

Math 351:03 — Fall 1999

MW4 SEC-217

Prof. Bumby

Workshop 9, Fields.

21. It is possible to have unique factorization without a Euclidean algorithm. A ring with this property is

$$O_{-19} = \left\{ \frac{a + b\sqrt{-19}}{2} : a, b \in \mathbb{Z}, a \equiv b \pmod{2} \right\}$$

(a) First, we need to see that these elements form a ring. The best way, although it is a little indirect, is to note that $\xi = (1 + \sqrt{-19})/2$ satisfies $\xi^2 = \xi - 5$ in \mathbb{C} , so that numbers of the form $c + d\xi$ are closed under addition and multiplication and form a subring of \mathbb{C} . Then show that every $c + d\xi$ can be written in the form of elements of O_{-19} , and every element of that form can be written as $c + d\xi$.

(b) The defining equation of ξ is irreducible over the field of integers mod 2, so $O_{-19}/(2)$ has 4 elements.

(c) The defining equation of ξ is irreducible over the field of integers mod 3, so $O_{-19}/(3)$ has 3 elements.

(d) If m is odd and $m|a^2 + 19b^2$ where a and b have no common odd factor, then $\gcd(m, b) = 1$, so $bx \equiv a \pmod{m}$ has a solution. This solution can be chosen to be odd and of absolute value less than or equal to m . This means that every ideal in O_{-19} is an integer times an ideal of the form

$$I = \left(m, \frac{k - \sqrt{-19}}{2} \right)$$

with odd m , odd k and $-m \leq k \leq m$ and $m|k^2 + 19$.

(e) If we write $k^2 + 19 = 4mm'$, then m' is odd and $4mm' \leq m^2 + 19$. Also,

$$\begin{aligned} I \cdot \frac{k + \sqrt{-19}}{2} &= \left(m \frac{k + \sqrt{-19}}{2}, \frac{k^2 + 19}{4} \right) \\ &= \left(\frac{k + \sqrt{-19}}{2}, m' \right) \cdot m \\ &= I' \cdot m. \end{aligned}$$

The ideal I' can be put in the same form as I with m' in place of m and k replaced by the appropriate quantity congruent to $-k$ modulo m' . This is sure to be simpler than I in the sense of having $m' < m$ unless $4m^2 \leq m^2 + 19$. This is equivalent to $3m^2 \leq 19$, but this is false for all odd $m > 1$.

... continued on other side

(f) If I' consists of the multiples of a single element $\alpha \in O_{-19}$, then the same will be true of I , and this gives the inductive step in a proof that all ideal of O_{-19} have single generators. Instead of giving the abstract proof of this, you should just follow these steps to find a single generator of the ideal

$$I = \left(23, \frac{21 - \sqrt{-19}}{2} \right).$$

(g) If there were a Euclidean algorithm, the smallest numbers, in the sense of that algorithm, other than ± 1 would be required to allow remainders of only $0, \pm 1$, but there are no elements that require fewer than 4 remainders.

22. When \mathbb{Z} is extended to include the square root of a positive quantity, there is a similar way to characterize ideals. For example, $O_{40} = \mathbb{Z}[x]/(x^2 - 10)$ creates a ring that contains a square root of 10.

(a) Show that the elements of this ring can be written in the form $a + b\sqrt{10}$ with integers a and b .

(b) Show that every ideal of O_{40} can be written in the form

$$c(n, \sqrt{10} - k)$$

where c and n are positive integers, k is an integer, $n|k^2 - 10$ and $0 \leq |k| \leq n/2$.

(c) If

$$I = (n, \sqrt{10} - k),$$

and $k^2 - 10 = nn' > 0$, then

$$I \cdot (\sqrt{10} + k) = (\sqrt{10} + k, n') \cdot n.$$

As long as this is possible, $n' \leq n/4$, so every ideals can be related to an ideal with $n \leq 10$ and $k \in \{0, \pm 1, \pm 2, \pm 3\}$.

(d) If $n > \sqrt{10}$, one more step will give an ideal with $n \leq \sqrt{10}$. Once n has been made this small, it is convenient to restrict to $k > 0$, and to take k as large as possible in the given residue class modulo n . This keeps n' from getting too large, and forces the process to cycle through finitely many different descriptions of ideals. This will discover if an ideal has a single generator, although we don't have everything necessary to prove that. However, in contrast to problem 21, there is always a reason to continue this process, and the cycling will lead to a unit in the ring other than ± 1 . Find this unit for O_{40} . Indeed, there are two different cycles of these "reduced" ideals, but they lead to the same unit.