

## Problem Set #3: Mysteries

MAYBE in order to understand mankind, we have to look at the word itself. Basically, it's made up of two separate words — “mank” and “ind.” What do these words mean? It's a mystery, and that's why so is mankind.

Throughout,  $D$  denotes a squarefree integer,  $D \neq 1$ . As usual,  $\mathcal{O}_D = \mathbf{Z} + \mathbf{Z}\tau$ , where  $\tau = \sqrt{D}$  when  $D \equiv 2, 3 \pmod{4}$  and  $\tau = \frac{1+\sqrt{D}}{2}$  when  $D \equiv 1 \pmod{4}$ .

### PUZZLES

These problems are intended as definition chases, understanding checks, applications of known theorems, and/or straightforward generalizations of familiar arguments.

0. Supply the proof, omitted in class, that  $\text{Id}(\mathcal{O}_D)$  is atomic: Every  $I \in \text{Id}(\mathcal{O}_D)$  is a finite product of irreducibles (atoms).

Suggestion. WOP on  $\|I\|$ . Keep in mind that the ideal norm is multiplicative and that  $\|I\| = 1$  if and only if  $I$  is the unit ideal (1).

1. (alternative characterizations of prime ideals) Let  $P$  be an ideal of a Ring  $R$ . All of the following are equivalent:
  - (a)  $P$  is **prime** as defined in class:  $P$  is proper, and whenever  $P \supseteq IJ$  for ideals  $I, J \subseteq R$ , either  $P \supseteq I$  or  $P \supseteq J$ .
  - (b)  $P$  is proper, and whenever  $ab \in P$  for elements  $a, b \in R$ , either  $a \in P$  or  $b \in P$ .
  - (c) the quotient ring  $R/P$  is an integral domain.
2. For  $P \in \text{Id}(\mathcal{O}_D)$ :  $P$  is irreducible in  $\text{Id}(\mathcal{O}_D)$  (is an atom)  $\iff P$  is a prime ideal of  $\mathcal{O}_D$ .
3. (gcds, lcms, and prime factorizations) Let  $I$  and  $I'$  be nonzero ideals of  $\mathcal{O}_D$ , and factor  $I = \prod_P P^{e_P}$  and  $I' = \prod_P P^{e'_P}$ , where  $P$  runs over nonzero prime ideals of  $\mathcal{O}_D$ . (Despite appearances, these are really *finite* products:  $e_P = e'_P = 0$  for all but finitely many prime ideals  $P$ .) Then

$$I + I' = \prod_P P^{\min\{e_P, e'_P\}} \quad \text{and} \quad I \cap I' = \prod_P P^{\max\{e_P, e'_P\}}.$$

4. **Using that  $\text{Id}(\mathcal{O}_D)$  is a UFM**, prove: Every ideal of  $\mathcal{O}_D$  is principal  $\Rightarrow \mathcal{O}_D$  is a UFD.

It is a standard fact from college Algebra — not to be confused with the course College Algebra — that *every* PID is a UFD! Ask your counselor if you are curious and haven't seen this! But you can and should do this problem without that general result.

5. Give a rigorous proof that  $\mathbf{Z}[\tau] \simeq \mathbf{Z}[x]/(m(x))$ , where  $m(x) = x^2 - D$  when  $D \equiv 2, 3 \pmod{4}$ , and  $m(x) = x^2 - x + \frac{1-D}{4}$  when  $D \equiv 1 \pmod{4}$ .

## CONUNDRUMS

6. Let  $P$  be a nonzero prime ideal of  $\mathcal{O}_D$ . Let  $p$  be the (unique) prime of  $\mathbf{Z}$  for which  $P$  divides  $(p)$ .
  - a)  $\mathcal{O}_D/P$  is a field.
  - b) The map  $\mathbf{Z}/p\mathbf{Z} \rightarrow \mathcal{O}_D/P$  given by  $a \bmod p \mapsto a \bmod P$  is an injective homomorphism.
7. Assume  $\mathcal{O}_D$  is a Unique Factorization Domain. Prove that every ideal of  $\mathcal{O}_D$  is principal.  
 Start by showing that if  $\pi$  is irreducible in  $\mathcal{O}_D$ , then  $(\pi)$  is a prime ideal. Then argue that every nonzero prime ideal of  $\mathcal{O}_D$  divides a product of principal prime ideals.
8. Assume  $f(x) \in \mathbf{Z}[x]$  is nonconstant. Then  $f(x)$  has a root in  $\mathbf{Z}_p$  for infinitely many primes  $p$ .
9. There are infinitely many primes  $p$  in  $\mathbf{Z}$  that split in  $\mathcal{O}_D$ .
10. (Kohnen) Assume that  $D > 0$  is squarefree with  $D \equiv 3 \pmod{4}$ . Let  $X \geq 2$ , and define

$$P_X = \left( \prod_{q \leq X, q \nmid D} q \right)^2 + D,$$

where the product over  $q$  is over all the primes not exceeding  $X$  and not dividing  $D$ .

- (a) There is at least one rational prime  $p$  dividing  $P_X$  with  $p \equiv 3 \pmod{4}$ .
- (b) If  $p$  is as in part (a), then  $D^{(p-1)/2} \equiv -1 \pmod{p}$ .
- (c) If  $p$  is as in part (a), then  $p$  is inert in  $\mathcal{O}_D$  and  $p > X$ . Since  $X$  can be taken arbitrarily large, there are infinitely many primes  $p$  that remain inert in  $\mathcal{O}_D$ .

In fact, for *any* squarefree  $D \in \mathbf{Z}$ ,  $D \neq 1$ , there are infinitely many primes  $p$  that remain inert in  $\mathcal{O}_D$ . This is a special case of the celebrated Chebotarev density theorem, but it admits an elementary (though intricate) proof. In fact, the same conclusion can be deduced from a problem that shows up later in the first-year problem sets. Keep your eyes peeled!

## TANGLES

11. (Birkhoff) The left and right pictures show the points of  $\mathcal{O}_{-7}$  and  $\mathcal{O}_{-19}$  in the complex plane (respectively), each surrounded by a circle of radius 1. Applying the method of prolonged staring, we deduce:  $\mathcal{O}_{-7}$  has a division algorithm with respect to the norm, but  $\mathcal{O}_{-19}$  does not. (How???) Determine **all** squarefree  $D < 0$  for which  $\mathcal{O}_D$  has a division algorithm with respect to the norm.

