

392 HOMEWORK 8 SOLUTIONS

Section 4.3: 1(a)(b), 2(a)(b), 5, 8, 10(a)(b) (When you've done question 10, you should know which out of the Gaussian integers  $1 + i$  and  $3 + i$  is irreducible in  $\mathbb{Z}[i]$  ...).

- 1(a) Find  $GCD(8 + 6i, 5 - 15i)$ .

*Solution. Euclidean algorithm.*

$$5 - 15i = (8 + 6i)(-1 - i) + 7 - i$$

$$8 + 6i = (7 - i)(1 + i) + 0$$

*Hence the GCD is  $7 - i$ .*

- 1(b) Find  $GCD(4 - i, 1 + i)$ .

*Solution. Euclidean algorithm.*

$$4 - i = (1 + i)(1 - 2i) + 1$$

*Hence GCD is 1.*

- 2(a) Factor 6 into irreducibles.

*Solution. Clearly  $6 = 2 \cdot 3 = (1+i)(1-i)3$ . Now  $1 \pm i$  are irreducible as their  $\phi$  is 2 which is prime. Also 3 is irreducible as we know primes congruent to 3 mod 4 are irreducible in  $\mathbb{Z}[i]$  by the results in section 4.3 in the book.*

- 2(b) Factor  $11 + 7i$  into irreducibles.

*Solution. Note  $\phi(11+7i) = 170 = 17 \cdot 2 \cdot 5$ . So if  $11+7i$  factors one of the factors must have  $\phi$  equal to 17, 2 or 5. The only Gaussian integers with those  $\phi$ 's are  $\pm 4 \pm i, \pm 1 \pm 4i, \pm 1 \pm i, \pm 1 \pm 2i, \pm 2 \pm i$ . Since we only care up to a unit and the units are  $\pm 1, \pm i$  we only need to consider  $4 + i, 1 + 4i, 1 + i, 1 + 2i$  and  $2 + i$ . Moreover all these ARE irreducibles since their  $\phi$  is prime.*

*Now search through these to find which ones really do divide  $11+7i$  in  $\mathbb{Z}[i]$ . You find*

$$11 + 7i = -i(1 + i)(4 + i)(1 + 2i).$$

*This is its factorization into irreducibles (note  $-i$  is a unit). People might get various other answers which are equivalent to this one on distributing the units  $\pm 1, \pm i$  in different ways!!!*

- 5 Suppose  $GCD(a, b) = 1$  and  $a^2 + b^2$  is odd. Show that  $GCD(a + ib, a - ib) = 1$ .

*Solution. Suppose  $GCD(a + ib, a - ib) = u + iv$ . So  $u + iv | a + ib$  and  $u + iv | a - ib$ . Hence,  $u + iv | 2a$  and  $u + iv | 2b$  (adding or taking the difference). We know that if  $z | w$  then  $\phi(z) | \phi(w)$  so this shows that  $u^2 + v^2 | 4a^2$  and  $u^2 + v^2 | 4b^2$ . Since  $GCD(4a^2, 4b^2) = 4$  this shows that  $u^2 + v^2 | 4$ , i.e.  $u^2 + v^2 = 1, 2$  or  $4$ . Also  $u + iv | a + ib$  so  $u^2 + v^2 | a^2 + b^2$ . Since that is odd,  $u^2 + v^2$  is odd. Hence,  $u^2 + v^2 = 1$  which shows that  $u + iv$  is a unit. So  $GCD(a + ib, a - ib) = 1$ .*

- 8 Prove or give a counterexample: if  $p \equiv 1 \pmod{4}$  then  $p$  can be written uniquely as a sum of two squares.

*Solution.* It depends a little how you interpret the question. If  $p$  is merely an odd number then it cannot be true, for instance  $25 = 0^2 + 5^2 = 4^2 + 3^2$ .

However if  $p$  is meant to be prime too, then it is true. For suppose  $p$  is a prime  $\equiv 1 \pmod{4}$  and that  $p = a^2 + b^2 = c^2 + d^2$  is written as a sum of two squares in two different ways. Then,  $p = (a + ib)(a - ib) = (c + id)(c - id)$  are factorizations of  $p$  into irreducibles in the Gaussian integers. By the uniqueness of factorization, it means that  $c + id = (a + ib)$  times a unit. Hence  $c = a, d = b$  or  $c = b, d = a$ . That is the pairs  $(a, b)$  and  $(c, d)$  are THE SAME if you allow reordering them.

10(a) Show  $\mathbb{Z}[i]/(1 + i) \cong \mathbb{Z}_2$ .

*Solution.* We need to find our favorite names for the equivalence classes under the relation  $a \equiv b \pmod{(1 + i)}$  if  $(1 + i)|(a - b)$  in  $\mathbb{Z}[i]$ . Given any Gaussian integer  $x + iy$  we can subtract  $y$  times  $(1 + i)$  to reduce it just to an ordinary integer. Then we can subtract an integer multiple of  $(1 - i)(1 + i) = 2$  to reduce it to either 0 or 1. Hence there are just two equivalence classes  $\bar{0}$  and  $\bar{1}$ . So the ring must be  $\mathbb{Z}_2$ , since it is the only ring with two elements.

10(b) Show  $\mathbb{Z}[i]/(3 + i) \cong \mathbb{Z}_{10}$ .

*Solution.* Finding favorite names like in (a) we reduce things to just integers modulo  $3 + i$  then subtracting a multiple of  $(3 + i)(3 - i) = 10$  we reduce to the numbers  $0, 1, 2, \dots, 9$ . These are not congruent mod  $3 + i$ , so our favorite names for the elements are simply  $\bar{0}, \bar{1}, \dots, \bar{9}$ . Clearly the arithmetic amongst these is the same as in the ring  $\mathbb{Z}_{10}$  so we're done.