PRIMALITY TESTING

1 Quadratic Residues

In solving congruence equations of higher degree the following result of Lagrange is basic

Theorem 1.1 *For a prime p the equation*

$$P(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n = 0 \pmod{p} \tag{1.1}$$

has at most n solutions.

Proof. The result is clear if $n = 1$. Thus we shall proceed by induction and assume that our assertion is true for polynomial equations of degree $n - 1$ or less. This given, note that for any b whatever we can write

$$P(x) - P(b) = a_1\,(x - b) + a_2\,(x^2 - b^2) + a_3\,(x^3 - b^3) + \cdots + a_n\,(x^n - b^n)$$

Factoring out $x - b$ we get

$$P(x) - P(b) = (x - b)\,Q(x) \tag{1.2}$$

where

$$Q(x) = a_1 + a_2\,(x + b) + a_3\,(x^2 + x\,b + b^2) + \cdots + a_n\,(x^{n-1} + x^{n-2}\,b + \cdots + b^{n-1})$$

Assume then that a and b are both solutions of (1.1). Setting $x = a$ in (1.2) gives

$$(a - b)\,Q(a) = P(a) - P(b) = 0 - 0 = 0 \pmod{p} \tag{1.3}$$

Now if a is not equal to $b \pmod{p}$, that is $a-b$ is not divisible by p, then (1.3) implies that $Q(a) = 0$ (mod p). In other words, except for at most one solution (say b) of the equation $P(x) = 0$, all the others are solutions of $Q(x) = 0$. However, $Q(x)$ is a polynomial of degree $n - 1$ at most and by the induction hypothesis the equation $Q(x) = 0$ can have no more that $n-1$ solutions. Thus (1.1) itself can have no more the n distinct solutions altogether. This completes the induction argument and the proof of the theorem.

Remark. It is customary to call the solutions of a polynomial equation $P(x) = 0$ the roots of the polynomial $P(x)$. Thus Lagrange's theorem may be rephrased by saying that any polynomial of degree n has no more than n roots mod p.

Note that these congruence equations may have no solution at all. For instance we can find no x such that

$$x^2 = 2 \pmod{5}$$

nor can we solve

$$x^2 = 8 \pmod{11} \tag{1.4}$$

This can be easily checked for (mod 5) we have

$$1^2 = 1,\ 2^2 = 4,\ 3^2 = 4,\ 4^2 = 1$$

a similar reasoning gives that (1.4) has no solution. Taking this into account we shall say that an integer a is a *quadratic residue* mod p if and only if the equation

$$x^2 - a = 0 \pmod p$$

has a solution x.

It will be convenient to denote the set of quadratic residues mod p by the symbol $QR[p]$. For instance we can easily check that we have

$$\begin{aligned} QR[7] &= \{1, 4, 2\} \\ QR[11] &= \{1, 4, 9, 5, 3\} \end{aligned}$$

We should note from these two examples that the number of quadratic residues is given by $(7-1)/2$ and $(11-1)/2$ respectively. This is in fact true in general.

Theorem 1.2 *Precisely 1/2 of the integers in* $\{1, 2, \ldots, p-1\}$ *are quadratic residues mod* p.

Proof.

Clearly all the quadratic residues in $\{1, 2, \ldots, p-1\}$ are obtained by reducing mod p the $p-1$ integers

$$1^2, 2^2, 3^2, \ldots, (p-1)^2 \tag{1.5}$$

However, since

$$(p-i)^2 = p^2 - 2\,p\,i + i^2 = i^2 \pmod p$$

we see that these numbers are equal in pairs. Indeed all the quadratic residues are obtained by taking only the first $(p-1)/2$ numbers in (1.5), namely

$$1^2, 2^2, 3^2, \ldots, ((p-1)/2)^2$$

Now it develops that these numbers are all distinct mod p since

$$i^2 - j^2 = (i-j)\,(i+j)$$

gives that we cannot have $i^2 = j^2$ mod p without p dividing one of the two numbers $i-j$ or $i+j$. However, if both i and j are no larger than $(p-1)/2$, p cannot divide $i+j$. Thus $i^2 = j^2$ forces $i = j$ in this case. Thus we see that we do have exactly $(p-1)/2$ quadratic residues as asserted.

There is a very useful and basic criterion to decide when a given integer is a quadratic residue. It can be stated as follows

Theorem 1.3 *For any prime* $p > 2$ *and any integer* a *not equal to 0* $\pmod p$ *we have*

$$a^{(p-1)/2} = \begin{cases} 1 & \text{if } a \in QR[p] \\ \\ -1 & \text{if } a \notin QR[p] \end{cases} \tag{1.6}$$

Proof.

Note that if $a = x^2$ with x not 0 mod p then Fermat's theorem gives

$$a^{(p-1)/2} = x^{p-1} = 1 \pmod{p}$$

Thus the first part of our assertion holds true. To prove the second part, note that the equation

$$x^{p-1} - 1 = 0 \pmod{p} \tag{1.7}$$

has (again by Fermat's theorem) exactly $p-1$ solutions in $\{1, 2, \ldots, p-1\}$. Note then that for $p > 2$ we have the factorization

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

now the first factor (by Lagrange's Theorem) can have no more than $(p-1)/2$ roots in $\{1, 2, \ldots, p-1\}$, but we have seen that all the $(p-1)/2$ quadratic residues are roots of the first factor. We must thus conclude that the remaining $(p-1)/2$ solutions of (1.7) must be roots of the second factor. In other words all the quadratic non-residues must satisfy the equation

$$x^{(p-1)/2} = -1 \pmod{p}$$

This completes our proof

2 The Legendre and Jacobi symbols

It is customary to set, for a given prime p and $a \neq 0$ mod p

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } a \in QR[p] \\ -1 & \text{if } a \notin QR[p] \end{cases} \tag{2.1}$$

(a/p) is referred to as the "Legendre symbol". It's definition can be extended to all a by setting

$$\left(\frac{a}{p}\right) = 0 \qquad \text{when} \qquad a = 0 \pmod{p}$$

Theorem 1.3 can then be restated by saying that for integers a and primes p we have

$$\left(\frac{a}{p}\right) = a^{(p-1)/2} \tag{2.2}$$

A remarkable consequence of this formula is that we must necessarily have that

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \tag{2.3}$$

This means in particular that the product of two quadratic non-residues is a quadratic residue, and that is not entirely obvious.

One of the most famous results of elementary number theory is the Quadratic Reciprocity Law discovered by Legendre and proved by young Gauss. It can be stated as follows

Theorem 2.1 *For any two primes p and q we have*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{(p-1)(q-1)/4}$$

The symbol (a/p) has been extended by Jacobi to a symbol $J(a,n)$ defined for values of n not necessarily prime. The definition of $J(a,n)$ for $n = p_1 p_2 \cdots p_k$ with $p_1, p_2, \ldots, p_k$ primes (not necessarily distinct) is

$$J(a,n) = \left(\frac{a}{p_1}\right)\left(\frac{a}{p_2}\right)\cdots\left(\frac{a}{p_k}\right)$$

This is simple enough. However it is not very useful in cases when the factorization of n into primes is not available. Fortunately, a combination of the Law of Quadratic Reciprocity together with other simple properties of the Legendre symbol yield us a beautiful recursive algorithm for evaluating $J(a,n)$ quite readily and without factorization. This result can be stated as follows

Theorem 2.2 *For any positive integers a and n (n odd) we have*

$$J(a,n) = \begin{cases} 1 & \text{if } a = 1 \\ J(a/2,n)(-1)^{(n^2-1)/8} & \text{if } a \text{ is even} \\ J(n \pmod a, a)(-1)^{(n-1)(a-1)/4} & \text{if } a > 1 \text{ and odd} \end{cases} \tag{2.4}$$

This result brings us to the heart of the matter for our applications to cryptography. We recall that the RSA encryption system requires the selection of very large random primes. This needs selecting a number at random, and then testing for its primality. For integers of large size the factorization problem can be quite laborious. It develops that the Jacobi symbol allows us to test for primality of n without carrying out its factorization. This is a remarkable idea due to Strassen and Solovay and it can be formulated as follows.

We note first that if n is prime then $J(a,n) = (a/n)$ and thus we must necessarily have

$$J(a,n) = a^{(n-1)/2} \pmod n$$

Thus if this identity fails to hold for any value of a in $[1, n-1]$ we can certainly conclude that n is not a prime! Since $J(a,n)$ can be computed quite fast using the recursion in (2.4), we can see that we may conclude that n is not a prime without much effort. However, we may ask what is the likelihood of running into such a helpful value of a in $[1, n-1]$. Now it develops that the following remarkable fact holds true:

Theorem 2.3 *If n is not a prime then for more than one half the integers in $\{1, \ldots, n-1\}$ one of the following two tests will fail*

$$\begin{cases} J(a,n) = a^{(n-1)/2} \\ (a,n) = 1 \end{cases} \tag{2.5}$$

This result yields us a method of selecting a prime at random in a given range as follows. We first pick an (odd) integer n at random in the given range. The Prime Number Theorem (not stated here) implies that the frequency of primes among numbers near m is $1/\log(m)$, so that we stand a “good” chance of picking a prime. This done we pick at random a certain (previously agreed upon) number k of integers $a_1, a_2, \ldots, a_k$ in the interval $\{1, \ldots, n-1\}$. We then carry out for each of them the test in (2.5). If n happened to be prime then it will pass all of these tests. On the other hand, if n is not a prime (by theorem 6) it will pass all of these tests with probability less than $(1/2)^k$. Now this number can be made as small as desired by choosing k large. For instance for $k = 50$ we can quite confidently conclude that an n which passes all 50 tests is a prime. In doing so the probability that we draw the wrong conclusion is less than 1 in 2^{50}, and these are odds considerably smaller than those we stake our lives upon daily!

Exercises:

1. Give the complete list of quadratic residues modulo 37.
2. Find all solutions of the quadratic equation

   $$x^2 + 12x + 40 = 0 \mod 37$$

   Hint: Complete the square.
3. Calculate the Legendre symbol $\left(\frac{11}{31}\right)$.
4. Does the equation $x^2 \equiv 11$ have a solution modulo 31? Explain.
5. Find the value of the Jacobi symbol $J(5, 21)$.
6. Compute the Jacobi symbol $J(17, 866731)$.
7. Compute the following values:

   (a) $\gcd(24, 601)$

   (b) $J(24, 601)$

   (c) $24^{300} \mod 601$

   What does this tell you about the primality of 601?