

189-346/377B: Number Theory

Assignment 2

Due: Wednesday, February 6

Questions with an asterisk () in front of them are compulsory only for the students who are registered in Math 377.*

1. Compute the greatest common divisor of $a = 9+49i$ and $b = 31+39i$ in the ring $\mathbf{Z}[i]$ of Gaussian integers, and express the result as a linear combination of a and b with coefficients in $\mathbf{Z}[i]$.

2. Recall that it was observed in class that the Diophantine equation $y^2+118 = x^3$ has a non-trivial solution, namely $(x, y) = (7, 15)$. Use this fact to show that $343 = 7^3$ admits two essentially different factorisations into irreducible elements in the ring $\mathbf{Z}[\sqrt{-118}]$. (You should show, of course, that all your factors are irreducible.)

* 3. Show that if an ideal I in the ring of integers of a number field admits a non-trivial factorisation $I = I_1I_2$, then I is properly contained in I_1 and I_2 . Conclude that I is irreducible if the quotient R/I is a field. Use this criterion and problem 2 to express $343 = 7^3$ as a product of irreducible ideals in $\mathbf{Z}[\sqrt{-118}]$. (As mentioned, but not proved, in class, such a factorisation is unique. You do not need to show your answer is unique, although the uniqueness will be useful in grading your solution!) Show that the cube of the ideal $(7, 15 + \sqrt{-118})$ is principal. (The fact that $\mathbf{Z}[\sqrt{-118}]$ has an ideal whose cube is principal implies that it has *class number divisible by three*. It is precisely this property that makes the Diophantine equation $y^2 + 118 = x^3$ somewhat subtle to analyse by the techniques discussed in class.)

The purpose of the next few problems is to get you to show that every positive integer can be written as a sum of four integer squares.

The *Hamilton quaternions* is the set \mathbf{H} of numbers of the form

$$a + bi + cj + dk,$$

where a, b, c and d are real numbers. Addition of these numbers (viewed as vectors in \mathbf{R}^4) is performed component-wise, and multiplication is performed using the usual distributive laws combined with the rules

$$i^2 = j^2 = k^2 = -1; \quad ij = -ji = k, \quad ki = -ik = j, \quad jk = -kj = i.$$

Note that multiplication in \mathbf{H} is not commutative. Aside from that, \mathbf{H} satisfies all the axioms of a (non-commutative) ring: existence of neutral elements for addition and multiplication (denoted 0 and 1 respectively), existence of additive inverses, commutativity of addition, associativity of both operations, distributivity of multiplication over addition, both on the left and on the right, etc. You are allowed to assume all of these basic properties of Hamilton's quaternions.

4. The *conjugate* of the quaternion $\alpha = a + bi + cj + dk$ is defined to be $\bar{\alpha} = a - bi - cj - dk$, and the *norm* of a quaternion is defined to be $|\alpha| = \alpha\bar{\alpha}$. Show that $|\alpha| = a^2 + b^2 + c^2 + d^2$, and conclude that \mathbf{H} is a division field, i.e., every non-zero element α has a multiplicative inverse (both on the left and right), i.e., an element α' satisfying $\alpha\alpha' = \alpha'\alpha = 1$.

5. Show that the set

$$R = \mathbf{Z} \left[i, j, \frac{1+i+j+k}{2} \right] = \left\{ a + bi + cj + d \frac{1+i+j+k}{2}, a, b, c, d \in \mathbf{Z} \right\}$$

is a subring of \mathbf{H} , i.e, that it is closed under both addition and multiplication, and that the norm of an element of R is a positive integer. This ring is sometimes called the ring of *integral*, or *Hurwitz*, quaternions. It is to \mathbf{H} as the Gaussian integers are to \mathbf{C} , essentially.

6. Show that the ring R is *Euclidean* in the sense that, for all $a, b \in R$ with $b \neq 0$, there exists $q, r \in R$ satisfying

$$a = qb + r, \quad \text{with } |r| < |b|.$$

7. A *left ideal* of R is a subset $I \subset R$ which is closed under addition and under *left multiplication* by elements of R :

$$a \in R, b \in I \Rightarrow ab \in I.$$

(The distinction between left and right ideals is critical in the setting where multiplication is non-commutative; in general a left ideal need not be closed under right multiplication by elements of R .) A left ideal is said to be *principal* if it is of the form

$$R\alpha = \{\gamma\alpha, \quad \gamma \in R\}.$$

Using the result of part 6, show that every left ideal $I \subset R$ is principal.

* 8. Given a prime p , show that there exists an element α of R whose norm is a multiple of p but not of p^2 .

9. Show that any prime number p is a sum of four integer squares. (Hint: let α be the element found in question 8, and apply the result of question 7 to the left ideal $I = R\alpha + Rp$.)

10. Using 9 and basic properties of the quaternions, show that every positive integer can be expressed as a sum of four integer squares. Give an example to show that this result is optimal, i.e., that there are integers that cannot be written as a sum of three integer squares.