Testing for Primeness

In this chapter we consider how to find large primes for use in the secret codes described in Chapter I-15.

The primitive element theorem says: If \( p \) is prime, then there is some natural number \( a < p \) whose order mod \( p \) is \( p - 1 \), that is, \( a^{p-1} \equiv 1 \) (mod \( p \)) and no smaller positive power of \( a \) is congruent mod \( p \) to 1. The converse is

**Proposition.** Suppose \( q \) is a natural number \( > 2 \). If there is some \( a < q \) such that the order of \( a \) mod \( q \) is exactly \( q - 1 \), then \( q \) is a prime number.

**Proof.** If \( q \) is not prime, then \( \phi(q) \), the number of natural numbers less than \( q \) which are relatively prime to \( q \), is less than \( q - 1 \); if \( a < q \), then either \( a \) is not relatively prime to \( q \), hence no power of \( a \) is congruent to 1 mod \( q \), or \( a \) is relatively prime to \( q \), in which case, by Euler's theorem, its order mod \( q \) must divide \( \phi(q) < q - 1 \).

Thus: \( q \) is prime iff there is an element of order exactly \( q - 1 \) mod \( q \).

How, then, do we decide whether a given number \( q \) is prime? We have a negative test, from Fermat's theorem:

\((-\) If \( a^{q-1} \not\equiv 1 \) (mod \( q \)) for some \( a < q \), then \( q \) is not prime.

We have a positive test, from the proposition:

\((+) \) If for some \( a \) the order of \( a \) (mod \( q \)) is \( q - 1 \), then \( q \) is prime.

Unfortunately, test \((+)\) is very impractical. For while it is very easy, using the strategy of Section I-11D, to decide whether \( a^{q-1} \equiv 1 \) (mod \( q \))
for any \(a\) and \(q\), it is much harder to prove that the order of \(a\) is \(q - 1\) (mod \(q\)). It has to be shown that for any prime \(p\) dividing \(q - 1\), \(a^{(q-1)/p} \equiv 1\) (mod \(q\)). And to do that, one must be able to factor \(q - 1\), a problem of almost the same size as that of factoring \(q\).

Here is a small example. Let \(q = 11213\). After checking that 11213 is not divisible by 2, 3, 5, 7, 11, and a few other small primes, we suspect that 11213 might be prime. We compute \(2^{11212} \mod 11213\) and verify that it is \(\equiv 1\) (mod 11213). To apply test (+) we must find the order of 2 mod 11213. So we have to factor 11212. Now 11212 = 2^2 \cdot 2803. Is 2803 prime? This problem is not much less difficult than the original problem. It turns out that 2803 is prime, and that neither \(2^{11212/2}\) nor \(2^{11212/2803}\) is congruent to 1 mod 11213; hence 2 is a primitive element mod 11213 and 11213 is prime.

If we took, instead of 11213, some 40-digit number \(q\), then to use (+) we would have to factor \(q - 1\), and chances are good that after factoring out all the obvious small prime factors one would be left with a factor of \(q - 1\) containing 35 or more digits and which we would have to factor—almost as hard a problem as factoring \(q\) itself.

So test (+) is not very helpful.

We might ask: Suppose we know only that \(q\) is a number for which \(2^q - 1 \equiv 1\) (mod \(q\)); how likely is it that \(q\) is prime?

The answer appears to be: excellent.

Call a number \(q\) fermatian if \(2^q - 1 \equiv 1\) (mod \(q\)).

Call a number \(q\) a pseudoprime if for all integers \(a\), \(a^q \equiv a\) (mod \(q\)).

Any prime is a pseudoprime. Any odd pseudoprime is fermatian: for if \(2^q \equiv 2\) (mod \(q\)) and \(q\) is odd, we can cancel a factor of 2 from each side.

It turns out that there are infinitely many fermatian numbers which are not primes.

**Proposition.** If \(f\) is a composite fermatian number, then so is \(2^f - 1\).

**Proof.** Suppose \(f = ab\), \(a > 1\), \(b > 1\). Let \(g = 2^f - 1\). Then \(g\) is composite, for

\[
2^{ab} - 1 = (2^a - 1)(1 + 2^a + \cdots + 2^{a(b-1)}).
\]

\((*)\)

Suppose \(2^f - 1 \equiv 1\) (mod \(f\)). We show \(2^{g-1} \equiv 1\) (mod \(g\)), that is, \(2^f - 1\) divides \(2^{g-1} - 1\). By \((*)\) it suffices to show that \(f\) divides \(g - 1\). Now since \(2^{f-1} \equiv 1\) (mod \(f\)), \(f\) divides \(2^{f-1} - 1\). Since \(g - 1 = 2^f - 1 - 1 = 2(2^{f-1} - 1)\), \(f\) divides \(g - 1\). So \(g\) is a composite fermatian number. \(\square\)

Despite this result, fermatians which are not prime are scarce, and pseudoprimes are even scarcer. There are 168 primes < 1000, but only three composite fermatians—341, 561 (the only composite pseudoprime) and 645; there are, according to D. H. Lehmer and P. Poulet, 5,761,455 primes under 100,000,000, but only 2043 composite fermatians and 252 composite pseudoprimes.