

1. Let  $\omega \in \mathbb{C}$  satisfy  $\omega^2 - p\omega + q = 0$  where  $p$  and  $q$  are integers such that  $p^2 - 4q$  is not the square of an integer. The *norm* of  $a + b\omega \in \mathbb{Z}[\omega]$  is

$$N(a + b\omega) := (a + b\omega)(a + b\bar{\omega}) := (a + b\omega)(a + b(p - \omega)).$$

It was shown in class that if  $(a, b) = 1$  then the natural map is an isomorphism

$$\mathbb{Z}/(N(a + b\omega))\mathbb{Z} \xrightarrow{\sim} \mathbb{Z}[\omega]/(a + b\omega)\mathbb{Z}[\omega].$$

Prove that for *any*  $a, b \in \mathbb{Z}$ ,  $|N(a + b\omega)|$  is the cardinality of  $\mathbb{Z}[\omega]/(a + b\omega)\mathbb{Z}[\omega]$ .

Hint. Multiplication by  $a + b\omega$  gives a group isomorphism

$$\mathbb{Z} \oplus \mathbb{Z} \cong \mathbb{Z}[\omega] \xrightarrow{\sim} (a + b\omega)\mathbb{Z}[\omega].$$

Use this to reduce the problem to where  $(a, b) = 1$ .

2. Assume that  $\mathbb{Z}[\omega]$  (as in 1.) is a UFD. Let  $\pi$  be a  $\mathbb{Z}$ -prime. Suppose there are integers  $a$  and  $b$ , not both divisible by  $\pi$ , such that  $\pi$  divides  $a^2 + pab + qb^2$ . Show that there are integers  $c$  and  $d$  such that  $\pi = \pm(c^2 + pcd + qd^2)$ . Deduce from this that if  $e = 1$  or  $e = 2$ , then  $\pi$  is of the form  $x^2 + ey^2 \iff -e$  is a square in  $\mathbb{Z}/\pi$ .

3. Let  $\omega \neq -1$  be a complex number satisfying  $\omega^3 = -1$ . We showed in class that  $\mathbb{Z}[\omega]$  is a Euclidean domain. HW6 #2 gives that  $\omega$  generates the group of units in  $\mathbb{Z}[\omega]$ .

(a) Let  $p > 3$  be an odd prime in  $\mathbb{Z}$ . Show that:

$$p \equiv 1 \pmod{6} \iff -1 \text{ has three cube roots in } \mathbb{Z}/p \iff -3 \text{ is a square in } \mathbb{Z}/p.$$

(b) Prove that every prime  $p > 0$  in  $\mathbb{Z}$  of the form  $p = 6n + 1$  can be represented in the form  $p = a^2 + ab + b^2$  ( $a > b > 0$ ) in *one and only one* way.

(c) Prove that every prime  $p > 0$  in  $\mathbb{Z}$  of the form  $p = 6n + 1$  can be represented in the form  $p = a^2 + 3b^2$  ( $a, b > 0$ ) in *one and only one* way.

(d) Prove that every *odd* prime  $p$  in  $\mathbb{Z}$  factors into primes in  $\mathbb{Z}[\sqrt{-3}]$ . What about  $p = 2$ ?

(OVER)

### Extra Credit Problem.

4. (a) Let  $F$  be a field in which  $2 \neq 0$ . Show that  $F$  has an element of multiplicative order 8 if and only if both  $-1$  and  $2$  are squares in  $F$ .

(b) (Stated by Fermat about 350 years ago; first published proof by Euler over 100 years later.) Prove that every prime  $p > 0$  in  $\mathbf{Z}$  of the form  $p = 8n + 1$  can be represented in the form  $p = a^2 + 2b^2$  ( $a > 0, b > 0$ ). How many such representations are possible for a given  $p$ ?

(c) Repeat problem (b) for  $p = 8n + 3$ .

You will need that  $2$  is not a square in  $\mathbf{Z}/p$ . Here is a sketch of one way to see this:

Let  $F$  be any finite field, of odd cardinality  $q$  ( $\Rightarrow 2 \neq 0$  in  $F$ ).

Let  $S \subset F$  be the set of all  $x$  such that  $x$  and  $x + 1$  are both nonzero squares, and let  $s$  be the cardinality of  $S$ .

- i) Show that  $x \in S \Leftrightarrow 1/x \in S$ ; and deduce that  $s$  is odd iff  $2$  is a square in  $F$ .
- ii) Show that  $\sigma \mapsto (\sigma + \sigma^{-1} - 2)/4$  is a two-to-one map from the set  $\Sigma$  of all squares  $\sigma \neq 0, 1, -1$  in  $F$  onto  $S$ .
- iii) The cardinality of  $\Sigma$  is  $\frac{q-3}{2}$  if  $-1$  is not a square, and  $\frac{q-5}{2}$  otherwise. (Why?)
- iv) Deduce that  $2$  is a square in  $F \iff q \equiv \pm 1 \pmod{8}$ .