Math 4527 (Number Theory 2)

Lecture #28 of 37 $\sim$ March 29, 2021

Factorization in $\mathbb{Z}[i]$, $\mathbb{Z}[\sqrt{-2}]$, and $\mathcal{O}_{\sqrt{-3}}$.

- Factorization in $\mathbb{Z}[i]$ and Sums of Two Squares
- Factorization in $\mathbb{Z}[\sqrt{-2}]$, and $\mathcal{O}_{\sqrt{-3}}$

This material represents §8.3.1-8.3.2 from the course notes.

Recall

Last time, we proved the Kummer-Dedekind factorization theorem:

Theorem (Factorization of (p) in $\mathcal{O}_D$)

Let p be a prime and let

$$q(x) = \begin{cases} x^2 - D & \text{for } D \equiv 2,3 \text{ mod } 4 \\ x^2 - x - (D-1)/4 & \text{for } D \equiv 1 \text{ mod } 4 \end{cases}, \text{ where}$$

$$\omega = \begin{cases} \sqrt{D} & \text{for } D \equiv 2,3 \text{ mod } 4 \\ (1+\sqrt{D})/2 & \text{for } D \equiv 1 \text{ mod } 4 \end{cases} \text{ is a root of } q(x).$$

If the polynomial $q(x)$ has a repeated root r modulo p then the ideal $(p) = (p, \omega - r)^2$ is the square of a prime ideal of norm p in $\mathcal{O}_D$, if $q(x)$ is irreducible modulo p then the ideal (p) is prime in $\mathcal{O}_D$ of norm p^2, and if $q(x)$ is reducible with distinct roots r, r' modulo p, then $(p) = (p, \omega - r) \cdot (p, \omega - r')$ factors as the product of two distinct ideals in $\mathcal{O}_D$ each of norm p.

This theorem tells us how to find prime ideals in $\mathcal{O}_D$.

Factorization in $\mathbb{Z}[i]$, I

Now we will discuss factorization in the Gaussian integers $\mathbb{Z}[i]$, which we have already shown to be a Euclidean domain, a principal ideal domain, and a unique factorization domain.

- We need only analyze the factorization of primes p, which is fully determined by the ideal factorization of (p) inside $\mathbb{Z}[i]$.
- Because $N(a+bi) = a^2 + b^2$, factorization in $\mathbb{Z}[i]$ is closely related to the question of writing an integer as the sum of two squares, and so by analyzing prime factorizations in $\mathbb{Z}[i]$, we can classify the integers that can be written as the sum of two squares.

Factorization in $\mathbb{Z}[i]$, II

Our first task is to write down 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.*

There are various ways to prove this result using modular arithmetic (which I usually discuss in Math 3527), but we can establish this result directly from our theorem on factoring the ideal (p).

Factorization in $\mathbb{Z}[i]$, III

Proof:

- Since $\mathbb{Z}[i]$ is Euclidean, we may equivalently find the ideal factors of the ideals (p) for integer primes p, which we may do by factoring $q(x) = x^2 + 1$ modulo p.
- For $p = 2$ we have $x^2 + 1 \equiv (x-1)^2$ mod 2. This gives the ideal factorization $(2) = (2, i+1)^2$, yielding the element factorization $2 = -(i+1)^2$.
- For $p \equiv 3$ mod 4, we claim $x^2 + 1$ is irreducible modulo p.
- To see this note that $\left(\frac{-1}{p}\right) \equiv (-1)^{(p-1)/2} \equiv -1 \pmod{p}$ by Euler's criterion, so -1 is not a square mod p.
- Thus, (p) is prime in $\mathbb{Z}[i]$, so the element p is irreducible and its norm is p^2.

Factorization in $\mathbb{Z}[i]$, IV

Proof (continued):

- Finally, suppose $p \equiv 1 \bmod 4$: then $\left(\frac{-1}{p}\right) \equiv (-1)^{(p-1)/2} \equiv 1 \pmod{p}$ by Euler's criterion, so $x^2 + 1$ factors modulo p, say as $x^2 + 1 \equiv (x - r)(x + r) \pmod{p}$.
- This gives the ideal factorization $(p) = (p, i - r) \cdot (p, i + r)$.
- Since $\mathbb{Z}[i]$ is a PID, the ideal $(p, i + r)$ is principal, say $(a + bi)$ for some a, b which we can compute by applying the Euclidean algorithm to p and $i + r$. Then the conjugate ideal $(p, r - i) = (p, i - r)$ is equal to $(a - bi)$.
- This yields the ideal factorization $(p) = (a + bi)(a - bi)$ and so we get the element factorization $p = (a + bi)(a - bi)$ up to a unit factor, which by rescaling we may assume is 1.
- This means $p = (a + bi)(a - bi) = a^2 + b^2$, and we have $N(a + bi) = a^2 + b^2 = p = N(a - bi)$, so both irreducible factors have norm p as claimed.

Factorization in $\mathbb{Z}[i]$, V

With the list of prime elements in hand, we can give a procedure for finding the prime factorization of an arbitrary Gaussian integer:

- 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.)

Factorization in $\mathbb{Z}[i]$, V

Example: Find the factorization of $7 - 11i$ into irreducibles in $\mathbb{Z}[i]$.

Factorization in $\mathbb{Z}[i]$, V

Example: Find the factorization of $7 - 11i$ into irreducibles in $\mathbb{Z}[i]$.

- We compute $N(7 - 11i) = 7^2 + (-11)^2 = 170 = 2 \cdot 5 \cdot 17$.
- Over $\mathbb{Z}[i]$, we find the factorizations $2 = -i(1 + i)^2$, $5 = (2 + i)(2 - i)$, and $17 = (4 + i)(4 - i)$.
- Now we just do trial division to find the correct elements dividing $4 + 22i$: we will get one copy of $1 + i$, one element from $\{2 + i, 2 - i\}$, and one from $\{4 + i, 4 - i\}$.
- Doing the trial division yields the factorization $7 - 11i = -i(1 + i)(2 - i)(4 + i)$.

Factorization in $\mathbb{Z}[i]$, VI

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

Factorization in $\mathbb{Z}[i]$, VI

Example: Find the factorization of $4 + 22i$ into irreducibles 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.)

Factorization in $\mathbb{Z}[i]$, VII

The primes appearing in the example above were small enough to factor over $\mathbb{Z}[i]$ by inspection, but if $p \equiv 1 \pmod 4$ 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.

- We have the ideal factorization $(p) = (p, i + r) \cdot (p, i - r)$ and then use the Euclidean algorithm to write $(p, i + r) = (a + bi)$. Thus, all we need to do is find a root r of the polynomial $x^2 + 1 \pmod p$, which is equivalent to finding a square root of -1 modulo p.
- We can do this using Euler's criterion: for any quadratic nonresidue u modulo p, Euler's criterion tells us that $u^{(p-1)/2} \equiv -1 \pmod p$, and so $u^{(p-1)/4}$ will be a square root of -1.

Factorization in $\mathbb{Z}[i]$, VIII

There is no general formula for identifying a quadratic nonresidue modulo an arbitrary prime p, but we can just search small residue classes (or random residue classes) until we find one.

- Indeed, we don't even need to test whether u is a quadratic residue: we can just try calculating $u^{(p-1)/4}$, which will either be a square root of -1 or a square root of $+1$, but in the latter case we will get ± 1 and thus know we need to try a different u.
- Then, as noted on the last slide, to compute the solution to $p = a^2 + b^2$ we can use the Euclidean algorithm in $\mathbb{Z}[i]$ to find a greatest common divisor of p and $r + i$ in $\mathbb{Z}[i]$: the result will be an element $\pi = a + bi$ with $a^2 + b^2 = p$.

Factorization in $\mathbb{Z}[i]$, IX

<u>Example</u>: Express the prime $p = 3329$ as the sum of two squares using the fact that $3^{(p-1)/4} \equiv 1729 \pmod{p}$.

Factorization in $\mathbb{Z}[i]$, IX

Example: Express the prime $p = 3329$ as the sum of two squares using the fact that $3^{(p-1)/4} \equiv 1729 \pmod{p}$.

- Our discussion on the last slides tells us that 1729 is a square root of -1 modulo p: indeed, we can double-check by computing $1729^2 + 1 = 898 \cdot 3329$.
- 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 can 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 Characterization of 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

Proof:

- 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.

Sums of Two Squares, III

Proof (continued):

- For the counting, 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 $\mathbb{Z}[i]$, which is $n = i^{-k}(1+i)^{2k}(\pi_1\overline{\pi_1})^{n_1}\cdots(\pi_k\overline{\pi_k})^{n_k}q_1^{m_1}\cdots q_d^{m_d}$.
- 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 $1 \leq i \leq k$.
- 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

Example: Find all ways of writing $n = 6649 = 61 \cdot 109$ as the sum of two squares.

Sums of Two Squares, IV

Example: Find all ways of writing $n = 6649 = 61 \cdot 109$ as the sum of two squares.

- Note n is the product of two primes each congruent to 1 modulo 4, so 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 earlier or by inspection), so 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: $(5 + 6i)(10 + 3i) = 32 + 75i$, 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.

Factorization in $\mathbb{Z}[\sqrt{-2}]$, I

We can use a similar approach to the one we used in $\mathbb{Z}[i]$ to study factorization in $\mathcal{O}_{\sqrt{-2}} = \mathbb{Z}[\sqrt{2}]$ and $\mathcal{O}_{\sqrt{-3}} = \mathbb{Z}[\frac{1+\sqrt{-3}}{2}]$, which in turn allows us to characterize the integers of the form $a^2 + 2b^2$ and $a^2 + 3b^2$.

- We will start with $\mathbb{Z}[\sqrt{-2}]$.
- By using a similar proof to the one we used for $\mathbb{Z}[i]$, we can establish that $\mathcal{O}_{\sqrt{-2}}$ is a Euclidean domain, hence is also a PID and a UFD.
- Also, the units in $\mathcal{O}_{\sqrt{-2}}$ are simply ± 1.

Factorization in $\mathbb{Z}[\sqrt{-2}]$, II

Our first task is to write down the irreducible elements:

Theorem (Irreducibles in $\mathcal{O}_{\sqrt{-2}}$)

Up to associates, the irreducible elements in $\mathcal{O}_{\sqrt{-2}}$ are as follows:

1. *The element $\sqrt{-2}$ (of norm 2).*
2. *The primes $p \in \mathbb{Z}$ congruent to 5 or 7 modulo 8 (of norm p^2).*
3. *The distinct irreducible factors $a + b\sqrt{-2}$ and $a - b\sqrt{-2}$ (each of norm p) of $p = a^2 + 2b^2$ where $p \in \mathbb{Z}$ is congruent to 1 or 3 modulo 8.*

The proof of this theorem is essentially the same as the one for the Gaussian integers, except that we have to factor $x^2 + 2$ modulo p rather than $x^2 + 1$.

Factorization in $\mathbb{Z}[\sqrt{-2}]$, III

Proof:

- Since $\mathbb{Z}[\sqrt{-2}]$ is Euclidean, we may equivalently find the ideal factors of the ideals (p) for integer primes p, which we may do by factoring $q(x) = x^2 + 2$ modulo p.
- For $p = 2$ we have $x^2 + 2 \equiv x^2 \bmod 2$, so we get the ideal factorization $(2) = (\sqrt{-2})^2$, yielding the element factorization $2 = -(\sqrt{-2})^2$.
- For $p \equiv 5$ or $7 \bmod 8$, the polynomial $x^2 + 2$ is irreducible modulo p: from one of the "secondary" relations from quadratic reciprocity, we know that -2 is a square modulo p if and only if p is congruent to 1 or 3 mod 8. Thus, for $p \equiv 5$ or $7 \bmod 8$, the ideal (p) is prime, so the element p is also prime.

Factorization in $\mathbb{Z}[\sqrt{-2}]$, IV

Proof (continued):

- If $p \equiv 1$ or 3 mod 8, the polynomial $x^2 + 2$ factors modulo p, say as $x^2 + 2 \equiv (x - r)(x + r) \pmod{p}$. Then we get the ideal factorization $(p) = (p, \sqrt{-2} - r) \cdot (p, \sqrt{-2} + r)$.
- Since $\mathbb{Z}[\sqrt{-2}]$ is a PID, we have $(p, \sqrt{-2} + r) = (a + b\sqrt{-2})$ for some a, b that we can compute by applying the Euclidean algorithm to p and $\sqrt{-2} + r$. The conjugate ideal $(p, r - \sqrt{-2}) = (p, \sqrt{-2} - r)$ is then $(a - b\sqrt{-2})$.
- This yields the ideal factorization $(p) = (a + b\sqrt{-2})(a - b\sqrt{-2})$ and so we get the element factorization $p = (a + b\sqrt{-2})(a - b\sqrt{-2})$ up to a unit factor, which by rescaling we may assume is 1.
- Then $p = (a + b\sqrt{-2})(a - b\sqrt{-2}) = a^2 + 2b^2$, and we have $N(a + b\sqrt{-2}) = a^2 + 2b^2 = p = N(a - b\sqrt{-2})$, so both irreducible factors have norm p as claimed.

Factorization in $\mathbb{Z}[\sqrt{-2}]$, V

We can use the same general factorization procedure as in $\mathbb{Z}[i]$ to compute element factorizations in $\mathbb{Z}[\sqrt{-2}]$.

- First, find the prime factorization of $N(a + b\sqrt{-2}) = a^2 + 2b^2$ over the integers $\mathbb{Z}$, and write down a list of all (rational) primes $p \in \mathbb{Z}$ dividing $N(a + b\sqrt{-2})$.
- Second, for each p on the list, find the factorization of p in the ring in $\mathbb{Z}[\sqrt{-2}]$, which we can do by solving $p = a^2 + 2b^2$ in integers a, b for $p \equiv 1, 3 \pmod 8$.
- We can find this factorization by inspection for small p, and for large p we can find a solution by solving the quadratic $r^2 \equiv -D \pmod p$ and then using the Euclidean algorithm to compute the gcd $a + b\sqrt{-D}$ of p and $\sqrt{-D} + r$ in $\mathcal{O}_{\sqrt{-D}}$.
- Finally, use trial division to determine which irreducible elements divide $a + b\sqrt{-D}$ in $\mathcal{O}_{\sqrt{-D}}$ and to which powers.

Factorization in $\mathbb{Z}[\sqrt{-2}]$, VI

Example: Find the prime factorization of $47 + 32\sqrt{-2}$ in $\mathbb{Z}[\sqrt{-2}]$.

Factorization in $\mathbb{Z}[\sqrt{-2}]$, VI

Example: Find the prime factorization of $47 + 32\sqrt{-2}$ in $\mathbb{Z}[\sqrt{-2}]$.

- We compute $N(47 + 32\sqrt{-2}) = 47^2 + 2 \cdot 32^2 = 3^2 \cdot 11 \cdot 43$, so the primes dividing the norm are 3, 11, and 43.
- Over $\mathbb{Z}[\sqrt{-2}]$, we find the factorizations
  $3 = 1^2 + 2 \cdot 1^2 = (1 + \sqrt{-2})(1 - \sqrt{-2})$,
  $11 = 3^2 + 2 \cdot 1^2 = (3 + \sqrt{-2})(3 - \sqrt{-2})$ and
  $43 = 5^2 + 2 \cdot 3^2 = (5 + 3\sqrt{-2})(5 - 3\sqrt{-2})$.
- Now we just do trial division to find the correct powers of each of these elements dividing $47 + 32\sqrt{-2}$: we will get two of $1 \pm \sqrt{-2}$ and one each of $3 \pm \sqrt{-2}$ and $5 \pm 3\sqrt{-2}$.
- Doing the trial division yields the factorization
  $47 + 32\sqrt{-2} = (1 + \sqrt{-2})^2(3 - \sqrt{-2})(5 - 3\sqrt{-2})$.

Factorization in $\mathbb{Z}[\sqrt{-2}]$, VII

We can use our characterization of primes in $\mathbb{Z}[\sqrt{-2}]$ to describe the integers that can be represented by the quadratic form $a^2 + 2b^2$:

Theorem (Integers of the Form $a^2 + 2b^2$)

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 or 3 modulo 8 and $q_1, \cdots, q_d$ are distinct primes congruent to 5 or 7 modulo 8. Then n can be written in the form $a^2 + 2b^2$ for integers a, b 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 $n = A^2 + 2B^2$ is equal to $2(n_1 + 1)(n_2 + 1) \cdots (n_k + 1)$.

Factorization in $\mathbb{Z}[\sqrt{-2}]$, VIII

Proof:

- The question of whether n can be written as $n = A^2 + 2B^2$ is equivalent to the question of whether n is the norm of an element $A + B\sqrt{-2} \in \mathbb{Z}[\sqrt{-2}]$.
- Write $A + B\sqrt{-2} = \rho_1 \rho_2 \cdots \rho_r$ 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 the classification of primes in $\mathbb{Z}[\sqrt{-2}]$, if ρ is irreducible in $\mathbb{Z}[\sqrt{-2}]$, then $N(\rho)$ is either 2, a prime congruent to 1 or 3 modulo 8, or the square of a prime congruent to 5 or 7 modulo 8. 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.

Factorization in $\mathbb{Z}[\sqrt{-2}]$, IX

Proof (continued):

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

Factorization in $\mathbb{Z}[\sqrt{-2}]$, X

Example: Determine whether 21, 101, and 292 can be written in the form $a^2 + 2b^2$ for integers a and b.

Factorization in $\mathbb{Z}[\sqrt{-2}]$, X

Example: Determine whether 21, 101, and 292 can be written in the form $a^2 + 2b^2$ for integers a and b.

- We have $21 = 3 \cdot 7$. Since there is a prime congruent to 7 mod 8 that occurs to an odd power, 21 is not of the form $a^2 + 2b^2$.
- The integer 101 is prime, and it is congruent to 5 modulo 8. Therefore, it cannot be written in the form $a^2 + 2b^2$.
- We have $292 = 2^2 \cdot 73$. Since 73 is congruent to 1 modulo 8, each odd prime is congruent to 1 or 3 modulo 8, so 292 can be written in the form $a^2 + 2b^2$.

Summary

We characterized the primes in $\mathbb{Z}[i]$, described how to compute factorizations in $\mathbb{Z}[i]$, and characterized the integers that are sums of two squares.

We characterized the primes in $\mathbb{Z}[\sqrt{-2}]$, described how to compute factorizations in $\mathbb{Z}[\sqrt{-2}]$, and characterized the integers of the form $a^2 + 2b^2$.

Next lecture: Factorization in $\mathcal{O}_{\sqrt{-3}}$, Diophantine equations