Chapter VI

Applications to Number Theory

VI.1 Theorem.

Let $R = \mathbb{Z}_p$, the ring of integers modulo $p$ where $p > 2$ is a prime integer and let $G$ be as in Theorem IV.1 and let $u \in U(RG)$, which depending on $\lambda_1=1, \lambda_2=2, \ldots, \lambda_m=p-1$. Then trace of $u^r = 0$ (i.e, the coefficient of the identity in $G$ of $u^r$), for $r = 1, 2, \ldots, p-2$.

Proof:- Since $\mathbb{Z}_p$ is a Halidon ring with index $m = p-1$, there is a primitive $m^{th}$ root of unity $\omega$ in $R$ and since $\omega^r \neq \omega^s$ for $r \neq s$ and $0 < r, s < m-1$ and $\omega^m = 1$, we can choose 2, 3, ..., $p-2$ as some distinct powers $\omega$. By Theorem IV.1, we have

$$\rho(u^r) = (\lambda_1^r, \lambda_2^r, \ldots, \lambda_m^r)$$

and using the remark of Theorem IV.5, we get

$$\text{trace of } u^r = (1/m) \left( \lambda_1^r + \lambda_2^r + \ldots + \lambda_m^r \right)$$

$$= (1/m)(1 + \omega^r + (\omega^r)^2 + \ldots + (\omega^r)^{m-1})$$

after rearranging the terms. Since $\omega$ is a primitive $m^{th}$ root of unity, using the definition we get trace of $u^r = (1/m).0 = 0$ for $r = 1, 2, \ldots, p-2$.

Now let us prove Lagrange and Wilson’s Theorems.

VI.2 Theorem.

Let $R = \mathbb{Z}_p$, the ring of integers modulo $p$ where $p > 2$ is a
prime integer and let $G$ be as in Theorem IV.1 and let $u \in U(R)$, which depending on $\lambda_1=1, \lambda_2=2, \lambda_m=p-1$. Then $S_r = 0 \pmod{p}$ for $r = 1, 2, \ldots, p-2$. [Lagrange's Theorem] and $1 + (p-1)! = 0 \pmod{p}$ [Wilson’s Theorem], where $S_r$’s are the elementary symmetric polynomials in $\lambda_1, \lambda_2, \lambda_m$.

Proof:- By Theorem VI.1, the trace of $u^r = 0$ for $r = 1, 2, \ldots, p-2$. Next we have to show that $\{1, u, u^2, \ldots, u^{m-1}\}$ is a linearly independent set over $R$.

Suppose $a_1 + a_2 u + a_3 u^2 + \ldots + a_m u^{m-1} = 0$

Since the trace of $u^r = 0$, for $r = 1, 2, \ldots, p-2$, we get $a_1 = 0$. Thus we have $a_2 u + a_3 u^2 + \ldots + a_m u^{m-1} = 0$.

Multiplying by $u^{-1}$ we get $a_2 + a_3 u + \ldots + a_m u^{m-2} = 0$.

Arguing as before we get $a_2 = 0, \ldots, a_m = 0$.

$\therefore \{1, u, u^2, \ldots, u^{m-1}\}$ is a linearly independent set over $R$.

i.e the map $\phi$ defined in Theorem IV.7 is a monomorphism as $u^m = 1$. $\therefore \text{Ker } \phi = \{0\}$.

Then again by Theorem IV.7 we have, there is a

$$y = \sum_{i=1}^{m} y_i g_i \in \text{Ker } \phi$$

s.t.

$$y_i = (-1)^{m-i+1} S_{m-i+1} \quad \text{if } i \neq 1$$

$$= 1 + (-1)^m S_m \quad \text{if } i = 1$$

95
where $S_i$'s are the elementary symmetric polynomials in $\lambda_1, \lambda_2, \ldots, \lambda_m$.

But $y_i = 0$ for each $i = 1, 2, \ldots, m$.

$$S_r = 0 \pmod{p} \quad \text{for } r = 1, 2, \ldots, p-2,$$

which is Lagrange's Theorem.

And

$$1 + (-1)^m S_m = 0 \pmod{p}$$

Since $p > 2$ is prime, $m = p-1$ is even and $(-1)^m$ is positive and

$$S_m = 1 \cdot 2 \cdot 3 \cdots (p-1)$$

$$= (p-1)!$$

Thus we have

$$1 + (p-1)! = 0 \pmod{p}$$

which is Wilson's Theorem.