Square root mod p. Given a prime $p > 2$ and an integer a, here is a method — ascribed to Daniel Shanks — for solving the congruence $x^2 \equiv a \pmod{p}$.

Let S denote the maximal 2-subgroup of the group C of prime residue classes modulo p. Then $S = C^N$, where $p - 1 = 2^s N$ with N odd. After checking that $a \in C^2$, put $r = a^{(N+1)/2}$ and $b = a^N$ in C. Note that

$$r^2 = ab \qquad \text{with} \qquad b \in S.$$

It now suffices to shave off the square root of b. To this avail, we pick a non-square and take its N-th power to obtain a generator c of S. Then we loop through the following computation, as long as $b \neq 1$.

1. By succesive squaring, determine the largest k such that $b \in S^{2^k}$ (N.B. $b \in S^2 \Rightarrow k > 0$.)
2. Replace r by $rc^{2^{k-1}}$ and b by bc^{2^k}. (N.B. The new b is in $S^{2^{k+1}}$). Loop if $k + 1 < s$.