Continued Fractions, Euclid's Algorithm, and Euclidean domains
MATH 414

Shawn Apodaca

1 Abstract

We will generalize both the Euclidean algorithm and a method of calculating continued fractions on Euclidean domains. We will then use these methods to find the greatest common denominator and continued fraction representation of $\frac{p}{q}$, where p, q are elements of the integers, Gaussian integers, or polynomials over the rationals.

2 Introduction

In this section, we will define continued fractions and some other relevant concepts and introduce notation.

2.1 Definitions and Notation

We begin immediately with a definition.

Definition 2.1.1. *A continued fraction is an expression of the form*

$$u_0 + \cfrac{1}{u_1 + \cfrac{1}{u_2 + \cfrac{1}{u_3 + \cfrac{1}{\ddots}}}}$$

We will denote a continued fraction by $[u_0; \mathbf{u}] = [u_0; u_1, u_2, u_3, \dots]$*, where* $\mathbf{u} = (u_1, u_2, u_3, \dots)$.

Note that u_0 may equal 0. In which case we may omit it. That is $[0; u_1, u_2, u_3, \dots] = [u_1, u_2, u_3, \dots]$. We may take $[\mathbf{u}]$ to be finite or infinite. In the case where $[\mathbf{u}] = [u_1, u_2, \dots, u_r]$ is finite, it may be simplified to a quotient. We call the denominator of this quotient the *continuant* of $\mathbf{u}$ and denote it by $|\mathbf{u}|$ or $|(u_1, u_2, \dots, u_r)|$. Further, we define $\mathbf{u}^- = (u_1, u_2, \dots, u_{r-1})$, $\mathbf{u}_- = (u_2, u_3, \dots, u_r)$, and $\{\mathbf{u}\} = (u_r, u_{r-1}, \dots, u_2, u_1)$. Finally, given $[\mathbf{u}]$, where $\mathbf{u}$ is finite with m components or infinite, the r^{th} *partial convergent*, where $r < m$, of $[\mathbf{u}]$ is the quotient $\frac{p_r}{q_r}$ such that $[u_0; u_1, u_2, \dots, u_r] = \frac{p_r}{q_r}$.

We will be primarily interested in finite continued fractions, so, unless stated otherwise, assume any $\mathbf{u}$ is finite. We will also write $\mathbf{uv}$ to mean $(u_1, \dots, u_r, v_1, \dots, v_r)$ [1].

2.2 Some Basic Results

Here we list and prove some simple results of our definitions. We will use that the partial convergents can be expressed recursively, without proof[1], as follows [2].

Proposition 2.2.1. *Let the* r^{th} *partial convergent of* $[u_0; \mathbf{u}]$ *be* $\frac{p_r}{q_r}$*. Then*

$$\begin{array}{llll} p_{-2} = 0, & p_{-1} = 1, & p_0 = u_0, & \dots \quad p_r = u_r p_{r-1} + p_{r-2} \\ q_{-2} = 1, & q_{-1} = 0, & q_0 = 1, & \dots \quad q_r = u_r q_{r-1} + q_{r-2} \end{array}$$

[1]For a proof, see Stein, *Elementary Number Theory: Primes, Congruences, and Secrets.*

Proposition 2.2.2. *Let* $\mathbf{u} = (u_1, u_2, \ldots, u_r)$. *Then*

$$|\mathbf{u}| = \begin{vmatrix} u_1 & 1 & 0 & 0 & \cdots & 0 \\ -1 & u_2 & 1 & 0 & \cdots & 0 \\ 0 & -1 & u_3 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & u_r \end{vmatrix}$$

Proof. By our definitions, $q_1 = u_1$ and $q_2 = u_2 q_1 + q_0 = u_2 u_1 + 1$, so proposition 2.2.2 clearly holds for $r = 1, 2$. For odd r, by normal operations on determinants, we have

$$|\mathbf{u}| = \begin{vmatrix} u_1 & 1 & 0 & 0 & \cdots & 0 \\ -1 & u_2 & 1 & 0 & \cdots & 0 \\ 0 & -1 & u_3 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & u_r \end{vmatrix} = \begin{vmatrix} 0 & 0 & 0 & 0 & \cdots & 0 & -1 & u_r \\ u_1 & 1 & 0 & 0 & \cdots & 0 & 0 & 0 \\ -1 & u_2 & 1 & 0 & \cdots & 0 & 0 & 0 \\ 0 & -1 & u_3 & 1 & \cdots & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & -1 & u_{r-1} & 1 \end{vmatrix}$$

We evaluate the determinant on the top row. Since r is even, this gives

$$|\mathbf{u}| = u_r q_{r-1} + \begin{vmatrix} u_1 & 1 & 0 & \cdots & 0 & 0 & 0 \\ -1 & u_2 & 1 & \cdots & 0 & 0 & 0 \\ 0 & -1 & u_3 & \cdots & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & u_{r-3} & 1 & 0 \\ 0 & 0 & 0 & \cdots & -1 & u_{r-2} & 0 \\ 0 & 0 & 0 & \cdots & 0 & -1 & 1 \end{vmatrix} = u_r q_{r-1} - \begin{vmatrix} 0 & 0 & 0 & \cdots & 0 & -1 & 1 \\ u_1 & 1 & 0 & \cdots & 0 & 0 & 0 \\ -1 & u_2 & 1 & \cdots & 0 & 0 & 0 \\ 0 & -1 & u_3 & \cdots & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & u_{r-3} & 1 & 0 \\ 0 & 0 & 0 & \cdots & -1 & u_{r-2} & 0 \end{vmatrix}$$

Evaluating again on the top row:

$$u_r q_{r-1} + q_{r-2} - 0 = u_r q_{r-1} + q_{r-2}$$

Where we have used that since the far right column of the resulting determinant contains only 0's, the determinant is 0. This is the exact formula we had used to express the continuant in proposition 2.2.1. □

We now prove a similar proposition for the numerator of a convergent.

Proposition 2.2.3. *Let* $\mathbf{u} = (u_1, u_2, \ldots, u_r)$. *Then*

$$p_r = |\mathbf{u}_-|$$

Proof. This follows immediately from the recursion formula for p_r, that $u_0 = 0$, and from the proof to proposition 2.2.2 [3]. □

3 Continued Fractions and The Euclidean Algorithm

In this section we will generalize the Euclidean algorithm, the notion of a greatest common denominator, and demonstrate the link between continued fractions and Euclidean domains.

3.1 The Euclidean Algorithm Over the Integers

We give the Euclidean algorithm for computing the greatest common divisor for two integers a, b.

Algorithm 3.1.1. *Given $a, b \in \mathbf{Z}$ where $a > b$.*

1. *Since $\gcd(a, b) = \gcd(|a|, |b|)$, assume $a > b > 0$. If $a = b$, return $\gcd(a, b) = b$ and terminate. If $b = 0$, return $\gcd(a, b) = a$ and terminate.*
2. *Use long division to write $a = bq + r$ where $0 \leq r < b$ where $q, r \in \mathbb{Z}$.*
3. *If $r = 0$, then $b \mid a$, return $\gcd(a, b) = b$ and terminate.*
4. *Set $a = b$ and $b = r$, go to step 2.*

This algorithm is only given as a convenience for the reader and will not be explicitly used. We will use a more general version of the Euclidean algorithm. For a proof, see Stein [4].

3.2 The Euclidean Algorithm over Euclidean Domains

We first define a Euclidean domain.

Definition 3.2.1. *A Euclidean domain is a commutative ring R with unit and no zero-divisor and a map $\lambda \colon R \setminus \{0\} \to \mathbb{N}$ such that given any $a, b \in R$, there exists $q, r \in R$ such that $r = 0$ or $a = qb + r$ where $\lambda(r) < \lambda(b)$ and given $a \neq 0$ and $b \neq 0$, $\lambda(a) \leq \lambda(ab)$.*

We will call λ a Euclidean valuation. The name *Euclidean* domain should be suggestive of the purpose for considering such a ring—the Euclidean algorithm. This gives us a method of calculating greatest common denominators in other Euclidean domains. Examples of Euclidean domains include the Gaussian integers and polynomials over the integers or rationals. The Euclidean algorithm holds over Euclidean domains with only minor changes [5].

Since any Euclidean domain is a ring, we can maintain the same meaning for an element d dividing another element a.

Definition 3.2.2. *Let E be a Euclidean domain and let $a, d \in E$. Then $d \mid a$ if there exists $c \in E$ such that $a = cd$.*

And we maintain a similar definition for the greatest common divisor.

Definition 3.2.3. *Let E be a Euclidean domain and let $a, b \in E$. Then $d \neq 0$ is the greatest common divisor if both*

1. *$d \mid a$ and $d \mid b$.*

2. If $h \mid a$ and $h \mid b$, then $h \mid d$.

Note that the greatest common divisor always exists for because 1 always divides any element. We now turn to the Euclidean algorithm over a Euclidean domain.

Algorithm 3.2.4. *Let E be a Euclidean domain. Given $a, b \in E$, such that $a, b \neq 0$ and where $\lambda(a) > \lambda(b)$.*

1. If $a = b$, return $\gcd(a, b) = b$ and terminate. If $b = 0$, return $\gcd(a, b) = a$ and terminate.

2. Use the division algorithm to write $a = bq + r$ where $0 \leq \lambda(r) < \lambda(b)$ and $q, r \in E$.

3. If $r = 0$, then $b \mid a$, return $\gcd(a, b) = b$ and terminate.

4. If $r \neq 0$, set $a = b$ and $b = r$, go to step 2.

Proof. Since E is a Euclidean domain, we have $a = bq + r$. So $a - bq = r$. Let $\gcd(a, b) = d$. Since $\gcd(a, b) = \gcd(a, b - na)$, we know $\gcd(a, b) = \gcd(b, r)$. So step 4 does not change the greatest common divisor. And since $\lambda(r) < \lambda(b)$ each time the division algorithm is performed, the algorithm will eventually terminate. □

With algorithm 3.2.4 in hand, we (finally) write down a method of computing a continued fraction. We will need to assume the Euclidean domain over which we are calculating the continued fraction is a division ring. From this point on, we will reserve the letter E for Euclidean domains that are division rings and λ for the Euclidean valuation associated with E. We are interested in elements of E of the form $\frac{p}{q}$ where $p, q \in E$, so we need to demonstrate that there is even a continued fraction representation of $\frac{p}{q}$.

Theorem 3.2.5. *Let $p, q \in E$ such that $q \neq 0$. Then there is a continued fraction representation of $\frac{p}{q}$.*

Proof. WLOG, assume $\gcd(p, q) = 1$. We perform algorithm 3.2.4 with inputs p, q. We get the chain

$$\begin{array}{rcll} p & = & u_0 q + r_1 & 0 < \lambda(r_1) < \lambda(q) \\ q & = & u_1 r_1 + r_2 & 0 < \lambda(r_2) < \lambda(r_1) \\ r_1 & = & u_2 r_2 + r_3 & 0 < \lambda(r_3) < \lambda(r_2) \\ & \vdots & & \\ r_{n-2} & = & u_{n-1} r_{n-1} + r_n & 0 < r_n < r_{n-1} \\ r_{n-1} & = & u_n r_n + 0 & 0 < \lambda(r_n) < \lambda(r_{n-1}) \end{array}$$

Dividing each line by the next (i.e., divide $p = u_0 q + r_1$ by b, etc.) and rewriting it.

$$\begin{array}{rcl} \frac{p}{q} & = & u_0 + \frac{r_1}{q} = u_0 + \frac{1}{\frac{q}{r_1}} \\ \\ \frac{q}{r_1} & = & u_1 + \frac{r_2}{r_1} = u_1 + \frac{1}{\frac{r_1}{r_2}} \\ & \vdots & \\ \frac{r_{n-1}}{r_n} & = & u_n \end{array}$$

Back substituting, we then get

$$\frac{p}{q} = u_0 + \cfrac{1}{u_1 + \cfrac{1}{u_2 + \cfrac{1}{\ddots + \cfrac{1}{u_n}}}}$$

So $\frac{p}{q} = [u_0; u_1, u_2, \ldots, u_n]$ [7]. □

Note that in the proof to theorem 3.2.5, we stumbled across an algorithm for calculating $\frac{p}{q}$.

Algorithm 3.2.6. *Let $p, q \in E$ where $q \neq 0$ and $\gcd(p, q) = 1$ and let $\frac{p}{q} = [u_0; \mathbf{u}]$.*

1. *If $q = 1$, then $u_0 = p$ and terminate. Set $i = 0$.*
2. *Use the division algorithm to write $p = u_i q + r_{i+1}$ where $0 \leq \lambda(r_{i+1}) < \lambda(q)$. Store u_i.*
3. *If $r_i = 0$, output $[u_0; \ldots, u_i]$*
4. *Set $p \leftarrow q$ and $q \leftarrow r_i$, add 1 to i, go to step 2.*

Proof. See the proof to theorem 3.2.5. □

Note that finding the continued fraction representation involves the same process as the calculating the greatest common divisor except we are interested in the part that was thrown out—the q in algorithm 3.2.4. Now that we are armed with a a method of calculating continued fractions in a more general setting, let's look at some of these settings.

4 Application: The Integers, Gaussian Integers, and Polynomials over a Field

In this section, we will look at applying algorithms 3.2.4 and 3.2.6 to several Euclidean domains.

4.1 The Integers

The integers are clearly a commutative division ring. To make $\mathbb{Z}$ a Euclidean domain, we define $\lambda \colon \mathbb{Z} \setminus \{0\} \to \mathbb{N}$ as $\lambda(n) = |n|$. As an example of the link between the Euclidean algorithm and calculating continued fractions, we simultaneously perform 3.2.4 9261 and 1291 and 3.2.6 on $\frac{9261}{1291}$.

$$
\begin{array}{rcrcrcr}
9261 &=& 1291 &\times& \mathbf{7} &+& 224 \\
1291 &=& 224 &\times& \mathbf{5} &+& 171 \\
224 &=& 171 &\times& \mathbf{1} &+& 53 \\
171 &=& 53 &\times& \mathbf{3} &+& 12 \\
53 &=& 12 &\times& \mathbf{4} &+& 5 \\
12 &=& 5 &\times& \mathbf{2} &+& 2 \\
5 &=& 2 &\times& \mathbf{2} &+& 1 \\
2 &=& 1 &\times& \mathbf{2} &+& 0
\end{array}
\qquad
\frac{9261}{1291} = \mathbf{7} + \cfrac{1}{\mathbf{5} + \cfrac{1}{\mathbf{1} + \cfrac{1}{\mathbf{3} + \cfrac{1}{\mathbf{4} + \cfrac{1}{\mathbf{2} + \cfrac{1}{\mathbf{2} + \cfrac{1}{\mathbf{2}}}}}}}}
$$

So $\gcd(9261, 1291) = 1$ and $\frac{9261}{1291} = [7; 5, 1, 3, 4, 2, 2, 2]$.

4.2 The Gaussian Integers

We start with a definition.

Definition 4.2.1. *The Gaussian integers is the set* $\{a + ib \mid a, b \in \mathbb{Z}\}$ *where* $i = \sqrt{-1}$.

It is now necessary to prove that the Gaussian integers are a Euclidean domain so we may use the algorithms 3.2.4 and 3.2.6. But we must first find a Euclidean valuation λ. We will use the notation $\bar{z}$ to indicate the complex conjugate of z and we will also use the fact, without proof, that the Gaussian integers are a commutative ring with no zero divisor.

Lemma 4.2.2. *Let* G *be the Gaussian integers. If* $\lambda \colon G \setminus \{0\} \to \mathbb{Z}^+$ *is defined* $\lambda(z) = z\bar{z}$*, then* λ *is a Euclidean valuation.*

Proof. Let $z_1, z_2 \in G$ such that z_1 and z_2 are nonzero, we have $\lambda(z_1 z_2) = z_1 z_2 \bar{z_1}\bar{z_2} = z_1 \bar{z_1} z_2 \bar{z_2} = \lambda(z_1)\lambda(z_2)$. Since we are in the Gaussian integers, $\lambda(z) \geq 1$. So $\lambda(z_1)\lambda(z_2) \geq \lambda(z_1)$. So $\lambda(z_1) \leq \lambda(z_1 z_2)$. □

We now prove that the Gaussian integers with λ from lemma 4.2.2 form a Euclidean domain. We first need a lemma.

Theorem 4.2.3. *The Gaussian integers with* $\lambda(z) = z\bar{z}$ *are a Euclidean domain.*

Proof. I make no attempt to reproduce the proof provided at Larry Freeman's blog [7]. □

We now use algorithm 3.2.4 and 3.2.6 to find both the greatest common divisor and the continued fraction representation of the complex numbers $z_1 = 112 + 313i$ and $z_2 = 254 + 108i$. We then have by algorithm 3.2.4 on z_1 and z_2 and algorithm 3.2.6 on $\frac{z_1}{z_2}$.

$$
\begin{array}{rcrcrcr}
112 + 313i &=& (254 + 108i) &\times& (\mathbf{1 + i}) &+& (-34 + 49i) \\
254 + 108i &=& (-34 - 39i) &\times& (\mathbf{-4 + 2i}) &+& (20 - 20i) \\
-34 - 39i &=& (20 - 20i) &\times& (\mathbf{-2i}) &+& (6 - 9i) \\
20 - 20i &=& (6 - 9i) &\times& (\mathbf{3 + i}) &+& (-7 + i) \\
6 - 9i &=& (-7 + i) &\times& (\mathbf{-1 + i}) &+& (-i) \\
-7 + i &=& (-i) &\times& (\mathbf{-i - 7i}) &+& 0
\end{array}
\tag{1}
$$

$$\frac{112+313i}{254+108i} = \frac{15563}{19045} + \frac{33703}{38090}i = \mathbf{1+i} + \cfrac{1}{\mathbf{-4+2i} + \cfrac{1}{\mathbf{-2i} + \cfrac{1}{\mathbf{3+i} + \cfrac{1}{\mathbf{-1+i} + \cfrac{1}{\mathbf{-1-7i}}}}}} \tag{2}$$

So $\gcd(112+313i, 254+108i) = -i$ or 1 and $\frac{112+313i}{254+108i} = [1+i; -4+2i, -2i, 3+i, -1+i, -1-7i]$.

4.3 Polynomials over the Rationals

We first define what we mean by polynomials over a field.

Definition 4.3.1. *We define the polynomials $F[x]$ over the field F as the set of all polynomials of the form*

$$a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$$

For $n \geq 0$ where $a_i \in F$ for all integers $i \geq 0$.

We define addition and multiplication of polynomials, and their inverses, in the familiar way from high school algebra. It is easy to check that the polynomials over a field form a commutative ring with no zero divisor. As was the case with the Gaussian integers, we will first find a map λ that is a Euclidean valuation. In preparation for this, we introduce the degree map.

Definition 4.3.2. *Let $p(x) = a_0 + a_1x + \cdots a_nx^n \in F[x]$. We define the degree map of $p(x)$ to be equal to the order of the highest order of x in $p(x)$. Explicitly, if $a_n \neq 0$, then $\deg p(x) = n$.*

The degree map is just the degree of the polynomial as it was in high school algebra. We now show that the degree map is a Euclidean valuation.

Lemma 4.3.3. *Let $F[x]$ be the ring of polynomials over the field F and let $p(x) = a_0 + a_1x + \cdots + a_nx^n$. Then the map $\lambda(p(x)) = \deg(p(x))$ is a Euclidean valuation.*

Proof. Let $q(x) = b_0 + b_1x + \cdots + b_kx^k \in F[x]$ where $b_k \neq 0$. Then $p(x)q(x) = a_0b_0 + (a_1b_0 + a_0b_1)x + a_nb_kx^{n+k}$. So $\lambda p(x)q(x) = n + k > n = \lambda p(x)$. If $q(x) = b_0 \neq 0$, then $\lambda p(x)q(x) = n = \lambda p(x)$. So we have shown $\lambda p(x) \leq \lambda p(x)q(x)$. So λ is a Euclidean valuation. □

We now prove the ring of polynomials over a field form a Euclidean domain.

Theorem 4.3.4. *The polynomial ring $F[x]$ over a field F with Euclidean valuation λ as defined in lemma 4.3.3 form a Euclidean domain.*

Proof. We already know $F[x]$ is a commutative ring with no zero divisor and λ is a Euclidean valuation, so all we need prove is a division algorithm. Let $f(x) = a_0 + a_1x + \cdots + a_mx^m \in F[x]$ and $g(x) = b_0 + b_1x + \cdots + b_nx^n \in F[x]$ where $a_m \neq 0$ and $b_n \neq 0$ and $\lambda(f(x)) \geq \lambda(g(x))$. Consider

$$\frac{a_m}{b_n}x^{m-n}g(x) = \frac{a_m}{b_n}b_0x^{m-n} + \frac{a_m}{b_n}b_1x^{m-n+1} + \cdots + a_mx^m$$

Note that a_mx^m is the same coefficient and same order as the highest order of $f(x)$. So if $h(x) = f(x) - \frac{a_m}{b_n}x^{m-n}g(x)$, then $\deg h(x) < \deg f(x)$. Then, by induction,

$$h(x) = q_1(x)g(x) + r(x)$$

Where $q_1(x), r(x) \in F[x]$ and $r(x) = 0$ or $\lambda(r(x)) < \lambda(g(x))$. So

$$h(x) = f(x) - \frac{a_m}{b_n}x^{m-n}g(x) = q_1(x)g(x) + r(x)$$

Solving for $f(x)$:

$$f(x) = \left(\frac{a_m}{b_n}x^{m-n} + q_1(x)\right)g(x) + r(x) = q(x)g(x) + r(x)$$

Where $q(x) = \frac{a_m}{b_n}x^{m-n} + q_1(x)$. And since $\lambda(g(x)) < \lambda(r(x))$, we have proved[1] a division algorithm [9]. So $F[x]$ with Euclidean valuation λ forms a Euclidean domain. □

We now apply algorithm 3.2.4 and 3.2.6 on to find both the greatest common divisor of the polynomials $p(x) = 3x^4 + x^2 - 2x - 1$ and $q(x) = 2x^2 + 1$ and the continued fraction representation of $\frac{p(x)}{q(x)}$.

$$\begin{aligned}
3x^4 + x^2 - 2x - 1 &= (2x^2 + 1) \times \left(\mathbf{\frac{3}{2}x^2} - \mathbf{\frac{1}{4}}\right) + \left(-2x - \tfrac{3}{4}\right) \\
2x^2 + 1 &= \left(-2x - \tfrac{3}{4}\right) \times \left(-\mathbf{x} + \mathbf{\frac{3}{8}}\right) + \tfrac{41}{32} \qquad (3) \\
-2x - \tfrac{3}{4} &= \tfrac{41}{32} \times \left(-\mathbf{\frac{64}{41}x} - \mathbf{\frac{24}{41}}\right) + 0
\end{aligned}$$

$$\frac{3x^4 + x^2 - 2x - 1}{2x^2 + 1} = \frac{3}{2}x^2 - \frac{1}{4} + \cfrac{1}{-x + \frac{3}{8} + \cfrac{1}{-\frac{64}{41}x - \frac{24}{41}}} \qquad (4)$$

Though we did not discuss it, it should be noted that we will typically insist that the greatest common divisor be *monic*. That is, the highest order term has coefficient 1 to ensure uniqueness. In our example, this amounts to noting that since $\lambda(\frac{41}{32}) = 0$, we then have $\gcd(p(x), q(x)) = 1$ and $\frac{p(x)}{q(x)} = [\frac{3}{2}x^2 - \frac{1}{4}; -x + \frac{3}{8}, -\frac{64}{41}x - \frac{24}{41}]$.

[1] This is taken from *Abstract Algebra* by Herstein and is presented here as a convenience to the reader.

5 Bibliography

1. Hensley, Doug. *Continued Fractions* (pp. 6)
2. Stein, William. *Elementary Number Theory: Primes, Congruences, and Secrets A Computational Approach* (pp. 97).
3. Hensley, Doug. *Continued Fractions* (pp. 6)
4. Stein, William. *Elementary Number Theory: Primes, Congruences, and Secrets A Computational Approach* (pp. 7).
5. Hensley, Doug. *Continued Fractions* (pp. 23)
6. Stein, William. *Elementary Number Theory: Primes, Congruences, and Secrets A Computational Approach* (pp. 101).
7. Freeman, Larry. http://fermatslasttheorem.blogspot.com/2005/06/division-algorithm-for-gaussian.html
8. Herstein, I. N.. *Abstract Algebra* (pp. 155)