MATH 467, Legendre, Jacobi symbol (LJ), Quadratic Congruences (QC)

Algorithm LJ. Given an integer m and a positive integer n, compute $\left(\frac{m}{n}\right)_J$.

1. Reduction loops.
   1.1. Compute $m \equiv m \pmod{n}$, so that the new m satisfies $0 \le m < n$. Put $t = 1$.
   1.2. While $m \ne 0$ {
   1.2.1. While m is even {put $m = m/2$ and, if $n \equiv 3$ or $5 \pmod{8}$, then put $t = -t$.}
   1.2.2. Interchange m and n.
   1.2.3. If $m \equiv n \equiv 3 \pmod{4}$, then put $t = -t$.
   1.2.4. Compute $m \equiv m \pmod{n}$, so that the new m satisfies $0 \le m < n$.
   }
2. Output.
   2.1. If $n = 1$, then return t.
   2.2. Else return 0.

The following are often attributed to Shanks (1973) & Tonelli (1891), but in principle go back to Euler, Legendre & Gauss.

Algorithm QC357/8. Given a prime $p \equiv 3, 5, 7 \pmod{8}$ and an a with $\left(\frac{a}{p}\right)_L = 1$, compute a solution to $x^2 \equiv a \pmod{p}$.

1. If $p \equiv 3$ or $7 \pmod{8}$, then compute $x \equiv a^{(p+1)/4} \pmod{p}$. Return x.

2. If $p \equiv 5 \pmod{8}$, then compute $x \equiv a^{(p+3)/8} \pmod{p}$. Compute $x^2 \pmod{p}$.
   2.1. If $x^2 \equiv a \pmod{p}$, then return x.
   2.2. If $x^2 \not\equiv a \pmod{p}$, then compute $x \equiv x2^{(p-1)/4} \pmod{p}$. Return x.

Algorithm QC1/8. Given a prime $p \equiv 1 \pmod{8}$ and an a with $\left(\frac{a}{p}\right)_L = 1$, compute a solution to $x^2 \equiv a \pmod{p}$. This algorithm will work for any odd prime, but the previous algorithm is faster for $p \not\equiv 1 \pmod{8}$.

1. Compute a random integer b with $\left(\frac{b}{p}\right)_L = -1$. In practice checking successively the primes $b = 2, 3, 5, \ldots$, or even crudely just the integers $b = 2, 3, 4, \ldots$, will find such a b quickly.

2. Factor out the powers of 2 in $p-1$, so that $p - 1 = 2^s u$ with u odd. Compute $d \equiv a^u \pmod{p}$. Compute $f \equiv b^u \pmod{p}$.

3. Compute an m so that $df^m \equiv 1 \pmod{p}$ as follows.
   3.1. Initialise $m = 0$.
   3.2. For each $i = 0, 1, \ldots, s-1$ compute $g \equiv (df^m)^{2^{s-1-i}} \pmod{p}$. If $g \equiv -1 \pmod{p}$, then put $m = m + 2^i$.
   3.3. Return m. This will satisfy $df^m \equiv 1 \pmod{p}$, and m will be even. (The mathematical proof of this is non–trivial.)

4. Compute $x \equiv a^{(u+1)/2} f^{m/2} \pmod{p}$. Return x.