Cantor-Zassenhaus split

Canonical name	CantorZassenhausSplit
Date of creation	2013-03-22 14:54:24
Last modified on	2013-03-22 14:54:24
Owner	mathwizard (128)
Last modified by	mathwizard (128)
Numerical id	8
Author	mathwizard (128)
Entry type	Algorithm
Classification	msc 13M10
Classification	msc 13P05
Classification	msc 11C99
Classification	msc 11Y99
Related topic	SquarefreeFactorization
Defines	distinct degree factorization

Assume we want to factor a polynomial $A \in \mathbb{F}_p[X]$, where p is a prime and $\mathbb{F}_p$ is the field with p elements. By using squarefree factorization we can assume that A is squarefree. The algorithm presented here now first splits A into polynomials A_i, where each irreducible factor of A_i has degree i. The main part will then be to factor these polynomials. The Cantor-Zassenhaus split is an efficient algorithm to achieve that. It uses random numbers, nevertheless it always returns a correct factorization.

1 The distinct degree factorization

To completely factor A we will first find polynomials A_d with $A = \prod A_d$, such that all irreducible factors of A_d have degree d. This is called the *distinct degree factorization*. Recall that if $P \in \mathbb{F}_p$ is an irreducible polynomial of degree d, then $K := \mathbb{F}_p[X]/P(X)\mathbb{F}_p[X]$ is a finite field with p^d elements. So every $x \in K^* = K\backslash\{0\}$ satisfies $x^{p^d-1} = 1$, so every $x \in K$ satisfies $x^{p^d} = x$, so P is a divisor of the polynomial $X^{p^d} - X \in \mathbb{F}_p[X]$ and every irreducible factor of $X^{p^d} - X$, which does not divide $X^{p^e} - X$ for some $e < d$. So we can easily find these A_d by introducing the series B_i with $B_1 = A$ and

$$B_{k+1} = \frac{A}{\gcd\left(B_k, X^{p^k} - X\right)}.$$

Then $A_d = \gcd(B_d, X^{p^d} - X)$.

2 The final splitting

We can now assume that we want to factor a polynomial A that has only irreducible factors of the known degree d.

2.1 Splitting for odd p

First assume that p is odd. Then we have the following

Lemma 1 *If A is as above, then for any $T \in \mathbb{F}_p[X]$ we have*

$$A = \gcd(A, T)\gcd(A, T^{\frac{p^d-1}{2}} - 1)\gcd(A, T^{\frac{p^d-1}{2}} + 1).$$

This is true because the roots of $X^{p^d} - X$ are exactly the elements of $\mathbb{F}_{p^d}$ and are all distinct in that field. So for any polynomial $T \in \mathbb{F}_p[X]$, the polynomial $T^{p^d} - T$ has also all elements of $\mathbb{F}_{p^d}$ as roots, so $X^{p^d} - X | T^{p^d} - T$. So as we have seen it is divisible by all irreducible polynomials of degree d, so it is divisible by A since A is squarefree. By noting that

$$T^{p^d} - T = T\left(T^{\frac{p^d-1}{2}} - 1\right)\left(T^{\frac{p^d-1}{2}} + 1\right)$$

is a decomposition with pairwise coprime factors, the claimed identity follows.

Now one can simply choose a random polynomial T of degree less than $2d$. Then it is likely that $B := \gcd(A, T^{\frac{p^d-1}{2}} - 1)$ is a non-trivial divisor of A. We can then start over with B and A/B instead of A.

In this algorithm quite large powers of T need to be computed. It is of course sufficient (and useful) to compute these powers modulo A, in order to keep the degree of the appearing polynomials low.

To illustrate this idea, we choose $d = 1$. This means that A is made up of different linear factors. Factorization is the achieved by finding zeroes. For this we could split $\mathbb{F}_p$ into three disjoint sets M, N and $\{0\}$, such that $M \cup N \cup \{0\} = \mathbb{F}_p$.Then we construct the polynomial

$$S = \prod_{\alpha \in M} (X - \alpha).$$

Obvioulsy it is now sufficient to factor the polynomials $B := \gcd(A, S)$ and $\frac{A}{B}$. If M and N were chosen wisely, these polynomials have lower degree than A. Now what is left is the choice of M and N. For the start it might be a good idea to consider the set of quadratic residues in $\mathbb{F}_p$, so choosing

$$M = \left\{ x \in \mathbb{F}_p : \left(\frac{x}{p}\right) = 1 \right\},$$

where $\left(\frac{x}{p}\right)$ denotes the Legendre symbol. This choice is almost what we want. It is known that M and N are now of equal size and also we know that

$$S = X^{\frac{p-1}{2}} - 1.$$

But if we want to apply the same method again to B and $\frac{A}{B}$, we need some randomness. To achieve this, we simply do not consider the set of all quadratic residues, but the set

$$M = \left\{ x \in \mathbb{F}_p : \left(\frac{x-t}{p} \right) = 1 \right\},$$

where $t \in \mathbb{F}_p$ is some random element. This gives us the polynomial

$$S = (X-t)^{\frac{p-1}{2}} - 1.$$

Actually we have now chosen a random monic polynomial T of degree $1 = 2d-1$ and are reducing the problem of factoring A to the problem of factoring $B := \gcd(A, T^{\frac{p-1}{2}} - 1)$ and $\frac{A}{B}$, as it was described above.

2.2 Splitting for $p = 2$

Let $p = 2$. Lemma **??** does not work here because in the proof we use that

$$T^{p^d-1} - 1 = \left(T^{\frac{p^d-1}{2}} - 1 \right) \left(T^{\frac{p^d-1}{2}} + 1 \right),$$

which requires p to be odd. However we can find something similar:

Lemma 2 *Let*

$$U(X) = X + X^2 + X^4 + \cdots + X^{2^{d-1}}$$

and A as above. Then for any $T \in \mathbb{F}_2[X]$ we have

$$A = \gcd(A, U \circ T) \cdot \gcd(A, U \circ T + 1).$$

This is because $(U \circ T)^2 = T^2 + T^4 + \cdots + T^{2^d}$, so

$$(U \circ T)(U \circ T + 1) = T^{2^d} - T$$

(we are in characteristic 2). Now this is a multiple of A and the identity follows.

This gives us an algorithm for factorization of A in the same way as above.