Number Theory

Monday, June 30, 2014 1:03 PM

Gaussian Integers

$\mathbb{Z}[i] = \{a+bi \mid a,b \in \mathbb{Z}\} \subset \mathbb{Q}(i) = \{x+yi \mid x,y \in \mathbb{Q}\} \subset \mathbb{C}$.

ring s.t. $\alpha,\beta \in \mathbb{Z}[i]$, $\alpha\beta = 0 \Rightarrow \alpha = 0$ or $\beta = 0$

not a fd. Since $2 \in \mathbb{Z}[i]$ no mult. inverse.

$\mathbb{Z}[i]^\times = \{\alpha \in \mathbb{Z}[i] \mid \exists \beta \in \mathbb{Z}[i] \text{ st. } \alpha\beta = 1\} = \{\pm 1, \pm i\}$.

Congruence in $\mathbb{Z}[i]$. $I \subset \mathbb{Z}[i]$ ideal. $\alpha \equiv \beta \ (I) \Leftrightarrow \alpha - \beta \in I$.

$I \subset \mathbb{Z}[i]$ ideal. $\Rightarrow I = (a)$ for some $a \in \mathbb{Z}[i]$. So.

$\alpha \equiv \beta \ (I) \Leftrightarrow a \mid \alpha - \beta$.

ring $\mathbb{Z}[i]/I = \{[\alpha] \mid \alpha \in \mathbb{Z}[i]\}$

2 operations: $[\alpha]+[\beta] = [\alpha+\beta]$.

$[\alpha][\beta] = [\alpha\beta]$.

Prop. $I \subset \mathbb{Z}[i]$ ideal, $I = (a)$, $a \in \mathbb{Z}[i]$, $a \neq 0$, then.

$\#(\mathbb{Z}[i]/I) = N(a) = a\bar{a}$.

Pf: let $a = x+yi$ ($x,y \in \mathbb{Z}$, $\gcd(x,y) = 1$)

We show that: for $\forall\ z+iw \in \mathbb{Z}[i]$ $\exists b \in \mathbb{Z}$ st. $z+ib \equiv b$ (I)

If we do this we are done. in the case $\gcd(x,y) = 1$.

wts. $z+iw \equiv$ integer (a). enough to show $i \equiv$ integer.

We know. $x+iy \equiv 0$ (a). $\Rightarrow iy \equiv -x$ (a).

if y has an inverse. y' mod a. (i.e. $yy' \equiv 1$ (a)).

then we have. $iy \equiv -x \Rightarrow iyy' \equiv -xy' \Rightarrow i \equiv -xy'$ (a)

xy' is an integer.

Note: $\gcd(y, x^2+y^2) = 1$.

if $\exists p$ s.t. $p \mid y$. $p \mid x^2+y^2 \Rightarrow p \mid y^2 \Rightarrow p \mid x^2 \Rightarrow p \mid (x,y) \Rightarrow$ not possible $\Rightarrow \gcd(y, x^2+y^2) = 1$.

So. $\exists y' \in \mathbb{Z}$ st. $yy' \equiv 1 \pmod{x^2+y^2}$.

$\Rightarrow yy' = 1 + f\cdot(x^2+y^2)$ for some $f \in \mathbb{Z}$.

$= 1 + f\cdot a\cdot\bar{a}$. $\Rightarrow yy' \equiv 1 \pmod{a}$

What if $\gcd(x,y) \neq 1$. Suppose $a = d(x'+iy')$, where $d > 0$.

$d = \gcd(x,y) \Rightarrow \gcd(x',y') = 1$.

$a = d(x'+iy') \Rightarrow N(a) = d^2(x'^2+y'^2)$

We'd like to show that, $\#\left(\mathbb{Z}[i]/(\alpha)\right) = d^2 \cdot \#\left(\frac{\mathbb{Z}[i]}{(x+iy)}\right)$.

Rk: 1) $\#(\mathbb{Z}[i]/(\alpha)) = |N(\alpha)| = |\alpha\bar{\alpha}|$ $\alpha \neq 0$.

2) $\#(\mathbb{Z}/(n)) = |n|$ $n \neq 0$.

$\mathbb{Z}[i]/(0) = \mathbb{Z}[i]$.

3) $\alpha = 1$.

Saw. $n \in \mathbb{Z}$. $\mathbb{Z}/(n)$ fd. $\Leftrightarrow$ n prime.

Prop. $\alpha \in \mathbb{Z}[i]$. $\mathbb{Z}[i]/(\alpha)$ fd. $\Leftrightarrow$ α irreducible.

Pf: $\Rightarrow$ if $\alpha = \beta\gamma$. where β, γ not units. then $[\alpha] = [\beta][\gamma]$

$\Rightarrow [0] = [\beta][\gamma]$.

Note that $[\beta] \neq 0$. if $[\beta] = 0$. $\beta = \alpha\alpha'$ $\Rightarrow \alpha = \beta\gamma = \alpha\alpha'\gamma$.

$\Rightarrow 1 = \alpha'\gamma$. $\Rightarrow \gamma$ unit $\times$.

Similarly. $[\gamma] \neq 0$.

We deduce how $[\beta]$ has no inverse. in $\mathbb{Z}[i]/(\alpha)$.

$[\beta][\gamma] = e \Rightarrow$ not int domain $\Rightarrow$ contradiction

If α irred. ---.

Ex. $\mathbb{Z}[i]/(2)$ not a fd, w/ 4 elements.

$2 = (1+i)(1-i) = i(1+i)^2$. $1+i \neq 2$.

$N(1 \pm i) = 2$. $\Rightarrow 1 \pm i$ not unit in $\mathbb{Z}[i]$.

Ex. $\mathbb{Z}[i]/(7)$ fd w/ 49 elements.

Ex. $\mathbb{Z}[i]/(5)$. $5 = (2+i)(2-i)$ irreducible.

w/ 25 elements but not a fd.

$\mathbb{Z}[i]/(5) \cong \mathbb{Z}/(5) \times \mathbb{Z}/(5)$.

Ex. $\pi \in \mathbb{Z}[i]$ irred $\alpha \in \mathbb{Z}[i]$ Then. $\alpha^{N(\pi)} \equiv \alpha \pmod{\pi}$.

Rk. F fd. $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_2 x^2 + a_1 x + a_0$. poly w/ $a_i \in F$.

Then $f(x)$ has at most n roots in F.

prime p. Consider $x^{p-1} - 1$. poly w/ coefficients in $\mathbb{Z}/(p)$. Then.

exactly $p-1$. roots in $\mathbb{Z}/(p)$.

We know that. $\forall a \in \mathbb{Z}/(p)$, $a \neq 0$. $a^{p-1} = 1$. So. a root of $x^{p-1} - 1 = 0$.

$\Rightarrow x^{p-1} - 1 = (x-1)(x-2)\cdots(x-(p-1))$.

Q: $(\mathbb{Z}/p)[i] = \{[a] + [b]i \mid [a], [b] \in \mathbb{Z}/(p)\}$. -1 is a square in $\mathbb{Z}/p$?

Lemma. $p \equiv 1 \ (4) \iff \exists x \in \mathbb{Z}$. St. $x^2 \equiv -1 \ (p)$. $p \neq 2$.

pf: ($\Rightarrow$). $x^{p-1} - 1 = (x^{\frac{p-1}{2}} - 1)(x^{\frac{p-1}{2}} + 1)$

the LHS has exactly $p-1$ roots in $\mathbb{Z}/(p)$, then both. $x^{\frac{p-1}{2}} - 1$. $x^{\frac{p-1}{2}} + 1$ has exactly $\frac{p-1}{2}$ roots in $\mathbb{Z}/(p)$.

$\Rightarrow x^{\frac{p-1}{2}} + 1$ has a root $\theta \in \mathbb{Z}/p$.

$p \equiv 1 (4) \Rightarrow \frac{p-1}{2} = 2k$. $\Rightarrow \theta^{2k} + 1 = 0$ in $\mathbb{Z}/(p)$. let $x = \theta^k$.

$\Rightarrow x^2 \equiv -1 \ (p)$.

Thm. Suppose p prime $p \neq 2$. TFAE.

1) p not irred in $\mathbb{Z}[i]$.
2) $p = \alpha\bar{\alpha}$ for some $\alpha \in \mathbb{Z}[i]$.
3) $\mathbb{Z}[i]/(p)$ not a fd.
4) $\exists x, y \in \mathbb{Z}$. St. $x^2 + y^2 = p$.
5) $p \equiv 1 \ (4)$.
6) $\exists z \in \mathbb{Z}$. $z^2 \equiv -1 \ (p)$.

pf: 4 $\Rightarrow$ 6. Suppose $p = x^2 + y^2$. for some $x, y \in \mathbb{Z}$.

$\Rightarrow x^2 \equiv -y^2 \pmod{p}$. $p \nmid y^2 \Rightarrow \exists y' \in \mathbb{Z}$ St. $yy' \equiv 1 \ (p)$

$\Rightarrow x^2 y'^2 = -y^2 y'^2 = -(yy')^2 = -1 \pmod{p}$

$\Rightarrow (xy')^2 \equiv 1 \pmod{p}$.

6 $\Rightarrow$ 1. if $\exists z \in \mathbb{Z}$ st. $z^2 \equiv -1 \ (p) \Rightarrow z^2 = rp - 1$ for some. $r \in \mathbb{Z}$. $\Rightarrow z^2 + 1 = rp$. $\Rightarrow p \mid (z+i)(z-i)$. in $\mathbb{Z}[i]$.

if p irreducible $\Rightarrow p$ prime $\Rightarrow p \mid z+i$. or $p \mid z-i$.

if $p \mid z+i \Rightarrow p(a+bi) = (z+i) \Rightarrow 1 = bp$. Contradiction

$\Rightarrow p$ not irreducible

1 $\Rightarrow$ 2. p not irred $\Rightarrow p = \beta\cdot\gamma$. non units. $\Rightarrow$.

$N(p) = N(\beta)N(\gamma) \Rightarrow p^2 = N(\beta)N(\gamma) \Rightarrow N(\beta).N(\gamma) \mid p^2$

$\Rightarrow$ non unit $\Rightarrow N(\beta) = N(\gamma) = p$.

$\Rightarrow p = N(p) = \beta \cdot \bar{\beta}$.

$4 \Rightarrow 5$. if $\exists x, y$ st. $x^2+y^2 = p$. $\Rightarrow x^2 \cdot y^2 \equiv 1$ or $0 \pmod 4$

p odd $\Rightarrow p \equiv 1 \pmod 4$.

Today 6 p.m. problem session.

@ E206.

---

pset 1 returned.

$\mathbb{Z}[\sqrt{-3}] = \{a+b\sqrt{-3} \mid a, b \in \mathbb{Z}\} \subset \mathbb{C}$.

the proof of Euclidean division failed.

$N(a+b\sqrt{-3}) = a^2+3b^2 \geq 0$.

Moreover, $\mathbb{Z}(\sqrt{-3})$ does not have UF. as 2 is irreducible but not prime. $2 \mid (1+\sqrt{-3})(1-\sqrt{-3})$.

Rk. $R = \mathbb{Z}\left(\frac{1+\sqrt{-19}}{2}\right) = \left\{a+b\cdot\frac{1+\sqrt{-19}}{2} \mid a, b \in \mathbb{Z}\right\}$.

It's possible to prove R has UF but not Euclidean division.

Rk R ring, no zero divisor.

* R has Euclidean division 1)
* Every ideal of R is principal. 2)
* R has unique factorization. 3).

Always true that 1) $\Rightarrow$ 2) $\Rightarrow$ 3). In general another directions don't work.

Ex. 2) $\not\Rightarrow$ 1). $R = \mathbb{Z}\left(\frac{1+\sqrt{-19}}{2}\right)$.

Ex $R = \mathbb{Z}[x]$. ring has 3) but not 2).

Ex. $\nexists h(x) \in R$ st. $I = h(x)R$.

$I = 2R + xR$. i.e. I is not principal.

Ex. $\alpha = 4$. $\beta = 2+2\sqrt{-3} \in \mathbb{Z}(\sqrt{-3})$.

Claim: $\nexists$ gcd (α, β) in $\mathbb{Z}(\sqrt{-3})$.

1) find all the divisors of α and β.

let $\alpha_1\alpha_2 = 4 \Rightarrow N(\alpha_1)N(\alpha_2) = N(4) = 16$

$\Rightarrow N(\alpha_1) = N(\alpha_2) = 4$. $\alpha_1 = \pm 1 \pm \sqrt{-3}$

$2+2\sqrt{-3} = \alpha_1\alpha_2 \Rightarrow N(\alpha_1)N(\alpha_2) = N(2+2\sqrt{-3}) = 4+12 = 16$.

$\Rightarrow$ common divisor $\pm(1+\sqrt{-3})$. but no one is divisible by all others.

$K = \mathbb{Q}(\sqrt{-3}) = \{a+b\sqrt{-3} \mid a,b \in \mathbb{Q}\}$. $\mathcal{O} = \mathbb{Z}\left[\frac{-1+\sqrt{-3}}{2}\right]$.

$\mathcal{O}$ is not a field.

$\zeta = \frac{-1+\sqrt{-3}}{2}$. ζ is a 3^{rd} root of unity. also primitive.

$\mathbb{Z}(\sqrt{-3}) \subset \mathcal{O} = \mathbb{Z}[\zeta]$ Eisenstein integers.

$N: \mathbb{Z}[\zeta] \longrightarrow \mathbb{Z}$.

$a+b\zeta \longrightarrow (a+b\zeta)(\overline{a+b\zeta})$

$= (a+b\zeta)(a+b\bar{\zeta}) = a^2 + ab(\zeta+\bar{\zeta}) + b^2$.

$= a^2+b^2-ab \geq 0$.

Prop. $\mathbb{Z}[\zeta]$ has Euclidean division algo. ($\Rightarrow$ every ideal of $\mathbb{Z}[\zeta]$ is principal, and $\mathbb{Z}[\zeta]$ has UFT).

Thm. $p \in \mathbb{Z}$ prime. $p > 0$. $p \neq 2, 3$. then $\exists x, y \in \mathbb{Z}$ st.

$p = x^2 + 3y^2 \Leftrightarrow -3$ square mod p.

Pf: Suppose -3 square mod p. $\Rightarrow -3 \equiv z^2 \pmod{p}$. $z \in \mathbb{Z}$.

$\Rightarrow z^2 = (\cdot p - 3$ for $c \in \mathbb{Z}$. consider inside $\mathbb{Z}(\sqrt{-3})$.

$\Rightarrow (z+\sqrt{-3})(z-\sqrt{-3}) = cp$.

$\Rightarrow p \mid (z+\sqrt{-3})(z-\sqrt{-3})$. in $\mathbb{Z}(\sqrt{-3}) \subset \mathbb{Z}[\zeta]$.

$\Rightarrow p \mid (z+\sqrt{-3})(z-\sqrt{-3})$ in $\mathbb{Z}[\zeta]$. Since $\mathbb{Z}[\zeta]$ UFT ring.

we have if p is irred in $\mathbb{Z}[\zeta]$, $\Rightarrow p$ would be prime $\Rightarrow$

$p \mid z+\sqrt{-3}$. or $p \mid z-\sqrt{-3}$. in $\mathbb{Z}[\zeta]$.

but if $p = (z+\sqrt{-3})(a+b\zeta)$. $\Rightarrow$ X. So p is reducible in $\mathbb{Z}[\zeta]$.

$\Rightarrow p = \alpha\beta$. , $\alpha\beta \in \mathbb{Z}[\zeta]$. non units.

$\Rightarrow N(p) = N(\alpha)N(\beta) \Rightarrow N(\alpha) = N(\beta) = p$.

Then $\exists \alpha \in \mathbb{Z}[\zeta]$ st. $N(\alpha) = p$. $N(\alpha) = a^2 + b^2 - ab$. Then let ζ^k be such that $\zeta^k \alpha \in \mathbb{Z}[\sqrt{\zeta}]$.

$p = N(\alpha) = N(\zeta^k \alpha) = x^2 + 3y^2$.