4.4 Primality Testing

The Contrapositive of Fermat's Theorem

By Fermat's theorem, if n is prime and $n \nmid a$, then $a^{n-1} \equiv 1 \pmod{n}$. Thus if $a^{n-1} \not\equiv 1 \pmod{n}$, n cannot be prime. This idea has interesting consequences.

Pretend we do not know if 33 is prime or not. If it were prime, then since $33 \nmid 2$ we would have $2^{32} \equiv 1 \pmod{33}$. But in fact,

$$2^{32} = (2^5)^6 2^2 = 32^6 2^2 \equiv (-1)^6 2^2 = 4 \pmod{33}.$$

Thus we have proved 33 is not prime, *without exhibiting a factor between* 1 *and* 33.

This looks like a promising way to distinguish primes from composites, although, of course, it is conceivable that n could be composite and still satisfy the conclusion of Fermat's theorem. Since telling which even integers are prime is easy enough, let us look at odd values of n. We take $a = 2$ for simplicity, and compute the least residue r of $2^{n-1} \pmod{n}$.

n	3	5	7	9	11	13	15	17	19	21	23	25	27	29	31	33
r	1	1	1	4	1	1	4	1	1	4	1	16	13	1	1	4

From this limited evidence we might conjecture that the converse of Fermat's theorem is also true, at least for $a = 2$, that is, that if $2^{n-1} \equiv 1 \pmod{n}$, then n is prime. Even if this is correct, however, it would be of limited use in determining the primality of large values of n without a more efficient way to compute 2^{n-1}. The computation of $2^{32} \pmod{33}$ above was facilitated by noticing that 33 was exactly 1 more than 32, a power of 2. This trick will not work in general.

Our point of view is that n is so large that we do not know if it is prime or not. Thus we cannot use Euler's theorem to simplify the calculation of 2^{n-1}, since computing $\phi(n)$ in any efficient way requires knowing the factorization of n into primes, and that is precisely what we do not know!

We can alway go back to deciding if the odd integer n is prime by checking it for divisiblity by odd integers $\leq \sqrt{n}$, by Theorem 2.8. (Although we really only need to check possible *prime* divisors, determining whether a large possible divisor is prime or not is more work than just dividing it into n.) This entails about $\sqrt{n}/2$ divisions. Thus any scheme to tell if n is prime needs fewer steps than this to be worth considering. Computing $2^{n-1} \pmod{n}$ by starting with 2 and multiplying $n-2$ times by 2, reducing modulo n as we go, takes $n-2$ multiplications and the same number of divisions, and so is not acceptable.

Modular Exponentiation

Fortunately there is a much more efficient way of computing powers modulo n. Suppose we wish to compute $a^d \pmod{n}$. As an example, we will compute the least residue of $848^{187} \pmod{1189}$, so that $a = 848$, $d = 187$, and $n = 1189$.

ELEMENTARY NUMBER THEORY, CHARLES VANDEN EYNDEN
WAVELAND PRESS 2nd EDN.

This seems to be a formidible task, but we will show how to do it using only a hand calculator.

We start by converting the exponent d to its base 2, or binary, representation. An easy way to do this is to successively divide d by 2, keeping track of the remainders (all of which are 0 or 1). For $d = 187$ we have

$$\begin{aligned} 187 &\equiv 93 \cdot 2 + 1 \\ 93 &\equiv 46 \cdot 2 + 1 \\ 46 &\equiv 23 \cdot 2 + 0 \\ 23 &\equiv 11 \cdot 2 + 1 \\ 11 &\equiv 5 \cdot 2 + 1 \\ 5 &\equiv 2 \cdot 2 + 1 \\ 2 &\equiv 1 \cdot 2 + 0 \\ 1 &\equiv 0 \cdot 2 + 1. \end{aligned}$$

Then the remainders, listed in reverse order, give the binary representation of d. In our example

$$\begin{aligned} d &= 187 = 10111011_2 \\ &= 1 \cdot 2^7 + 0 \cdot 2^6 + 1 \cdot 2^5 + 1 \cdot 2^4 + 1 \cdot 2^3 + 0 \cdot 2^2 + 1 \cdot 2^1 + 1 \\ &= 128 + 32 + 16 + 8 + 2 + 1. \end{aligned}$$

Now in order to compute a to the power $d \pmod{n}$ we use the calculator to successively square and reduce modulo n as follows. (A method for finding least residues with a hand calculator is given at the end of Section 1.2.)

k	$a^k \pmod{n}$
1	848
2	$848^2 \equiv 719{,}104 \equiv 948 \pmod{1189}$
4	$948^2 \equiv 898{,}704 \equiv 1009 \pmod{1189}$
8	$1009^2 \equiv 1{,}018{,}081 \equiv 297 \pmod{1189}$
16	$297^2 \equiv 88{,}209 \equiv 223 \pmod{1189}$
32	$223^2 \equiv 49{,}729 \equiv 980 \pmod{1189}$
64	$980^2 \equiv 960{,}400 \equiv 877 \pmod{1189}$
128	$877^2 \equiv 769{,}129 \equiv 1035 \pmod{1189}$

Then we have

$$\begin{aligned} 848^{187} &= 848^{128+32+16+8+2+1} \\ &= 848^{128} 848^{32} 848^{16} 848^{8} 848^{2} 848^{1} \\ &\equiv 1035 \cdot 980 \cdot 223 \cdot 297 \cdot 948 \cdot 848 \pmod{1189}. \end{aligned}$$

By multiplying out the last expression factor by factor, reducing modulo 1189 as we go, we find

$$848^{187} \equiv 190 \pmod{1189}.$$

Pseudoprimes

Now we return to the question of whether

$$2^{n-1} \equiv 1 \pmod{n} \tag{4.5}$$

is not only a necessary condition for n to be prime, by Fermat's theorem, but is also sufficient. The ancient Chinese believed this to be true.

The question has already been answered—did you catch it? In an example earlier in this section illustrating the modular exponentiation algorithm, we computed

$$2^{340} \equiv 1 \pmod{341}.$$

This has the form of (4.5) with $n = 341$. But 341 is not prime: $341 = 11 \cdot 31$. Thus (4.5) can be used to identify composite numbers but not primes. Nonetheless, numbers like 341 are rare.

DEFINITION. pseudoprime, pseudoprime to base a

We call a n a **pseudoprime** if $2^{n-1} \equiv 1 \pmod{n}$, but n is composite. More generally, a composite number n such that $a^{n-1} \equiv 1 \pmod{n}$ is called a **pseudoprime to base** a.

The smallest pseudoprime is 341, and was not discovered until 1819, so the Chinese could be excused for their assumption. Of course, bases other than 2 may also be used to identify composite numbers. For example,

$$3^{340} \equiv 56 \pmod{341},$$

providing a factorless proof that 341 is not prime.

Although there are infinitely many pseudoprimes to base 2 (see the problems at the end of this section), they are much rarer than primes. Thus if a randomly chosen integer n satisfies (4.5) it is probably prime. Even rarer are pseudoprimes to multiple bases. For example, there are only 1770 integers below $25 \cdot 10^9$ that are simultaneously pseudoprimes to the bases 2, 3, 5, and 7. Thus the primality of numbers less than $25 \cdot 10^9$ could be determined by testing Fermat's congruence with these four bases, then comparing any number passing all four tests with a list of the 1770 exceptions.

We might hope that for any composite number n, there is some base a for which Fermat's theorem could be used to show that n is composite. We hope in vain; there are composite integers, called **Carmichael numbers**, which are pseudoprimes to every base. That is, n is composite, but

$$a^{n-1} \equiv 1 \pmod{n}$$

whenever $(a, n) = 1$. The smallest is $561 = 3 \cdot 11 \cdot 17$. It was only proved in 1994, by Alford, Granville, and Pomerance, that there are infinitely many Carmichael numbers. Their proof was based on a suggestion of Paul Erdős

Mersenne and Fermat Numbers

By using Fermat's theorem with multiple bases to weed out most composite numbers, and then more sophisticated tests, the primality of numbers of up to 150 digits can be determined in a few seconds with a computer. For integers of a special form, such as Mersenne and Fermat numbers, even better methods are available, enabling the primality of far larger numbers to be determined.

The **Lucas-Lehmer test**, which has been used to identify many Mersenne primes, is a century-spanning theorem, since the 1878 test of the Frenchman Edouard Lucas was simplified by the American D. H. Lehmer in 1930. We define a sequence $S_1, S_2, \ldots$ by $S_1 = 4$, and $S_n = S_{n-1}^2 - 2$ for $n > 1$. For example, $S_2 = 4^2 - 2 = 14$ and $S_3 = 14^2 - 2 = 194$. The test says that if p is an odd prime, then $M_p = 2^p - 1$ is prime if and only if $S_{p-1} \equiv 0 \pmod{M_p}$.

As an example, take $p = 7$, so $M_p = 2^7 - 1 = 127$. Then $S_1 = 4, S_2 = 14, S_3 = 194 \equiv 67, S_4 \equiv 67^2 - 2 = 4487 \equiv 42, S_5 \equiv 42^2 - 2 = 1762 \equiv 111$, and $S_6 \equiv 111^2 - 2 = 12319 \equiv 0$, with all congruence modulo 127. This proves that 127 is prime.

An analogous test for Fermat numbers is the following.

Theorem 4.14 (Pepin's test). *If $n > 0$, the Fermat number $F_n = 2^{2^n} + 1$ is prime if and only if*

$$3^{(F_n-1)/2} \equiv -1 \pmod{F_n}. \tag{4.6}$$

Proof. We will only prove the "if" part here, but a proof of the "only if" part is in the problems for Section 5.4. Assume (4.6). Then if p is any prime dividing F_n we have

$$3^{(F_n-1)/2} \equiv -1 \pmod{p}$$

by part (6) of Theorem 1.16 (so $p \neq 3$), and squaring gives

$$3^{F_n-1} \equiv 1 \pmod{p}.$$

Let k be the order of 3 modulo p. Theorem 4.6 says that k divides $F_n - 1 = 2^{2^n}$. Thus $k = 2^t$ for some integer $t \leq 2^n$. Suppose $t < 2^n$. Then we can raise both sides of the congruence $3^k \equiv 1 \pmod{p}$ to the power $2^{2^n-t-1} \geq 1$ to get

$$1 \equiv (3^k)^{2^{2^n-t-1}} = 3^{2^t(2^{2^n-t-1})} = 3^{2^{2^n-1}} = 3^{2^{2^n}/2} = 3^{(F_n-1)/2} \equiv -1 \pmod{p}.$$

But this means $p = 2$, which is impossible.

We must have $t = 2^n$ and $k = 2^{2^n} = F_n - 1$. Now by Fermat's theorem $k \leq p - 1$. Thus $p \geq k + 1 = F_n$. Since p is a divisor of F_n, we must have $p = F_n$. Thus F_n is prime. □

Example. Use Pepin's test to show that $F_3 = 257$ is prime.

By the part of Pepin's test proved above, it suffices to show that $3^{(257-1)/2} = 3^{128} \equiv -1 \pmod{257}$. But $3^2 \equiv 9$, $3^4 \equiv 81$, $3^8 \equiv 81^2 \equiv 136$, $3^{16} \equiv 136^2 \equiv 249$, $3^{32} \equiv 249^2 \equiv 64$, $3^{64} \equiv 64^2 \equiv 241$, and $3^{128} \equiv 241^2 \equiv 256 \equiv -1$, with all