Factoring Patterns in the Gaussian Plane

Steve Phelps

Introduction

This paper describes discoveries made at the Park City Mathematics Institute, 2002, as well as some proofs. Before the summer I understood Apollonian circles, inversion, complex number, and the like and had a frame of reference when trying to find patterns in the factors. When first looking for patterns, I noticed them because of my prior knowledge. Without that prior knowledge, I might not have discovered the patterns shared here. Some things here are accessible to high school students, but others are stated without proof but with references for the interested reader.

2002 morning problem solving sessions focused on the Gaussian integers. Geometrically, Gaussian integers represent the lattice points of the Cartesian coordinate plane as in Figure 1.

The Gaussian Integers are the lattice points in the coordinate plane

Algebraically, the Gaussian integers are a subset of the complex numbers. Symbolically, let \( \mathbb{G} \) be the set of Gaussian integers. Then

\[
\mathbb{G} = \left\{ a + ib : a, b \in \mathbb{Z} \text{ and } i = \sqrt{-1} \right\}
\]
One goal of the morning problem solving sessions was to determine those integers that can be written as the sum of two squares. For example, $13 = 2^2 + 3^2$. However, 7 cannot be written as the sum of two squares. Furthermore, some numbers can be written as the sum of two squares in more than one way. Observe that $50 = 7^2 + 1^2 = 5^2 + 5^2$. The key to determining which numbers could and could not be written as the sum of two squares was the multiplication and factorization of Gaussian integers.

**Multiplying Gaussian Integers**

The nature of some morning activities led to the multiplication of Gaussian integers. For those familiar with multiplying complex numbers, the ordinary complex multiplication will do:

$$(a+bi)(c+di) = (ac-bd) + i(ad+bc)$$

For those less familiar, a “hiking” analogy is appropriate. To explore the effects of multiplying $2+3i$ by ordinary integers or by integer multiples of $i$, pretend you are standing at the origin of a graph, facing in the direction of $2+3i$. If multiplying by an ordinary integer, say 2, simply step off two $2+3i$ “steps” in the direction of $2+3i$. If multiplying by $-2$, take two $2+3i$ “steps” backwards. If multiplying by $i$, before taking any steps, turn $90^\circ$ to the left, then take one $2+3i$ step. If multiplying by $2i$, turn $90^\circ$ to the left, then take two $2+3i$ steps. Multiplying by negative integer multiples of $i$ has the same effect, except requires turning $90^\circ$ to the right before taking any steps as in Figure 2.

![Figure 2. Some multiples of $2+3i$](image-url)
Figure 3 shows more Gaussian integer multiples of \( 2 + 3i \). Plotting all the multiples has the effect of creating a lattice-sort of road map showing how to get from the origin to any other multiple of \( 2 + 3i \). The lattice can also be obtained by rotating the coordinate plane about the origin through an angle of \( \theta = \tan^{-1}\left(\frac{3}{2}\right) \) radians, followed by a dilation centered at the origin with a scale factor of \( \sqrt{13} \). The essence of this lattice is that it shows how to get from the origin to any multiple of \( 2 + 3i \).

**Figure 3.**
A lattice of multiples of \( 2 + 3i \)

**Finding other products**

One challenge is to find more than one way to express a Gaussian integer as the product of two Gaussian integers. There is a correct way to do this and an incorrect way to do this. For example, \( 13 = (2 + 3i)(2 - 3i) \). However, 13 can also be written as \((3 + 2i)(3 - 2i)\). This would not count as a “different” way of expressing 13. The factors used are called “associates.” Associates are two Gaussian integers who differ only by a factor of \( i, -i, \) or \(-1\). For example, notice that \( 2 + 3i = i(3 - 2i) \). We are looking for
two products whose factors are not associates. For example, $50 = (5 + 5i)(1 - i)$ and $50 = (7 + i)(7 - i)$. But how does one find these factors? Guess and check could certainly be a method one might employ (but not a very efficient one). A different method of finding factors is based on the geometry of the multiplication algorithm, and on the geometry of the circle, particularly, the fact that a right angle can be inscribed in a semi-circle.

**A Method for Factoring Integers**

The following described method for factoring integers is based on circles and right angles. The right angles are found in the multiplication of Gaussian integers (multiplying by $i$ or $-i$). To illustrate this method, we find the Gaussian factors of 10. In Figure 4, stand at the origin facing $1 + 3i$, and take one $1 + 3i$ step forward (multiplying by 1). Turn to the right (multiplying by $-i$) and take three $1 + 3i$ steps forward (multiplying by $-3i$). The result is 10. In total, $1 + 3i$ is multiplied by 1 followed by $-3i$, or using the distributive property, $(1 + 3i)(1 - 3i) = 10$.

![Figure 4. One way to factor 10](image)

It is easy to find this factorization of 10. But are there others? In Figure 4, notice the right angle at $1 + 3i$. From elementary geometry, there is a circle through $1 + 3i$, the origin and 10. Furthermore, this circle contains nine other lattice points other than 10 and...
the origin as seen in Figure 5. Each one of these lattice points can be used to factor 10 into two Gaussian factors. Associated with each lattice point is a right triangle whose hypotenuse is the segment from the origin to 10 as in Figure 6.

In practice, one need not work with all the triangles in Figure 6, only the triangles in the first quadrant.

*Figure 5.*
The lattice points on the circle
**A specific example: Factoring 10 using the lattice point 2+4i**

Let’s explore the right triangle created by the lattice point 2+4i (the triangle associated with 2+4i) and see what factors that lattice point reveals. In Figure 7, the triangle associated with 2+4i contains four other lattice points: 1+2i, 4+3i, 6+2i, and 8+i. These lattice points on the triangle can be used to determine the factors of 10.

Stand at the origin and face the lattice point 2+4i. Taking a step requires that it be to another lattice point on the triangle in the direction of 2+4i. Furthermore, every step must be the same size and requires planning. Standing at the origin, there are two choices for the first step: 2+4i, or 1+2i, leading half way to the lattice point 2+4i.

Standing at the origin facing the lattice point 2+4i, take two 1+2i steps (multiplying 1+2i by 2). That leads to 2+4i. Standing at 2+4i, turn 90° to the right (multiplying by −i) and take four 1+2i steps (multiplying by −4i). That leads to 10. In total, 1+2i by 2, followed by −4i. Using the distributive property,

\[(1+2i)(2−4i)=10\]
What happens if we start out taking one $2 + 4i$ step? That step leads to the lattice point. Turning $90^\circ$ to the right (multiplying by $-i$) and taking two $2 + 4i$ steps (multiplying by $-2i$), leads 10. Using the distributive property, $(2 + 4i)(1 - 2i) = 10$.

Though the factorization method is essentially the same as the other one (the factors are associates), it nevertheless is a factorization, and the lattice point led to four factors of 10: $2 + 4i, 2 - 4i, 1 + 2i, and 1 - 2i$. Is it true that each lattice point on the circle is a factor of 10? No. Referring back to Figure 6, for $9 + 3i$ to be a factor, one needs to take a whole number of $9 + 3i$ steps along both legs of the associated right triangle. Standing at the origin and taking one $9 + 3i$ step leads to the lattice point. Turning right requires a step that is a multiple of $9 + 3i$ which is impossible.

The factors of 10 revealed by each lattice point are seen in Table 1. Readers should verify that these are indeed factors (not by multiplying, but by employing the methods of this article). For those familiar with the workings of complex numbers, the factors occur in conjugate pairs $a \pm ib$. And of course, these are not the only Gaussian factors of 10; 1, 2, 5, and 10 are left off the list for now. Not because they are not Gaussian integers, for they are. Each is of the form $a + bi$ with $b = 0$. The list of factors
can be expanded by considering all the associates of each factor. For example, if \( 2 + i \) is a factor of 10, then so are \(-1 + 2i\), \(1 - 2i\) and \(-2 - i\). Using only the factors in Table 1, “What other patterns are there in the Gaussian factors of 10?”

<table>
<thead>
<tr>
<th>Lattice Points</th>
<th>Factors</th>
</tr>
</thead>
<tbody>
<tr>
<td>5 + 5i</td>
<td>1 + i, 1 - i, 5 - 5i, 5 + 5i</td>
</tr>
<tr>
<td>8 + 4i</td>
<td>2 + i, 2 - i, 4 + 2i, 4 - 2i</td>
</tr>
<tr>
<td>9 + 3i</td>
<td>3 + i, 3 - i</td>
</tr>
<tr>
<td>2 + 4i</td>
<td>1 + 2i, 1 - 2i, 2 + 4i, 2 - 4i</td>
</tr>
<tr>
<td>1 + 3i</td>
<td>1 + 3i, 1 - 3i</td>
</tr>
</tbody>
</table>

Patterns in the Gaussian Factors of 10

![Figure 8. The Gaussian Factors of 10](image-url)
Seeing all the Gaussian factors of 10 as in Figure 8 should be convincing that there is indeed some sort of pattern or structure to the factors that begs for further study. There is obviously rotational symmetry and reflection symmetry thanks to the associate factors. Is there any other symmetry or structure that is hidden in the factors? Pursuing this question is where things really get interesting.

Step back for a moment and examine the factors of 10 associated with the lattice point \(2 + 4i\). Graphing them, there seems to be nothing exceptionally interesting except for the reflection symmetry in the \(x\)-axis due to the conjugate pairs seen in Figure 9. However, with an understanding of elementary geometry and knowledge of quadrilaterals, these factors are recognized as the vertices of an isosceles trapezoid. Isosceles trapezoids are cyclic, which means their vertices lie on a circle. So the factors of 10 associated with the lattice point \(2 + 4i\) lie on a circle. Now, three non-linear random points are all that are needed to determine a unique circle. The probability that four random points be contained in one circle is rather small (in fact, the probability is zero). Granted, these may not be random points, but there must be something up here for the factors to be concyclic.

Figure 9.
The factors associated with the lattice point \(2 + 4i\) lie on a circle.
What about the other lattice points? It is easy for the lattice points $5 + 5i$ and $8 + 4i$ because they have two pairs of conjugate pair factors. The factors for each will lie on a circle. The factors for $1 + 3i$ and $9 + 3i$ do lie on a circle, but they seem to break the pattern as seen in Figure 10. Verifying this is worth the effort and cements an understanding of how the factoring method works.

![Diagram](image.png)

**Figure 10.**

The factors on circles, with one circle that does not fit the pattern.

And what about the ordinary integer factors 1, 2, 5, and 10? In Figure 11, these factors are shown to lie on circles, too, providing stronger evidence that there is something funny about the circle that seems to break the pattern. However, all the other circles required 4 points! How can a circle be determined through 2 and 5? The answer to this question lies in what are known as *coaxal circles*. After discussing these circles, we explore the circles that make up a coaxal system of circles and gain a better understanding on how to make all the factors fit the pattern. Moreover, we extend the pattern in a number of unsuspecting ways.
Coaxal Circles – an Introduction

Figure 12 is an example of coaxal circles, or a coaxal system of circles. In Figure 12, there are two distinctly different “families” of circles – one blue and the other red. The blue family of circles passes through the points $A$ and $B$. The red family of circles seems to “shrink” towards the point $A$ and $B$. Points $A$ and $B$ are referred to as the limiting points of the coaxal system. Furthermore, points $A$ and $B$ lie on the blue line. This blue line is considered to be a circle in the blue family. Consider it to be a circle of infinite radius. Likewise, there appears to be a red line perpendicular to the blue line (indeed, it is the perpendicular bisector of $A$ and $B$). It, too, is considered to be a circle of infinite radius, and is a full-fledged member of the red family.
A Coaxal System of Circles

What is intriguing about a coaxal system is that every blue circle intersects every red circle at a $90^\circ$ angle. Thus, the blue circles and red circles are orthogonal. Given that every circle in one family is orthogonal to every circle in the other, it seems reasonable to consider the two perpendicular lines to be a part of their respective families. The two perpendicular lines serve as a sort of axis for the system (hence the name coaxal), in that every circle of the blue family has its center on the red perpendicular, and every circle in the red family has its center on the blue perpendicular.

The red family of circles is a special family of circles known as Apollonian circles. Apollonian circles are defined as follows: given two points – $A$ and $B$ – and a point $P$, an Apollonian circle is the locus of points satisfying

$|P - A| = k|P - B|$

where $|P - A|$ is the distance from $P$ to $A$, $|P - B|$ the distance from $P$ to $B$, and $k$ is a constant, $k \geq 0$. In layman’s terms, an Apollonian circle is the collection of points $P$ whose distance from a given point $A$ is a multiple of its distance from another given point $B$ as seen in Figure 13.

![Figure 13. Some Apollonian circles with a red one for $k = 0.59$](image)

A proof that the definition of Apollonian circles (the red circles) define a family of coaxal circles

In Figure 12, coaxal circles have centers lying on the $x$-axis (the red circles) or $y$-axis (the blue circles). Therefore, let the limit points be located at $A(-a,0)$ and $B(a,0)$. 

Furthermore, the centers of these circles will be located on the x-axis. Let point $P(x, y)$ be such that $d(P, B) = k \cdot d(P, A)$ where $d(A, P)$ means the distance from $A$ to $P$ and $k \geq 0$. This is the definition of Apollonian circles. Using the distance formula yields

$$(x-a)^2 + y^2 = k^2 \left((x-(-a))^2 + y^2\right)$$

or

$$(x-a)^2 + y^2 = k^2 \left((x+a)^2 + k^2y^2\right).$$

Expanding we have

$$x^2 - 2ax + a^2 + y^2 = k^2x^2 + 2ka^2 + k^2a^2 + k^2y^2.$$ Collecting like terms we have

$$(1-k^2)x^2 - 2a(1+k^2)x + (1-k^2)y^2 = (k^2 - 1)a^2.$$ Dividing to make the leading coefficient 1 we have

$$x^2 - 2a\frac{(1+k^2)}{(1-k^2)}x + y^2 = -a^2.$$ Completing the square we have

$$x^2 - 2a\frac{(1+k^2)}{(1-k^2)}x + \left[a\frac{(1+k^2)}{(1-k^2)}\right]^2 + y^2 = \left[a\frac{(1+k^2)}{(1-k^2)}\right]^2 - a^2.$$ Simplifying, we get

$$\left(x - a\frac{(1+k^2)}{(1-k^2)}\right)^2 + y^2 = a^2\left[\frac{(1+k^2)}{(1-k^2)} - 1\right]^2.$$ Letting $\lambda = \frac{1+k^2}{1-k^2}$, the equation above becomes

$$\left(x - a\lambda\right)^2 + y^2 = a^2\left(\lambda - 1\right)^2.$$ This is the equation of a circle of radius $r = a(\lambda - 1)$ and center $(a\lambda, 0)$. Hence, every circle in the red family has a radius of $r = a(\lambda - 1)$ and center $(a\lambda, 0)$. We have established that the definition of Apollonian circles does indeed describe a family of circles.

So as to understand these red circles better, examine what happens to $\lambda = \frac{1+k^2}{1-k^2}$ as $k$ varies among the all possible values for $k \geq 0$. Two values of $k$ which are of
interest are when $k = 0$ and when $k = 1$ (this is a zero of the denominator). When $k = 0$, $\lambda = 1$. We glean two bits of information about the circles. First of all, by the definition of Apollonian circles, $d(P, B) = k \cdot d(P, A)d(P, B) = k \cdot d(P, A)$; therefore, $d(P, B) = 0$. Hence, point $P$ and point $B$ are the same point. Second of all, when $k = 0$, $\lambda = 1$, and that corresponds to a circle centered at $(a, 0)$ of radius $r = 0$. Again, this means point $P$ and point $B$ are the same point. Hence, when $\lambda = 1$, $P$ is one of the limiting points of the system.

When $k = 1$, $\lambda$ is undefined (but $\lambda$ approaches $\infty$ as $k$ approaches 1). As above, we obtain information about the nature of the circle associated with $k = 1$ from both the definition of Apollonian circles and from the equation $(x - a\lambda)^2 + y^2 = a^2 (\lambda - 1)^2$. From the definition of Apollonian circles, $d(P, B) = d(P, A)$. This is the definition of the perpendicular bisector of points $A$ and $B$. From the equation of the circle, as $\lambda$ approaches $\infty$, the center of the circle moves along the $x$-axis away from the origin, and the radius of the circle approaches $\infty$. In essence, this corresponds to a circle centered at a point infinitely far from the origin along the $x$-axis with an infinite radius.

When $0 < k < 1$, $d(P, B) < d(P, A)$, which implies that point $P$ is closer to point $B$ than to point $A$. Indeed, $\lambda$ is always positive for these values of $k$. From the equation of the circles, the center of the circle lies to the right of $B(a, 0)$ on the $x$-axis. The radius is $a(\lambda - 1) = a\lambda - a$, so the distance from the origin to the center of the circle is greater than the radius of the circle, hence, these circles do not intersect the $y$-axis.

When $k > 1$, $d(P, B) > d(P, A)$, which implies that point $P$ is closer to point $A$ than to point $B$. Indeed, $\lambda$ is always negative for these values of $k$. From the equation of the circles, the center of the circle lies to the left of $A(-a, 0)$ on the $x$-axis.

We now know the “structure” of the red family – the Apollonian family – of circles. They all have an equation of the form $(x - a\lambda)^2 + y^2 = a^2 (\lambda - 1)^2$ where $\lambda = \frac{1 + k^2}{1 - k^2}$. Depending on the value of the parameter $\lambda(k)$ where $k \geq 0$, we obtain every circle in the family. We now establish a value of $a$ for the coaxal system that is derived from the factors of 10.
Coaxal Circles for the Gaussian Factors of 10.

Figure 14 has circles colored blue and red to represent the coaxal family to which they belong. Points $A$ and $B$ are the limiting points of the coaxal family – every circle in the blue family (provided we can find others) must pass through those two points. If we determine the coordinates of those limiting points, we see that point $A$ has coordinates $\left(-\sqrt{10}, 0\right)$ and point $B$ has coordinates $\left(\sqrt{10}, 0\right)$. Points $A$ and $B$ are located at the square roots of 10 on the real axis!

Using the blue circles to determine the value of $a$ is $\sqrt{10}$.

In Figure 14, choose a particular pair of factors of 10, say, $2 + i$ and $4 - 2i$. The product of these two factors is 10 with a circle from the blue family that passes through them both. Recalling that each circle in the blue family must have its center in the $y$-axis, every circle must have an equation of the form

$$x^2 + (y-h)^2 = r^2.$$  However, every one of these circles passes through the limiting points $A(-a,0)$ and $B(a,0)$. Using the Pythagorean Theorem, we rewrite the equation of the blue circles as $x^2 + (y-h)^2 = h^2 + a^2$, or by expanding and collecting like terms,

$$x^2 + y^2 - 2hy = a^2.$$  

We know two points on this circle: $(2,1)$ and $(4,-2)$. Therefore,

$$2^2 + 1^2 - 2h = 5 - 2h = a^2 \quad \text{and} \quad 4^2 + (-2)^2 - 2(-2)h = 20 + 4h = a^2$$

or
\[ 5 - 2h = 20 + 4h \]

or

\[ h = -\frac{5}{2} \]

This means that \( a^2 = 10 \) or \( a = \pm \sqrt{10} \).

Do we obtain the same result for another pair of factors, say, \( 1 + 3i \) and \( 1 - 3i \)? As above, they must satisfy the equation \( x^2 + y^2 - 2hy = a^2 \), so

\[ 1^2 + 3^2 - 2(3)h = 10 - 6h = a^2 \quad \text{and} \quad 1^2 + (-3)^2 - 2(-3)h = 10 + 6h = a^2 \]

or

\[ 10 - 6h = 10 + 6h \]

or

\[ h = 0 \]

This means that \( a^2 = 10 \) or \( a = \pm \sqrt{10} \).

Now consider the coaxal circles further. In Figure 14, if there are other circles in the blue family, they must all be orthogonal to the circles in the red family. Furthermore, based on the discussion of coaxal circles, their centers must lie on the \( y \)-axis. Likewise, if there are other circles in the red family, they must be orthogonal to every circle in the blue family. Just as with the blue circles, every circle in the red family has its center on the \( x \)-axis. Again, referring back to the coaxal circles discussion, the \( y \)-axis must be a member of the red family of circles, and the \( x \)-axis must be a member of the blue circles. If we consider the ordinary integer factors of 10 (1, 2, 5, and 10) all lie on the \( x \)-axis, and the axis passes through the limiting points \( A \) and \( B \), is seems even more reasonable to think that the \( x \)-axis is a member of the blue family of circles.

With an understanding of coaxal circles, in particular, where the centers of the circles lie, we construct circles from both families that pass through the Gaussian factors of 10 as in Figure 15. To see a comparison, the factors are included with and without the circles.
Recall any circle from the blue family intersects any circle from the red family at a 90°. Furthermore, circles from different families intersect in two points. Granted, the two circles need not intersect at a lattice point (which is a Gaussian integer), however, we explore two circles from this coaxal system – one circle from each family – that intersect at Gaussian integers as in Figure 16. In this particular example, the intersection points of the circles are $1 - i$ and $5 + 5i$. The product of these two intersection points is 10. Each pair of factors of 10 is the pair of intersection points of a circle in the blue family and a circle from the red family.
Figure 16.

The intersection points are the factor pairs of 10!

Now consider two other circles whose intersections points are not Gaussian integers. In Figure 17, point $K$ is approximately $-1.21 + 1.35i$ and point $L$ is approximately $-3.69 - 4.12i$. Their product is 10.

Figure 17.

The product of the intersections of any two circles is 10!
Other Oddities of the Gaussian Factors.

There are some other strange behaviors referred to earlier. Recall that 

\[ 13 = (2 + 3i)(2 - 3i) \]

It appears that 13 is not a prime number in the Gaussian integers! 13 has no factors other than 1 and 13 in the ordinary integers; however, we can find factors in the Gaussian integers. 13 has sixteen Gaussian factors seen in Figure 18. Though having relatively few factors, we can still construct a coaxal system of circles with a circle from each family passing through two factors of 13. Indeed, if 13 can be factored as \( \alpha \beta \), then there is a circle from each family that passes through \( \alpha \) and \( \beta \).

The limiting points of this coaxal system are \( \pm \sqrt{13} \).

\[ \text{Figure 18.} \]
\text{The Gaussian Factors of 13! 13 is not prime!} \]

Gaussian Factors of 20.

To provide other examples of Gaussian factor patterns, consider the Gaussian factors of 20 in Figure 19. When graphed in the plane, the factors look strikingly similar to the factors of 10. Though not in the figure, the limiting points are indeed \( \pm \sqrt{20} \).
Figure 19a.
The Gaussian Factors of 20

Figure 19b.
The Gaussian Factors of 20 with the Coaxal Circles
References.


