3.4. If $n = 232250619601$, then n is composite and again $a^{n-1} \not\equiv 1 \bmod n$ only when $(a, n) > 1$, but in this case the proportion of Fermat witnesses is a little over 37%. With a random number generator I found a Fermat witness for n on the second try.

Example 3.5. Let $n = 11004252611041$. This number is composite (and Wolfram Alpha factors it pretty quickly), but when I ran the Fermat test on 100 random values of a mod n I did not find any Fermat witness. Try this yourself.

4. Fermat False Positives: Carmichael Numbers

It turns out that if we run the Fermat test 10 times and don't find a Fermat witness, we are not justified on probabilistic grounds in believing that n is a prime number: there are composite n for which the only Fermat witnesses are gcd witnesses. In this case Theorem 3.1 can't be applied and we can't be sure if the proportion of Fermat witnesses will be large at all.

Definition 4.1. A composite n for which there are no Fermat witnesses relatively prime to n is called a *Carmichael number*. Equivalently, n is a Carmichael number when n is composite and $(a, n) = 1 \Longrightarrow a^{n-1} \equiv 1 \bmod n$.

This name honors Robert Carmichael, who found several such numbers in the early 20th century, listing several at the end of [2] and giving more examples in [3]. Here are the first five Carmichael numbers:

$$561, \ 1105, \ 1729, \ 2465, \ 2821.$$

The numbers in Examples 3.3, 3.4, and 3.5 are Carmichael numbers too. There is no known computationally efficient algorithm to determine if a general integer is Carmichael, but Alford, Granville, and Pomerance [1] proved that there are infinitely many Carmichael numbers, so there's never a point beyond which they stop appearing.

Carmichael was not the first person to study Carmichael numbers. Twenty-five years earlier Šimerka [4] found the first 7 Carmichael numbers, but this work was published in a Czech math journal that was not widely read. It might be more appropriate to use the name Šimerka number instead of Carmichael number, but it's too late.

When we run the Fermat test t times without finding a Fermat witness, and t is large, we should be morally convinced that n is either a prime number or a Carmichael number.[3] Let's express this idea in probabilistic language. If n is composite and not a Carmichael

[3]As Tom Roby likes to say, Carmichael numbers belong to the Fermat witness protection program.

number then Theorem 3.1 assures us that over half the numbers from 1 to $n-1$ are Fermat witnesses for n, so not finding a Fermat witness after t tests is as likely as flipping a coin t times and having the same side come up each time, which has probability $1/2^t$. In fact it is *less likely* than that since the proportion of Fermat witnesses is over 50%. Therefore the "probability" that n is a prime or a Carmichael number if no Fermat witness is found after t trials is *greater than* $1 - 1/2^t$. This heuristic reasoning has an error related to conditional probability that should be fixed with Bayes' rule, but we will not discuss that here.

To summarize, the **Fermat test** for a number $n \geq 2$ is the following:

(1) Randomly pick an integer a from 1 to $n-1$.
(2) Check if $a^{n-1} \equiv 1 \bmod n$.
(3) If $a^{n-1} \not\equiv 1 \bmod n$ then stop the test and declare (correctly) "n is composite." (We know n has a nontrivial factorization, but the test does not give us one.)
(4) If $a^{n-1} \equiv 1 \bmod n$ then repeat step 1.
(5) If the test runs t times without terminating then say "n is prime or Carmichael with probability greater than $1 - 1/2^t$."

For example, if the test is run 10 times (using $t = 10$) and $a^{n-1} \equiv 1 \bmod n$ each time then we should say "n is prime or Carmichael with probability greater than $1 - 1/2^{10} \approx .99902$."

References

[1] W. R. Alford, A. Granville, C. Pomerance, *There are infinitely many Carmichael numbers*, Ann. of Math. **139** (1994), 703–722.
[2] R. D. Carmichael, *Note on a New Number Theory Function*, Bulletin Amer. Math. Soc. **16** (1910), 232–238.
[3] R. D. Carmichael, *On composite P which satisfy the Fermat congruence $a^{P-1} \equiv 1 \bmod P$*, Amer. Math. Monthly **19** (1912), 22–27.
[4] V. Šimerka *Zbytky z arithemetické posloupnosti* (*On the remainders of an arithmetic progression*), Časopis pro pěstování matematiky a fysiky **14** (1885), 221–225.