

$$\zeta = e^{2\pi i/m} \quad m \geq 2 \quad m \in \mathbb{Z}$$

$$\mathbb{Z}[\zeta] = \left\{ u \in \mathbb{C} \mid u = a_0 + a_1 \zeta + \dots + a_r \zeta^r, \right. \\ \left. a_0, \dots, a_r \in \mathbb{Z} \right\}.$$

$1 \in \mathbb{Z}[\zeta]$, $\mathbb{Z}[\zeta]$ is closed under addition and multiplication.

Lemma. If $u \in \mathbb{Z}[\zeta]$ then there exists

$$f(t) = t^m + b_{m-1}t^{m-1} + \dots + b_1t + b_0, \quad b_i \in \mathbb{Z}$$

and $f(1) = 0$.

Proof. $\varphi^m = 1$, $\varphi^s = \varphi^{q_m+r}$ $q \in \mathbb{Z}$,

$0 \leq r < m$. Conclusion

If $u \in \mathbb{Z}[\varphi]$ then $u = a_0 + a_1 \varphi + \dots + a_{m-1} \varphi^{m-1}$.

$$u \varphi^j = \sum_{i=0}^{m-1} c_{ji} \varphi^i \quad j = 0, \dots, m-1$$

$c_{ji} \in \mathbb{Z}$.

$$\underline{\varphi} = \begin{bmatrix} \varphi^0 \\ \varphi^1 \\ \vdots \\ \varphi^{m-1} \end{bmatrix}$$

$$C = [c_{ij}] \quad c_{ij} \in \mathbb{Z}$$

$C\underline{y} = u\underline{y} \Rightarrow u$ is
an eigenvalue for C . Let
 $f(t) = \det(tI - C) = t^m + \sum_{0 < i < m} b_i t^i$
 $f(u) = 0$. QED

Lemma. $\mathbb{Q} \cap \mathbb{Z}[T] = \mathbb{Z}$.

Proof. Consider $z = \frac{a}{b}$ $b > 0$
 $\gcd(a, b) = 1$.

$$z = \frac{a}{b}$$

Assume $z \in \mathbb{Z}[i]$ so

$$\exists t^m + d_{m-1}t^{m-1} + \dots + d_1t + d_0 = f(t)$$

$d_i \in \mathbb{Z}$ so that $f(z) = 0$,

$$\left(\frac{a}{b}\right)^m + d_{m-1}\left(\frac{a}{b}\right)^{m-1} + \dots + d_1\left(\frac{a}{b}\right) + d_0 = 0$$

Multiply by b^m

$$a^m + d_{m-1}a^{m-1}b + \dots + d_1ab^{m-1} + d_0b^m = 0$$

$\Rightarrow b \mid a^m$, $\gcd(b, a) = 1 \Rightarrow \Leftarrow$ (contradict; wrong)

We say that $u, v \in \mathbb{Z}[\vartheta]$
are equivalent modulo $d > 0$
 $d \in \mathbb{Z}$ if
 $u - v \in d \mathbb{Z}[\vartheta]$

ie $u - v = dw$ $w \in \mathbb{Z}[\vartheta]$.

Lemma. If $u, v \in \mathbb{Z}$ and
 u, v are ~~congruent~~ equivalent
modulo d then $u \equiv v \pmod{d}$.

We are assuming that

Proof. $u - v = dw \quad w \in \mathbb{Z}[\sqrt{d}]$

Thus $\frac{u-v}{d} = w \Rightarrow \frac{u-v}{d} = r \in \mathbb{Z}$
 $\mathbb{Q} \nearrow \mathbb{Z}[\sqrt{d}] \Rightarrow u \equiv v \pmod{d}$

We can write for $u, v \in \mathbb{Z}[\sqrt{d}]$, $d > 0$
 $d \in \mathbb{Z}$

$u \equiv v \pmod{d}$ to

mean that $u - v = dw$, $w \in \mathbb{Z}[\sqrt{d}]$.

We now prove quadratic reciprocity.

Let $p \in \mathbb{Z}$, p ~~is~~ ^{an odd} prime

Assert that

$$(a+b)^p \equiv a^p + b^p \pmod{p}.$$

$a, b \in \mathbb{Z}[\vartheta].$

$$(a+b)^p = a^p + \sum_{j=1}^{p-1} \binom{p}{j} a^{p-j} b^j + b^p$$

if $1 \leq j \leq p-1$ then $p \mid \binom{p}{j}$.

$$\zeta = e^{2\pi i/m}$$

$$(a_1 + \dots + a_r)^p \equiv a_1^p + \dots + a_r^p \pmod{p}$$

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

$$\chi(a) = \left(\frac{a}{p}\right), \quad g_1(x) = \sum_{j=0}^{p-1} \binom{j}{p} \zeta^j$$

$q \neq p$ odd prime.

$$g_1(x)^q \equiv \sum_{j=0}^{p-1} \binom{j}{p} \zeta^{qj} \pmod{q}$$

$$\equiv g_q(x) \pmod{q}$$

$$g_q(x) = \chi(q') g_1(x) = \left(\frac{q'}{p}\right) g_1(x).$$

$$\left(\frac{q'}{p}\right) = \left(\frac{q}{p}\right), \quad q'q \equiv 1 \pmod{p}.$$

$$g_1(x)^q = \left(\frac{q}{p}\right) g_1(x).$$

$$g_1(x)^2 = (-1)^{\frac{p-1}{2}} p^{\frac{q-1}{2}}$$

$$g_1(x)^{q-1} = (g_1(x)^2)^{\frac{q-1}{2}} \equiv \left[(-1)^{\frac{p-1}{2}} p^{\frac{q-1}{2}} \right]^{\frac{q-1}{2}} \equiv (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}} \left(\frac{p}{q}\right) \pmod{q}$$

$$g_1(x)^q \equiv (-1)^{\frac{p-1}{2} \frac{q-1}{2}} \left(\frac{p}{q}\right) g_1(x) \pmod{q}$$

$$\equiv \left(\frac{q}{p}\right) g_1(x) \pmod{q}$$

$$(-1)^{\frac{p-1}{2} \frac{q-1}{2}} \left(\frac{p}{q}\right) (-1)^{\frac{p-1}{2}} p \equiv \left(\frac{q}{p}\right) (-1)^{\frac{p-1}{2}} p \pmod{q}$$

QED.

Euler's formula p/a then

$$a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \pmod{p}$$

v primitive root mod p .

$$\left(\frac{v}{p}\right) = -1.$$

$$v^{p-1} = 1$$

$$\text{But } v^{\frac{p-1}{2}} \neq 1$$

$$a \equiv v^k \pmod{p} \quad 0 \leq k \leq p-2$$

$$\left(\frac{a}{p}\right) = \left(\frac{v^k}{p}\right) = \left(\frac{v}{p}\right)^k = (-1)^k.$$

$$v^{\frac{p-1}{2}} \equiv -1 \pmod{p} \Rightarrow (v^k)^{\frac{p-1}{2}} \equiv (-1)^k \pmod{p}$$