NON-EXAMPLE: $f(x) = 1+3x+2x^2 \in \mathbb{Z}[x]$ has reduction to $\mathbb{F}_2[x]$ given by $\bar{f}(x) = 1+x$, which is irreducible, but of lower degree

And in fact, $f(x) = (1+x)(1+2x)$ is not irreducible in $\mathbb{Q}[x]$.

proof of PROP: Given $f(x) \in \mathbb{Z}[x]$ reducible,

say $f(x) = g(x)h(x)$ with $\deg(g), \deg(h) > 0$ and $\deg(f) = \deg(g)+\deg(h)$

then applying $\mathbb{Z}[x] \to \mathbb{F}_p[x]$ gives

$\bar{f}(x) = \bar{g}(h)\,\bar{h}(x)$ with $\deg(\bar{g})+\deg(\bar{h}) = \deg(\bar{f}) = \deg(f)$ (by hypothesis)

$\deg(g) = \deg(\bar{g})$, $\deg(h) = \deg(\bar{h})$, $\deg(\bar{g}), \deg(\bar{h}) > 0$

i.e. it is a proper factorization in $\mathbb{F}_p[x]$. ∎

REMARK: Unlike factoring in $\mathbb{Z}$, there is a fast algorithm for factoring in $\mathbb{F}_p[x]$, called Berlekamp's algorithm, from 1967.

2/27/2019

Another useful reduction trick:

Eisenstein's Criterion: If $f(x) = a_n x^n + a_{n-1}x^{n-1} + \dots + a_1 x + a_0 \in \mathbb{Z}[x]$ (PROP 12.4.6)

has some prime p in $\mathbb{Z}$ with $p \nmid a_n$,

$p \mid a_0, a_1, \dots, a_{n-1}$,

but $p^2 \nmid a_0$,

then f is irreducible in $\mathbb{Q}[x]$.

EXAMPLE: $x^5 - 24x^3 + 70x^2 - 10x + 6$ is irreducible in $\mathbb{Q}[x]$

using Eisenstein's criterion at $p=2$:

$p \nmid 1 = a_5$

$p \mid 6, -10, 70, -24, 0$
$\quad\;\; = a_0 \;\; a_1 \;\; a_2 \;\; a_3 \;\; a_4$

$p^2 \mid 6$
$\quad = a_0$

Proof of Eisenstein: If $f(x)=g(x)h(x)$ in $\mathbb{Q}[x]$, then this is also true in $\mathbb{Z}[x]$, so reduce $\mathbb{Z}[x] \longrightarrow \mathbb{F}_p[x]$

to give $\bar{f}(x) = \bar{g}(x)\,\bar{h}(x) \Rightarrow \bar{g}(x)=\bar{g}_r x^r$, $\bar{h}(x)=\bar{h}_s x^s$ for some r,s with $r+s=n$

$\bar{f}(x) = \bar{a}_n x^n$

unique factorization in $\mathbb{F}_p[x]$, for example

$$\Rightarrow g(x)=g_r x^r+\dots+g_1x+g_0$$
$$h(x)=h_s x^s+\dots+h_1x+h_0$$

where $g_0, g_1, \dots, g_{r-1}$ and $h_0, h_1, \dots, h_{s-1}$ $\Big\} \in p\mathbb{Z}$

$\Rightarrow a_0 = g_0h_0 \in p^2\mathbb{Z}$. Contradiction ∎

---

§12.5 Primes in $\mathbb{Z}[i]$ and solving $x^2+y^2=n$

It turns out that understanding the primes (= irreducibles) in $\mathbb{Z}[i]$ comes down to knowing primes p in $\mathbb{Z}$ and which ones stay prime in $\mathbb{Z}[i]$, versus factoring further $p=\pi\cdot\bar{\pi}$ in $\mathbb{Z}[i]$

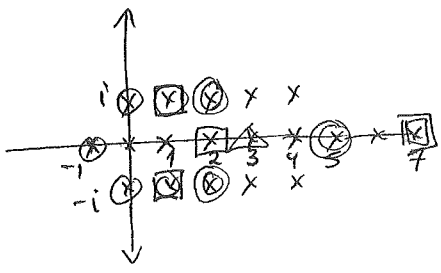
e.g. $2 = (1+i)(1-i)$ $(=(i-1)(-i-1))$ not prime in $\mathbb{Z}[i]$

3 is prime in $\mathbb{Z}[i]$

$5 = (2+i)(2-i)$ not prime in $\mathbb{Z}[i]$

7 is prime in $\mathbb{Z}[i]$

⋮



PROPOSITION:

(a) $\pi = a+bi$ is prime in $\mathbb{Z}[i]$

$\iff$ $\bar{\pi} = a-bi$ is prime

(b) For π prime in $\mathbb{Z}[i]$, $\|\pi\|^2 = \pi\bar{\pi}$ is either a prime p in $\mathbb{Z}$ (for a prime p in $\mathbb{Z}$ that is not prime in $\mathbb{Z}[i]$)

or a prime squared p^2 in $\mathbb{Z}$

(for a prime p that is associate to π, hence stays prime in $\mathbb{Z}[i]$)

(c) Conversely, every prime p in $\mathbb{Z}$

either stays prime in $\mathbb{Z}[i]$,

or factors $p = \pi\bar{\pi}$ for some prime π in $\mathbb{Z}[i]$,

with the latter occurring $\iff$ $p = a^2+b^2$ for some $a,b \in \mathbb{Z}$ $(=(a+bi)(a-bi))$

proof: (a): If $\pi = \alpha\beta$ is a proper factorization in $\mathbb{Z}[i]$

then $\bar{\pi} = \bar{\alpha}\cdot\bar{\beta}$ is a proper factorization (since units $\mathbb{Z}[i]^\times = \{\pm 1, \pm i\}$ are closed under conjugation)

(b): Given $\pi = a+bi$ prime,

$$\|\pi\|^2 = \pi\bar{\pi} = (a+bi)(a-bi) = a^2+b^2 \in \mathbb{Z}$$

so factor it in $\mathbb{Z}$, giving $\pi\bar{\pi} = p_1 p_2 \cdots p_r$ for some primes $p_i \in \mathbb{Z}$

Then factor the p_i in $\mathbb{Z}[i]$, giving

$$\pi\bar{\pi} = \alpha_1\alpha_2 \cdots\cdots \alpha_s \text{ for some primes } \alpha_i \in \mathbb{Z}[i]$$

Uniqueness of factorization forces $s=2$, so either

- $r=1$ and $\pi\bar{\pi} = p_1 = p$ for some prime $p \in \mathbb{Z}$ that is not prime in $\mathbb{Z}[i]$

or

- $r=2$ and $\pi\bar{\pi} = p_1 p_2$, where π is associate to p_1 ($\pi = \pm p_1$ or $\pm i p_1$) (by reindexing)

and then $\pi\bar{\pi} = p_1^2 = p^2$, where p is prime in $\mathbb{Z}[i]$ since it is associate to π.

(c): Given a prime p in $\mathbb{Z}$,

factor it in $\mathbb{Z}[i]$ as $p = \pi_1 \pi_2 \cdots \pi_r$ for primes π_i in $\mathbb{Z}[i]$

But then $p = \bar{p} = \bar{\pi}_1 \bar{\pi}_2 \cdots \bar{\pi}_r$ forces (via uniqueness of factorization) that one can relabel this

$$p = \underbrace{(\pi_1 \cdot \bar{\pi}_1)}_{\in\{2,3,\ldots\}} \underbrace{(\pi_2 \cdot \bar{\pi}_2)}_{\in\{2,3,\ldots\}} \cdots \underbrace{(\pi_k \cdot \bar{\pi}_k)}_{\in\{2,3,\ldots\}} \cdot \underbrace{\pi_{k+1}}_{=\bar{\pi}_{k+1}} \cdot \cdots \cdot \underbrace{\pi_\ell}_{=\bar{\pi}_\ell}$$

$$\in\{2,3,\ldots\} \qquad \in\{2,3,\ldots\}$$

p prime in $\mathbb{Z}$ $\Rightarrow$ either $p = \pi_1 \cdot \bar{\pi}_1$, not prime in $\mathbb{Z}[i]$

or $p = \pi_1 = \bar{\pi}_1$, prime in $\mathbb{Z}[i]$. ∎

So why did 2, 5 factor further, but 3, 7 did not?

THEOREM: (12.5.3) T.F.A.E. for a prime p in $\mathbb{Z}$:

(a) p factors further as $p = \pi\bar{\pi}$ in $\mathbb{Z}[i]$ (so $p = a^2+b^2$ with $a,b \in \mathbb{Z}$ where $\pi = a+bi$)

(b) $\mathbb{Z}[i]/(p)$ is not a field

(c) $\mathbb{F}_p[x]/(x^2+1)$ is not a field

(d) $x^2 = -1$ has a solution in $\mathbb{F}_p$

EXAMPLES: $2 = (1+i)(1-i)$

(e) $p = 2$ or $p \equiv 1 \bmod 4$

Proof: (a) $\Leftrightarrow$ (b): $\mathbb{Z}[i]$ is a P.I.D., so $\mathbb{Z}[i]/(p)$ is a field

$\Leftrightarrow$ (p) is maximal

$\Leftrightarrow$ p is irreducible/prime

$\Leftrightarrow$ p does not factor further.

(b) $\Leftrightarrow$ (c): Check that the rings $\mathbb{Z}[i]/(p)$, $\mathbb{F}_p[x]/(x^2+1)$ are isomorphic, as both are isomorphic to $\mathbb{Z}[x]/(p, x^2+1)$:

one can check $\mathbb{Z}[x] \xrightarrow{\varphi_1} \mathbb{Z}[i]/(p)$

$x \longmapsto i + (p) =: \bar{i}$

and $\mathbb{Z}[x] \xrightarrow{\varphi_2} \mathbb{F}_p[x]/(x^2+1)$

$x \longmapsto \bar{x}$

both are surjective and have $\ker(\varphi_1) = \ker(\varphi_2) = (p, x^2+1) \subset \mathbb{Z}[x]$.

[This is an instance of using Noether's 3rd isomorphism theorem: For ideals $I, J \subset R$

$R/I+J \cong (R/I)/\bar{J}$

and $R/I+J \cong (R/J)/\bar{I}$ ← so these two rings must be isomorphic

Above $R = \mathbb{Z}[x]$, $I = (p)$, $J = (x^2+1)$, $I+J = (p, x^2+1)$]

2/29/2019 >

(c) $\Leftrightarrow$ (d): $\mathbb{F}_p[x]/(x^2+1)$ is a field

$\Leftrightarrow (x^2+1)$ is maximal in $\mathbb{F}_p[x]$

$\Leftrightarrow x^2+1$ is irreducible in $\mathbb{F}_p[x]$

$\Leftrightarrow x^2+1 = 0$ has no roots $x \in \mathbb{F}_p$

$\Leftrightarrow x^2 = -1$ has no solution $x \in \mathbb{F}_p$

(d) $\Leftrightarrow$ (e): $x^2 = -1$ has a solution in $\mathbb{F}_2$, namely $x = \bar{1}$ ($\mathbb{F}_2 = \{\bar{0}, \bar{1}\}$)

For odd prime p, where $-\bar{1} \neq +\bar{1}$ in $\mathbb{F}_p$, then $\bar{x}^2 = -\bar{1} \Rightarrow \bar{x}^4 = +\bar{1}$

so $\bar{x}$ is an element of $\mathbb{F}_p^\times$ of order exactly 4. Since $\mathbb{F}_p^\times$ is cyclic, such an $\bar{x}$ exists $\Leftrightarrow$ 4 divides $|\mathbb{F}_p^\times| = p-1 \Leftrightarrow p \equiv 1 \bmod 4$ ∎