

(3) Find the mult inverse of $2+5i$ in

(4) similar. Study these. $\mathbb{Z}[i]/(31)$.

Recall: How to compute $\frac{1}{2+5i}$ in $\mathbb{C}$.

Get rid of i in the denominator!

$$\frac{1}{2+5i} = \frac{(2-5i)}{(2-5i)} \cdot \frac{1}{2+5i} = \frac{2-5i}{29}$$

$$= \frac{2}{29} + \frac{-5}{29}i$$

Can do the same in $\mathbb{Z}[i]_{(7)}$

$$\frac{1}{2+5i} = \frac{(2-5i)}{(2-5i)} \cdot \frac{1}{2+5i} = \frac{2-5i}{29}$$

$$= \frac{2}{29} + \frac{-5}{29}i$$

$$\frac{2}{29} \text{ in } \mathbb{Z}_{31\mathbb{Z}} \quad \frac{-5}{29}i \text{ in } \mathbb{Z}_{31\mathbb{Z}}$$

So compute $\frac{1}{29}$ in $\mathbb{Z}/31\mathbb{Z}$ then simplify.

Get $\frac{1}{29} = 15 \pmod{31}$.

$$\frac{1}{2+5i} = \frac{2}{29} + \frac{-5}{29}i$$

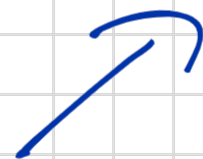
$$= \underline{15} \cdot 2 + 15 \cdot (-5)i$$

$$= 30 + 18i.$$

To find mult. inverse of $a+b\sqrt{D}$

in $\mathbb{Z}[\sqrt{D}]/(n)$
if it exists.

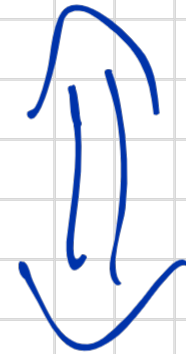
$$\frac{1}{a+b\sqrt{D}} = \frac{a-b\sqrt{D}}{a^2-b^2D} = \frac{a}{a^2-b^2D} + \frac{-b}{a^2-b^2D}\sqrt{D}$$



Can compute this as long as
 $\gcd(a^2-b^2D, n) = 1.$

(5) and (6) $\sim \exists a + b\sqrt{D}$ a quadratic integer?

$$\underline{a, b \in \mathbb{Q}}$$



$$x^2 - 2ax + a^2 - b^2D$$

has integer coefficients

i.e. $2a$ is an integer and $a^2 - b^2D$ is an integer.

(5) Is $\frac{1+\sqrt{5}}{2}$ a quadratic integer?

"
 $\frac{1}{2} + \frac{1}{2}\sqrt{5}$
 $a = \frac{1}{2} \quad b = \frac{1}{2} \quad D = 5$

$$2a = 2 \cdot \frac{1}{2} = 1 \quad \checkmark$$

$$\underline{a^2 - b^2 D} = \frac{1}{4} - \frac{5}{4} = -1 \quad \checkmark$$

Should know how to check, but
don't need to be able to do (b).

$$\frac{1}{29} \equiv 15 \pmod{31} \quad \text{just means}$$

15 is the mult.

inverse of 29 mod 31,

Euclidean alg + unram-cl.

$$31 = 29 \cdot 1 + 2$$

$$1 = 29 - 14 \cdot (2)$$

$$29 = 14 \cdot 2 + 1, \nearrow$$

$$1 = 29 - 14(31 - 1 \cdot 29)$$

$$1 = 15 \cdot 29 - 14 \cdot 31$$

$$\text{so} \quad 1 \equiv 15 \cdot 29 \pmod{31}$$

so 15 is the mult. inverse of 29 mod 31.