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 6.

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.

Primes in extensions of the integers, part II

Matthew Gherman and Adam Lott

2 February 2020

3 Legendre symbols and quadratic reciprocity

Let us recall the notation from last week:

- d is a squarefree integer with $d \equiv 2$ or $3 \bmod 4$.
- p is an odd rational prime.
- $f_d(x) = x^2 - d$ is the minimal polynomial of $\mathbb{Z}[\sqrt{d}]$.

Also recall our main theorem from last week:

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.*

The goal for this week is to use this to prove an even better theorem. Before we can get there, we need to develop some new ideas (NOTE: if you were in math circle last year and remember the unit on quadratic reciprocity, most of this will be familiar to you).

Let p be a rational prime. Notice that mod p, some numbers can be written as squares of other numbers, and some can not.

Exercise 11. For each of the given a and p, decide whether or not there exists b such that $a \equiv b^2 \bmod p$.

(a) $a = 2$, $p = 5$

(b) $a = 3$, $p = 11$

(c) $a = 5$, $p = 13$

Definition 10. Let p be a rational prime and $a \not\equiv 0 \bmod p$. If there exists b such that $a \equiv b^2 \bmod p$, then we say a is a *quadratic residue* mod p. If no such b exists, then a is a *nonresidue*

Definition 11. Let p be a rational prime and a be any integer. The *Legendre symbol* is defined as

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{a is a quadratic residue mod } p \\ -1 & \text{a is a nonresidue} \\ 0 & a \equiv 0 \bmod p \end{cases}$$

Exercise 12. Prove that the Legendre symbol is multiplicative: for any a, b,

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right).$$

If you remember the quadratic reciprocity unit from last year, you may remember the following two key theorems (which we will state but not prove).

Theorem 2 (Euler's criterion, special cases)**.** *Let p be an odd rational prime. Then*

$$\left(\frac{-1}{p}\right) = \begin{cases} 1 & p \equiv 1 \mod 4 \\ -1 & p \equiv 3 \mod 4 \end{cases}$$

and

$$\left(\frac{2}{p}\right) = \begin{cases} 1 & p \equiv 1, 7 \mod 8 \\ -1 & p \equiv 3, 5 \mod 8 \end{cases}.$$

Theorem 3 (Quadratic reciprocity)**.** *Let p and q be odd rational primes. Then:*

- *If $p \equiv 1$ or $q \equiv 1$ mod 4, then $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$*
- *If $p \equiv q \equiv 3$ mod 4, then $\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right)$*

Exercise 13. Show that the quadratic reciprocity theorem is equivalent to the statement

$$\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}\left(\frac{q}{p}\right).$$

4 An even cooler theorem

Now we are finally able to state and prove a much more useful criterion for determining splitting behaviors.

Theorem 4. *Let p be a rational prime. Then, in $\mathbb{Z}[\sqrt{d}]$, p is prime if and only if $\left(\frac{d}{p}\right) = -1$.*

Exercise 14. Prove Theorem 4 by applying Theorem 1.

This theorem is useful because it tells us that the splitting behavior of p in $\mathbb{Z}[\sqrt{d}]$ depends *only on the residue class* *of d mod p.* In particular, in order to determine the behavior of p in $\mathbb{Z}[\sqrt{d}]$, we now only need to determine all of the quadratic residues mod p. Therefore, for a given p, we can immediately classify its behavior in $\mathbb{Z}[\sqrt{d}]$ for *all* d. The next exercise walks through an example.

Exercise 15. Let $p = 13$.

(a) List all of the quadratic residues mod 13.

(b) Give a complete characterization of the behavior of 13 in $\mathbb{Z}[\sqrt{d}]$ for all d. (Your answer should look like: "13 is prime in $\mathbb{Z}[\sqrt{d}]$ if and only if $d \equiv$ __ mod 13)

(c) For $d = 3$ and $d = 10$, find an example illustrating that 13 is not prime in $\mathbb{Z}[\sqrt{d}]$. (NOTE: if this question contradicts your answer to part (b), go back and find your mistake)

So far, Theorem 4 tells us that given p, we can classify the behavior for all d. What if we want to ask the opposite question? Given d, how can we classify the behavior of all p? The key is quadratic reciprocity. Theorem 4 says that the only thing we care about is $\left(\frac{d}{p}\right)$. If we factor

$$d = (-1)^j 2^k q_1 \cdots q_r \qquad \text{where the } q_i \text{ are odd primes and } j, k = 0 \text{ or } 1 \text{ (recall } d \text{ is squarefree)}$$

then we have

$$\left(\frac{d}{p}\right) = \left(\frac{-1}{p}\right)^j \left(\frac{2}{p}\right)^k \left(\frac{q_1}{p}\right) \cdots \left(\frac{q_r}{p}\right). \tag{1}$$

Theorem 2 tells us that $\left(\frac{-1}{p}\right)$ and $\left(\frac{2}{p}\right)$ depend only on the residue of p mod 4 and mod 8, and Theorem 3 tells us that $\left(\frac{q_i}{p}\right)$ depends only on the residue of p mod q_i. Therefore, given d, we should be able to give a complete classification of the behavior of p based only on the residue of p mod $8d$. In fact, we can do even better:

Exercise 16. Prove that the value of $\left(\frac{d}{p}\right)$ actually depends only on the residue of p mod $4d$. (HINT: it would only depend on the residue mod $8d$ if $k = 1$ in (1). What does this imply?)

Combining everything above allows us to write down another nice theorem.

Theorem 5. *The behavior of a rational prime p in $\mathbb{Z}[\sqrt{d}]$ depends only on the residue class of p mod $4d$.*

If the explanation above was a bit too abstract, don't worry, the next section will walk you through some concrete examples.

5 Examples

5.1 A simple example: $d = -5$

Let us fix $d = -5$. We want to give a complete characterization of which rational primes p are still prime in $\mathbb{Z}[\sqrt{d}]$, and which are not.

Exercise 17. In Theorem 4, we proved that the behavior of p in $\mathbb{Z}[\sqrt{-5}]$ is completely determined by the value of the Legendre symbol $\left(\frac{-5}{p}\right)$. Using the multiplicative property of the Legendre symbol and quadratic reciprocity, prove that

$$\left(\frac{-5}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{p}{5}\right).$$

Exercise 18. Prove that if p_1 and p_2 are two different rational primes and $p_1 \equiv p_2 \bmod -20 = 4 \cdot -5$, then $\left(\frac{-5}{p_1}\right) = \left(\frac{-5}{p_2}\right)$ and therefore p_1 and p_2 have the same behavior in $\mathbb{Z}[\sqrt{-5}]$. This shows why the beavior of p depends only on the residue of p mod $4d$. NOTE: arithmetic mod -20 is the same as arithmetic mod 20 (if you don't believe this, remember what the original definition of modular arithmetic is).

Exercise 19. Complete the table below for a complete characterization of the behavior of *all* rational primes p in $\mathbb{Z}[\sqrt{-5}]$. (Sanity check: Why are there no rows for 5 or 15 or any even number?)

p mod -20	$\left(\frac{-20}{p}\right)$	Still prime in $\mathbb{Z}[\sqrt{-5}]$? (Y/N)	Example (if previous column is N)
1			
3			
7			
9			
11			
13			
17			
19			

5.2 A more complicated example: $d = -30$

Repeat the steps of the previous subsection using $d = -30$.

Exercise 20. (a) Prove that

$$\left(\frac{-30}{p}\right) = -\left(\frac{-1}{p}\right)\left(\frac{2}{p}\right)\left(\frac{p}{3}\right)\left(\frac{p}{5}\right).$$

(b) Prove that if $p_1 \equiv p_2 \bmod 120$, then p_1 and p_2 have the same behavior in $\mathbb{Z}[\sqrt{-30}]$.

(c) Start filling out a similar table (the full table would have too many rows, but if you're bored feel free to fill out as much as you want)

p mod 120	Still prime in $\mathbb{Z}[\sqrt{-30}]$? (Y/N)	Example (if previous column is N)
1		
7		
11		
13		
17		
19		
23		
$\vdots$		

6 Optional: general rings

Definition 12. A *ring* R is a set equipped with two operations: $+$ and $\cdot$ that satisfy the following axioms.

(1) $(a+b)+c = a+(b+c)$ for all $a,b,c \in R$ (we say $+$ is associative).
(2) $a+b = b+a$ for all $a,b \in R$ (we say $+$ is commutative).
(3) There is an element $0 \in R$, named the zero element, such that $0+a = a$ for all $a \in R$.
(4) For each $a \in R$ there is an element $-a \in R$ such that $a+(-a) = 0$ (each element has an additive inverse).
(5) $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ for all $a,b,c \in R$ (we say that $\cdot$ is associative).
(6) There is an element $1 \in R$, named one, such that $1 \cdot a = a$ for all $a \in R$.
(7) $a \cdot (b+c) = (a \cdot b) + (a \cdot c)$ for all $a,b,c \in R$ (multiplication is left distributive with respect to addition).
(8) $(b+c) \cdot a = (b \cdot a) + (c \cdot a)$ (multiplication is right distributive with respect to addition).

If you are already familiar with some algebraic structures, you might notice that the first four axioms make R an abelian group under addition.

Definition 13. A ring R is *commutative* if $a \cdot b = b \cdot a$ for all $a,b \in R$.

Exercise 21. (a) Convince yourself that $\mathbb{Z}$ with our typical notions of addition and multiplication is a commutative ring.

(b) Check that the set $\mathbb{Z}/4\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}\}$ has the structure of a commutative ring under addition and multiplication modulo 4.

(c) Check that the set of all 2×2 matrices with entries in the real numbers, $M_2(\mathbb{R})$, is a ring under matrix addition and matrix multiplication. Can you find two matrices A and B so that AB is not equal to BA?

Ring theory is often the study of rings with extra structure. Over the course of this section, we will define "nice" versions of rings.

Definition 14. An element $a \in R$ is a *left zero divisor* if $ab = 0$ for some $b \in R$. An element $a \in R$ is a *right zero divisor* if $ba = 0$ for some $b \in R$. When R is commutative, the left zero divisors coincide with right zero divisors so we simply call them *zero divisors*.

Definition 15. An *integral domain* R is a ring in which $ab = 0$ implies $a = 0$ or $b = 0$. Equivalently, an integral domain is a ring with no non-zero zero divisors.

Exercise 22. Show that in an integral domain with $a \neq 0$, then $ab = ac$ implies $b = c$.

Exercise 23. In the examples from Exercise 21, which rings are integral domains?

We note that the rational numbers $\mathbb{Q}$, the real numbers $\mathbb{R}$, and the complex numbers $\mathbb{C}$ under the usual notions of addition and multiplication are rings. However, each non-zero element in these rings has a multiplicative inverse. Much can be said of sets with this added structure. We define the general notion below.

Definition 16. A *field* is a commutative ring such that each non-zero element $a \in F$ is invertible. In other words, there is some $b \in F$ such that $ab = 1$ where 1 is the multiplicative identity of F.

Exercise 24. Show that a field F does not have any non-zero zero divisors.

The aforementioned fields $(\mathbb{Q}, \mathbb{R}, \mathbb{C})$ have infinitely many elements, but there are extremely nice examples of fields with only finitely many elements.

Exercise 25. For which values of n is $\mathbb{Z}/n\mathbb{Z}$ a field under addition and multiplication modulo n?

We can write every complex number $\alpha \in \mathbb{C}$ as $a + bi$ where $a, b \in \mathbb{R}$ and $i^2 = -1$. Thus, we can write $\mathbb{C} = \mathbb{R}[i]$ where $\mathbb{R}[i] = \{a + bi : a, b \in \mathbb{R}\}$, which is the same notation used throughout the worksheet. It is clear that there is a copy of $\mathbb{R}$ contained in $\mathbb{C}$, mainly the set of all elements $a + bi$ where $b = 0$. This is an example of a *field extension*. Analyzing the situation further, we see that $\mathbb{C}$ is $\mathbb{R}$ where we adjoin, $i = \sqrt{-1}$, a root of the polynomial $x^2 + 1$. The field extension $\mathbb{C}$ over $\mathbb{R}$ is characterized by this polynomial $x^2 + 1$, connecting field extensions to roots of polynomials. This connection leads to rich results in Galois theory.

Exercise 26. In Exercise 25, we should have found that $\mathbb{Z}/p\mathbb{Z}$ is a field if and only if p is a prime. In particular, we will focus on the case $p = 2$.

(a) Find all polynomials of degree 2 with coefficients in $\mathbb{Z}/2\mathbb{Z}$ that cannot be factored over $\mathbb{Z}/2\mathbb{Z}$. Each of these polynomials can be used to construct a finite field of order $2^2 = 4$.

(b) Find all polynomials of degree 3 with coefficients in $\mathbb{Z}/2\mathbb{Z}$ that cannot be factored over $\mathbb{Z}/2\mathbb{Z}$. Each of these polynomials can be used to construct a finite field of order $2^3 = 8$.

(c) Why is it more difficult to find all the polynomials of degree ≥ 4 that cannot be factored over $\mathbb{Z}/2\mathbb{Z}$?