

16.3 Prove Theorem 16.3. You can follow the outline below.

1. First observe that  $r\bar{r}$  is a factorization of  $N(r)$  in  $\mathbb{Z}[i]$  as a product of Gaussian integers. Use the unique factorization theorem to deduce that every factorization of  $N(r)$  in  $\mathbb{Z}[i]$  as a product of irreducible Gaussian integers has two factors.

$$\text{For } r = a + bi, N(r) = (a + bi)(a - bi) = r\bar{r}$$

So for any  $r \in \mathbb{Z}[i]$  of the form  $a + bi$ , it has conjugate  $\bar{r} = a - bi$ , such that  $N(r) = r\bar{r}$

That is,  $N(r)$  is the product of irreducible Gaussian integers and has two factors

2. Observe that since  $r$  is not 0 or a unit in  $\mathbb{Z}[i]$ , its norm  $N(r)$  is an integer greater than 1. Introduce notation for a prime factorization of  $N(r)$  in  $\mathbb{Z}$ , say  $N(r) = p_1 \cdots p_t$ . Be aware that the primes  $p_j$  may or may not be irreducible in  $\mathbb{Z}[i]$ ; nothing is assumed about this. (Recall as an example that 2 is prime in  $\mathbb{Z}$ , but it is not irreducible in  $\mathbb{Z}[i]$ , since it factors as  $2 = (1 + i)(1 - i)$ ). In any case, each prime  $p_j$  is a Gaussian integer ( $p_j = p_j + 0i$ ), and therefore factors uniquely in  $\mathbb{Z}[i]$  as a product of one or more Gaussian integers. Argue that there must exist a factorization of  $N(r)$  in  $\mathbb{Z}[i]$  as a product of at least  $t$  irreducible Gaussian integers, and that therefore, by the first part,  $t$  equals 1 or 2.

$r$  is not a unit and is not 0, so  $N(r) > 1$

$N(r)$  is just an element in  $\mathbb{Z}$ , so we can find the prime factorization of it,

Say prime factorization  $N(r) = p_1 \cdots p_t$  for  $p_j \in \mathbb{Z}$

But we know that each  $p_j$  is a Gaussian integer, of the form  $p_j = p_j + 0i$

So  $N(r)$  factors in  $\mathbb{Z}[i]$  as a product of one or more Gaussian integers.

So there must exist a factorization of  $N(r)$  in  $\mathbb{Z}[i]$  as a product of at least  $t$  irreducible Gaussian integers,

$$N(r) = (p_1 + 0i) \cdots (p_t + 0i)$$

But by the first part, we know that  $t$  can be either 1 or 2.

3. Suppose that  $t = 2$ . Then  $N(r) = r\bar{r} = p_1 p_2$ . Using the unique factorization theorem, deduce that  $r$  differs from either  $p_1$  or  $p_2$  by multiplication by a unit of  $\mathbb{Z}[i]$ . Conclude that there is a prime number  $p$  in  $\mathbb{Z}$  such that  $r$  equals one of the four numbers  $p, -p, pi, -pi$ . Notice that in all four of these cases,  $N(r) = p^2$

Suppose that  $t = 2$

$$\text{Then } N(r) = r\bar{r} = p_1 p_2$$

Then by the unique factorization theorem, we have that  $r$  differs from either  $p_1$  or  $p_2$  by multiplication by a unit of  $\mathbb{Z}[i]$

So there is a prime number  $p$  in  $\mathbb{Z}$  such that  $r$  equals one of the four numbers,  $p, -p, pi, -pi$ .

In each case,  $N(r) = p^2$

4. Suppose that  $t = 1$ . To simplify notation, write  $p_1$  simply as  $p$ . Thus,  $N(r) = p$ . Write  $r$  as  $a + bi$ , for integers  $a, b$ . Observe that if either  $a, b$  is 0, then  $N(r)$  cannot

be a prime number. Thus,  $a, b$  are both nonzero. Observe that  $p = N(r) = r\bar{r} = (a + bi)(a - bi) = a^2 + b^2$

Suppose that  $t = 1$ . Then say  $N(r) = p$

Claim: for  $r = a + bi$ , for  $a, b \in \mathbb{Z}$ , then if either of  $a, b$  is 0,  $N(r)$  cannot be prime

case:  $a, b = 0$ : Then  $N(r) = (0 + 0i)(0 - 0i) = 0$ , then  $N(r)$  is not prime

case:  $a = 0, b \neq 0$ : Then  $N(r) = (a + 0i)(a - 0i) = a^2$ , then  $N(r)$  is the square of  $a$ , not prime

case:  $b = 0, b \neq 0$ : Then  $N(r) = (0 + i)(0 - i) = 1$ , then  $N(r)$  is not prime.

So  $a, b$  must both be nonzero.

Then for  $p = N(r) = r\bar{r} = (a + bi)(a - bi) = a^2 + b^2$

16.6 Let us examine the two smallest rings of the form  $\mathbb{Z}_m[i]$

1. According to the definitions, the ring  $\mathbb{Z}_2[i]$  consists of all elements of the form  $a + bi$ , with  $a, b \in \mathbb{Z}_2$ . Deduce that  $\mathbb{Z}_2[i]$  consists of four elements,  $0, 1, i, 1 + i$

An element in  $\mathbb{Z}_2[i]$  is of the form  $a + bi$ , for  $a, b \in \mathbb{Z}_2$

Then  $r \in \mathbb{Z}_2[i]$  is one of  $0 + 0i, 1 + 0i, 0 + i, 1 + i$

2. Using these four elements, make addition and multiplication tables for  $\mathbb{Z}_2[i]$ , the way we did for fruit rings in Section 6.3

x	0	1	i	1 + i
0	0	0	0	0
1	0	1	i	1 + i
i	0	i	1	1 + i
1 + i	0	1 + i	1 + i	0

3. Review the multiplication table and answer the following questions:

a) Are there zero divisors in  $\mathbb{Z}_2[i]$ ?

Yes,  $1 + i$  is a zero divisor in  $\mathbb{Z}_2[i]$

b) Does every nonzero element of  $\mathbb{Z}_2[i]$  have a multiplicative inverse?

No,  $1 + i$  does not have a multiplicative inverse

c) Is  $\mathbb{Z}_2[i]$  a field?

No, since not all nonzero elements in  $\mathbb{Z}_2[i]$  have multiplicative inverses

4. Perform a similar analysis for the ring  $\mathbb{Z}_3[i]$ , starting with the observation that it contains nine distinct elements. List these elements, do not bother with the addition table, but make a multiplication table for  $\mathbb{Z}_3[i]$ . Use the table to answer the following questions:

X	0	1	2	i	1+i	2+i	2i	1+2i	2+2i
0	0	0	0	0	0	0	0	0	0
1	0	1	2	i	1+i	2+i	2i	1+2i	2+2i
2	0	2	1	2i	2+2i	1+2i	i	2+i	1+i
i	0	i	2i	2	2+i	2+2i	1	1+i	1+2i
1+i	0	1+i	2+2i	2+i	2i	1	1+2i	2	i
2+i	0	2+i	1+2i	2+2i	1	i	1+i	2i	2
2i	0	2i	i	1	1+2i	1+i	2	2+2i	2+i
1+2i	0	1+2i	2+i	1+i	2	2i	2+2i	i	1
2+2i	0	2+2i	1+i	1+2i	i	2	2+i	1	2i

a) Are there zero divisors in  $\mathbb{Z}_3[i]$ ?

No

b) Does every nonzero element of  $\mathbb{Z}_3[i]$  have a multiplicative inverse?

Yes

c) Is  $\mathbb{Z}_3[i]$  a field?

Yes, since every nonzero element has a multiplicative inverse

16.9 Prove theorem 16.9 by following the steps below:

1. Review the construction of the polynomial congruence rings in order to observe that the ring  $\mathbb{F}_p[x]_{x^2+1}$  consists of elements of the form  $c + d\gamma$  where  $c, d$  are in  $\mathbb{F}_p$ , the element  $\gamma$  satisfies the rule  $\gamma^2 = -1$ , and multiplication is given by the rule  $(c + d\gamma)(e + f\gamma) = (ce - df) + (cf + de)\gamma$ .
2. Compare this to the defining description of the ring  $\mathbb{F}_p[i]$  given above. Notice that the descriptions are the same, except that we use  $\gamma$  in one case and  $i$  in the other.
3. Conclude that  $\mathbb{F}_p[x]_{x^2+1}$  and  $\mathbb{F}_p[i]$  are essentially the same rings; that is, they are identical except for a change in notation.

16.12 Theorem 16.15: Suppose  $p$  is a prime number satisfying  $p \equiv 1 \pmod{4}$

1. The equation  $x^2 + y^2 = p$  has integer solutions,  $p$  factors nontrivially in  $\mathbb{Z}[i]$ , the polynomial  $x^2 + 1$  factors nontrivially in  $\mathbb{F}_p[x]$ , and  $-1$  is a square in  $\mathbb{F}_p$
2. There are eight solutions to the equation  $x^2 + y^2 = p$ . Each solution  $(a, b)$  corresponds to a pair of irreducible Gaussian integers  $a + bi$  and  $a - bi$  such that  $p = (a + bi)(a - bi)$

Prove theorem 16.15