squarefree factorization

Canonical name	SquarefreeFactorization
Date of creation	2013-03-22 14:54:20
Last modified on	2013-03-22 14:54:20
Owner	mathwizard (128)
Last modified by	mathwizard (128)
Numerical id	5
Author	mathwizard (128)
Entry type	Algorithm
Classification	msc 11Y99
Classification	msc 11C99
Classification	msc 13P05
Classification	msc 13M10
Related topic	CantorZassenhausSplit

Given a polynomial $A \in \mathbb{F}_p[X]$, where p is a prime and $\mathbb{F}_p$ is the field with p elements, we want to find a decomposition

$$A = \prod_{i=1}^{n} A_i^i$$

with squarefree polynomials A_i, which are pairwise coprime. Since we are in a field, we can assume that A is monic. Since A has a unique factorization we can take A_i to be the product of all irreducible divisors P of A with $v_P(A) = i$, where $v_P(A)$ is the number such that $P^{v_P(A)}$ divides A but $P^{v_P(A)+1}$ does not, so such a decomposition exists.

If A is in the desired form, we have for the derivative A' of A:

$$A' = \sum_{i=1}^{n} \prod_{j \neq i} i A_j^j A_i' A_i^{i-1}. \tag{1}$$

Now let $T := \gcd(A, A')$. For every irreducible polynomial P dividing T we can determine $v_P(T)$ in the following way: P must divide A_m for some value of m (then it does not divide any other A_i). Then for all $i \neq m$ the v_P of the ith summand in equation (**??**) is at least m and for the mth summand it is $m - 1$ (A_m' is not divisible by P since A_m is squarefree) if $p \nmid m$ and 0 if $p|m$ (because of the factor m in that summand). So we find $v_P(T) = m - 1$ if $p \nmid m$ and $v_P(T) = m$ if $p|m$ (equality holds because $T|A$). So we obtain

$$T = \gcd(A, A') = \prod_{p \nmid i} A_i^{i-1} \prod_{p|i} A_i^i.$$

Now we define two sequences (T_i) and (V_i) by $T_1 = T$ and

$$V_1 = \frac{A}{T} = \prod_{p \nmid i} A_i.$$

Then set $V_{k+1} = \gcd(T_k, V_k)$ if $p \nmid k$ and $V_{k+1} = V_k$ if $p|k$ and set $T_{k+1} = \frac{T_k}{V_{k+1}}$. By induction one finds

$$V_k = \prod_{i \geq k, p \nmid i} A_i;$$

$$T_k = \prod_{i \geq k-1, p \nmid i} A_i^{i-k} \prod_{p|i} A_i^i.$$

So for $p \nmid k$ it follows $A_k = \frac{V_k}{V_{k+1}}$, so for $p \nmid k$ we can continue as long as V_k is non-constant. When V_k is constant, we have

$$T_{k-1} = \prod_{p|i} A_i^i.$$

Assume $A_i(X) = a_k X^k + \cdots + a_1 X + a_0$, then with $i = lp$

$$A_i^{lp} = a_k^{lp} X^{klp} + \cdots + a_1^{lp} X^{lp} + a_0^{lp} = a_k X^{klp} + ... + a_1 X^{lp} + a_0,$$

so we can set $Y := X^p$ and have $T_{k-1} = U^p(X) = U(Y)$. Now we can decompose U by using the algorithm recursively.

In practice one can easily compute T using Euclid's algorithm. Then one computes the sequences (V_i) and (T_i) to get the A_k. The algorithm is needed as a first step when one wants to find the prime decomposition of a polynomial, because it reduces the problem to the problem of factoring a squarefree polynomial.