Robert Garbary, Fall 2014. Some random stuff about elementary number theory.

Chapter 1

Week 2 - stuff about $\mathbb{Z}[i]$

Assume the following result is true:

Theorem 1.1. *Let p be a prime which satisfies $p-1$ is a multiple of 4. Then there exists an integer C so that p is a multiple of C^2+1.*

Today, under the assumption that the above result is true, we are going to prove the following result:

Theorem 1.2. *Let p be a prime which satisfies $p-1$ is a multiple of 4. Then there exist integers a, b so that $p = a^2 + b^2$.*

How are we going to go from point 1 to point 2? By studying properties of $\mathbb{Z}[i]$! Recall that $\mathbb{Z}[i]$, the collection of **gaussian integers**, to be the collection of all 'numbers' of the form

$$a + ib$$

where $a, b \in \mathbb{Z}$ (are integers). Here, i is some 'symbol' that satisfies $i^2 = -1$.

Given a gaussian integer $z = c + id$, we define it's **length** or **norm** to be

$$N(z) = c^2 + d^2$$

For example, $N(2-3i) = 2^2 + (-3)^2 = 13$, while $N(i) = N(0 + i(1)) = 0^2 + 1^2 = 1$. Notice that the expression $c^2 + d^2$ is inherently a sum of squares. Let's look at some properties of the norm.

- **1**: If z, w are both gaussian integers, then $N(zw) = N(z)N(w)$.
  Proof: Write $z = a + ib$ and $w = c + id$ for integers a, b, c, d. As we've calculated before, we have that
  $$zw = (ac - bd) + i(ad + bc)$$
  and thus
  $$N(zw) = (ac - bd)^2 + (ad + bc)^2$$
  On the other hand, we have that $N(z) = a^2 + b^2$ and $N(w) = c^2 + d^2$. Therefore,
  $$N(z)N(w) = (a^2 + b^2)(c^2 + d^2)$$
  From the problems last week (specifically, problem 4), these two terms are equal. Therefore $N(zw) = N(z)N(w)$.

- **2**: $N(z) = 1$ if and only if z equals one of $1, -1, i, -i$.
  Proof: Let $z = a + ib$, and suppose that $N(z) = 1$, ie that $a^2 + b^2 = 1$. Since a^2 and b^2 are both non-negative and are integers, the only way this can be true is if $a^2 = 1$ and $b^2 = 0$, or $a^2 = 0$ and $b^2 = 1$. But since a, b are integers, this forces us to have either $a = \pm 1, b = 0$, or $a = 0, b = \pm 1$. In the first case, we get $z = \pm 1$, and in the second case we get $z = \pm i$.

- **3**: Suppose that $AB = 1$ for some $A, B \in \mathbb{Z}[i]$. Then $A = \pm 1$ or $\pm i$, and likewise for B.
  Proof: We have the equality $AB = 1$. Let's apply N to both sides; since $AB = 1$, we must have that $N(AB) = N(1)$. Of course, $N(1) = 1$, while $N(AB) = N(A)N(B)$. So $N(A)N(B) = 1$. Since $N(z) \in \mathbb{Z}^{\geq 0}$ for all $z \in \mathbb{Z}[i]$, we thus have that $N(A) = N(B) = 1$. By property 2 above, we are done!

Last week we talked about how prime numbers are special inside of the natural numbers in terms of unique factorization. We're going to make this a bit more precise today, and we're going to state things inside $\mathbb{Z}$ instead of $\mathbb{N}$. Since 1 is special, we are also going to call any number that multiplies to give 1. More specifically: if we have a, b satisfying $ab = 1$, we will call a and b both **units**. In $\mathbb{Z}$ there are two units: 1 and -1. In $\mathbb{Z}[i]$ there are 4 units: 1,-1, i, and -i - this follows by part 3 of what we proved. We are going to define in $\mathbb{Z}$ instead of in $\mathbb{N}$ what it means to be prime.

Here is the definition. A non-zero integer x is called **irreducible** if it is not a unit, and whenever we write $x = ab$, we have that either a or b is a unit. An element x is **reducible** if it can be factored into at least 2 irreducible elements. Two elements x, y are called **associates** if $x = uy$ for some unit u.

Let's figure out all the different types of elements in $\mathbb{Z}$:

- Units: ± 1

- Irreducibles: All primes and their negatives. What are the associates to 5? Just 5 and -5. More generally, if p is a prime, then the associates of p are p and $-p$.

- Reducibles: Non-prime non-unit numbers such as 4,6. If n is reducible, then all it's associates are n and $-n$.

How many ways can we factor -6 into irreducibles times a unit? There are many ways:

$$\begin{aligned} -6 &= -1 \bullet 2 \bullet 3 \\ &= -1 \bullet -2 \bullet -3 \\ &= 2 \bullet -3 \\ &= -2 \bullet 3 \end{aligned}$$

Here is what is true now for unique factorization:

Theorem 1.3. *Let $x \in \mathbb{Z}$ be non-zero and not a unit. Then x may be written as a unit times a product of irreducible elements:*

$$x = up_1 ... p_k$$

The factorization is unique in the following sense: if

$$x = vq_1 ... q_m$$

is another such factorization, then $m = k$, and p_i is an associate of some q_j.

Because of this theorem, we call $\mathbb{Z}$ a **unique factorization domain** (UFD).

Example 1.4. See what this theorem says about the previous example.

Given integers a, b, we say that **a divides b**, written $a|b$, if $b/a \in \mathbb{Z}$; equivalently, if $ca = b$ for some $c \in \mathbb{Z}$. For example, we have that $4|12$, while we don't have that $-6|7$. We can now state a result called **Euclid's Lemma**:

Lemma 1.5. *Let p be an irreducible integer, and let $a, b \in \mathbb{Z}$. Suppose that $p|ab$. Then either $p|a$ or $p|b$.*

Amazing, **everything we just stated holds in $\mathbb{Z}[i]$ also**: unique factorization and Euclid's lemma. For example, while -17 is irreducible in $\mathbb{Z}$, it is not irreducible in $\mathbb{Z}[i]$, since $-17 = (-1)(1+4i)(1-4i)$. There are other ways to factor it as well. For example, $-17 = (-i)(-1+4i)(-4+i)$, but we haven't contradicted 'uniqueness': in these two expressions, 1+4i and -4+i are associates, since (1+4i)(i)=(-4+i), and 1-4i and (-1+4i) are associates, since (1-4i)(-1)=(-1+4i). Cool.

What does all this stuff have to do with primes as sums of squares? Let's do it. Assume the following result:

Theorem 1.6. *Let p be a prime which satisfies $p-1$ is a multiple of 4. Then there exists an integer C so that p is a multiple of C^2+1.*

Let p be such a prime, we're going to prove that p may be written as a sum of two squares. By the theorem, there exists an integer C so that $p|_{\mathbb{Z}} C^2+1$. This also means that $p|_{\mathbb{Z}[i]} C^2+1$, ie that $p|_{\mathbb{Z}[i]}(C+i)(C-i)$.

Now, in $\mathbb{Z}[i]$, p is either irreducible or it is reducible. We're going to prove that p is reducible, by assuming it is irreducible and finding a contradiction.

Assume that p is irreducible. By Euclid's lemma, then p either divides $C+i$ or $C-i$. Assume that p divides $C+i$. This says that $\frac{C+i}{p} = \frac{C}{p} + i(\frac{1}{p}) \in \mathbb{Z}[i]$, which is ridiculous, since $1/p \notin \mathbb{Z}$. Similarly, p cannot divide $C-i$. So p can't be irreducible because this would contradict Euclid's lemma.

So p must be reducible inside $\mathbb{Z}[i]$. This means that it factors inside $\mathbb{Z}[i]$ as zw where z, w are not units. Apply N to the equation

$$p = zw$$

to get

$$p^2 = N(z)N(w)$$

Since we are inside the integers and p is a prime, it must be that either both $N(z)$ and $N(w)$ are p, or one of them is p^2 and the other is 1. However, this second option can't happen: if one of them, say z, satisfies $N(z) = 1$, thenw e would have that z is a unit. However, we are assuming that neither z nor w are units. Therefore we must have that $N(z) = N(w) = p$. But hang on a second: let's say $z = a + ib$ for integers a, b. Then $p = N(z) = a^2 + b^2$, ie p is a sum of squares! Holy crap.