Properties of $\mathbb{Z}[\omega]$

Gautham Anne

1 $\mathbb{Z}[\omega]$

Theorem 1.1. *The Norm of Z[ω] is* $a^2 - ab + b^2$.

Proof. Ummm do it yourself :) □

Lemma 1.2. *If α prime in* $\mathbb{Z}[\omega]$*, then N(α) = p or* p^2*, where p is a rational prime. Moreover, if N(α) =* p^2*, then α and p are associates.*

Lemma 1.3. *If N(α) prime in* $\mathbb{Z}$*, then α prime in* $\mathbb{Z}[\omega]$.

Proof. An exercise to the reader. □

Lemma 1.4. *If p, a rational prime, is congruent to 2 mod 3, then it is prime in* $\mathbb{Z}[\omega]$*.If* $p \equiv 1 \pmod 3$*,* $p = \pi\overline{\pi}$*, π prime in* $\mathbb{Z}[\omega]$*. Also,* $3 = -\omega^2(1-\omega)^2$.

Theorem 1.5. *Modding out* $\mathbb{Z}[\omega]$ *by a prime α will result in a field with N(α) elements.*

Proof. An exercise to the reader. Hint: $\mathbb{Z}[\omega]$ is a UFD, so π prime $\implies$ π irreducible. □

Theorem 1.6. *If α prime in* $\mathbb{Z}[\omega]$*, and* $\alpha \nmid \pi$ *then* $\alpha^{N(\pi)-1} \equiv 1 \pmod \pi$

Proof. Hint: Analog of FLT with Theorem 1.5. □

Theorem 1.7. *If π prime in Z[ω] with norm ≠ 3,*

$$\alpha^{(N(\alpha)-1)/3} \equiv \omega^m \pmod \pi$$

for unique m = 0, 1, or 2.

Lemma 1.8. *Let F be a finite field with q elements, such that F* is cyclic with q-1 elements. Then for* $\alpha \in F^*$*,* $x^n = \alpha$ *has solutions iff* $\alpha^{(q-1)/d} = 1$*, where d = gcd(q-1,n).*

Proof. Hint: Define a group isomorphism from F* to $\mathbb{Z}_{q-1}$ and take a look at the generator. What can you set α to equal? □

Definition 1.9. *Define the Cubic Legendre Symbol as*

$$\left(\frac{a}{\pi}\right)_3 = \begin{cases} a^{(N(\alpha)-1)/3}, & \text{if } \pi \nmid a \\ 0, & \pi \mid a \end{cases}$$

Theorem 1.10. ***(Properties of Cubic Legendre Symbol)***

1. $a^{(N(\alpha)-1)/3} \equiv 1 \pmod{\pi}$
2. *Is multiplicative*
3. *If* $\alpha \equiv \beta \pmod{\pi}$ *then* $\left(\frac{\alpha}{\pi}\right)_3 = \left(\frac{\beta}{\pi}\right)_3$

Proof. You can prove these :0 □

Lemma 1.11. $\overline{\left(\frac{\alpha}{\pi}\right)_3} = \left(\frac{\overline{\alpha}}{\overline{\pi}}\right)_3 = \left(\frac{\alpha^2}{\pi}\right)_3$, *where* $\overline{\alpha}$ *is the complex conjugate of* α.

Proof. An exercise to the reader. □

Theorem 1.12. *Let* π *be a prime such that* $N(\pi) = p \equiv 1 \pmod{3}$. *Then exactly one of the associates of* π *are primary.*

Theorem 1.13. *If* $q \equiv 2 \pmod{3}$, *then every integer is a cubic residue mod q.*

Proof. Yikeydoodles. □

Lemma 1.14. *If a and* $b \in \mathbb{Z}[\omega]$ *primary, then -ab is also primary.*

Proof. Nah I'm good. □

Theorem 1.15. *Let* π_1, π_2 *be primes in* $\mathbb{Z}[\omega]$. *Then,* $\left(\frac{\pi_1}{\pi_2}\right)_3 = \left(\frac{\pi_2}{\pi_1}\right)_3$ *where* $N(\pi_1) \neq N(\pi_2)$ *and* $N(\pi_1), N(\pi_2) \neq 3$.

Proof. Ummmmmmmm □