Primes in extensions of the integers

Matthew Gherman and Adam Lott

26 January 2020

1 Introduction

Today, we will be working with algebraic structures called *rings*. On a basic level, a ring is a set where we have two operations that we refer to as addition and multiplication. The integers $\mathbb{Z}$ with our typical notions of addition and multiplication is our primary example of a ring. We will now introduce a family of rings with slightly more complicated elements than just the integers. If you are interested, there is an optional section on general rings (with a formal definition) in Section **??**.

Definition 1. Define $\mathbb{Z}[\sqrt{d}] = \{a + b\sqrt{d} : a, b \in \mathbb{Z}\}$. It is read "$\mathbb{Z}$ adjoin square root of d". We will call this a *quadratic extension of the integers.* Addition and multiplication in this number system are defined in the way you might expect:

$$\begin{aligned}(a + b\sqrt{d}) + (a' + b'\sqrt{d}) &= (a + a') + (b + b')\sqrt{d} \\ (a + b\sqrt{d}) \cdot (a' + b'\sqrt{d}) &= (aa' + dbb') + (ab' + a'b)\sqrt{d}\end{aligned}$$

Notation. For the rest of this worksheet, we will assume that d **is a squarefree integer** (meaning that no prime appears more than once in the prime factorization of d) and that $d \equiv 2$ **or** 3 **(mod 4)**. We will also always let p **be an odd prime**[1].

Question. Why do we insist that d be squarefree? (No need to write anything down, just think about it)

Definition 2. A *unit* in $\mathbb{Z}[\sqrt{d}]$ is an element u for which there exists some $v \in \mathbb{Z}[\sqrt{d}]$ with $uv = 1$. We say that $\alpha, \beta \in \mathbb{Z}[\sqrt{d}]$ are *associates* if $\alpha = u\beta$ for some unit $u \in \mathbb{Z}[\sqrt{d}]$.

Exercise 1. For each of the following, list as many units as you can. Can you prove that you've found all of them?

(a) $\mathbb{Z}$

(b) $\mathbb{Z}[\sqrt{-1}]$

(c) $\mathbb{Z}[\sqrt{-3}]$

[1] When $d \equiv 1 \bmod 4$ or $p = 2$, all of the theorems we will prove need to be adjusted very slightly, but the ideas are the same.

(d) (CHALLENGE) $\mathbb{Z}[\sqrt{5}]$ (HINT: there are infinitely many)

It turns out there is a nice way to detect whether or not an element of $\mathbb{Z}[\sqrt{d}]$ is a unit.

Definition 3. Let $\alpha = a + b\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$. The *norm* of α is defined as $N(\alpha) = a^2 - b^2 d$. Note that $N(\alpha)$ is always an element of $\mathbb{Z}$.

Exercise 2. Show that $N(\alpha\beta) = N(\alpha)N(\beta)$.

Exercise 3. (a) Show that $u \in \mathbb{Z}[\sqrt{d}]$ is a unit if and only if $|N(u)| = 1$.

(b) Go back to Exercise 1, parts (a)-(c), and determine *all* possible units. If you are up for a challenge, try part (d) also.

In the integers, we think of a prime number p as an integer whose factors are only 1 and p. In general, this is the definition of an irreducible number.

Definition 4. Let $\alpha, \beta \in \mathbb{Z}[\sqrt{d}]$. We say that α *divides* β if there exists another $x \in \mathbb{Z}[\sqrt{d}]$ such that $\alpha x = \beta$.

Examples.
(1) In $\mathbb{Z}[\sqrt{2}]$, $1 + \sqrt{2}$ divides -1 because $(1 + \sqrt{2})(1 - \sqrt{2}) = -1$.
(2) In $\mathbb{Z}[\sqrt{-3}]$, $(2 + \sqrt{-3})$ divides $5 - \sqrt{-3}$ because $(2 + \sqrt{-3})(1 - \sqrt{-3}) = 5 - \sqrt{-3}$.
(3) In $\mathbb{Z}[\sqrt{-1}]$, $1 + \sqrt{-1}$ does not divide $2 + \sqrt{-1}$ (can you prove it?)

Definition 5. An element $\alpha \in \mathbb{Z}[\sqrt{d}]$ is *irreducible* if whenever $\alpha = xy$ with $x, y \in \mathbb{Z}[\sqrt{d}]$, one of x or y is a unit. In other words, there are no non-trivial ways to factor α.

Definition 6. An element $\pi \in \mathbb{Z}[\sqrt{d}]$ is *prime* if it satisfies the following property: If π divides a product $\alpha\beta$ with $\alpha, \beta \in \mathbb{Z}[\sqrt{d}]$, then π divides α or π divides β.

The ideas of prime and irreducible coincide when we are working with integers, but in general they can be different.

Exercise 4. (a) Show that any prime α in $\mathbb{Z}[\sqrt{d}]$ is irreducible. (Hint: Prove the contrapositive.)

(b) Prove that 2 is irreducible in $\mathbb{Z}[\sqrt{-5}]$ but it is not prime.

(c) (CHALLENGE) Prove that in $\mathbb{Z}[\sqrt{-1}]$, if α is irreducible then it is also prime.

Notation. For the rest of the worksheet, we will use the phrase *rational prime* to mean a prime/irreducible element of $\mathbb{Z}$. The letter p will always be reserved for an odd rational prime (i.e. $p \neq 2$).

2 Behavior of primes

Recall from the beginning of class that rational primes p can either remain prime or become not prime when they are considered as elements of $\mathbb{Z}[\sqrt{d}]$.

Exercise 5. For each of the following pairs (p, d), determine (with proof) if p is still prime in $\mathbb{Z}[\sqrt{d}]$.
(HINT: The norm map may be useful.)

(a) $d = 2$, $p = 7$

(b) $d = -2$, $p = 7$ (you may assume that in $\mathbb{Z}[\sqrt{-2}]$, “prime” is the same as “irreducible”)

(c) $d = -2$, $p = 3$

(d) $d = -1$, $p = 3$ (you may assume that in $\mathbb{Z}[\sqrt{-1}]$, "prime" is the same as "irreducible")

(e) $d = 6$, $p = 3$

The rest of this worksheet will be dedicated to answering the following question – given p and d, how can we decide whether or not p is prime in $\mathbb{Z}[\sqrt{d}]$?

2.1 A quick review of polynomials (and some new stuff too)

Definition 7. A *polynomial with integer coefficients* is an expression of the form $p(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$ where each a_i is an integer and x is a variable. In this worksheet, we will only be working with *monic quadratic polynomials* – polynomials of the form $x^2 + ax + b$, where a and b are integers.

Definition 8. A quadratic polynomial $p(x) = x^2 + ax + b$ with integer coefficients is said to be *reducible* if it can be factored $p(x) = (x - u)(x - v)$ for some integers u, v. If no such factorization is possible, then $p(x)$ is said to be *irreducible.*

Exercise 6. Determine if each of the following polynomials are irreducible.

(a) $p(x) = x^2 - 4$

(b) $p(x) = x^2 + 1$

(c) $p(x) = x^2 - 5x + 6$

(d) $p(x) = x^2 + 2x + 10$

Exercise 7. Prove that a monic quadratic polynomial $p(x)$ is irreducible if and only if there are no integer solutions to $p(x) = 0$.

We will be working with polynomials mod p. Arithmetic with polynomials mod p works the same way as with numbers mod p – any time you see a coefficient, you can reduce it to its lowest residue class mod p (but you can *not* reduce the exponents on x). The definitions of reducible and irreducible polynomials are the same as above, with "=" replaced by "$\equiv$ mod p".

Exercise 8. (a) Expand and simplify $(x^2 + 2x + 5)(2x^2 - 4x + 2)$ mod 7.

(b) Find all solutions to $x^2 + 4x + 3 = 0$ mod 5.

(c) Is $x^2 + x + 4$ irreducible mod 5? What about $x^2 + x + 2$ mod 3?

(d) (CHALLENGE) Prove that $f(x) = x^2 + ax + b$ is irreducible mod p if and only if $f(x) \equiv 0$ mod p has no solutions.

2.2 A cool theorem

Definition 9. For any squarefree $d \in \mathbb{Z}$, define the polynomial $f_d(x) = x^2 - d$. This is sometimes called the *minimal polynomial* of $\mathbb{Z}[\sqrt{d}]$.

Exercise 9. What are the roots of $f_2(x)$? What are the roots of $f_3(x)$? What are the roots of $f_d(x)$ in general?

We see from the previous exercise that the roots of $f_d(x)$ are $\pm\sqrt{d}$. This is not an integer since we chose d to not have repeated factors in its prime factorization. We say that $f_d(x)$ is minimal because it is the polynomial of lowest degree with $\sqrt{d}$ as a root.

Let us now investigate the relationship between the behavior of a rational prime p in $\mathbb{Z}[\sqrt{d}]$ and the polynomial $f_d(x)$ mod p.

Exercise 10. For each of the following pairs (d, p), factor $f_d(x)$ mod p if possible, and determine if p is prime in $\mathbb{Z}[\sqrt{d}]$.

(a) $d = 3$, $p = 3$

(b) $d = -6$, $p = 7$

(c) $d = 2$, $p = 11$ (you may assume “prime” = “irreducible”)

(d) $d = -2$, $p = 7$ (same assumption)

Do you notice a pattern?

The previous exercise is suggestive of the following general theorem, the proof of which is beyond the scope of this worksheet.

Theorem 1. *Let p be a rational prime and d be a squarefree integer. Then p is prime in $\mathbb{Z}[\sqrt{d}]$ if and only if $f_d(x)$ is irreducible mod p.*

Theorem 1 is nice because it gives a complete characterization of how rational primes behave in $\mathbb{Z}[\sqrt{d}]$. However, in practice it can be difficult to figure out the factorization of $f_d(x)$ mod p. Next week, we will see how to translate Theorem 1 into a new criterion which is much easier to check in practice.