11/5/04 Rajini H.

$R = \{x^3 : x \in \mathbb{F}_p^*\}$ $\quad (\mathbb{F}_p^* : R) = 3.$

$\mathbb{F}_p = \{0\} \cup R \cup S \cup T$

$M_p = \left(q\frac{[R,R,R]}{m} + 1\right) \Rightarrow = q\frac{[RTS]}{m}.$

Cubic Gauss Sums

Recall: pth roots of unity:

$\zeta = e^{\frac{2\pi i}{p}}$

pth roots of unity are $\zeta^0, \zeta^1, \zeta^2, \ldots \zeta^{p-1}$.

$\zeta^a = \zeta^b$ iff $a \equiv b \bmod p$.

If $a, b \in \mathbb{F}_p$ then $\zeta^{a+b} = \zeta^a \zeta^b$.

$\alpha_1, \alpha_2, \alpha_3 \in \mathbb{C}$.

$$\alpha_1 = \sum_{r \in R} \zeta^r \qquad \alpha_2 = \sum_{s \in S} \zeta^s \qquad \alpha_3 = \sum_{t \in T} \zeta^t.$$

Each α_i is a sum of distinct powers of ζ.

We will find the equation with integer coefficients that has $\alpha_1, \alpha_2, \alpha_3$ as roots.

$$\alpha_2 \alpha_3 = \sum_{s \in S} \sum_{t \in T} \zeta^{s+t} = \sum_{s \in S, t \in T} \zeta^{s+t} = \sum_{x \in \mathbb{F}_p} N_x \zeta^x$$

where N_x = # of pairs (s,t) s.t. $s+t = x$.

Observe: $r \in R$

$N_x = [ST\{x\}] = [rS, rT, \{-rx\}] = [S, T, \{-rx\}] = N_{rx}$.

N_x depends only on the coset R, S, T that x belongs to.

$$mN_x = [STR_x] = \begin{cases} [STR] & \text{if } x \in R \\ [STS] & \text{if } x \in S \\ [STT] & \text{if } x \in T \end{cases}$$

Define $a, b, c \in \mathbb{Z}$ s.t.

$[STR] = ma$, $[STS] = mb$, $[STT] = mc$.

$$M_p = \frac{9[RTS]}{m} = 9a.$$

$\alpha_2\alpha_3 = a\alpha_1 + b\alpha_2 + c\alpha_3$.

$\alpha_3\alpha_1 = a\alpha_2 + b\alpha_3 + c\alpha_1$

$\alpha_1\alpha_2 = a\alpha_3 + b\alpha_1 + c\alpha_2$

$0 = \zeta^p - 1 = (\zeta - 1)(\zeta^{p-1} + \cdots + 1) \quad \zeta \neq 1$.

$\Rightarrow \zeta^{p-1} + \zeta^{p-2} + \cdots + 1 = 0$.

$\alpha_1 + \alpha_2 + \alpha_3 = -1$

$\alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3 = (a+b+c)(\alpha_1 + \alpha_2 + \alpha_3) = -(a+b+c)$

$m(a+b+c) = [STR] + [STS] + [STT]$

$= [ST|F_p^*] = [ST|F_p] - [ST\{0\}] = m^2$.

So $\alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3 = -m$.

~~$\alpha_1 + \alpha_2 + m$~~

$\alpha_1^2 + \alpha_2^2 + \alpha_3^2 = (\alpha_1 + \alpha_2 + \alpha_3)^2 - 2(\alpha_2\alpha_1 + \alpha_2\alpha_3 + \alpha_3\alpha_1)$

$= 1 + 2m$.

$\alpha_1 \alpha_2 \alpha_3$

$\alpha_1(\alpha_2\alpha_3) = \alpha_1(a\alpha_1 + b\alpha_2 + c\alpha_3)$

$\alpha_2(\alpha_1\alpha_3) = \alpha_2(a\alpha_2 + b\alpha_3 + c\alpha_1)$

$\alpha_3(\alpha_1\alpha_2) = \alpha_3(a\alpha_3 + b\alpha_1 + c\alpha_2)$

$3\alpha_1\alpha_2\alpha_3 = a(1+2m) + (b+c)(-m) = a + km$

$k = 3a - m.$

$* M_p = 9a = 3(k+m) = 3k + p - 1.$

$\alpha_1, \alpha_2, \alpha_3$ are the roots of

$F(t) = (t-\alpha_1)(t-\alpha_2)(t-\alpha_3) =$

$\left(t^3 + t^2 - mt \mp \frac{a+4m}{3}\right)$

Discriminant of F:

$D_1 =$

$\sqrt{D_1} = (\alpha_1 - \alpha_2)(\alpha_1 - \alpha_3)(\alpha_2 - \alpha_3)$

$= (b-c)\left(\alpha_1^2 + \alpha_2^2 + \alpha_3^2 - \sum_{i \neq j} \alpha_i \alpha_j\right)$

$= (b-c)(1+3m)$

$= (b-c)p.$

$\beta_i = 1 + 3\alpha_i$

$(\beta_1 + \beta_2 + \beta_3) = 0$

$(\beta_1\beta_2 + \beta_2\beta_3 + \beta_1\beta_3) = -3p.$

$(\beta_1\beta_2\beta_3) = (3k-2)p.$

G_i polynomial with β_i's as roots.

$$G(t) = t^3 - 3_p t - (3k-2)p.$$

Let $A = (3k-2)$

$$M_p = 3k + p - 1 = p + 1 + A.$$

Recall $4_p = A^2 + 27B^2$ $\quad A \equiv 1 \bmod 3.$

and $M_p = p + 1 + A$

Want to show that this A is the A in the theorem.

$$D_G = -4(-3_p)^3 - 27(A_p)^2 = 4 \cdot 27_p{}^3 - 27A^2p^2$$

$$\beta_i - \beta_j = 3(\alpha_i - \alpha_j)$$

$$D_G = (27)^2 D_F$$

$$4 \cdot 27_p{}^3 - 27A^2p^2 = 27^2 D_F = 27^2(b-c)^2p^2$$

Cancelling $27p^2$

$$4_p = A^2 + 27B^2 \quad \text{where } (b-c) = B.$$

and $A = 3k - 2 \equiv 1 \bmod 3.$

$$M_p = p + 1 + A.$$

$A \equiv 1 \bmod 3 \quad 4_p = A^2 + 27B^2$

want to show that the condition determine a unique A.

Assume there exists another A', B'

$\therefore$ some algebra

$$AB_1 - A_1B = 0.$$

$$\lambda = \frac{A_1}{A} = \frac{B_1}{B} \Rightarrow \lambda = 1 \Rightarrow A_1 = A.$$