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

Chapter 1

Week 1

We use the symbol $\mathbb{N}$ to denote the collection of **natural numbers**:

$$0, 1, 2, 3, 4, ...$$

Let's ask some questions having to do with natural numbers. People in math invent problems just for the sake of answering them, so it should come as no surprise that these questions were asked, even by the greeks.

Question 1.1. *Can every number be written as a single square?*

Answer 1.2. *Of course not, what a ridiculous question! The numbers* 2 *and* 3 *are not squares. The first few squares are* 0*,* 1*,* 4*, and* 9*.*

How silly. Let's move on.

Question 1.3. *Can every number be written as a sum of two squares?*

Answer 1.4. *This is again an "of course not"', though it's slightly less "of coursy". The numbers* 0 *and* 1*, and* 2 *are both a sum of two squares:*

$$0 = 0^2 + 0^2$$
$$1 = 1^2 + 0^2$$
$$2 = 1^2 + 1^2$$

but we can't write 3 *as a sum of two squares: if we only use* 0^2*'s and* 1^2*'s, we've already seen what numbers we get, and once we use a* 2^2*, our number is too big!*

Can you guess what the next question is?

Question 1.5. *Can every number be written as a sum of three squares?*

Answer 1.6. *The answer is still no, but this is not so obvious. The numbers* 1 *through* 6 *can all be written as a sum of three squares, but the number* 7 *can not. Why not? Certainly our sum can't have a* 3^2 *showing up, since that is already too big. Furthermore, we can't have two* 2^2*'s showing up: that bring us to 8, which is already too big! Thus we can have at most one* 2^2*, and the other terms can be* 0^2 *or* 1^2*. None of these combinations give us 7!*

Next:

Question 1.7. *Can every number be written as a sum of four squares?*

Answer 1.8. *Yes - it's obvious! Just kidding, it's not obvious at all, but it is true. This result is known as* ***Lagrange's four-square theorem****. It was proven in around 1770.*

Example 1.9. Let's write 107 as a sum of three squares. We can't use a 10^2, since then we would be trying to right 7 as a sum of three squares, which isn't happening anytime soon. If we use a 9^2, then we are reduced to writing $107 - 9^2 = 26$ as a sum of three squares: this we can do, since $26 = 5^2 + 1^2 + 0^2$. So

$$107 = 9^2 + 5^2 + 1^2 + 0^2$$

Great so we answered the question. We can all go home now. Except the 18th century mathematicians still need to pay their mortgages. So we need to come up with a new question.

For a natural number n at least 2, we say that n is **prime** if whenever you write n as a product of two natural numbers, say $n = ab$, we have that either $a = 1$ or $b = 1$. The first few primes numbers are 2, 3, 5, 7, and 11. (Sometimes people put a "..." after listing the first few primes. I don't really know why; this suggests to me that the pattern is believed to be clear.)

Prime numbers are the fundamental building block of multiplication:

Fact 1.10. *Suppose I give you a number N, which is at least 2. Then there is one and only one way to write N as a product of prime numbers.*

This fact is sometimes called *the fundamental theorem of arithmetic*, but that takes a lot of words. Cool: so it seems like primes are sort of important. Since we've already answered (or at least I've told you the answer) about all natural numbers, let's focus on just the primes : that mortgage won't pay itself. Of course, asking which primes are squares themselves is just silly: none of them are.

Question 1.11. *Which prime numbers are a sum of two squares?*

Let's work out the first few:

$$\begin{aligned}
2 &= 1^1 + 1^2 \\
3 &: \text{NO} \\
5 &= 1^2 + 2^2 \\
7 &: \text{NO} \\
11 &: \text{NO} \\
13 &= 2^2 + 3^2 \\
17 &= 1^2 + 4^2 \\
19 &: \text{NO} \\
23 &: \text{NO} \\
29 &= 2^2 + 5^2 \\
31 &: \text{NO} \\
37 &= 1^2 + 6^2 \\
41 &= 4^2 + 5^2
\end{aligned}$$

There is a pattern here: try to find it. Still stuck? Let's first throw away 2 and only look at the other primes (which are all odd). Instead of looking at the primes, let's take away one from each prime:

$$\begin{aligned}
3-1 &= 2 : NO \\
5-1 &= 4 : YES \\
7-1 &= 6 : NO \\
11-1 &= 10 : NO \\
13-1 &= 12 : YES \\
17-1 &= 16 : YES \\
19-1 &= 18 : NO \\
23-1 &= 22 : NO \\
29-1 &= 28 : YES \\
31-1 &= 30 : NO \\
37-1 &= 36 : YES \\
41-1 &= 40 : YES
\end{aligned}$$

See the pattern yet? It seems to be the primes p for which the answer is YES are precisely the primes p for which $p-1$ is a multiple of 4. This turns out to be right: it was proved by Euler in 1749. Here is the full result:

Theorem 1.12. *Let p be an odd prime. Then p may be written as a sum of two squares if and only if $p-1$ is a multiple of 4.*

This is what we're going to try to prove over the next few weeks. The main reason this problem is interesting is not because we are trying to write primes as a sum of squares (though that is interesting). The reason this problem is interesting is because of the techniques that we are going to use to attack this problem. Pretty soon, we are going to be deep in the world of complex numbers and finite fields.

That being said, we can do part of this theorem right now. The theorem says 'if and only if'. It means the theorem actually contains two statements (for the price of one). Part one of theorem 1.12 says

If p is an odd prime which is written as a sum of two squares, then $p-1$ is a multiple of 4

This part we can prove without any special tools: let's do it.

Proof. Let's assume that p is written as a sum of two squares: say we have some integers a, b so that $p = a^2 + b^2$. Recall that the square of an even number is even, and the square of an odd number is odd. Since p is odd, we must have that one of a, b is even, and the other is odd. Let's assume a is odd (if b was our odd number, we could just relabel them). So then b is even. This means we may write

$$\begin{aligned}
a &= 2k+1 \\
b &= 2l
\end{aligned}$$

for some natural numbers k and l. But then we have

$$\begin{aligned} p-1 &= a^2+b^2-1 \\ &= (2k+1)^2+(2l)^2-1 \\ &= 4k^2+4k+1-4l^2-1 \\ &= 4(k^2+k-l^2) \end{aligned}$$

and therefore $p-1$ is a multiple of 4. Proved! □

It's the other part of theorem 1.12 that is hard to prove: that is, the following statement

If $p-1$ is a multiple of 4, then p may be written as a sum of two squares.

Attacking this is going to be tricky. We're going to introduce a 'ring' (whatever that means) called the **Gaussian Integers**, which we denote by $\mathbb{Z}[i]$. What is this mysterious object? It is the collection of all (complex) numbers of the form

$$a+ib \text{ where } a,b \in \mathbb{Z}.$$

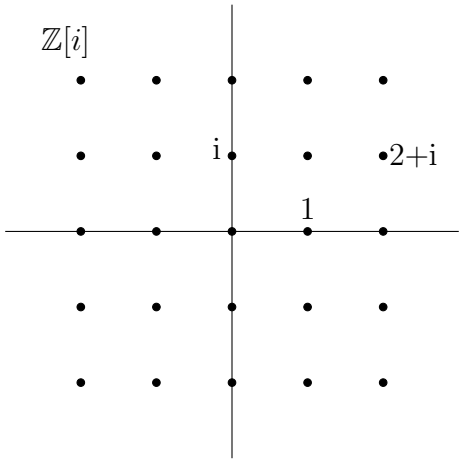
Here, i is some symbol that satisfies $i^2=-1$. A number of the form $a+bi$ for $a,b \in \mathbb{Z}$ is called a **gaussian integer**. We define $\mathbb{Z}[i]$ to be the collection of all guassian integers. Just like the usual integers $\mathbb{Z}$, we can add and multiply two guassian integers to get a gaussian integer. How do we do this?

$$\begin{aligned} (3+81i)+(17-26i) &= (3+17)+(81-26)i \\ &= 20+55i \end{aligned}$$

For the multiplication we just 'distribute' it out:

$$\begin{aligned} (1+2i)(-3+4i) &= 1(-3)+1(-4i)+2i(-3)+(2i)(4i) \\ &= -3-4i-6i+8i^2 \\ &= -3-4i-6i-8 \\ &= -11-10i \end{aligned}$$

If you like pictures, we can draw a picture:



In the picture above, $\mathbb{Z}[i]$ is the collection of all the "dots". The addition isn't so bad: in the example done above, all we do is add the "x-components" and add the "y-components". By the multiplication is a bit trickier - we won't explain it in terms of our picture.

What does $\mathbb{Z}[i]$ have to do with our problem about sums of squares? Suppose instead we were trying to answer a different question: what numbers n can be written as a *difference of squares*? More concretely, let's say we were trying to ask if there are natural numbers a, b so that

$$7 = a^2 - b^2$$

How might we tackle this? We would **factor** the right handside:

$$\begin{aligned} 7 &= a^2 - b^2 \\ &= (a-b)(a+b) \end{aligned}$$

and proceed as follows: since 7 is prime, one of $a-b$ and $a+b$ must be ± 1, while the other one must be ± 7. Since $a, b \geq 0$, it must be the case that $a+b \geq 0$. Also we have that $a-b \leq a+b$. Therefore we must have that

$$\begin{aligned} a+b &= 7 \\ a-b &= 1 \end{aligned}$$

Solving these equations gives that $a = 4$ and $b = 3$, and sure enough: $7 = 4^2 - 3^2$.

We can apply this factoring strategy to a sum of squares as well, but we end up inside $\mathbb{Z}[i]$: for example,

$$\begin{aligned} 13 &= 2^2 + 3^2 \\ &= (2+3i)(2-3i) \end{aligned}$$

Mind = blown? We're going to answer the problem as follows: we're going to show that if p is a prime with $p-1$ a multiple of 4, then p factors inside $\mathbb{Z}[i]$ as $(a-ib)(a+ib)$ for some $a, b \in \mathbb{Z}$. So we need to study the properties of $\mathbb{Z}[i]$.

That's what the second week will be about. More specifically, we're going to prove the desired result, assuming the following result:

Theorem 1.13. *If p is a prime satisfying $p-1$ is a multiple of 4, then there exists some integer a so that p is a multiple of a^2+1.*

In week 3, we're going to prove theorem 1.13. This will involve an introduction to the world of finite fields!