Introduction to Number Theory
Supplement on Gaussian Integers

Spring 2016

Last Updated: April 12, 2016

This is a secondary supplemental note on the Gaussian integers, written for my Spring 2016 Elementary Number Theory Class at Brown University.

In this note, we cover the following topics.

(1) Assumed prerequisites from other lectures.
(2) Which regular integer primes are sums of squares?
(3) How can we classify all Gaussian primes?

1. Assumed Prerequisites

Although this note comes shortly after the previous note on the Gaussian integers, we covered some material from the book in the middle. In particular, we will assume use the results from chapters 20 and 21 from the textbook.

Most importantly, for p a prime and a an integer not divisible by p, recall the Legendre symbol $\left(\frac{a}{p}\right)$, which is defined to be 1 if a is a square mod p and -1 if a is not a square mod p. Then we have shown Euler's Criterion, which states that

$$a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \pmod{p}, \tag{1}$$

and which gives a very efficient way of determining whether a given number a is a square mod p.

We used Euler's Criterion to find out exactly when -1 is a square mod p. In particular, we concluded that for each odd prime p, we have

$$\left(\frac{-1}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1 \pmod 4 \\ -1 & \text{if } p \equiv 3 \pmod 4 \end{cases}. \tag{2}$$

Finally, we assume familiarity with the notation and ideas from the previous note on the Gaussian integers.

2. Understanding When $p = a^2 + b^2$.

Throughout this section, p will be a normal odd prime. The case $p = 2$ is a bit different, and we will need to handle it separately. When used, the letters a and b will denote normal integers, and q_1, q_2 will denote Gaussian integers.

We will be looking at the following four statements.

(1) $p \equiv 1 \pmod 4$

(2) $\left(\frac{-1}{p}\right) = 1$
(3) p is *not* a Gaussian prime
(4) $p = a^2 + b^2$

Our goal will be to show that each of these statements are equivalent. In order to show this, we will show that

$$(1) \implies (2) \implies (3) \implies (4) \implies (1). \tag{3}$$

Do you see why this means that they are all equivalent?

This naturally breaks down into four lemmas.

We have actually already shown one.

Lemma 1. (1) $\implies$ (2).

Proof. We have already proved this claim! This is exactly what we get from Euler's Criterion applied to -1, as mentioned in the first section. □

There is one more that is somewhat straightfoward, and which does not rely on going up to the Gaussian integers.

Lemma 2. (4) $\implies$ (1).

Proof. We have an odd prime p which is a sum of squares $p = a^2 + b^2$. If we look mod 4, we are led to consider

$$p = a^2 + b^2 \pmod 4. \tag{4}$$

What are the possible values of $a^2 \pmod 4$? A quick check shows that the only possibilites are $a^2 \equiv 0, 1 \pmod 4$.

So what are the possible values of $a^2 + b^2 \pmod 4$? We must have one of $p \equiv 0, 1, 2 \pmod 4$. Clearly, we cannot have $p \equiv 0 \pmod 4$, as then $4 \mid p$. Similarly, we cannot have $p \equiv 2 \pmod 4$, as then $2 \mid p$. So we necessarily have $p \equiv 1 \pmod 4$, which is what we were trying to prove. □

For the remaining two pieces, we will dive into the Gaussian integers.

Lemma 3. (2) $\implies$ (3).

Proof. As $\left(\frac{-1}{p}\right) = 1$, we know there is some a so that $a^2 \equiv -1 \pmod p$. Rearranging, this becomes $a^2 + 1 \equiv 0 \pmod p$.

Over the normal integers, we are at an impasse, as all this tells us is that $p \mid (a^2 + 1)$. But if we suddenly view this within the Gaussian integers, then $a^2 + 1$ factors as $a^2 + 1 = (a + i)(a - i)$.

So we have that $p \mid (a + i)(a - i)$. If p were a Gaussian prime, then we would necessarily have $p \mid (a + i)$ or $p \mid (a - i)$. (Do you see why?)

But is it true that p divides $a + i$ or $a - i$? For instance, does p divide $a + i$? No! If so, then $\frac{a}{p} + \frac{i}{p}$ would be a Gaussian integer, which is clearly not true.

So p does not divide $a + i$ or $a - i$, and we must therefore conclude that p is not a Gaussian prime. □

Lemma 4. (3) $\implies$ (4).

Proof. We now know that p is not a Gaussian prime. In particular, this means that p is not irreducible, and so it has a nontrivial factorization in the Gaussian integers. (For example, 5 is a regular prime, but it is not a Gaussian prime. It factors as $5 = (1+2i)(1-2i)$ in the Gaussian integers.)

Let's denote this nontrivial factorization as $p = q_1 q_2$. By nontrivial, we mean that neither q_1 nor q_2 are units, i.e. $N(q_1), N(q_2) > 1$. Taking norms, we see that $N(p) = N(q_1)N(q_2)$.

We can evaluate $N(p) = p^2$, so we have that $p^2 = N(q_1)N(q_2)$. Both $N(q_1)$ and $N(q_2)$ are integers, and their product is p^2. Yet p^2 has exactly two different factorizations: $p^2 = 1 \cdot p^2 = p \cdot p$. Since $N(q_1), N(q_2) > 1$, we must have the latter.

So we see that $N(q_1) = N(q_2) = p$. As q_1, q_2 are Gaussian integers, we can write $q_1 = a + bi$ for some a, b. Then since $N(q_1) = p$, we see that $N(q_1) = a^2 + b^2$. And so p is a sum of squares, ending the proof. □

Notice that $2 = 1 + 1$ is also a sum of squares. Then all together, we can say the following theorem.

Theorem 5. *A regular prime p can be written as a sum of two squares,*

$$p = a^2 + b^2, \tag{5}$$

exactly when $p = 2$ or $p \equiv 1 \pmod 4$.

A remarkable aspect of this theorem is that it is entirely a statement about the behaviour of the regular integers. Yet in our proof, we used the Gaussian integers in a very fundamental way. Isn't that strange?

You might notice that in the textbook, Dr. Silverman presents a proof that does not rely on the Gaussian integers. While interesting and clever, I find that the proof using the Gaussian integers better illustrates the deep connections between and around the structures we have been studying in this course so far. Everything connects!

Example. *The prime 5 is $1 \pmod 4$, and so 5 is a sum of squares. In particular, $5 = 1^2 + 2^2$.*

Example. *The prime 101 is $1 \pmod 4$, and so is a sum of squares. Our proof is not constructive, so a priori we do not know what squares sum to 101. But in this case, we see that $101 = 1^2 + 10^2$.*

Example. *The prime 97 is $1 \pmod 4$, and so it also a sum of squares. It's less obvious what the squares are in this case. It turns out that $97 = 4^2 + 9^2$.*

Example. *The prime 43 is $3 \pmod 4$, and so is not a sum of squares.*

3. Classification of Gaussian Primes

In the previous section, we showed that each integer prime $p \equiv 1 \pmod 4$ actually splits into a product of two Gaussian numbers q_1 and q_2. In fact,

since $N(q_1) = p$ is a regular prime, q_1 is a Gaussian irreducible and therefore a Gaussian prime (can you prove this? This is a nice midterm question.)

So in fact, $p \equiv 1 \pmod 4$ splits in to the product of two Gaussian primes q_1 and q_2.

In this way, we've found infinitely many Gaussian primes. Take a regular prime congruent to 1 (mod 4). Then we know that it splits into two Gaussian primes. Further, if we know how to write $p = a^2 + b^2$, then we know that $q_1 = a + bi$ and $q_2 = a - bi$ are those two Gaussian primes.

In general, we will find all Gaussian primes by determining their interaction with regular primes.

Suppose q is a Gaussian prime. Then on the one hand, $N(q) = q\overline{q}$. On the other hand, $N(q) = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$ is some regular integer. Since q is a Gaussian prime (and so $q \mid w_1 w_2$ means that $q \mid w_1$ or $q \mid w_2$), we know that $q \mid p_j$ for some regular integer prime p_j.

So one way to classify Gaussian primes is to look at every regular integer prime and see which Gaussian primes divide it. We have figured this out for all primes $p \equiv 1 \pmod 4$. We can handle 2 by noticing that $2 = (1+i)(1-i)$. Both $(1 + i)$ and $(1 - i)$ are Gaussian primes.

The only primes left are those regular primes with $p \equiv 3 \pmod 4$. We actually already covered the key idea in the previous section.

Lemma 6. *If $p \equiv 3 \pmod 4$ is a regular prime, then p is also a Gaussian prime.*

Proof. In the previous section, we showed that if p is not a Gaussian prime, then $p = a^2 + b^2$ for some integers a, b, and then $p \equiv 1 \pmod 4$. Since $p \not\equiv 1 \pmod 4$, we see that p is a Gaussian prime. □

In total, we have classified all Gaussian primes.

Theorem 7. *The Gaussian primes are given by*

1. $(1 + i), (1 - i)$
2. *Regular primes $p \equiv 3 \pmod 4$*
3. *The factors $q_1 q_2$ of a regular prime $p \equiv 1 \pmod 4$. Further, these primes are given by $a \pm bi$, where $p = a^2 + b^2$.*

4. Concluding Remarks

I hope that it's clear that the regular integers and the Gaussian integers are deeply connected and intertwined. Number theoretic questions in one constantly lead us to investigate the other. As one dives deeper into number theory, more and different integer-like rings appear, all deeply connected.

Each time I teach the Gaussian integers, I cannot help but feel the sense that this is a hint at a deep structural understanding of what is really going on. The interplay between the Gaussian integers and the regular integers is one of my favorite aspects of elementary number theory, which is one reason why I deviated so strongly from the textbook to include it. I hope you enjoyed it too.