Math 75 notes, Lecture 26

P. Pollack and C. Pomerance

The $n-1$ Primality Test

To review a bit, we have the following result.

Theorem 1. *Suppose n is an integer with $n > 2$, $F \mid n-1$, $F > \sqrt{n}$,*

$$a^F \equiv 1 \pmod{n}, \quad \gcd(a^{F/q} - 1, n) = 1$$

for each prime $q \mid F$. Then n is prime.

Note that if n is prime and g is a primitive element for the finite field $\mathbb{F}_n$, then $a = g^{(n-1)/F}$ satisfies the conditions of the theorem. So, it should not be hard to come up with an element a that works, as long as we have F working for us. Now it is not hard to find a divisor F of $n-1$ that exceeds $\sqrt{n}$, for example $F = n-1$ works. But, the trick is that we also need to know the prime factors of F, and factoring integers in general is difficult for us. Thus, the $n-1$ test works for special numbers n where we happen to know a large, fully factored divisor of $n-1$. The prime candidates (pun intended) are the Fermat numbers $n = 2^{2^k} + 1$, where we can take $F = n-1$. And using some elementary number theory, one can show for such numbers n with $k \geq 1$, that we can take $a = 3$ in the theorem.

But if we are given a number where it is difficult to get a large, fully factored divisor of $n-1$, this test is not so good. Well, finite fields to the rescue.

The Finite Field Primality Test

Suppose we are given a number $n > 1$ that we think is prime, and now we wish to prove it prime. If we knew a large, fully factored, divisor F of $n-1$, we could use the $n-1$ test, but suppose the best we can do is to come up with a large, fully factored divisor of $n^k - 1$ for some small k. For example, if $k = 2$, we have $n^k - 1 = (n-1)(n+1)$, and if $n+1$ happens to be easy to factor, we'd be in business. Now $n^k - 1$ suggests we are dealing with the multiplicative group of $\mathbb{F}_{n^k}$, if only n were a prime. So, this suggests a procedure where we go ahead and try to construct this field, and do something like the $n-1$ test there.

Recall how we construct the finite field $\mathbb{F}_{p^k}$. This involves finding an irreducible polynomial $f \in \mathbb{F}_p[x]$ of degree k. Let's try to do this mod n, where we think, but are not sure, that n is prime.

Say we have a monic polynomial $f \in (\mathbb{Z}/(n))[x]$ of degree k such that

$$x^{n^k} \equiv x \pmod{f(x)}, \quad \gcd(x^{n^j} - x, f(x)) = 1 \ \text{ for } \ j = 1, 2, \ldots, \lfloor k/2 \rfloor. \tag{1}$$

We have seen that if n is prime, these conditions are easy to check, and they hold if and only if the degree-k polynomial f is irreducible.

If n is not prime, there is a word of caution about checking the conditions in (1). That is, when trying to do the gcd calculation via Euclid's algorithm, there are intermediate polynomial divisions where the divisor polynomial may not be monic. Well if c is the leading coefficient, one can make the divisor polynomial monic by multiplying by c^{-1}. This too is found via Euclid's algorithm, but in $\mathbb{Z}$; one does the extended gcd with the integers c, n. Doing so may have the unintended consequence of finding a nontrivial factor of n, and so it not only fails to find an inverse for c, but it proves that n is not prime. Well, that's fine, at that point it would be wise to give up trying to prove that n is prime!

So, say we have succeeded in finding some f which satisfies the conditions in (1). Let

$$R = (\mathbb{Z}/(n))[x]/(f(x)),$$

so that the ring R would be the finite field $\mathbb{F}_{n^k}$ if n were prime.

Theorem 2. *Suppose n, k, f satisfy (1) and that R is as above. Suppose too that $F \mid n^k-1$ and $F > \sqrt{n}$. Say $g \in (\mathbb{Z}/(n))[x]$ satisfies*

1. $g(x)^F \equiv 1 \pmod{f(x)}$,
2. $\gcd(g(x)^{F/q}-1, f(x)) = 1$ *for each prime* $q \mid F$,
3. *the polynomial* $h(t) = (t-g(x))(t-g(x)^n)\dots(t-g(x)^{n^{k-1}})$, *viewed as a polynomial in* $R[t]$, *is actually in* $(\mathbb{Z}/(n))[t]$.

Then each prime factor p of n satisfies $p \equiv n^j \pmod{F}$ for some $j = 0, 1, \dots, k-1$. So, if none of the residues $n^j \pmod{F}$ for $j = 0, 1, \dots, k-1$ are proper factors of n, then n is prime.

Note that if we view g as an element of R, then item 1. is saying that $g^F = 1$, while item 2. is saying that $g^{F/q}-1$ is a unit in R for each prime $q \mid F$.

Proof. Let p be a prime factor of n, and for objects reduced modulo n, such as $f(x)$, $g(x)$, we put bars over the top to indicate we take a further reduction modulo p. So, $\bar{f}$ is a polynomial in $\mathbb{F}_p[x]$ that is monic of degree k. It may not be irreducible, so let f_1 be an irreducible factor, and let K be the finite field $\mathbb{F}_p[x]/(f_1)$. Item 1. in the theorem imlies that $\bar{g}^F \equiv 1 \pmod{f_1}$, while item 2. implies that $\bar{g}^{F/q}-1$ is coprime to f_1 for each prime $q \mid F$. Thus, $\bar{g}$ corresponds to an element of $K^\times$ of order F. Now item 3. says that the polynomial $h(t)$, when reduced mod $f(x)$ is in $(\mathbb{Z}/(n))[t]$. So, if it is further reduced mod p it is in $(\mathbb{Z}/(p))[t]$, that is, $\mathbb{F}_p[t]$. That is,

$$\bar{h}(t) = (t-\bar{g})(t-\bar{g}^n)\dots(t-\bar{g}^{n^{k-1}}) \in \mathbb{F}_p[t].$$

But any polynomial over $\mathbb{F}_p$ has the property that if α is a root, so is α^p. Now, we know the roots of $\bar{h}$, they are quite visible: they are $\bar{g}, \bar{g}^n, \dots, \bar{g}^{n^{k-1}}$. Thus, $\bar{g}^p = \bar{g}^{n^j}$, for some $j = 0, 1, \dots, k-1$. We have already decided that the multiplicative order of $\bar{g}$ is F, so we must have $p \equiv n^j \pmod{F}$, for some $j = 0, 1, \dots, k-1$. This is the first assertion of the theorem. For the second assertion, note that if n is composite, then its least prime factor p must satsify $p \le \sqrt{n} < F$, so if $p \equiv n^j \pmod{F}$, then p is in fact equal to the reduction of n^j modulo F. $\square$

The Lucas–Lehmer test for Mersenne primes

Over two millennia ago, Euclid showed that if one has a prime n of the form 2^p-1, then $n(n+1)/2$ is *perfect*. (A perfect number is one that it is equal to the sum of its proper divisors.) For example, $n = 3 = 2^2-1$ is prime, so $n(n+1)/2 = 6$ is perfect; indeed the proper divisors of 6 are 1, 2, and 3, and their sum is 6. Try it out for $n = 2^3-1 = 7$; it works. So, interest was there from the start of mathematics in primes of the form 2^p-1. It is not hard to show, and presumably Euclid knew this, that a necessary condition that 2^p-1 be prime is that the exponent p is itself prime. Indeed, if the exponent $p = ab$, then $2^a-1 \mid 2^p-1$, so 2^p-1 is not prime. However, presumably Euclid also knew that this condition is not sufficient, since he did not give the case $p = 11$ as giving a perfect number. Indeed, $2^{11}-1 = 23 \cdot 89$.

In the 17th century, a French monk named Mersenne came up with a conjecture about which exponents p give primes for 2^p-1 for p up to about 250. Over the years, it was found that Mersenne was mostly wrong, but he was correct in predicting so few of them. His name is now attached to primes of this form. It is interesting that a century later, Euler proved that every even perfect number is in the form given by Euclid. It is still not known if there are any odd perfect numbers; this and the question of whether there are infinitely many Mersenne primes may be thought of as perhaps the oldest unsolved problems in mathematics.

For us, we are interested in how hard it is to detect whether a number $n = 2^p-1$ is prime. This seems perfectly set up for the Finite Field Primality Test since we can take $k = 2$ and $F = 2^p = n+1 \mid n^2-1$. In fact, there is even a prescription on what to take for $f(x)$ and $g(x)$.

Theorem 3. *Suppose p is an odd prime and $n = 2^p-1$. Then n is prime if and only if*

$$x^{(n+1)/2} \equiv -1 \pmod{x^2 - 4x + 1} \tag{2}$$

in $(\mathbb{Z}/(n))[x]$.

Proof. We first show that if (2) holds, then n is prime. Let $f(x) = x^2 - 4x + 1$. We first prove that (2) implies (1). Note that

$$x^2 - 4x = f(x) - 1 \equiv -1 \pmod{f(x)}, \quad \text{so} \quad x(4-x) \equiv 1 \pmod{f(x)}.$$

Thus,

$$x^n \equiv x^n x(4-x) \equiv x^{n+1}(4-x) \equiv 4 - x \pmod{f(x)},$$

using the square of the congruence (2) for the last step. Thus,

$$x^n - x \equiv 4 - 2x \pmod{f(x)}.$$

To see that $4-2x$ is coprime to $f(x)$, it is sufficient to show that $2-x$ is coprime to $f(x)$, since n is odd and so 2 is a unit. But $(2-x)^2 = 4 - 4x + x^2 \equiv 3 \pmod{f(x)}$, and 3 is a unit as well (since $3 \mid 2^j-1$ if and only if j is even). Thus, we have

$$\gcd(x^n - x, f(x)) = 1.$$

We also must show that $x^{n^2} \equiv x \pmod{f(x)}$. But (2) taken to the power $2(n-1)$ gives $x^{n^2-1} \equiv 1 \pmod{f(x)}$, so it follows that $x^{n^2} \equiv x \pmod{f(x)}$. Thus, if $n = 2^p - 1$ with p an odd prime and $f(x) = x^2 - 4x + 1$, we have that (1) holds.

We now show that if (2) holds, then n is prime. First note that with $F = n + 1$ and $g(x) = x$, we have item 1. of Theorem 2. Further, the only prime q that divides F is $q = 2$, so that $g(x)^{F/q} = x^{(n+1)/2}$, so that $g^{F/q} - 1 \equiv -2 \pmod{f(x)}$, using (2). But, since 2 is a unit mod n, it follows that item 2. holds as well. It remains to check that item 3. holds. But,

$$(t - x)(t - x^n) = t^2 - (x + x^n)t + x^{n+1},$$

and we have already seen above that $x^n \equiv 4 - x \pmod{f(x)}$ and $x^{n+1} \equiv 1 \pmod{f(x)}$. Thus, $h(t)$ collapses to $t^2 - 4t + 1$. Quite suspicious, no? Do you know why this happened?

Thus, by Theorem 2, if (2) holds, then n is prime.

We now show the converse. That is, we show that if $n = 2^p - 1$ is prime, where p is an odd prime, then (2) holds. For this we will use the following two facts from elementary number theory, namely that if n is a prime that is $\pm 1 \pmod 8$, then 2 is a square mod n, and if n is a prime that is $\pm 5 \pmod{12}$, then 3 is not a square mod n. But, if $n = 2^p - 1$ for p an odd prime, then $n \equiv -1 \pmod 8$ and $n \equiv 7 \pmod{12}$. Thus, 2 is a square mod n and 3 is a nonsquare, so $2^{(n-1)/2} \equiv 1 \pmod n$, and $f(x) = (x - 2)^2 - 3$, so that $f(x)$ is irreducible in $\mathbb{F}_n[x]$.

In particular, we can use $f(x)$ to construct the finite field with n^2 elements: $\mathbb{F}_{n^2} = \mathbb{F}_n[x]/(f(x))$. We compute $(x - 1)^{n+1}$ two ways in this field. First, we have

$$(x - 1)^2 = x^2 - 2x + 1 = 2x$$

in $\mathbb{F}_{n^2}$, so

$$(x - 1)^{n+1} = (2x)^{(n+1)/2} = 2^{(n+1)/2}x^{(n+1)/2} = 2 \cdot 2^{(n-1)/2}x^{(n+1)/2} = 2x^{(n+1)/2},$$

using what we learned above about 2 being a square. For the other way of computing this power, we have

$$(x - 1)^{n+1} = (x - 1)^n(x - 1) = (x^n - 1)(x - 1).$$

But $x^n = 4 - x$ (do you know why?), so this last expression is $(3 - x)(x - 1) = -x^2 + 2x - 3 = -2$. Thus, equating the two calculations, we have

$$2x^{(n+1)/2} = -2,$$

which immediately shows that (2) holds. □

The Lucas–Lehmer test is often described sort of antiseptically as follows: For an odd prime p, the number $n = 2^p - 1$ is prime if and only if $v_{p-1} = 0$, where the sequence $v_1, v_2, \ldots$ is recursively defined by $v_1 = 4$ and $v_{j+1} = v_j^2 - 2 \pmod n$. This is easy to program of course, but it completely hides what is going on. It is not hard to show that this version of the test follows from the above ideas.

For further reading see *Prime numbers: a computational perspective* by R. Crandall and C. Pomerance. One can also find material there on the polynomial time deterministic primality test that was discovered in India in 2002. This test too uses finite fields.