A CONCRETE EXAMPLE OF PRIME BEHAVIOR IN QUADRATIC FIELDS

CASEY BRUCK

1. Abstract

The goal of this paper is to provide a concise way for undergraduate mathematics students to learn about how prime numbers behave in quadratic fields. This paper will provide students with some basic number theory background required to understand the material being presented. We start with the topic of quadratic fields, number fields of degree two. This section includes some basic properties of these fields and definitions which we will be using later on in the paper. The next section introduces the reader to prime numbers and how they are different from what is taught in earlier math courses, specifically the difference between an irreducible number and a prime number. We then move onto the majority of the discussion on prime numbers in quadratic fields and how they behave, specifically when a prime will ramify, split, or be inert. The final section of this paper will detail an explicit example of a quadratic field and what happens to prime numbers within it. The specific field we choose is $\mathbf{Q}(\sqrt{-5})$ and we will be looking at what forms primes will have to be of for each of the three possible outcomes within the field.

2. Quadratic Fields

One of the most important concepts of algebraic number theory comes from the factorization of primes in number fields. We want to construct

Date: March 17, 2017.

a way to observe the behavior of elements in a field extension, and while number fields in general may be a very complicated subject beyond the scope of this paper, we can fully analyze quadratic number fields.

Definition 1. A number is said to be *square free* if when decomposed into a product of prime numbers there are no repeated factors.

Definition 2. A *quadratic field* is a field of the form

$$\mathbf{Q}\left(\sqrt{d}\right) = \left\{a + b\sqrt{d} \mid a, b \in \mathbf{Q}\right\}$$

where d is a square free integer.

Our definition of a quadratic field does not include a way to analyze the different values of d. We introduce this through a set of polynomials that are dependent on the value of k in the congruence

$$d \equiv k \mod 4.$$

This appears in [1, Proposition 1.2, Chapter 3] and we appropriate it as a definition in our paper.

Definition 3. The *minimal polynomial* for a quadratic number field $\mathbf{Q}(\sqrt{d})$ is defined as

$$f_d(x) = \begin{cases} x^2 - d & d \equiv 2, 3 \mod 4; \\ x^2 - x + \frac{1-d}{4} & d \equiv 1 \mod 4. \end{cases}$$

This is important because the roots of the polynomial $f_d(x)$, $\pm\sqrt{d}$, are used to define the quadratic field $\mathbf{Q}(\sqrt{d})$.

Next, we need to define the ring of integers in a quadratic field, denoted $\mathcal{O}_K$, for $K = \mathbf{Q}\left(\sqrt{d}\right)$. We use discussion from [5, Introduction] in order to come up with the definitions that follow.

Definition 4. If $\alpha \in \mathcal{O}_K$ is an element of a quadratic field we define the *ring* $\mathbf{Z}[\alpha]$ to be the set

$$\mathbf{Z}[\alpha] = \{a + b \cdot \alpha \mid a, b \in \mathbf{Z}\}.$$

We can apply the above definition to determine how we construct the integers in a quadratic field. We define the ring of integers in a quadratic field in terms of d via [1, Proposition 2.24, Chapter 2],

Definition 5. Let $K = \mathbf{Q}\left(\sqrt{d}\right)$ be a quadratic field. If $d \equiv 2, 3 \mod 4$, then $\mathcal{O}_K = \mathbf{Z}[\sqrt{d}]$. If $d \equiv 1 \mod 4$, then $\mathcal{O}_K = \mathbf{Z}[\frac{1+\sqrt{d}}{2}]$.

To distinguish between integers of $\mathcal{O}_K$ and the more familiar integers in $\mathbf{Z}$, we refer to the latter as *rational integers*.

Next, we want to introduce the norm of a quadratic field. The norm is used to map elements of a larger field into a subfield. Since quadratic fields are extensions of the rational numbers, we want to send elements of the form $a + b\sqrt{d}$ to $\mathbf{Q}$.

Definition 6. Let K be a quadratic number field. We define the *norm* of an element $\alpha = a + b\sqrt{d} \in K$ as

$$N_{K/\mathbf{Q}}(\alpha) = a^2 - b^2 d.$$

Norms help us identify elements of quadratic fields called units. These will help us when we talk about the factorization of numbers in a field and what we describe as associates in Definition 11.

Definition 7. An element $u \in \mathbf{Z}[x]$ is a *unit* if and only if $N_{K/\mathbf{Q}}(u) = 1$.

The final piece of information we need for quadratic fields is the discriminant of the quadratic field extension. The discriminant of an algebraic number field is a value that determines the relative size of that number field.

Discriminants are very important and are used in one of the computations that can be used to find out how prime numbers act in quadratic fields, specifically we will be using the discriminant in Lemma 2 in Section 3.1 below. In a quadratic field extension the discriminant is defined as:

Definition 8. Let K=$\mathbf{Q}(\sqrt{d})$ be a quadratic number field. We define the *discriminant*, Δ_K, as

$$\Delta_K = \begin{cases} d, & \text{if } d \equiv 1 \mod 4; \\ 4d, & \text{if } d \equiv 2, 3 \mod 4. \end{cases}$$

3. Prime Numbers

The first definition of prime numbers that we encounter in mathematics is: A number $p \in \mathbf{Z}$ is prime if and only its only divisors are 1 and itself. This is true in the integers, but in more general rings of integers $\mathcal{O}_K$, this definition is actually for that of an *irreducible* number, not a prime number.

Definition 9. We define a number $n \in \mathcal{O}_K$ to be *irreducible* if there exist $a, b \in \mathcal{O}_K$ such that $n = ab$ implies that a or b is a unit. If n is not irreducible, then it is said to be *reducible*.

It just so happens that these groups of numbers are identical when dealing with the rational integers. In general, the set of all prime numbers is contained within the set of all irreducibles so all prime numbers are irreducible, but not all irreducible numbers are prime. This means that, in particular, any number that is reducible cannot be prime.

One of the first results a student of number theory learns is Euclid's Lemma:

Lemma 1. *If a prime p divides a product of integers ab, then p must divide a or b.*

We take this lemma as the definition of prime numbers in quadratic fields.

Definition 10. Let $a, b, p \in \mathcal{O}_K$. We say that p is *prime* if $p \mid ab$ implies $p \mid a$ or $p \mid b$.

Let's introduce some easy examples of how specific primes will behave in specific fields.

Example. Take $p = 5$ in $\mathbf{Z}[\sqrt{5}]$. Clearly in this field we still have 1 and 5 so we can write $5 = 5 \cdot 1$.

But, in this field, is there another way to compute the number 5? Based on previous definitions

$$\mathbf{Z}[\sqrt{5}] = \left\{ a + b\sqrt{5} | a, b \in \mathbf{Z} \right\}.$$

In order to show 5 is reducible in $\mathbf{Z}[\sqrt{5}]$ we use Definition 9. Since $N(\sqrt{5}) = 5$, which is greater than 1, we know that $\sqrt{5}$ is not a unit and 5 is reducible therefore not prime. We need to show that $\sqrt{5}$ is prime in order to complete showing that 5 is not prime in the field. To show that $\sqrt{5}$ is a prime in $\mathbf{Z}[\sqrt{5}]$ we need to show it is irreducible. We do this through the norm, $N(\sqrt{5}) = 5$. We can right this as the product of two norms such that $N\sqrt{5}) = N(\alpha)N(\beta)$. This can be written as $5 = N(\alpha)N(\beta)$ and by Euclid's Lemma, $5 \mid N(\alpha$ or $5 \mid N(\beta)$. Since the norm maps elements to the rational numbers and 5 is prime in the rational numbers we have that $\sqrt{5}$ is a prime, as desired.

Definition 11. We define two primes of $\mathcal{O}_K$ to be *associates* if they differ by a unit. That is if we have a unit, u and two primes, $\mathfrak{p}_1$ and $\mathfrak{p}_2$, we consider these primes to be associates if $\mathfrak{p}_1 = u \cdot \mathfrak{p}_2$.

If we can factor a number in two ways we do not consider these to be distinct factorizations if they involve swapping out associates to achieve this

factorization. This helps us in removing some inconsistencies in the logic behind our definitions in Definition 12.

Now that we have enough prior knowledge we can move onto the main section of this paper, how primes behave in quadratic fields.

3.1. **Behavior of Primes in Quadratic Fields.** First, let us examine what to look for regarding primes in quadratic fields. Primes behave in one of three ways when looked at in a quadratic field extension: either they split, they ramify, or they become inert.

Definition 12. Let $p \in \mathbf{Z}$ be a rational prime, and let $K = \mathbf{Q}(\sqrt{d})$ be a quadratic field.

(1) If there exist distinct primes (i.e. not associates) $\mathfrak{p}_1, \mathfrak{p}_2 \in \mathcal{O}_K$ such that $p = \mathfrak{p}_1\mathfrak{p}_2$, then p is *split*.
(2) If there exists a prime $\mathfrak{p} \in \mathcal{O}_K$ such that $p = u \cdot \mathfrak{p}^2$, then p is *ramified*, where u is a unit a discussed in definition 7.
(3) If there exists a prime $\mathfrak{p} \in \mathcal{O}_K$ such that $p = \mathfrak{p}$, then p is *inert*.

Example. Now take $p = 2$ in $\mathbf{Z}[\imath]$, this will allow us to give an example of when a unit must be allowed to obtain the true behavior of a prime. Then $2 = 2 \cdot 1$, since $2, 1 \in \mathbf{Z}[\imath]$.

$$\mathbf{Z}[\imath] = \{a + b\imath | a, b \in \mathbf{Z}\}$$

But we also have $2 = (1 + \imath)(1 - \imath)$. Then 2 factors non-trivially in $\mathbf{Z}[\imath]$, but we will introduce some definitions later that show $p = 2$ must be ramified. This is solved by looking at the equation

$$2 = \imath(1 - \imath)^2.$$

If we expand the right hand side of this equation we see that it is indeed equal to 2. In this case we have $\imath$ acting as a unit for the associates $-\imath$ and $\imath$.

Additionally in the last section, we introduced what $f_d(x)$ looks like for the different values of $d \equiv k \mod 4$. Using this, we can give an alternative characterization of inert, ramified, and split primes according to how $f_d(x)$ behaves mod p based on the discussion on [1, pg. 56].

Theorem 1. *A rational prime p is inert in $\mathcal{O}_K$ if and only if $f_d(x)$ is irreducible modulo p; it splits if and only if $f_d(x)$ modulo p factors into two different linear polynomials; and it ramifies if and only if $f_d(x)$ modulo p is the square of a linear polynomial.*

These relationships allow us to introduce a lemma that allows us to easily determine the ramified primes in a quadratic field.

Lemma 2. *Let $K = \mathbf{Q}(\sqrt{d})$ be a quadratic field. Then a rational prime p is ramified in $\mathcal{O}_K$ if and only if $p \mid \Delta_K$.*

Proof. By Theorem 1, we want to show that $f_d(x)$ factors as the square of a linear polynomial if and only if $p \mid \Delta_K$.
First consider the case when $d \equiv 2, 3 \mod 4$.

($\Rightarrow$) Let $f_d(x)$ modulo p be the square of a linear polynomial modulo p. Then $x^2 - d \equiv (x + \alpha)^2 \equiv x^2 + 2\alpha x + \alpha^2 \mod p$, by matching coefficients we have $2\alpha \equiv 0 \mod p$ and $\alpha^2 \equiv -d \mod p$. By Lemma 1 we know that $p \mid 2\alpha$ implies that $p \mid 2$ or $p \mid \alpha$. Since we are working in rational primes if $p \mid 2$ then specifically $p = 2$. Since $\Delta_K = 4d$ if $p = 2$ then $p \mid \Delta_K$ as desired. If $p \mid \alpha$ then $p \mid \alpha^2$ as well so $p \mid d$ by the congruences above, so it follows that $p \mid \Delta_K$. So in either case of $p \mid 2$ or $p \mid \alpha$ we have that $p \mid \Delta_K$.

($\Leftarrow$) Let $p \mid \Delta_K$ Then we have $p \mid d$ or $p \mid 2$. If $p \mid 2$ then $x^2 - d \equiv x^2 + 1 \mod 2$ or $x^2 - d \equiv x^2 \mod 2$. If we have the second case then we have $f_d(x)$ as the square of a linear polynomial modulo 2 as desired. If we have $x^2 - d \equiv x^2 + 1 \mod 2$ then we have $x^2 - d \equiv (x+1)^2 \mod 2$ since if we expand this polynomial on the right we get $x^2 + 2x + 1$. When reduced modulo 2 we have $x^2 + 1$ which again is equivalent to $(x+1)^2 \mod 2$ and $f_d(x)$ is the square of a linear polynomial modulo 2 as desired. If $p \mid d$ then $x^2 - d \equiv x^2 \mod p$ and $f_d(x)$ is the square of a linear polynomial modulo p as desired.

Now consider the case when $d \equiv 1 \mod 4$.

($\Rightarrow$) Let $f_d(x)$ modulo p be the square of a linear polynomial modulo p. Then $x^2 - x + \frac{1-d}{4} \equiv (x+\alpha)^2 \equiv x^2 + 2\alpha x + \alpha^2 \mod p$. By matching coefficients we have $2\alpha \equiv -1 \mod p$ and $\alpha^2 \equiv \frac{1-d}{4} \mod p$. If $2\alpha \equiv -1 \mod p$ then we can square both sides and get $4\alpha^2 \equiv 1 \mod p$. One of our congruences above is that $\alpha^2 \equiv \frac{1-d}{4} \mod p$. We can multiple by 4 on both sides to get $4\alpha^2 \equiv 1 - d \mod p$. Since we know that $4\alpha^2 \equiv 1 \mod p$ then $1 - d \equiv 1 \mod p$ so we have that $d \equiv 0 \mod p$ and $p \mid \Delta_K$ as desired.

($\Leftarrow$) Let $p \mid \Delta_K$. Then we have $p \mid d$ and $f_d(x) \equiv x^2 - x + \frac{1}{4} \equiv (x - \frac{1}{2})^2 \mod p$. So $f_d(x)$ is the square of a linear polynomial modulo p as desired. $\square$

One corollary to Lemma 2 is that it implies only finitely many primes ramify in any quadratic field. This is because the discriminant is finite so it has finitely many prime divisors.

Example. Let $K = \mathbf{Q}\left(\sqrt{-6}\right)$, so $\mathcal{O}_K = \mathbf{Z}\left[\sqrt{-6}\right]$.
Take $p = 2$. Then by Lemma 2 we know that 2 ramifies since $\Delta_K = -24$ and 2 divides -24.

For $p = 5$,

$$\begin{aligned} x^2 + 6 &\equiv x^2 + 5x + 6 \mod 5. \\ &\equiv (x+2)(x+3) \mod 5. \end{aligned}$$

so 5 splits in $\mathcal{O}_K$.

In this example we showed how two primes act in the quadratic field $\mathbf{Q}\left(\sqrt{-6}\right)$, and it was fairly simple to do.

The difficulty comes in when we take an arbitrary prime p and need to determine how it behaves within a quadratic field. Since there are infinitely many prime numbers and thus infinitely many quadratic field extensions it is infeasible to brute force a solution for all cases. So we need a way to determine the behavior of all primes in any specific quadratic field. This is done through the *Legendre symbol*.

Definition 13. Let p be an odd prime. We define the *Legendre symbol* by

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if a is a non-zero square modulo p;} \\ 0 & \text{if } a \equiv 0 \mod p; \\ -1 & \text{if a is not a square modulo p.} \end{cases}$$

We compute the Legendre Symbol as $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \mod p$. One of the properties this has is that if $n = ab$ and we are looking for $\left(\frac{n}{p}\right)$ then we can decompose n as its divisors and $\left(\frac{n}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$ in other words the Legendre Symbol is a multiplicative function. Also if $a \equiv b \mod p$ then $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$. Now that we have a way our way of determining the behavior of primes we need to formalize a way to conceptually analyze all primes in any quadratic field.

The next determining theorem we have to use is described in [1, Theorem 3.6, Chapter 3] on page 72.

Theorem 2. *If p,q are distinct odd primes then*

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

We can rearrange this equation to be in the following form:

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

This theorem gives us a much simpler way to determine the value of $\left(\frac{d}{p}\right)$. Based on discussion in [2, Quadratic Reciprocity] we can introduce a Proposition to deal with the special cases of this theorem namely when $p = 2$ and when $p = -1$.

Proposition 1.

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = \begin{cases} 1 \text{ if } p \equiv 1 \mod 4, \\ -1 \text{ if } p \equiv -1 \mod 4. \end{cases} \tag{2}$$

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} 1 \text{ if } p \equiv \pm 1 \mod 8, \\ -1 \text{ if } p \equiv \pm 3 \mod 8. \end{cases} \tag{3}$$

We can determine the properties of a prime by using the Legendre symbol through a proposition that appears in [1, Proposition 1.6, Chapter 3].

Proposition 2. *Let $K = \mathbf{Q}(\sqrt{d})$ be a quadratic number field and let p be an odd rational prime. Then p splits in K if and only if $\left(\frac{d}{p}\right) = 1$; it ramifies in K if and only if $\left(\frac{d}{p}\right) = 0$; and it is inert in K if and only if $\left(\frac{d}{p}\right) = -1$.*

Proof. From 5, in $\mathbf{Q}(\sqrt{d})$ we have $\mathcal{O}_K = \mathbf{Z}[\frac{d+\sqrt{d}}{2}]$ as the ring of integers. By 3 the minimal polynomial for this ring is

$$f_d(x) = x^2 - dx + \frac{d^2-d}{4} = (x^2 - \frac{d+\sqrt{d}}{2})(x^2 - \frac{d-\sqrt{d}}{2}).$$

Let p be an odd prime.

If $d \equiv 0 \mod p$ then

$$f_d(x) \equiv x^2 \mod p,$$

so p is ramified by Theorem 1.

If $d \equiv n^2 \mod p$ then

$$f_d(x) \equiv (x - \frac{n^2+n}{2})(x - \frac{n^2-n}{2}) \mod p,$$

so p is split by Theorem 1 as it is the product of two distinct linear polynomials.

If $d \not\equiv n^2 \mod p$ then $f_d(x)$ modulo p cannot be factored and

$$f_d(x) \equiv (x-\alpha)(x-\beta),$$

so by Theorem 1 p is inert. □

We can also use this same quadratic field and ring of integers to deal with when we have a prime that is not odd, i.e. $p = 2$.

Proposition 3. *Let $K = \mathbf{Q}(\sqrt{d})$ be a quadratic number field and let $p = 2$. Then p splits in K if and only if $\left(\frac{d}{p}\right) = 1$; it ramifies in K if and only if $\left(\frac{d}{p}\right) = 0$; and it is inert in K if and only if $\left(\frac{d}{p}\right) = -1$.*

Proof. We focus on $d \mod 8$ instead of $d \mod 2$ due to 1. If $d \equiv 0 \mod 8$ then $d^2 - d \equiv 0 \mod 8$ so $\frac{d^2-d}{4} \equiv 0 \mod 2$ and

$$f_d(x) \equiv x^2 \mod 2,$$

so 2 is ramified.

If $d \equiv 1 \mod 8$ then $d^2 - d \equiv 0 \mod 8$ and

$$f_d(x) \equiv x^2 + x \equiv x(x+1) \mod 2,$$

so 2 is split.

If $d \equiv 4 \mod 8$ then $d^- d \equiv 4 \mod 8$ and

$$f_d(x) \equiv x^2 + 1 \equiv (x+1)^2 \mod 2,$$

so 2 is ramified.

If$d \equiv 5 \mod 8$ then $d^2 - d \equiv 4 \mod 8$, and $\frac{d^2-d}{4} \equiv 1 \mod 2$ and

$$f_d(x) \equiv x^2 + x + 1 \mod 2,$$

so 2 is inert. □

Now we can look at any $\mathbf{Q}\left(\sqrt{d}\right)$ with discriminant $D = (-1)^a\, 2^b\, p_1 \cdots p_n$, in which all the p_i are distinct primes. From the above discussion that the Legendre symbol is a multiplicative function we have that

$$\left(\frac{D}{p}\right) = \left(\frac{-1}{p}\right)^a \left(\frac{2}{p}\right)^b \left(\frac{p_1}{p}\right) ... \left(\frac{p_n}{p}\right).$$

Based on our previous work we can see that this equation depends only on $p \mod 4$ and $p \mod 8$ for $\left(\frac{-1}{p}\right)^a$ and $\left(\frac{2}{p}\right)^b$. For the rest of the terms in the equation we can see that they are dependent on $p \mod p_i$. The combination of these relationships allows us to come to the following conclusion.

Corollary 1. *The factorization of an odd prime p in $\mathbf{Q}(\sqrt{d})$ depends only on the residue $p \mod 4d$.*

With this corollary, we can easily describe a prime in any quadratic field by factoring $4d$ into the product of distinct primes. Now that we have everything in terms of prime numbers, we can use quadratic reciprocity to solve for each $p \mod 4d$ and determine whether it splits or stays inert. Primes that ramify are the primes which divide the discriminant and are already being accounted for.

4. An Explicit Example

We are interested in the specific quadratic field:

$$\mathbf{Q}\left(\sqrt{-5}\right)$$

and determining what primes split, which ramify, and which stay inert.

We start with determining the discriminant of our specific fields, since $-5 \equiv 3 \mod 4$ then the discriminant is -20. Now we need to factor our discriminant into the product of distinct primes. This is very easily done,

$$-20 = -1 * 2^2 * 5.$$

So based on Lemma 2 we have presented all primes will ramify and we will be looking at all other odd primes modulo 20 which is equivalent to primes modulo -20.

All of our computations are of the form:

$$\left(\frac{-20}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{2}{p}\right)^2\left(\frac{5}{p}\right). \tag{4}$$

Example. Take (7) as above and $p = 3$.

$$\left(\frac{-20}{3}\right) = \left(\frac{-1}{3}\right)\left(\frac{2}{3}\right)^2\left(\frac{5}{3}\right)$$

Since $3 \equiv -1 \mod 4$ then $\left(\frac{-1}{3}\right) = -1$, for every p, $\left(\frac{2}{p}\right)^2$ is equal to 1, and we apply quadratic reciprocity to our equation to the resultant equation:

$$\left(\frac{-20}{3}\right) = (-1)(-1)^{\frac{5-1}{2}\frac{3-1}{2}}\left(\frac{3}{5}\right)$$

We can simplify this equation to get

$$\left(\frac{-20}{3}\right) = (-1)\left(\frac{3}{5}\right),$$

computing $\left(\frac{3}{5}\right)$ to arrive at our final answer:

$$\left(\frac{-20}{3}\right) = (-1)(-1) = 1.$$

So 3 splits in $\mathbf{Q}\left(\sqrt{-5}\right)$.

Now take $p = 11$.

$$\left(\frac{-20}{11}\right) = \left(\frac{-1}{11}\right)\left(\frac{2}{11}\right)^2\left(\frac{5}{11}\right)$$
$$\left(\frac{-20}{11}\right) = (-1)(-1)^{10}\left(\frac{11}{5}\right)$$
$$\left(\frac{-20}{11}\right) = (-1)(1)(1) = -1$$

Since $\left(\frac{-20}{11}\right) = -1$ then 11 is inert in $\mathbf{Q}\left(\sqrt{-5}\right)$.

Doing all of those computations for each prime modulo 20 we receive the following results:

$p \mod 20$	$\left(\frac{-20}{p}\right) =$	prime behavior
1	1	splits
3	1	splits
7	1	splits
9	1	splits
11	-1	inert
13	-1	inert
17	-1	inert
19	-1	inert

This table allows up to look at all odd primes modulo 20 and see how they will behave in $\mathbf{Q}\left(\sqrt{-5}\right)$. We see that 15 is not on the table and this because there are no primes that are 15 modulo 20 since they will always be divisible by 5. Now we have shown computations for computing the prime behavior in a specific quadratic field we can appropriate this for any quadratic field to discover the behavior of primes in that field.

References

[1] T. Weston, *Algebraic Number Theory* https://www.math.wisc.edu/ mmwood/748Fall2016/weston.pdf

[2] S. Mack-Crane, *Prime Splitting in Quadratic Fields, pt. 2* https://math.berkeley.edu/ sander/blog/prime-splitting-in-quadratic-fields-part-ii

[3] S. Mack-Crane, *Prime Splitting in Quadratic Fields, pt. 1* https://math.berkeley.edu/ sander/blog/prime-splitting-in-quadratic-fields-part-i

[4] D. Tall and I. Stewart, *Algebraic Number Theory and Fermat's Last Theorem, Third Edition*

[5] K. Conrad, *Factoring in Quadratic Fields* http://www.math.uconn.edu/ kconrad/blurbs/gradnumthy/quadraticgrad.pdf