

$$\text{So } (a_j) = (a_{j+1}) = \dots$$

Non UFD.

$$\mathbb{Z}[\sqrt{-5}]$$

$$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$$

$2, 3, 1 + \sqrt{-5}, 1 - \sqrt{-5}$ are all irreducible.

$$\text{If } (a + b\sqrt{-5})(c + d\sqrt{-5}) = 2$$

$$\begin{cases} ac - 5bd = 2 \\ ad + bc = 0 \end{cases} \quad \text{hard to solve}$$

Instead

$$|a + b\sqrt{-5}|^2 |c + d\sqrt{-5}|^2 = 4$$

$$(a^2 + 5b^2)(c^2 + 5d^2) = 4$$

$$\Rightarrow a^2 + 5b^2 = 1, 2, 4 \text{ has to be } 1$$

$$(a + b\sqrt{-5})(c + d\sqrt{-5}) = 1 + \sqrt{-5}.$$

$$(a^2 + 5b^2)(c^2 + 5d^2) = 6.$$

$$a^2 + 5b^2 = 1, 2, 3, 6$$

$$c^2 + 5d^2 = 1, 6.$$

The units in $\mathbb{Z}[\sqrt{-5}]$ are ± 1 .

(Similar method by taking $1 \cdot 1$)

Application.

$$\text{GCD: } d \mid a, \quad d \mid b.$$

if $e \mid a, e \mid b$, then
 $e \mid d$.

$$a = p_1 \cdots p_m$$

$$b = q_1 \cdots q_n.$$

compare $p_1 \cdots p_m$
 $q_1 \cdots q_n$.

a, b coprime if $\text{GCD}(a, b) = 1$.

Fermat's Last theorem:

$$x^n + y^n = z^n \quad xy z \neq 0$$

has no integer solutions.

Polynomial version:

$$f^n + g^n = h^n$$

has no solution in $\mathbb{Q}[t]$ such that

$$\text{g.c.d}(f, g) = 1, \quad \deg f \geq 1.$$

Pf: Assume there is solution

$$(f, g, h).$$

Choose (f, g, h) such that

$\deg f + \deg g + \deg h$ achieves minimum

$$f^n = \prod_{k=0}^{n-1} (h - \zeta_k g)$$

$$\zeta_k = e^{\frac{2\pi i}{n} \cdot k}$$

$$\text{g.c.d.}(h, g) = 1 \Rightarrow$$

$$\text{g.c.d.}(h - \zeta_k g, h - \zeta_l g) = 1$$

for $k \neq l$

(why! h, g can be represented by $h - \zeta_k g$ and $h - \zeta_l g$.

$$\text{Let } H = h - \zeta_k g$$

$$G = h - \zeta_l g$$

$$h = \frac{\zeta_l H - \zeta_k G}{\zeta_l - \zeta_k}$$

$$g = \frac{H - G}{\zeta_l - \zeta_k}$$

From UFD.

$$h - \xi_i g = (x_i(t))^n.$$

$n \geq$

$$\begin{aligned} h - g &= x(t)^n \\ h - \xi_1 g &= y(t)^n \\ h - \xi_2 g &= z(t)^n. \end{aligned} \quad \left. \begin{array}{l} \\ \\ \end{array} \right\} \Rightarrow \text{solve for } g$$

\Rightarrow after absorbing constants to the n -th power.

$$x(t)^n + y(t)^n = z(t)^n.$$

with lower degrees.