Primality Tests: Pseudoprimes and Wilson's Theorem

Ryan C. Daileda

Trinity University

Number Theory

Introduction

Fermat's Little Theorem yields an interesting *primality test*: a way to determine whether or not a given $n \in \mathbb{N}$ is prime or composite.

The "interesting" part is that it can show n is composite *without actually factoring it.*

This is the most important feature of all modern primality tests, as it averts the need for a (computationally infeasible) number of trial divisions.

Recall

Last time we proved the following Corollary to Fermat's Little Theorem.

Theorem 1

Let $p \in \mathbb{N}$ be prime. For any $a \in \mathbb{Z}$, $a^p \equiv a \pmod{p}$.

This provides us with our first *primality test*: given a modulus $n \in \mathbb{N}$ and a *base* $a \in \mathbb{Z}$

$$\boxed{a^n \not\equiv a \pmod{n} \quad \Rightarrow \quad n \text{ is composite.}}$$

For instance, if $n = 6$ and $a = 2$ we have

$$2^6 = 64 \equiv 4 \not\equiv 2 \pmod{6},$$

proving (in a very roundabout way) that 6 must be composite.

Examples

A somewhat more realistic example is provided by the 60 digit integer

$$n = 189620700613125325959116839007\backslash\backslash 395234454467716598457179234021.$$

Using the repeated squaring algorithm, it takes Maple (running on my 10-year-old MacBook Pro) 0.008 seconds to report that

$$2^n \equiv 632791764458445479937889492928\backslash\backslash 176722198136293257642423324 89 \pmod{n},$$

thereby proving that n must be composite.

It takes Maple 1000 times as long (about 8 seconds) to produce the actual prime factorization

$$\begin{aligned} n = \; & (282174488599599500573849980909)\times \\ & (671998030559713968361666935769). \end{aligned}$$

It also took only thousandths of a second for Maple to determine that the 99 digit integer

$$\begin{aligned} n = \; & 706113762068412435747683199935230\backslash\backslash \\ & 839398684490635512212296530712933\backslash\backslash \\ & 315635896349355029272628861810919 \end{aligned}$$

is composite, by showing that $2^n \not\equiv 2 \pmod{n}$.

I crashed Maple trying to actually factor n (it's the product of two 50 digit primes).

Pseudoprimes

But this primality test isn't foolproof: the converse of Fermat's Little Theorem is *false*.

For example, consider the integer $n = 341$. Since $341 = 11 \cdot 31$, n is composite.

But $2^{10} = 1024 = 3 \cdot 11 \cdot 31 + 1$ so that

$$2^{11} = 2 \cdot 2^{10} \equiv 2 \pmod{31} \quad \Rightarrow \quad 2^{341} = (2^{11})^{31} \equiv 2^{31} \equiv 2 \pmod{31},$$
$$2^{31} = 2(2^{10})^3 \equiv 2 \pmod{11} \quad \Rightarrow \quad 2^{341} = (2^{31})^{11} \equiv 2^{11} \equiv 2 \pmod{11},$$

by (the corollary to) Fermat's Little Theorem.

It follows that $2^{341} \equiv 2 \pmod{341}$, by the CRT.

Composite integers that pass the Fermat primality test for the base $a = 2$ are called *pseudoprimes*.

The smallest four pseudoprimes are $n = 341, 561, 645, 1105$. One can show there are infinitely many.

A composite integer n that passes the Fermat primality test for the base a (i.e. $a^n \equiv a \pmod{n}$) is called a *pseudoprime to the base a*.

It is known that there are infinitely many pseudoprimes to any given base. However, they are very rare: for $n \leq 10^6$ there are only 247 of them.

So if an integer passes the Fermat primality test for a given base, it is *probably* prime.

Carmichael Numbers

One might hope to recover a true primality test by requiring that $a^n \equiv a \pmod{n}$ *for all* $a \in \mathbb{Z}$.

We may as well restrict to the case that $(a, n) = 1$, since if $(a, n) > 1$ (which is easily checked via the EA), then n is composite.

However, even under these much stronger restrictions, there are still exceptions. These are known as *Carmichael numbers*.

The smallest, found in 1910 by Carmichael, is $n = 561$.

561 is a Carmichael Number

Notice that $561 = 3 \cdot 11 \cdot 17$. Therefore $(a, 561) = 1$ implies that

$$(a, 3) = (a, 11) = (a, 17) = 1.$$

Fermat's Little Theorem gives

$$a^{560} = (a^2)^{280} \equiv 1^{280} \equiv 1 \pmod 3,$$

$$a^{560} = (a^{10})^{56} \equiv 1^{56} \equiv 1 \pmod{10},$$

$$a^{560} = (a^{16})^{35} \equiv 1^{35} \equiv 1 \pmod{17}.$$

It follows from the CRT that $a^{560} \equiv 1 \pmod{561}$, and hence $a^{561} \equiv a \pmod{561}$. So 561 is a Carmichael number.

How Many Carmichael Numbers Are There?

Carmichael himself conjectured that there are infinitely many of the numbers that now bear his name.

In 1994, Alford, Granville and Pomerance succeeded in proving Carmichael's conjecture.

They showed that if $C(n)$ is the number of Carmichael numbers less than n, then

$$C(n) > n^{2/7},$$

for all sufficiently large n.

So although there are infinitely many exceptions to the "strong" Fermat primality test, they are exceedingly rare.

Torsion in Abelian Groups

We can develop a more complete (though practically less useful) primality test by analyzing a certain quantity that arose in our proof of Fermat's Little Theorem.

Let G be an abelian group and let $n \in \mathbb{N}$.

The *n-torsion subgroup* of G is

$$G(n) = \{a \in G \mid a^n = e\}.$$

One can show that $G(n)$ is closed under the group operation (and inversion) in G and is thereby a group in its own right.

We will primarily be interested in 2-torsion:

$$G(2) = \{a \in G \mid a^2 = e\} = \{a \in G \mid a = a^{-1}\}.$$

That is, $G(2)$ consists of the elements of G that are their own inverses (like -1 under multiplication).

Recall that our proof of Fermat's Little Theorem involved multiplying together all of the elements in a finite abelian group.

The value of this product is directly related to the 2-torsion in the group as follows.

Lemma 1

Let G be a finite abelian group. Then

$$\prod_{x \in G} x = \prod_{x \in G(2)} x.$$

Proof of Lemma 1

Let $a \in G$. If $a \neq a^{-1}$, then we can pair a with a^{-1} in the product $\prod_{x \in G} x$, yielding a factor of e.

The only elements that cannot be paired and cancelled are those for which $a = a^{-1}$.

These are precisely the elements of $G(2)$. The result follows. □

We will primarily be interested in applying Lemma 1 to the multiplicative group

$$(\mathbb{Z}/n\mathbb{Z})^\times = \{a + n\mathbb{Z} \,|\, (a, n) = 1\}.$$

In terms of congruences, the product of Lemma 1 amounts to

$$\prod_{\substack{1 \le a \le n \\ (a,n)=1}} a \pmod{n}.$$

We will eventually determine the value of this remainder for arbitrary n. For now we assume $n = p$ is prime.

In this case we have

$$\prod_{\substack{1 \le a \le n \\ (a,p)=1}} a = (p-1)!$$

If $G = (\mathbb{Z}/p\mathbb{Z})^\times$, then $a + p\mathbb{Z} \in G(2)$ if and only if

$$\begin{aligned}(a+p\mathbb{Z})^2 = 1 + p\mathbb{Z} &\Leftrightarrow a^2 \equiv 1 \pmod{p} \\ &\Leftrightarrow p | a^2 - 1 = (a-1)(a+1) \\ &\Leftrightarrow p | a-1 \text{ or } p | a+1 \\ &\Leftrightarrow a \equiv \pm 1 \pmod{p}.\end{aligned}$$

Then, according to Lemma 1, we have

$$(p-1)! \equiv 1 \cdot (-1) \equiv -1 \pmod{p}.$$

This is *Wilson's Theorem*.

Theorem 2 (Wilson's Theorem)

Let $p \in \mathbb{N}$ be prime. Then $(p-1)! \equiv -1 \pmod{p}$.

Conjectured by Wilson around 1770, Theorem 2 was first proven by Lagrange in 1771.

Lagrange also noted that the converse holds: if n is composite, then $(n-1)! \not\equiv -1 \pmod{n}$.

You have already proven this much easier result:

- In assignment 3, you showed that $(n-1)! \equiv 0 \pmod{n}$ if $n \geq 6$ is composite;
- And $3! = 6 \equiv 2 \pmod{4}$.

Wilson's Theorem therefore provides an infallible (although computationally intractable) primality test.

As an aside, we mention that using Wilson's Theorem, in 1964 Willans derived the formula

$$p_n = 1 + \sum_{m=1}^{2^n} \left[\sqrt[n]{n} \left(\sum_{j=1}^{m} \left[\cos^2 \pi \frac{(j-1)! + 1}{j} \right] \right)^{-1/n} \right]$$

for the nth prime number, where $[x]$ denotes the greatest integer less than or equal to x.

Even using modern computers, however, this formula cannot be used to compute more than the first few primes.

So we turn our attention to an entirely different application of Wilson's Theorem.

$\sqrt{-1} \bmod p$

Let $p \in \mathbb{N}$ be prime and consider the quadratic congruence

$$x^2 \equiv -1 \pmod{p} \iff x^2 + 1 \equiv 0 \pmod{p}.$$

Solutions to this congruence can be regarded as square roots of -1 modulo p.

Our final goal for the day is to prove the following classification of the primes for which this congruence can be solved.

Theorem 3

Let $p \in \mathbb{N}$ be an odd prime. Then the congruence $x^2 + 1 \equiv 0 \pmod{p}$ has a solution iff $p \equiv 1 \pmod{4}$.

Proof of Theorem 3

For the forward implication, suppose that $a^2 \equiv -1 \pmod{p}$.

Then $(a, p) = 1$ and Fermat's Little Theorem gives

$$1 \equiv a^{p-1} \equiv (a^2)^{\frac{p-1}{2}} \equiv (-1)^{\frac{p-1}{2}} \pmod{p}.$$

Since $1 \not\equiv -1 \pmod{p}$ (why?), this implies that $\frac{p-1}{2}$ is even. That is,

$$\frac{p-1}{2} = 2k \quad \Rightarrow \quad p - 1 = 4k \quad \Rightarrow \quad p \equiv 1 \pmod{4}.$$

For the reverse implication we first notice that

$$\begin{aligned}(p-1)! &= 1\cdot 2\cdots\left(\frac{p-1}{2}\right)\left(\frac{p+1}{2}\right)\cdots(p-2)(p-1)\\ &= 1\cdot 2\cdots\left(\frac{p-1}{2}\right)\left(p-\frac{p-1}{2}\right)\cdots(p-2)(p-1)\\ &\equiv (-1)^{\frac{p-1}{2}}\left(\left(\frac{p-1}{2}\right)!\right)^2 \pmod{p}.\end{aligned}$$

Therefore, by Wilson's Theorem,

$$\left(\left(\frac{p-1}{2}\right)!\right)^2 \equiv (-1)^{\frac{p-1}{2}+1} \equiv (-1)^{\frac{p+1}{2}} \pmod{p}.$$

If $p \equiv 1 \pmod 4$, then

$$p+1 \equiv 2 \pmod 4 \iff \frac{p+1}{2} \equiv 1 \pmod 2.$$

That is, $\frac{p+1}{2}$ is odd. Thus

$$\left(\left(\frac{p-1}{2}\right)!\right)^2 \equiv -1 \pmod{p},$$

so that $x = \left(\frac{p-1}{2}\right)!$ solves $x^2 \equiv -1 \pmod{p}$. □

Remarks.

- Note that the proof we have given is, in principle, constructive.
- This result is intimately connected with the *splitting* of p in the *number field* $\mathbb{Q}(\sqrt{-1})$.
- We will give a somewhat less ad hoc proof using *primitive roots* later.

Examples

The smallest prime that is congruent to 1 modulo 4 is $p = 5$. According to our proof

$$x = (\frac{5-1}{2})! = 2! = 2$$

solves $x^2 \equiv -1 \pmod 5$, which is easily checked.

The next $p \equiv 1 \pmod 4$ is $p = 13$. Here we need

$$x = \left(\frac{13-1}{2}\right)! = 6! = 30 \cdot 12 \cdot 2 \equiv 4 \cdot (-1) \cdot 2 \equiv 5 \pmod{13}.$$

And, indeed, $5^2 = 25 \equiv -1 \pmod{13}$.