ABSTRAK

Misalkan F adalah lapangan berhingga dengan q elemen dan dinotasikan dengan $GF(q)$, α suatu elemen primitif dari $GF(q)$ dan suatu akar dari $x^n - 1$, maka $\alpha^n = 1$ dan α disebut akar satuan primitif ke $-n$. Dengan demikian $f(x) = x^n - 1$ mempunyai akar satuan primitif ke $-n$. Misalkan β suatu akar satuan primitf ke $-n$ dari $GF(q^m)$, polinomial minimal dari β atas $GF(q)$ adalah $m_\beta(x)$ dan dapat dinyatakan dalam bentuk : $m_\beta(x) = \prod_{i=0}^{t-1}\left(x - \beta^{q^i}\right)$ dimana t bilangan bulat positif terkecil sedemikian sehingga $\beta^{q^t} = \beta$. Selanjutnya $m_\beta(x)$ adalah suatu faktor dari $x^n - 1$ atas $GF(q)$ Dengan menggunakan tabel log Zech's ($1 + \alpha^i = \alpha^{z(i)}$), perluasan $m_\beta(x)$ mudah dievaluasi. Metode lain untuk pemfaktoran $f(x) = x^n - 1$ atas $GF(q)$ adalah dengan menggunakan operasi – operasi PPT (pembagi persekutuan terbesar) antara $f(x)$ dan $g(x)$ dengan derajat $g(x) < n - 1$ dan memenuhi $[g(x)]^q \equiv g(x)(\text{mod } f(x))$. Selanjutnya $f(x) = \prod_{s \in F} \text{PPT } (f(x), g(x) - s)$.

ABSTRACT

Let F is finite field with q elements and denoted by $GF(q)$, α is a primitive element of $GF(q)$ and a root of $x^n - 1$, then $\alpha^n = 1$ and α is called a primitive n^{th} root of unity. Hence $f(x) = x^n - 1$ has primitive n^{th} root of unity. Let β is a primitive n^{th} root of unity of $GF(q^m)$, minimal polynomial of β over $GF(q)$ is $m_\beta(x)$ and can be written in the form : $m_\beta(x) = \prod_{i=0}^{t-1}\left(x - \beta^{q^i}\right)$ where t is the smallest positive integer such that $\beta^{q^t} = \beta$. Then $m_\beta(x)$ is a factor of $x^n - 1$ over GF(q). Using the Zech's log table ($1 + \alpha^i = \alpha^{z(i)}$), expanding $m_\beta(x)$ is easy to evaluate. Another method for factoring $f(x) = x^n - 1$ over GF(q) is using appropriate gcd (the great common divisor) operations between $f(x)$ and $g(x)$ where deg $g(x) < n - 1$ and satisfying $[g(x)]^q \equiv g(x) (\text{mod } f(x))$. Then $f(x) = \prod_{s \in F} \gcd(f(x), g(x) - s)$.