# factorization of primitive polynomial

| | |
|---|---|
| Canonical name | FactorizationOfPrimitivePolynomial |
| Date of creation | 2013-03-22 19:20:30 |
| Last modified on | 2013-03-22 19:20:30 |
| Owner | pahio (2872) |
| Last modified by | pahio (2872) |
| Numerical id | 4 |
| Author | pahio (2872) |
| Entry type | Algorithm |
| Classification | msc 12D99 |
| Classification | msc 26C05 |
| Synonym | primitive factors of primitive polynomial |
| Related topic | EliminationOfUnknown |

As an application of the http://planetmath.org/EliminationOfUnknownparent entry we take the factorization of a primitive polynomial of $\mathbb{Z}[x]$ into http://planetmath.org/Prim prime factors. We shall see that the procedure may be done by performing a finite number of tests.

Let

$$a(x) \;=:\; a_nx^n+a_{n-1}x^{n-1}+\ldots+a_0$$

be a primitive polynomial in $\mathbb{Z}[x]$.

By the rational root theorem and the factor theorem, one finds all first-degree prime factors $x-a$ and thus all primitive prime factors of the polynomial $a(x)$.

If $a(x)$ has a primitive quadratic factor, then it has also a factor

$$x^2+px+q \tag{1}$$

where $p$ and $q$ are rationals (and conversely). For settling the existence of such a factor we treat $p$ and $q$ as unknowns and perform the long division

$$a(x):(x^2+px+q).$$

It gives finally the remainder $b(p,\,q)\,x+c(p,\,q)$ where $b(p,\,q)$ and $c(p,\,q)$ belong to $\mathbb{Z}[p,\,q]$. According to the http://planetmath.org/EliminationOfUnknownparent entry we bring the system

$$\begin{cases}b(p,\,q) \;=\; 0\\ c(p,\,q) \;=\; 0\end{cases}$$

to the form

$$\begin{cases}\bar{b}(q) \;=\; 0\\ \bar{c}(p,\,q) \;=\; 0\end{cases}$$

and then can determine the possible rational solutions $(p,\,q)$ of the system via a finite number of tests. Hence we find the possible quadratic factors (1) having rational coefficients. Such a factor is converted into a primitive one when it is multiplied by the gcd of the denominators of $p$ and $q$.

Determining a possible cubic factor $x^3+px^2+qx+r$ with rational coefficients requires examination of a remainder of the form

$$b(p,\,q,\,r)\,x^2+c(p,\,q,\,r)\,x+d(p,\,q,\,r).$$

In the needed system

$$\begin{cases} b(p,\, q,\, r) &= \; 0 \\ c(p,\, q,\, r) &= \; 0 \\ d(p,\, q,\, r) &= \; 0 \end{cases}$$

we have to perform two eliminations. Then we can act as above and find a primitive cubic factor of $a(x)$. Similarly also the primitive factors of higher degree. All in all, one needs only look for factors of degree $\leq \frac{n}{2}$.

# References

[1] K. Väisälä: *Lukuteorian ja korkeamman algebran alkeet.* Tiedekirjasto No. 17. Kustannusosakeyhtiö Otava, Helsinki (1950).