Math 3527 (Number Theory 1)

Lecture #27

Factorization in $\mathbb{Z}[i]$:

- Reducible and Irreducible Elements in $\mathbb{Z}[i]$
- Prime Factorization in $\mathbb{Z}[i]$
- Fermat's Theorem on Sums of Two Squares
- Pythagorean Triples

This material represents §4.4.1 from the course notes.

Irreducible Elements, I

The goal of this lecture is to study prime factorization in $\mathbb{Z}[i]$ and then discuss a few of its applications to number theory in $\mathbb{Z}$.

Notation: We will reserve the letter p for a prime integer (in $\mathbb{Z}$), and we will use π to denote an irreducible element in $\mathbb{Z}[i]$. (The use of the letter π is traditional, and should not cause confusion with the real number π.)

Irreducible Elements, II

We first recall a few properties of the norm map on $\mathbb{Z}[i]$ that we will use frequently:

Proposition (Norm Properties)

The units in $\mathbb{Z}[i]$ are $\{\pm 1, \pm i\}$. Also, if $N(\alpha) = p$ for a prime p, then α is irreducible.

Proof:

- We previously showed α is a unit if and only if $N(\alpha) = \pm 1$.
- Since $N(a + bi) = a^2 + b^2$, there are no elements of negative norm. It is then easy to see that $N(a + bi) = 1$ precisely if $a + bi$ is one of ± 1, $\pm i$, so these are the only units.
- We also showed that $N(\alpha) = \pm p$ where p is a prime, then α is irreducible, which immediately gives the second statement.

Irreducible Elements, III

The norm map is an extremely important tool for understanding factorization in $\mathbb{Z}[i]$ (in fact, in some sense it is almost our *only* tool!), since it allows us to transfer information from $\mathbb{Z}[i]$ into $\mathbb{Z}$, whose arithmetic we understand better.

- To start: observe that if $\pi \in \mathbb{Z}[i]$, then π certainly divides $N(\pi) = \pi \cdot \overline{\pi}$ in $\mathbb{Z}[i]$.
- So if π is irreducible in $\mathbb{Z}[i]$, then since irreducibles are prime elements in a Euclidean domain, this means that π must divide one of the (integer) prime factors of the integer $N(\pi)$.
- Thus, to identify the irreducible elements of $\mathbb{Z}[i]$, we need to study how primes $p \in \mathbb{Z}$ factor in $\mathbb{Z}[i]$.

Irreducible Elements, IV

Proposition (Reducibility and Sums of Squares)

If p is a prime integer, then p is irreducible in $\mathbb{Z}[i]$ if and only if p is not the sum of two squares (of integers). In particular, 2 is reducible in $\mathbb{Z}[i]$, while any prime congruent to 3 modulo 4 is irreducible in $\mathbb{Z}[i]$.

Irreducible Elements, IV

Proposition (Reducibility and Sums of Squares)

If p is a prime integer, then p is irreducible in $\mathbb{Z}[i]$ if and only if p is not the sum of two squares (of integers). In particular, 2 is reducible in $\mathbb{Z}[i]$, while any prime congruent to 3 modulo 4 is irreducible in $\mathbb{Z}[i]$.

Examples:

- The primes 3, 7, 11, and 19 are irreducible in $\mathbb{Z}[i]$ because they are each congruent to 3 modulo 4.
- The primes $5 = 2^2 + 1^2$, $89 = 8^2 + 5^2$, and $109 = 10^2 + 3^2$ are not irreducible in $\mathbb{Z}[i]$ because they can all be expressed as the sum of two squares.

Irreducible Elements, V

Proof:

- Suppose p is a prime in $\mathbb{Z}$ and that p has a factorization $p = (a + bi)(c + di)$ for some nonunits $a + bi$, $c + di$ in $\mathbb{Z}[i]$.
- Taking norms yields $p^2 = N(p) = (a^2 + b^2)(c^2 + d^2)$.
- Now, since $a + bi$ and $c + di$ are not units, both $a^2 + b^2$ and $c^2 + d^2$ must be greater than 1.
- The only possibility is $a^2 + b^2 = c^2 + d^2 = p$, so we see that $p = a^2 + b^2$ for some integers a and b.
- Conversely, if $p = a^2 + b^2$ for some integers a and b, we immediately have the factorization $p = (a + bi)(a - bi)$.
- For the last statement, clearly $2 = 1^2 + 1^2$.
- Also, every square is either 0 or 1 modulo 4, so the sum of two squares cannot be congruent to 3 modulo 4.

Irreducible Elements, VI

It remains to analyze what happens with primes congruent to 1 modulo 4.

Examples:

- We have $5 = 2^2 + 1^2$ so $5 = (2 + i)(2 - i)$ factors.
- We have $13 = 3^2 + 2^2$ so $13 = (3 + 2i)(3 - 2i)$ factors.
- We have $17 = 4^2 + 1^2$ so $17 = (4 + i)(4 - i)$ factors.
- We have $29 = 5^2 + 2^2$ so $29 = (5 + 2i)(5 - 2i)$ factors.
- We have $37 = 6^2 + 1^2$ so $37 = (6 + i)(6 - i)$ factors.
- We have $41 = 5^2 + 4^2$ so $41 = (5 + 4i)(5 - 4i)$ factors.

Based on these examples (try some larger primes yourself!) it appears that such primes always factor into a product of two complex-conjugate irreducible factors in $\mathbb{Z}[i]$.

Irreducible Elements, VII

Proposition (Factorization of 1 Mod 4 Primes)

If p is a prime integer and $p \equiv 1 \pmod 4$, then p is a reducible element in the ring $\mathbb{Z}[i]$, and its factorization into irreducibles is $p = (a + bi)(a - bi)$ for some a and b with $a^2 + b^2 = p$.

We will take a somewhat indirect approach to this proof.

- First, we will show that there exists some integer n such that p divides $n^2 + 1$.
- Then we will exploit this (seemingly very weak) statement to show that p is reducible in $\mathbb{Z}[i]$.

Irreducible Elements, VIII

Proof:

- For the first part, let p be a prime of the form $p = 4k + 1$ and let u be a primitive root modulo p (which we have shown, two lectures ago, necessarily exists).
- Then $u^{4k} \equiv 1 \mod p$, so $u^{2k} \equiv -1 \pmod{p}$, since its square is 1 but it cannot equal 1 (as otherwise u would have order $\leq 2k$ and thus not be a primitive root).
- Then $u^k = n$ is an element whose square is -1 modulo p, so p divides the integer $n^2 + 1$.

Irreducible Elements, IX

Proof (continued):

- Now, we know p divides $n^2 + 1 = (n+i)(n-i)$ in $\mathbb{Z}[i]$.
- Since p is a real number, if p divides one of $n \pm i$ then taking complex conjugates would show that p also divides the other. But this is not possible, since then p would divide $(n+i) - (n-i) = 2i$, which it clearly does not.
- Therefore, p is not a prime element in $\mathbb{Z}[i]$, so it must be reducible. By the previous proposition, this means there exist integers a and b with $p = a^2 + b^2$.
- Then $N(a+bi) = N(a-bi) = a^2 + b^2 = p$, and so these two elements are both irreducible.
- Hence the factorization of p in $\mathbb{Z}[i]$ is $p = (a+bi)(a-bi)$, as claimed.

Irreducible Elements, X: Marks The Spot

Putting the two previous results together gives us a characterization of the irreducible elements in $\mathbb{Z}[i]$:

Theorem (Irreducibles in $\mathbb{Z}[i]$)

Up to associates, the irreducible elements in $\mathbb{Z}[i]$ are as follows:

1. *The element $1 + i$ (of norm 2).*
2. *The primes $p \in \mathbb{Z}$ congruent to 3 modulo 4 (of norm p^2).*
3. *The distinct irreducible factors $a + bi$ and $a - bi$ (each of norm p) of $p = a^2 + b^2$ where $p \in \mathbb{Z}$ is congruent to 1 modulo 4.*

Irreducible Elements, XI: This One Goes To 11

Proof:

- The above propositions show that each of the listed elements are irreducible elements, so we only need to show that there are no others.
- So suppose $\pi = a + bi$ is an irreducible element in $\mathbb{Z}[i]$.
- Then $N(\pi) = p_1 p_2 \cdots p_k$ for some (integer) primes $p_i \in \mathbb{Z}$.
- Since π is a prime element, it must divide one of the p_i.
- But we have characterized how p_i factors into irreducibles in $\mathbb{Z}[i]$, so it must be associate to one of the elements on our list above. Hence our list is complete up to associates, as claimed.

Prime Factorizations, I

Using the characterization of irreducible elements, we can describe a method for factoring an arbitrary Gaussian integer into irreducibles. (This is the "prime factorization" in $\mathbb{Z}[i]$.)

- First, find the prime factorization of $N(a+bi) = a^2 + b^2$ over the integers $\mathbb{Z}$, and write down a list of all (rational) primes $p \in \mathbb{Z}$ dividing $N(a+bi)$.
- Second, for each p on the list, find the factorization of p over the Gaussian integers $\mathbb{Z}[i]$.
- Finally, use trial division to determine which of these irreducible elements divide $a+bi$ in $\mathbb{Z}[i]$, and to which powers. (The factorization of $N(a+bi)$ can be used to determine the expected number of powers.)

Prime Factorizations, II

Example: Find the prime factorization of $4 + 22i$ in $\mathbb{Z}[i]$.

Prime Factorizations, II

Example: Find the prime factorization of $4 + 22i$ in $\mathbb{Z}[i]$.

- We compute $N(4 + 22i) = 4^2 + 22^2 = 2^2 \cdot 5^3$. The primes dividing $N(4 + 22i)$ are 2 and 5.
- Over $\mathbb{Z}[i]$, we find the factorizations $2 = -i(1 + i)^2$ and $5 = (2 + i)(2 - i)$.
- Now we just do trial division to find the correct powers of each of these elements dividing $4 + 22i$.
- Since $N(4 + 22i) = 2^2 \cdot 5^3$, we should get two copies of $1 + i$ and three elements from $\{2 + i, 2 - i\}$.
- Doing the trial division yields the factorization $4 + 22i = -i \cdot (1 + i)^2 \cdot (2 + i)^3$. (Note that in order to have powers of the same irreducible element, we left the unit $-i$ in front of the factorization.)

Prime Factorizations, III

Example: Find the prime factorization of $27 - 19i$ in $\mathbb{Z}[i]$.

Prime Factorizations, III

Example: Find the prime factorization of $27 - 19i$ in $\mathbb{Z}[i]$.

- We compute $N(27 - 19i) = 27^2 + 19^2 = 2 \cdot 5 \cdot 109$.
- Over $\mathbb{Z}[i]$, we find the factorizations $2 = -i(1+i)^2$, $5 = (2+i)(2-i)$, and $109 = (10+3i)(10-3i)$.
- Now we just do trial division to find the correct powers of each of these elements dividing $4 + 22i$.
- Since $N(4 + 22i) = 2 \cdot 5 \cdot 109$, we should get one copy of $1 + i$, one element from $\{2 + i, 2 - i\}$, and one element from $\{10 + 3i, 10 - 3i\}$.
- Doing the trial division yields the factorization $27 - 19i = -i(1 + i)(2 + i)(10 - 3i)$.

Prime Factorizations, IV

In these two examples, the primes appearing were small enough to factor over $\mathbb{Z}[i]$ by inspection (e.g., $109 = (10 + 3i)(10 - 3i)$).

However, if p is large then it is not so obvious how to factor p in $\mathbb{Z}[i]$. We briefly explain how to find this expression algorithmically.

Prime Factorizations, V

Per the proof, we first want to find n such that p divides $n^2 + 1$.

- This is equivalent to finding a square root of -1 modulo p.
- In our proof, we constructed such a value using a primitive root u: specifically, we took $n = u^{(p-1)/4}$.
- However, we do not usually need to expend that much effort: in fact, if we just choose a random unit u, then as we will show (fairly soon!), each u has a 50% chance of having $u^{(p-1)/2} \equiv -1 \pmod{p}$, so selecting random values will quickly let us find one.
- Assuming we do this calculation (which is very efficient using successive squaring) to find such a u, we take $n = u^{(p-1)/4} \pmod{p}$.

Prime Factorizations, VI

Now suppose we have n such that p divides $n^2 + 1$.

- If we factor $p = \pi\overline{\pi}$ in $\mathbb{Z}[i]$, then since π divides $n^2 + 1 = (n + i)(n - i)$ and π is a prime element, either π divides $n + i$ or π divides $n - i$. Equivalently, either π divides $n + i$ or $\overline{\pi}$ divides $n + i$.
- Furthermore, since p clearly does not divide $n + i$, we see that exactly one of π and $\overline{\pi}$ divides $n + i$. Therefore, either π or $\overline{\pi}$ is a greatest common divisor of p and $n + i$ in $\mathbb{Z}[i]$.
- Thus, to find a and b such that $p = a^2 + b^2$, we can use the Euclidean algorithm in $\mathbb{Z}[i]$ to find a greatest common divisor of p and $n + i$ in $\mathbb{Z}[i]$: the result will be an element $\pi = a + bi$ with $a^2 + b^2 = p$.

Prime Factorizations, VII

Example: Express the prime $p = 3329$ as the sum of two squares.

Prime Factorizations, VII

Example: Express the prime $p = 3329$ as the sum of two squares.

- By successive squaring we can compute $2^{(p-1)/2} \equiv 1 \pmod{p}$ so $u = 2$ will not work, but $3^{(p-1)/2} \equiv -1 \pmod{p}$.
- Thus, our discussion above tells us that $3^{(p-1)/4} \equiv 1729$ is a square root of -1 modulo p: indeed, $1729^2 + 1 = 898 \cdot 3329$.
- Now we compute the gcd of $1729 + i$ and 3329 in $\mathbb{Z}[i]$ using the Euclidean algorithm:

$$\begin{aligned} 3329 &= 2(1729 + i) + (-129 - 2i) \\ 1729 + i &= -13(-129 - 2i) + (52 - 25i) \\ -129 - 2i &= (-2 - i)(52 - 25i) \end{aligned}$$

- The last nonzero remainder is $52 - 25i$, and indeed we see that $3329 = 52^2 + 25^2$.

Sums of Two Squares, I

As a corollary to our characterization of the irreducible elements in $\mathbb{Z}[i]$, we can deduce the following theorem of Fermat on when an integer is the sum of two squares:

Theorem (Fermat's Theorem on Sums of Two Squares)

Let n be a positive integer, and write $n = 2^k p_1^{n_1} \cdots p_k^{n_k} q_1^{m_1} \cdots q_d^{m_d}$, where $p_1, \cdots, p_k$ are distinct primes congruent to 1 modulo 4 and $q_1, \cdots, q_d$ are distinct primes congruent to 3 modulo 4. Then n can be written as a sum of two squares in $\mathbb{Z}$ if and only if all the m_i are even. Furthermore, in this case, the number of ordered pairs of integers (A, B) such that $n = A^2 + B^2$ is equal to $4(n_1 + 1)(n_2 + 1) \cdots (n_k + 1)$.

Sums of Two Squares, II

<u>Preuve</u> (*partie première*):

- Observe that the question of whether n can be written as the sum of two squares $n = A^2 + B^2$ is equivalent to the question of whether n is the norm of a Gaussian integer $A + Bi$.
- Write $A + Bi = \rho_1 \rho_2 \cdots \rho_r$ as a product of irreducibles (unique up to units), and take norms to obtain $n = N(\rho_1) \cdot N(\rho_2) \cdot \cdots \cdot N(\rho_r)$.
- By our classification, if ρ is irreducible in $\mathbb{Z}[i]$, then $N(\rho)$ is either 2, a prime congruent to 1 modulo 4, or the square of a prime congruent to 3 modulo 4.
- Hence there exists such a choice of ρ_i with $n = \prod N(\rho_i)$ if and only if all the m_i are even.
- This establishes the first part of the theorem.

Sums of Two Squares, III

Preuve (*partie deuxième*):

- For the counting part, since the factorization of $A+Bi$ is unique, to find the number of possible pairs (A,B), we need only count the number of ways to select terms for $A+Bi$ and $A-Bi$ from the factorization of n over $\mathbb{Z}[i]$.
- The factorization is
  $n=(1+i)^{2k}(\pi_1\overline{\pi_1})^{n_1}\cdots(\pi_k\overline{\pi_k})^{n_k}q_1^{m_1}\cdots q_d^{m_d}$.
- Up to associates, we must choose
  $A+Bi=(1+i)^k(\pi_1^{a_1}\overline{\pi_1}^{b_1})\cdots(\pi_k^{a_k}\overline{\pi_k}^{b_k})q_1^{m_1/2}\cdots q_d^{m_d/2}$,
  where $a_i+b_i=n_i$ for each $1\le i\le k$.
- Since there are n_i+1 ways to choose the pair (a_i,b_i), and 4 ways to multiply $A+Bi$ by a unit, the total number of ways is $4(n_1+1)\cdots(n_k+1)$, as claimed.

Sums of Two Squares, IV

<u>Example</u>: Determine whether 4044 can be written as the sum of two squares.

- We factor $4044 = 2^2 \cdot 3 \cdot 337$.
- Since 3 is a prime congruent to 3 modulo 4 that appears in the factorization to an odd power, our characterization dictates that it cannot be written as the sum of two squares.

Sums of Two Squares, IV

Example: Determine whether 4044 can be written as the sum of two squares.

- We factor $4044 = 2^2 \cdot 3 \cdot 337$.
- Since 3 is a prime congruent to 3 modulo 4 that appears in the factorization to an odd power, our characterization dictates that it cannot be written as the sum of two squares.

Example: Determine whether 9945 can be written as the sum of two squares.

- We factor $9945 = 3^2 \cdot 5 \cdot 13 \cdot 17$.
- Since the only prime appearing in the factorization congruent to 3 mod 4 is 3, and it has an even power, our characterization dictates that 9945 can be written as the sum of two squares.

Sums of Two Squares, V

Example: Find all ways to write 6649 as the sum of two squares.

Sums of Two Squares, V

Example: Find all ways to write 6649 as the sum of two squares.

- We factor $6649 = 61 \cdot 109$. This is the product of two primes each congruent to 1 modulo 4, so (per our formula) it can be written as the sum of two squares in 16 different ways.
- We compute $61 = 5^2 + 6^2$ and $109 = 10^2 + 3^2$ (either by the algorithm we described or by inspection).
- Then the 16 ways can be found from the different ways of choosing one of $5 \pm 6i$ and multiplying it with $10 \pm 3i$.
- Explicitly: we have $(5 + 6i)(10 + 3i) = 32 + 75i$ and $(5 + 6i)(10 - 3i) = 68 + 45i$, so we obtain the sixteen ways of writing 6649 as the sum of two squares as $(\pm 32)^2 + (\pm 75)^2$, $(\pm 68)^2 + (\pm 45)^2$, and the eight other decompositions with the terms interchanged.

Sums of Two Squares, VI

Example: Find 3 ways to write 7650 as the sum of two squares.

Sums of Two Squares, VI

Example: Find 3 ways to write 7650 as the sum of two squares.

- We factor $7650 = 2 \cdot 3^2 \cdot 5^2 \cdot 17$. Since the only prime congruent to 3 modulo 4 (namely 3) appears with an even exponent, 7650 can be written by the sum of two squares.
- Since $5 = (2+i)(2-i)$ and $17 = (4+i)(4-i)$, the possible ways can be found by multiplying $1+i$, 3, two of $2 \pm i$, and one of $4 \pm i$.
- We get $(1+i)(3)(2+i)^2(4+i) = -33+81i$, $(1+i)(3)(2+i)^2(4-i) = 9+87i$, and $(1+i)(3)(2+i)(2-i)(4+i) = 45+75i$.
- These yield $7650 = 33^2 + 81^2 = 9^2 + 87^2 = 45^2 + 75^2$.
- The other possible products yield sums equivalent to these. (Indeed, we can see that there are no others using the formula for the number of expansions and deleting the 8-fold duplication of each solution.)

Pythagorean Triples, I

As another application of our results, we can prove a classical characterization of the Pythagorean triples of integers (a, b, c) such that $a^2 + b^2 = c^2$ (so named because these represent the side lengths of a right triangle).

- If $a^2 + b^2 = c^2$ for integers a, b, c, note that if two of a, b, c are divisible by a prime p, then so is the third. We can then "reduce" the triple (a, b, c) by dividing each term by p to obtain a new triple (a', b', c') with $(a')^2 + (b')^2 = (c')^2$.
- For this reason it is sufficient to characterize the primitive Pythagorean triples with $\gcd(a, b, c) = 1$.
- For primitive triples, since a and b cannot both be odd (since then $a^2 + b^2 \equiv 2 \pmod 4$ cannot be a perfect square) we see that exactly one of a, b is even.

Pythagorean Triples, II

We can give a fairly simple characterization of all the primitive Pythagorean triples:

Theorem (Primitive Pythagorean Triples)

Every primitive Pythagorean triple, of positive integers (a, b, c) *with* $a^2 + b^2 = c^2$ *with* $\gcd(a, b, c) = 1$ *and* a *even, is of the form* $(a, b, c) = (2st,\ s^2 - t^2,\ s^2 + t^2)$*, for some relatively prime integers* $s > t$ *of opposite parity. Conversely, any such triple is Pythagorean and primitive.*

It is easy to see that $(2st)^2 + (s^2 - t^2)^2 = (s^2 + t^2)^2$ simply by multiplying out, and it is likewise not difficult to see that if s and t are relatively prime and have opposite parity, then $\gcd(s^2 - t^2, s^2 + t^2) = 1$ so this triple is primitive.

Pythagorean Triples, III

Proof:

- To show (a, b, c) must be of the desired form, suppose $a^2 + b^2 = c^2$ and factor in $\mathbb{Z}[i]$ as $(a + bi)(a - bi) = c^2$.
- We claim that $a + bi$ and $a - bi$ are relatively prime in $\mathbb{Z}[i]$: any gcd must divide $2x$ and $2y$, hence divide 2. However, $a + bi$ is not divisible by the prime $1 + i$, since a and b are of opposite parity.
- Hence, since $a + bi$ and $a - bi$ are relatively prime and have product equal to a square, by the uniqueness of prime factorization in $\mathbb{Z}[i]$, there exists some $s + it \in \mathbb{Z}[i]$ and some unit $u \in \{1, i, -1, -i\}$ such that $a + bi = u(s + ti)^2$.
- Thus, $a + bi = u\left[(s^2 - t^2) + (2st)i\right]$. Since a is even, b is odd, and both are positive, we see $u = -i$ and $s > t$.
- Then $a = 2st$, $b = s^2 - t^2$, and $c = s^2 + t^2$, as claimed.

Pythagorean Triples, IV

Here are the first few primitive Pythagorean triples:

s	t	Side Lengths
2	1	3, 4, 5
3	2	5, 12, 13
4	1	8, 15, 17
4	3	7, 24, 25
5	2	20, 21, 29
5	4	9, 40, 41
6	1	12, 35, 37
6	5	11, 60, 61

s	t	Side Lengths
7	2	28, 45, 53
7	4	33, 56, 65
7	6	13, 84, 85
8	1	16, 63, 65
8	3	48, 55, 73
8	5	39, 80, 89
8	7	15, 112, 113

Pythagorean Triples, V

For non-primitive triples, we can just scale primitive triples by an arbitrary integer:

Corollary (Arbitrary Pythagorean Triples)

Every Pythagorean triple of positive integers (a, b, c) with $a^2 + b^2 = c^2$ is of the form $(a, b, c) = (2kst,\ k(s^2 - t^2),\ k(s^2 + t^2))$, for some relatively prime integers $s > t$ of opposite parity and some integer k.

For example, taking $k = 2$, $s = 2$, $t = 1$ produces the non-primitive triple $(6, 8, 10)$.

Pythagorean Triples, VI

Example: Find all Pythagorean triangles with a side of length 51.

Pythagorean Triples, VI

<u>Example</u>: Find all Pythagorean triangles with a side of length 51.

- We break into cases based on the possible values of k.
- If $k = 1$, then if 51 is the hypotenuse we get $s^2 + t^2 = 51$. But since $51 = 3 \cdot 17$ is divisible by a prime congruent to 3 mod 4 to an odd power, 51 is not the sum of two squares.
- If 51 is a leg we get $s^2 - t^2 = 51$, so that $(s - t)(s + t)$ $= 1 \cdot 51 = 3 \cdot 17$, with solutions $s = 26$, $t = 25$ (sides $51 - 1300 - 1301$) and $s = 10$, $t = 7$ (sides $51 - 140 - 149$).
- If $k = 3$, if 51 is the hypotenuse we get $s^2 + t^2 = 17$ with solution $s = 4$, $t = 1$ (sides $24 - 45 - 51$).
- If 51 is a leg we get $s^2 - t^2 = 17$; factoring gives $(s - t)(s + t) = 1 \cdot 17$ so $s = 9$, $t = 8$ (sides $51 - 432 - 435$).
- If $k = 17$ then we want a side of length 3, which can only be the leg with $s = 2$, $t = 1$ (sides $51 - 68 - 85$).
- Since $k = 51$ cannot occur, we have found all possibilities.

Summary

We discussed the relationship between irreducible elements in $\mathbb{Z}[i]$ and sums of two squares.

We characterized the irreducible elements in $\mathbb{Z}[i]$ and described a prime factorization algorithm in $\mathbb{Z}[i]$.

We proved Fermat's characterization of the integers that are the sum of two squares, and described methods for computing all ways of writing an integer as a sum of two squares.

We studied Pythagorean triples and described how to find them all.

Next lecture: Solving Polynomial Congruences.