$\mathbb{Z}[i] = \mathbb{Z}[\sqrt{-1}]$

$=$ all of the complex numbers

$a+bi$ such that $a, b \in \mathbb{Z}$.

(Gaussian integers).

E.g. $(1+2i)(3+4i) = 3 + 6i + 4i + \overset{-8}{\overset{\parallel}{8i^2}}$

$= -5 + 10i.$

$\mathbb{Z}[i]$ is a ring.

Can do modular arithmetic!

Mod 3 $(1+2i)(i) = -2 + i \equiv 1 + i \mod 3$

$\mathbb{Z}[i]/(3)$ is just congruence classes mod 3 in $\mathbb{Z}[i]$

elements are represented by

$a + bi \quad a, b \in \mathbb{Z}/3\mathbb{Z}$.

Exercise 3 - (1)

Write out multiplication tables for

$$\mathbb{F}_3[x]/(x^2+1) \quad \text{and} \quad \mathbb{Z}[i]/(3)$$

$a + bx$ $\qquad$ $a, b \in \mathbb{Z}/3\mathbb{Z} = \mathbb{F}_3$ $\qquad$ $a + bi$

$\mathbb{F}_3[x]/(x^2+1)$ $\quad a+bx \quad a,b\in\mathbb{F}_3$

	0	1	2	x	$2x$	$1+x$	$1+2x$	$2+x$	$2+2x$
0	0	0	0	0	0	0	0	0	0
1	0	1	2	x	$2x$	$1+x$	$1+2x$	$2+x$	$2+2x$
2	0	2	1	$2x$	x	$2+2x$	$2+x$	$1+2x$	$1+x$
x	0	x							
$2x$	0	$2x$							
$1+x$	0	$1+x$				$(1+x)(1+x)$ $=1+2x+x^2$ $=2x$			
$1+2x$	0	$1+2x$							
$2+x$	0	$2+x$							
$2+2x$	0	$2+2x$							

$\mathbb{Z}/(n) = \mathbb{Z}/n\mathbb{Z}$ means integers modulo n

$0, 1, 2, \ldots, n-1$ $\leftarrow$ standard representatives

add / multiply in $\mathbb{Z}$, but then <u>shift back</u> by a multiple of n to land in $0, \ldots, n-1$.

$\hookrightarrow$ divide by n and take the remainder

In $\mathbb{Z}/5\mathbb{Z}$

$$3 \cdot 4 = 12 \overset{\text{shift back}}{\rightsquigarrow} 2 \qquad 12 = 5 \cdot 2 + \underline{\underline{2}}$$

$\mathbb{K}[x] / (x^3 + x^2 + x + 1)$.

Standard reps = polynomial of degree ≤ 2.

E.g. $x^4 \equiv r(x) \mod x^3 + x^2 + X + 1$

$$\underline{x^4} = q(x)(x^3+x^2+x+1) + \underline{r(x)}$$

Compute using polynomial long division.

$\mathbb{F}_3[x]/_{x^2+1}$

Representatives = all polynomials of degree ≤ 1

$\mathbb{F}_3 = 0, 1, 2.$ $\quad a + bx \quad a, b \in \mathbb{F}_3$

$0 = 0 + 0x$	$1 = 1 + 0x$	$2 = 2 + 0x$
$x = 0 + 1x$	$1 + x$	$2 + x$
$2x = 0 + 2x$	$1 + 2x.$	$2 + 2x.$

$(1+2x)(2+2x)$ $\rightsquigarrow$ first multiply in $\mathbb{F}_3[x]$,

then shift by

$(1+2x)(2+2x)$

$= (1\cdot 2) + (2x\cdot 2) + (2x)(2x) + 1(2x)$

$= 2 + x + x^2 + 2x$

$= 2 + x^2$ ⟵ product in $\mathbb{F}_3[x]$

need to shift by multiple of x^2+1 to get degree ≤ 1.

subtract x^2+1

$= \boxed{1}$ ⟵ Answer in $\mathbb{F}_3[x]/(x^2+1)$

a multiple of x^2+1 to get something of degree ≤ 1.

||

Take the remainder when we divide by x^2+1.

(Could do multiplication in $\mathbb{Z}[x]$
then reduce mod 3
then mod x^2+1.)