Cantor-Zassenhaus algorithm

Let p be a prime number. The Cantor-Zassenhanhaus algorithm is an algorithm for factoring polynomials with integer coefficients over $\mathbf{Z}_p$, under the assumption that all its zeroes are in $\mathbf{Z}_p$. It is based on the following principles:

1. $\mathbf{Z}_p$ coincides with the zeros of the polynomial $\chi = x^p - x$ over $\mathbf{Z}_p$. More precisely, if we write

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

   we see that the zeros of the three factors are $x = 0$, the squares in $\mathbf{Z}_p^*$ and the non-squares in $\mathbf{Z}_p^*$, respectively.
2. Let f be a polynomial with integer coefficients. Denote by the same symbol f also its projection to $\mathbf{Z}_p[X]$ (i.e. taking the coefficients modulo p). Then $\alpha \in \mathbf{Z}_p$ is a zero of f over $\mathbf{Z}_p$ if and only if $(x - \alpha)$ divides $\gcd(f, x^p - x)$.

Note that for $p \gg 0$, the polynomial $x^p - x$ has a very high degree. To reduce the computation to polynomials of lower degree, we use the following tricks:

3. We compute either $\gcd(f, x^{(p-1)/2} - 1)$ or $\gcd(f, x^{(p-1)/2} + 1)$, namely we search for the zeros of f which are squares and the ones which are non-squares. To compute $\gcd(f, x^{(p-1)/2} - 1)$, we exploit the fact that if

$$x^{(p-1)/2} - 1 = q(x)f(x) + r(x), \qquad \text{with } \deg(r) < \deg(f), \tag{$*$}$$

   then

$$\gcd(f(x), x^{(p-1)/2} - 1) = \gcd(f(x), r(x)). \tag{$**$}$$

   Note that $r(x)$ is nothing but $x^{(p-1)/2} - 1 \bmod f$. Relation (*) can be obtained by division with remainder between polynomials with coefficients in a field. To compute $r(x)$ efficiently , we compute the power $x^{(p-1)/2}$ in the ring $\mathbf{Z}_p[x]/(f(x))$ and then subtract 1. This can be done in time $O(d^2 \log^3 p)$, where $d = \deg f$,
   In this way (**) is reduced to a gcd between two polynomials of degree $\leq \deg(f)$. What we get is

$$s(x) := \gcd(f, r(x)) = \prod_{\alpha_i} (x - \alpha_i),$$

where α_i runs over the zeros of f in $\mathbf{Z}_p$, which are squares in $\mathbf{Z}_p$.

(Analogous statements hold for $x^{(p-1)/2} + 1$).

Obtaining a zero of f is equivalent to produce a degree one factor of $\gcd(f, x^{(p-1)/2} - 1)$
(or of $\gcd(f, x^{(p-1)/2} + 1)$).

4. Letting $t = 1, 2, 3 \ldots$, we compute

$$\gcd(r(x+1), s(x)),\ \gcd(r(x+2), s(x)), \ldots$$

   until we get a non-trivial polynomial, i.e. different from constant and $s(x)$ (it is likely that only a few gcd's are sufficient...)
   Assume $t(x) = \gcd(r(x + t_0), s(x))$ non-trivial, for some t_0. Then

$$t(x) = \prod_{\alpha_i} (x - \alpha_i),$$

where α_i runs over the zeros of f in $\mathbf{Z}_p$, with the property that both α_i and $\alpha_i + t_0$ are a squares in $\mathbf{Z}_p$.

The degrees of $t(x)$ and of $s(x)/t(x)$ are stricltly smaller than the degree of $s(x)$. Now the procedure can be iterated until we get to degree 1.