

How to determine  $f(x)$  irreducible or not  
in  $\mathbb{Q}[\bar{x}]$ ?

Useful facts:

①  $f(x) = \underbrace{c f_0(x)}_{\in \mathbb{Z}[\bar{x}] \text{ primitive}}$   
 $f_0(x)$  irreducible in  $\mathbb{Z}[\bar{x}]$   
 $\Leftrightarrow f_0(x)$  irreducible in  $\mathbb{F}_p[\bar{x}]$ .

②  $\Upsilon_p: \mathbb{Z}[\bar{x}] \rightarrow \mathbb{F}_p[\bar{x}]$

Prop:  $f(x) \in \mathbb{Z}[\bar{x}]$ ,

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_0.$$

$p \nmid a_n$ . If  $\Upsilon_p(f(x)) = \bar{f}(x)$  is  
irreducible in  $\mathbb{F}_p[\bar{x}]$ , then

$f(x)$  is irreducible in  $\mathbb{Q}[\bar{x}]$ .

Pf: Assume  $f(x)$  is reducible.

$$\text{then } f(x) = g(x) \cdot h(x).$$

with  $g, h \in \mathbb{Z}[x]$ , and

$$\deg g \geq 1, \quad \deg h \geq 1.$$

$$\bar{f} = \bar{g} \cdot \bar{h}, \quad \deg \bar{f} = n \quad (\neq 0)$$

$$\Rightarrow \deg \bar{g} + \deg \bar{h} = n$$

$$\deg g + \deg h = n.$$

$$\deg \bar{g} \leq \deg g, \quad \deg \bar{h} \leq \deg h.$$

$$\text{so } \deg \bar{g} = \deg g, \quad \deg \bar{h} = \deg h \\ \geq 1 \qquad \qquad \qquad \geq 1.$$

so  $\bar{f} = \bar{g} \bar{h}$  is a proper factorization.

$\bar{g}$  is a proper divisor of  $\bar{f}$ .

(contradiction with  $\bar{f}$  being irreducible.)

Ex:  $f(x) = x^3 + x + 1$ .

$\bar{f}(x)$  is irreducible in  $\mathbb{F}_2[x]$ .

How to find irreducible polynomials  
in  $\mathbb{F}_p[x]$  ...

List all of them. (Sieve method)

$\mathbb{F}_2[x]$ .

deg 1.  $x, x+1$

deg 2.  ~~$x^2$~~ ,  ~~$x^2+1$~~ ,  $x^2+x+1$ .

deg 3.  ~~$x^3$~~ ,  ~~$x^3+1$~~ ,  $x^3+x+1$ ,

~~$x^3+x$~~ ,  ~~$x^3+x^2+x+1$~~ .

$x^3+x^2+1$ ,  ~~$x^3+x^2$~~ ,  ~~$x^3+x^2+x$~~ .

deg 4. . . .

Key point to use the proposition:

Select the correct prime  $p$ .

Eisenstein criterion:

$f(x) \in \mathbb{Z}[x]$  primitive.

①  $p \nmid a_n$

②  $p \mid a_i, \quad i = n-1, \dots, 1, 0$

③  $p^2 \nmid a_0$

Then  $f(x)$  is irreducible.

Pf: Assume  $f(x) = g(x) \cdot h(x)$

$$\bar{f}(x) = a_n x^n = \bar{g}(x) \cdot \bar{h}(x)$$

then  $\bar{g}(x) = c \cdot x^m$

$$\bar{h}(x) = d x^{n-m}$$

$$\text{So } g(x) = (x^{m_1} \dots + c_0$$

$$h(x) = d x^{n-m_1} \dots d_0.$$

$$p \mid c_0, \quad p \mid d_0.$$

$$\text{So } p^2 \mid a_0 = c_0 d_0.$$

Contradiction!

$$\text{Ex: } f(x) = x^5 + 20x^4 + 5x^3 + 15.$$

$$\text{choose } p = 5$$

Ex: (cyclotomic polynomial)

$$\Phi_p(x) = x^{p-1} + x^{p-2} + \dots + 1.$$

$$= \frac{x^p - 1}{x - 1} \quad \text{is irreducible.}$$

$$\Phi_p(x) \cdot (x-1) = x^p - 1$$

change of variable

$$y = x - 1$$

$$\mathbb{F}_p(y+1) \cdot y = (y+1)^p - 1$$

$$= y^p + \binom{p}{1} y^{p-1} + \dots + \binom{p}{i} y^{p-i} + py$$

$$\mathbb{F}_p(y+1) = y^{p-1} + p y^{p-2} + \dots + \binom{p}{i} y^{p-i-1}$$

Also

$$p \mid \binom{p}{i} \text{ for } 1 \leq i \leq p-1.$$

$$\text{because } \binom{p}{i} = \frac{p(p-1) \dots (p-i+1)}{i \cdot (i-1) \dots 1}$$

$$\binom{p}{i} \cdot i \cdot (i-1) \dots 1 = p(p-1) \dots (p-i+1)$$

$$p \nmid i, \quad p \nmid i-1, \quad \dots$$

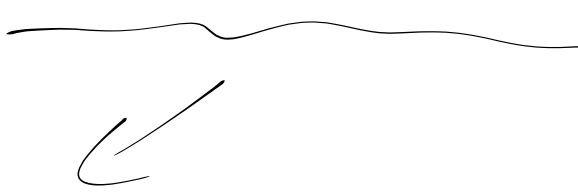
so  $\mathcal{P} \mid (P_i)$

Apply Eisenstein criterion  $\Rightarrow$

$\mathcal{P}_p(y+1)$  is irreducible.

The proof also helps you to do  
factorization in  $\mathbb{Z}[x]$ .

$$f(x) = g(x) \cdot h(x) \Rightarrow \bar{f}(x) = \bar{g}(x) \cdot \bar{h}(x),$$

  
This gives some hint  
how to find  $g(x), h(x)$

Gauss primes:

Q: When is  $p$  prime in  $\mathbb{Z}$ . equal to sum of two squares?

$$p = m^2 + n^2 \quad (p \text{ odd prime})$$

Prop:  $p$  is sum of two squares iff

$p$  is reducible in  $\mathbb{Z}[i]$ .

pf: 
$$p = m^2 + n^2$$

$$\Rightarrow p = (m+ni)(m-ni)$$

$$m, n \neq 0$$

If 
$$p = (a+bi)(c+di)$$

$$p^2 = (a^2+b^2)(c^2+d^2)$$

$$\Rightarrow a^2+b^2 = 1, p, p^2$$

But  $a+bi, c+di$  are not units.



$$\text{So } a^2 + b^2 = p$$

Prop:  $p$  is a prime element in  $\mathbb{Z}(i)$

$$\Leftrightarrow p \equiv 3 \pmod{4}$$

Pf:  $p$  is not a prime  $(\Rightarrow)$

$$p \equiv 1 \pmod{4} \quad \therefore$$

$p$  is not a prime  $(\Rightarrow)$

$\mathbb{Z}(i)/(p)$  is not a field.

$$\begin{aligned} \mathbb{Z}(i)/(p) &= \mathbb{Z}(x)/(x^2+1, p) \\ &= \mathbb{F}_p(x)/(x^2+1) \end{aligned}$$

So  $\mathbb{Z}(i)/(p)$  is not a field

$(\Rightarrow) x^2+1$  has a root in  $\mathbb{F}_p$

If  $p \equiv 1 \pmod{4}$ , then

$(\mathbb{F}_p)^\times \cong (\mathbb{Z}/(p-1)\mathbb{Z})$  has

a subgroup  $\cong \mathbb{Z}/4\mathbb{Z}$

choose  $x \in \mathbb{Z}/4\mathbb{Z}$  as a generator

$$x^4 = 1, \quad x \neq 1, \quad x^2 \neq 1, \quad x^3 \neq 1$$

$$x^4 - 1 = (x^2 + 1)(x^2 - 1) = (x^2 + 1)(x+1)(x-1)$$

$$1 = x^2 + 1 = 0, \quad x^2 = -1$$

If  $\exists x \in \mathbb{F}_p$ ,  $x^2 = -1$ ,

then  $x \neq 1$ ,  $x^2 \neq 1$ ,  $x^3 = -x \neq 1$ ,

$$x^4 = 1.$$

$\langle x \rangle$  has order 4, so  $4 \mid p-1$

Conclusion:  $p = m^2 + n^2$  has solutions

$$m, n \in \mathbb{Z} \text{ iff}$$

$$p \equiv 1 \pmod{4}.$$