

A REPRESENTAÇÃO GEOMÉTRICA DE CORPOS FINITOS . Dijiani Ludovino Guanais, Edson Donizete de Carvalho – Matemática - Departamento de Matemática– Faculdade de Engenharia – Campus de Ilha Solteira

Neste trabalho, mostraremos um procedimento para se representar geometricamente os elementos de corpo finitos F_{p^2} em um polígono fundamental que seja proveniente de uma tesselação regular de R^2 .

Um polígono regular P é dito polígono fundamental em R^2 , se for possível recobrir R^2 , a partir de cópias idênticas de P , de tal forma que a união destas cópias recobre todo R^2 , e de que a interseção destas cópias seja vazia.

É fato conhecido que em R^2 os polígonos fundamentais regulares dados por triângulos, quadrados e hexágonos..

Consideremos que $q = p^2$, com p , um inteiro primo, sabemos que $F_q^* = F_q - \{0\}$ é um grupo cíclico multiplicativo, isto é, existe ao menos um elemento $\beta \in F_q^*$ tal que β gera todos os elementos de F_q^* . Assim, temos que $\beta^{q-1} = 1$, ou seja, β é raiz do polinômio $p(x) = x^{q-1} - 1 \in F_p[X]$.

No intuito de fornecer uma representação geométrica para os elementos de F_{p^2} , seguiremos as seguintes etapas:

Etapa 1: Consideremos a fatoração do polinômio $p(x) = x^{q-1} - 1$ em elementos irredutíveis em $F_p[X]$. Supomos que seja da forma $p(x) = p_1^{n_1}(x) \dots p_k^{n_k}(x)$.

Etapa 2: Consideremos um polinômio de grau 2 da Etapa 1; suponhamos que seja $p_i(x)$, para algum $i \in \{1, \dots, k\}$, determinemos suas raízes em C (corpo dos números complexos).

Etapa 3: Seja $\alpha \in C$ uma das raízes encontradas na Etapa 2. Por outro lado, sabemos que:

$$F_q \cong \frac{F_p[X]}{p_i(x)} \cong F_p(\alpha) = \{a + b\alpha : a, b \in F_p\}. \text{ (Equação 1)}$$

Observação: Lembremos de que os elementos de F_p podem ser vistos como classes resto de inteiros módulo o inteiro primo p .

A Etapa 3, juntamente com a Observação, fornecem as condições necessárias para representarmos geometricamente os elementos de F_{p^2} em um polígono fundamental P .

A conclusão deste trabalho, é de que teremos uma distribuição uniforme no quadrado, se $\alpha \in Z[i] = \{a + bi : a, b \in Z\}$.

Caso, $\alpha \in Z[\omega] = \{a + b\omega : a, b \in Z\}$, onde $\omega^6 = 1$, teremos uma distribuição no

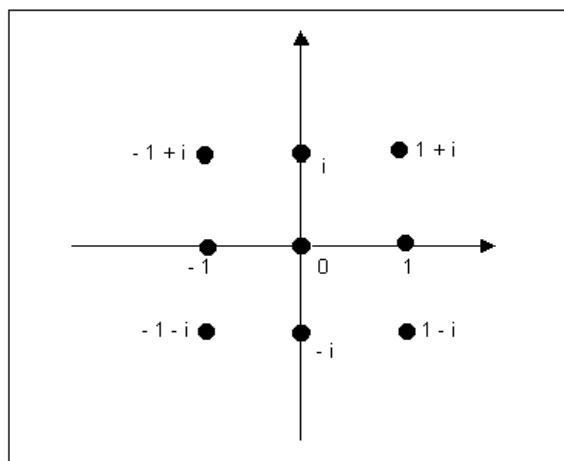
hexágono regular.

Como exemplo consideremos $p = 3$, logo o polinômio a considerar sobre F_3 , é dado por $p(x) = x^8 - 1$.

Tomando sua fatoraço em F_3 , obtemos $p(x) = x^8 - 1 = (x + 1)(x + 2)(x^4 + 1)(x^2 + 1)$.

Considerando $\alpha = i$, como raiz de $p_i(x) = x^2 + 1$, aplicando a equaço 1 em α .

Teremos que $F_9 \cong F_3(\alpha) = \{-1 + i, i, 1 + i, -1, 0, 1, -1 - i, -i, 1 - i\}$, está uniformemente distribuídos em um quadrado como na figura abaixo.



Referências Bibliográficas:

- [1] ARMSTRONG, M.A., Groups and Symmetry, Springer-Verlag, New York, 1988.
- [2] HERSTEIN, I.N. Tópicos em Àlgebra, 2^a ed., Wiley, New York, 1975.
- [3] STEWART I. and Tall D., Algebric Number Theory, Chapman & Hall, New York, 1987.