Using logarithms to do computations

Fix $p = 37$. Then 2 is a primitive root.

The discrete logarithm values are given by the following.

b	1	2	3	4	5	6	7	8	9
$\text{dlog}_2(b)$	36	1	26	2	23	27	32	3	16

b	10	11	12	13	14	15	16	17	18
$\text{dlog}_2(b)$	24	30	28	11	33	13	4	7	17

b	19	20	21	22	23	24	25	26	27
$\text{dlog}_2(b)$	35	25	22	31	15	29	10	12	6

b	28	29	30	31	32	33	34	35	36
$\text{dlog}_2(b)$	34	21	14	9	5	20	8	19	18

Example: Use the logarithm table to compute the following $\pmod{37}$:

(1) $25 \cdot 16$ (2) 28^{32} (3) 9^{-1}

(4) x satisfying $20x \equiv 3$ (5) $3x^{30} \equiv 4$

Chapter 35: Number Theory and Imaginary Numbers

Let $i = \sqrt{-1}$.

Chapter 35: Number Theory and Imaginary Numbers

Let $i = \sqrt{-1}$. Then

$$\mathbb{C} = \{a + bi \mid a, b \in \mathbb{R}\}.$$

Chapter 35: Number Theory and Imaginary Numbers

Let $i = \sqrt{-1}$. Then

$$\mathbb{C} = \{a + bi \mid a, b \in \mathbb{R}\}.$$

addition:

$$(a + bi) + (c + di) = (a + c) + (b + d)i$$

Chapter 35: Number Theory and Imaginary Numbers

Let $i = \sqrt{-1}$. Then

$$\mathbb{C} = \{a + bi \mid a, b \in \mathbb{R}\}.$$

addition:

$$(a + bi) + (c + di) = (a + c) + (b + d)i$$

multiplication:

$$(a + bi) * (c + di) = ac + adi + cbi + bd(i)^2$$

Chapter 35: Number Theory and Imaginary Numbers

Let $i = \sqrt{-1}$. Then

$$\mathbb{C} = \{a + bi \mid a, b \in \mathbb{R}\}.$$

addition:

$$(a + bi) + (c + di) = (a + c) + (b + d)i$$

multiplication:

$$(a + bi) * (c + di) = ac + adi + cbi + bd(i)^2 = (ac - bd) + (ad + bc)i$$

Chapter 35: Number Theory and Imaginary Numbers

Let $i = \sqrt{-1}$. Then

$$\mathbb{C} = \{a + bi \mid a, b \in \mathbb{R}\}.$$

addition:

$$(a + bi) + (c + di) = (a + c) + (b + d)i$$

multiplication:

$$(a + bi) * (c + di) = ac + adi + cbi + bd(i)^2 = (ac - bd) + (ad + bc)i$$

division:

$$\frac{a + bi}{c + di}$$

Chapter 35: Number Theory and Imaginary Numbers

Let $i = \sqrt{-1}$. Then

$$\mathbb{C} = \{a + bi \mid a, b \in \mathbb{R}\}.$$

addition:

$$(a + bi) + (c + di) = (a + c) + (b + d)i$$

multiplication:

$$(a + bi) * (c + di) = ac + adi + cbi + bd(i)^2 = (ac - bd) + (ad + bc)i$$

division:

$$\frac{a + bi}{c + di} = \frac{(a + bi)(c - di)}{(c + di)(c - di)}$$

Chapter 35: Number Theory and Imaginary Numbers

Let $i = \sqrt{-1}$. Then

$$\mathbb{C} = \{a + bi \mid a, b \in \mathbb{R}\}.$$

addition:

$$(a + bi) + (c + di) = (a + c) + (b + d)i$$

multiplication:

$$(a + bi) * (c + di) = ac + adi + cbi + bd(i)^2 = (ac - bd) + (ad + bc)i$$

division:

$$\begin{aligned}\frac{a + bi}{c + di} &= \frac{(a + bi)(c - di)}{(c + di)(c - di)} \\ &= \frac{(ac + bd) + (bc - ad)i}{c^2 + d^2}\end{aligned}$$

Chapter 35: Number Theory and Imaginary Numbers

Let $i = \sqrt{-1}$. Then

$$\mathbb{C} = \{a + bi \mid a, b \in \mathbb{R}\}.$$

addition:

$$(a + bi) + (c + di) = (a + c) + (b + d)i$$

multiplication:

$$(a + bi) * (c + di) = ac + adi + cbi + bd(i)^2 = (ac - bd) + (ad + bc)i$$

division:

$$\begin{aligned}\frac{a + bi}{c + di} &= \frac{(a + bi)(c - di)}{(c + di)(c - di)} \\ &= \frac{(ac + bd) + (bc - ad)i}{c^2 + d^2} \\ &= \left(\frac{ac + bd}{c^2 + d^2}\right) + \left(\frac{bc - ad}{c^2 + d^2}\right) i\end{aligned}$$

Try: Compute $(2 + 3i)^3$, $(2 + 3i)(-1 + 4i)$, $\dfrac{2 + 3i}{-1 + 4i}$, and $\dfrac{5 - i}{1 + 2i}$.

Galois integers:

$$\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\} \subseteq \mathbb{C}.$$

Galois integers:

$$\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\} \subseteq \mathbb{C}.$$

For $a + bi, c + di \in \mathbb{Z}[i]\ldots$

Galois integers:

$$\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\} \subseteq \mathbb{C}.$$

For $a + bi, c + di \in \mathbb{Z}[i]\ldots$

addition:

$$(a + bi) + (c + di) = (a + c) + (b + d)i \in \mathbb{Z}[x]\checkmark$$

Galois integers:

$$\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\} \subseteq \mathbb{C}.$$

For $a + bi, c + di \in \mathbb{Z}[i] \ldots$

addition:

$$(a + bi) + (c + di) = (a + c) + (b + d)i \in \mathbb{Z}[x] \checkmark$$

multiplication:

$$(a + bi) * (c + di) = (ac - bd) + (ad + bc)i \in \mathbb{Z}[x] \checkmark$$

Galois integers:

$$\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\} \subseteq \mathbb{C}.$$

For $a + bi, c + di \in \mathbb{Z}[i]\ldots$

addition:

$$(a + bi) + (c + di) = (a + c) + (b + d)i \in \mathbb{Z}[x] \checkmark$$

multiplication:

$$(a + bi) * (c + di) = (ac - bd) + (ad + bc)i \in \mathbb{Z}[x] \checkmark$$

division:

$$\frac{a + bi}{c + di} = \left(\frac{ac + bd}{c^2 + d^2}\right) + \left(\frac{bc - ad}{c^2 + d^2}\right) i$$

not always in $\mathbb{Z}[i]$!

Galois integers:

$$\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\} \subseteq \mathbb{C}.$$

For $a + bi, c + di \in \mathbb{Z}[i]\ldots$

addition:

$$(a + bi) + (c + di) = (a + c) + (b + d)i \in \mathbb{Z}[x]\checkmark$$

multiplication:

$$(a + bi) * (c + di) = (ac - bd) + (ad + bc)i \in \mathbb{Z}[x]\checkmark$$

division:

$$\frac{a + bi}{c + di} = \left(\frac{ac + bd}{c^2 + d^2}\right) + \left(\frac{bc - ad}{c^2 + d^2}\right) i$$

not always in $\mathbb{Z}[i]$!

For $m, n \in \mathbb{Z}[i]$, we say m divides n if there is some $k \in \mathbb{Z}[i]$ such that $mk = n$.

Factorization.

Every integer $n \geqslant 2$ has a unique factorization into primes.

Factorization.

Every integer $n \geqslant 2$ has a unique factorization into primes.
(Up to rearrangement of prime factors!)

Factorization.

Every integer $n \geqslant 2$ has a unique factorization into primes.
(Up to rearrangement of prime factors!)

Every integer $n \neq 0$ has a unique factorization into primes, up to multiplication by units:

$$n = (-1)^k p_1^{r_1} \cdots p_\ell^{r_\ell}$$

with primes $p_1 < p_2 < \cdots < p_\ell$, and k unique up to parity.

Factorization.

Every integer $n \geqslant 2$ has a unique factorization into primes. (Up to rearrangement of prime factors!)

Every integer $n \neq 0$ has a unique factorization into primes, up to multiplication by units:

$$n = (-1)^k p_1^{r_1} \cdots p_\ell^{r_\ell}$$

with primes $p_1 < p_2 < \cdots < p_\ell$, and k unique up to parity. (Recall: a unit is a divisor of 1; i.e. a number that has a multiplicative inverse.)

Factorization.

Every integer $n \geqslant 2$ has a unique factorization into primes.
(Up to rearrangement of prime factors!)

Every integer $n \neq 0$ has a unique factorization into primes, up to multiplication by units:

$$n = (-1)^k p_1^{r_1} \cdots p_\ell^{r_\ell}$$

with primes $p_1 < p_2 < \cdots < p_\ell$, and k unique up to parity.
(Recall: a unit is a divisor of 1; i.e. a number that has a multiplicative inverse.)

Ex. $10 = 2 \cdot 5 = (-1)^2 \cdot 2 \cdot 5 = (-1)^4 \cdot 2 \cdot 5 = \cdots$.

Factorization.

Every integer $n \geqslant 2$ has a unique factorization into primes.
(Up to rearrangement of prime factors!)

Every integer $n \neq 0$ has a unique factorization into primes, up to multiplication by units:

$$n = (-1)^k p_1^{r_1} \cdots p_\ell^{r_\ell}$$

with primes $p_1 < p_2 < \cdots < p_\ell$, and k unique up to parity.
(Recall: a unit is a divisor of 1; i.e. a number that has a multiplicative inverse.)

Ex. $10 = 2 \cdot 5 = (-1)^2 \cdot 2 \cdot 5 = (-1)^4 \cdot 2 \cdot 5 = \cdots$.

Units in $\mathbb{Z}[i]$: 1, -1, i, $-i$,... More?

Factorization.

Every integer $n \geqslant 2$ has a unique factorization into primes.
(Up to rearrangement of prime factors!)

Every integer $n \neq 0$ has a unique factorization into primes, up to multiplication by units:

$$n = (-1)^k p_1^{r_1} \cdots p_\ell^{r_\ell}$$

with primes $p_1 < p_2 < \cdots < p_\ell$, and k unique up to parity.
(Recall: a unit is a divisor of 1; i.e. a number that has a multiplicative inverse.)

Ex. $10 = 2 \cdot 5 = (-1)^2 \cdot 2 \cdot 5 = (-1)^4 \cdot 2 \cdot 5 = \cdots$.

Units in $\mathbb{Z}[i]$: 1, -1, i, $-i$,... More? Solve

$$(a + bi) * (c + di) = 1 + 0i$$

Factorization.

Every integer $n \geqslant 2$ has a unique factorization into primes.
(Up to rearrangement of prime factors!)

Every integer $n \neq 0$ has a unique factorization into primes, up to multiplication by units:

$$n = (-1)^k p_1^{r_1} \cdots p_\ell^{r_\ell}$$

with primes $p_1 < p_2 < \cdots < p_\ell$, and k unique up to parity.
(Recall: a unit is a divisor of 1; i.e. a number that has a multiplicative inverse.)

Ex. $10 = 2 \cdot 5 = (-1)^2 \cdot 2 \cdot 5 = (-1)^4 \cdot 2 \cdot 5 = \cdots$.

Units in $\mathbb{Z}[i]$: 1, -1, i, $-i$,... More? Solve

$$(a + bi) * (c + di) = 1 + 0i,$$

namely

$$ac - bd = 1 \quad \text{and} \quad ad + bc = 0.$$

Factorization.

Every integer $n \geqslant 2$ has a unique factorization into primes.
(Up to rearrangement of prime factors!)

Every integer $n \neq 0$ has a unique factorization into primes, up to multiplication by units:

$$n = (-1)^k p_1^{r_1} \cdots p_\ell^{r_\ell}$$

with primes $p_1 < p_2 < \cdots < p_\ell$, and k unique up to parity.
(Recall: a unit is a divisor of 1; i.e. a number that has a multiplicative inverse.)

Ex. $10 = 2 \cdot 5 = (-1)^2 \cdot 2 \cdot 5 = (-1)^4 \cdot 2 \cdot 5 = \cdots$.

Units in $\mathbb{Z}[i]$: 1, -1, i, $-i$,... More? Solve

$$(a + bi) * (c + di) = 1 + 0i,$$

namely

$$ac - bd = 1 \quad \text{and} \quad ad + bc = 0.$$

We'll show there are no more solutions momentarily.

Units in $\mathbb{Z}[i]$: ± 1, $\pm i$.

Units in $\mathbb{Z}[i]$: ± 1, $\pm i$.

Primes in $\mathbb{Z}[i]$? For any $\alpha \in \mathbb{Z}[i]$, we have

$$\alpha = 1 \cdot \alpha = (-1)(-\alpha) = i(-i\alpha) = (-i)(i\alpha)$$

so $\pm 1, \pm i$, $\pm \alpha$, and $\pm i\alpha$ all "divide" α.

Units in $\mathbb{Z}[i]$: ± 1, $\pm i$.

Primes in $\mathbb{Z}[i]$? For any $\alpha \in \mathbb{Z}[i]$, we have

$$\alpha = 1 \cdot \alpha = (-1)(-\alpha) = i(-i\alpha) = (-i)(i\alpha)$$

so $\pm 1, \pm i$, $\pm\alpha$, and $\pm i\alpha$ all "divide" α.

We say $\beta \in \mathbb{Z}[i]$ is prime if the only divisors of β are of the form u or $u\beta$, where u is a unit.

Units in $\mathbb{Z}[i]$: ± 1, $\pm i$.

Primes in $\mathbb{Z}[i]$? For any $\alpha \in \mathbb{Z}[i]$, we have

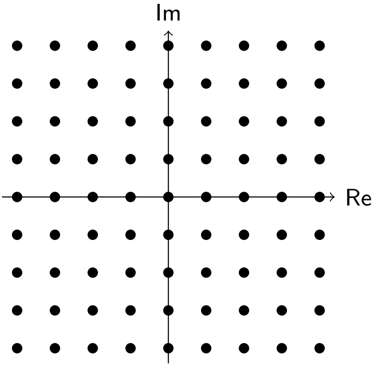
$$\alpha = 1 \cdot \alpha = (-1)(-\alpha) = i(-i\alpha) = (-i)(i\alpha)$$

so $\pm 1, \pm i$, $\pm\alpha$, and $\pm i\alpha$ all "divide" α.

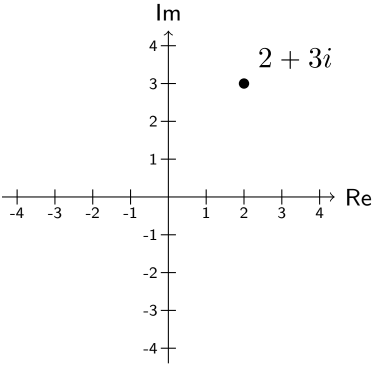
We say $\beta \in \mathbb{Z}[i]$ is prime if the only divisors of β are of the form u or $u\beta$, where u is a unit.

How do we compute primes?

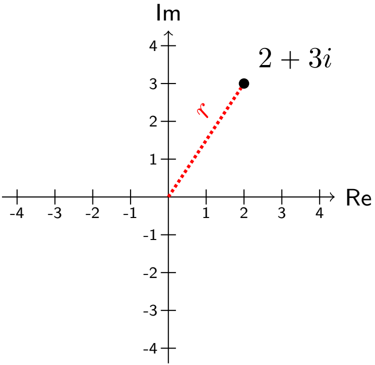
Draw $\mathbb{Z}[i]$ in the complex plane as a lattice of points:



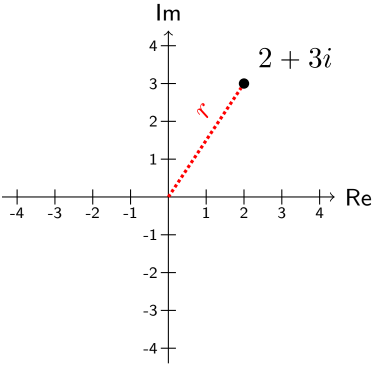
Draw $\mathbb{Z}[i]$ in the complex plane as a lattice of points:



Draw $\mathbb{Z}[i]$ in the complex plane as a lattice of points:



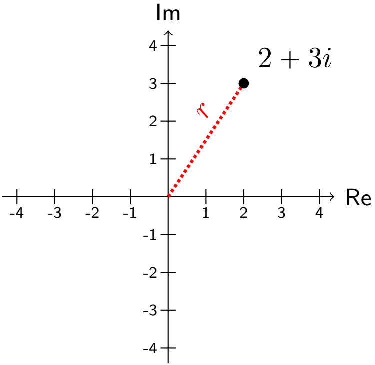
Draw $\mathbb{Z}[i]$ in the complex plane as a lattice of points:



Define

$$N : \mathbb{Z}[i] \to \mathbb{Z}_{\geqslant 0} \quad \text{by} \quad a + bi \mapsto a^2 + b^2$$

Draw $\mathbb{Z}[i]$ in the complex plane as a lattice of points:

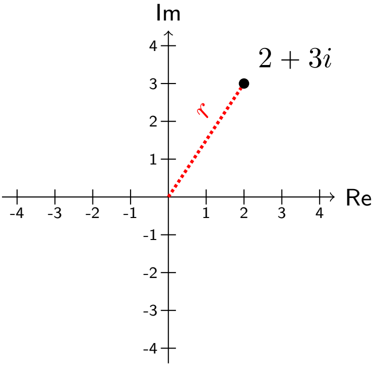


Define

$$N : \mathbb{Z}[i] \to \mathbb{Z}_{\geqslant 0} \quad \text{by} \quad a + bi \mapsto a^2 + b^2,$$

so that $r = \sqrt{N(a+bi)}$.

Draw $\mathbb{Z}[i]$ in the complex plane as a lattice of points:



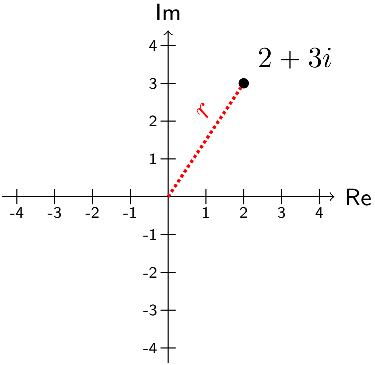
Define

$$N : \mathbb{Z}[i] \to \mathbb{Z}_{\geqslant 0} \quad \text{by} \quad a + bi \mapsto a^2 + b^2,$$

so that $r = \sqrt{N(a+bi)}$. Also

$$\frac{a+bi}{c+di} = \left(\frac{ac+bd}{N(c+di)}\right) + \left(\frac{bc-ad}{N(c+di)}\right) i.$$

Draw $\mathbb{Z}[i]$ in the complex plane as a lattice of points:



Define

$$N : \mathbb{Z}[i] \to \mathbb{Z}_{\geqslant 0} \quad \text{by} \quad a+bi \mapsto a^2+b^2,$$

so that $r = \sqrt{N(a+bi)}$. Also

$$\frac{a+bi}{c+di} = \left(\frac{ac+bd}{N(c+di)}\right) + \left(\frac{bc-ad}{N(c+di)}\right) i.$$

We call N a norm of $\mathbb{Z}[i]$.

Norm

Define

$$N : \mathbb{Z}[i] \to \mathbb{Z}_{\geqslant 0} \quad \text{by} \quad a + bi \mapsto a^2 + b^2.$$

Claim: For $\alpha, \beta \in \mathbb{Z}[i]$, we have

$$N(\alpha\beta) = N(\alpha)N(\beta).$$

Norm

Define

$$N : \mathbb{Z}[i] \to \mathbb{Z}_{\geqslant 0} \quad \text{by} \quad a + bi \mapsto a^2 + b^2.$$

Claim: For $\alpha, \beta \in \mathbb{Z}[i]$, we have

$$N(\alpha\beta) = N(\alpha)N(\beta).$$

Back to units: If α is a unit, then there is some β for which $\alpha\beta = 1$.

Norm

Define

$$N : \mathbb{Z}[i] \to \mathbb{Z}_{\geqslant 0} \quad \text{by} \quad a + bi \mapsto a^2 + b^2.$$

Claim: For $\alpha, \beta \in \mathbb{Z}[i]$, we have

$$N(\alpha\beta) = N(\alpha)N(\beta).$$

Back to units: If α is a unit, then there is some β for which $\alpha\beta = 1$. So

$$1 = N(1)$$

Norm

Define

$$N : \mathbb{Z}[i] \to \mathbb{Z}_{\geqslant 0} \quad \text{by} \quad a + bi \mapsto a^2 + b^2.$$

Claim: For $\alpha, \beta \in \mathbb{Z}[i]$, we have

$$N(\alpha\beta) = N(\alpha)N(\beta).$$

Back to units: If α is a unit, then there is some β for which $\alpha\beta = 1$. So

$$1 = N(1) = N(\alpha\beta)$$

Norm

Define

$$N : \mathbb{Z}[i] \to \mathbb{Z}_{\geqslant 0} \quad \text{by} \quad a + bi \mapsto a^2 + b^2.$$

Claim: For $\alpha, \beta \in \mathbb{Z}[i]$, we have

$$N(\alpha\beta) = N(\alpha)N(\beta).$$

Back to units: If α is a unit, then there is some β for which $\alpha\beta = 1$. So

$$1 = N(1) = N(\alpha\beta) = N(\alpha)N(\beta).$$

Norm

Define

$$N : \mathbb{Z}[i] \to \mathbb{Z}_{\geqslant 0} \quad \text{by} \quad a + bi \mapsto a^2 + b^2.$$

Claim: For $\alpha, \beta \in \mathbb{Z}[i]$, we have

$$N(\alpha\beta) = N(\alpha)N(\beta).$$

Back to units: If α is a unit, then there is some β for which $\alpha\beta = 1$. So

$$1 = N(1) = N(\alpha\beta) = N(\alpha)N(\beta).$$

So $N(\alpha) = N(\beta) = 1$.

Norm

Define

$$N : \mathbb{Z}[i] \to \mathbb{Z}_{\geqslant 0} \quad \text{by} \quad a + bi \mapsto a^2 + b^2.$$

Claim: For $\alpha, \beta \in \mathbb{Z}[i]$, we have

$$N(\alpha\beta) = N(\alpha)N(\beta).$$

Back to units: If α is a unit, then there is some β for which $\alpha\beta = 1$. So

$$1 = N(1) = N(\alpha\beta) = N(\alpha)N(\beta).$$

So $N(\alpha) = N(\beta) = 1$. What are integer solutions to $a^2 + b^2 = 1$?

Norm

Define

$$N : \mathbb{Z}[i] \to \mathbb{Z}_{\geqslant 0} \quad \text{by} \quad a + bi \mapsto a^2 + b^2.$$

Claim: For $\alpha, \beta \in \mathbb{Z}[i]$, we have

$$N(\alpha\beta) = N(\alpha)N(\beta).$$

Back to units: If α is a unit, then there is some β for which $\alpha\beta = 1$. So

$$1 = N(1) = N(\alpha\beta) = N(\alpha)N(\beta).$$

So $N(\alpha) = N(\beta) = 1$. What are integer solutions to $a^2 + b^2 = 1$?

Theorem

The units in $\mathbb{Z}[i]$ are $\{\pm 1, \pm i\}$.

Define

$$N : \mathbb{Z}[i] \to \mathbb{Z}_{\geqslant 0} \quad \text{by} \quad a + bi \mapsto a^2 + b^2.$$

For $\alpha, \beta \in \mathbb{Z}[i]$, we have $N(\alpha\beta) = N(\alpha)N(\beta)$.

Back to primes: Is 2 prime in $\mathbb{Z}[i]$?

Define

$$N : \mathbb{Z}[i] \to \mathbb{Z}_{\geqslant 0} \quad \text{by} \quad a + bi \mapsto a^2 + b^2.$$

For $\alpha, \beta \in \mathbb{Z}[i]$, we have $N(\alpha\beta) = N(\alpha)N(\beta)$.

Back to primes: Is 2 prime in $\mathbb{Z}[i]$?

Suppose we have

$$(a + bi)(c + di) = 2.$$

Define

$$N : \mathbb{Z}[i] \to \mathbb{Z}_{\geqslant 0} \quad \text{by} \quad a + bi \mapsto a^2 + b^2.$$

For $\alpha, \beta \in \mathbb{Z}[i]$, we have $N(\alpha\beta) = N(\alpha)N(\beta)$.

Back to primes: Is 2 prime in $\mathbb{Z}[i]$?

Suppose we have

$$(a + bi)(c + di) = 2.$$

Taking N of both sides, we get

$$(a^2 + b^2)(c^2 + d^2) = 4.$$

Define

$$N : \mathbb{Z}[i] \to \mathbb{Z}_{\geqslant 0} \quad \text{by} \quad a + bi \mapsto a^2 + b^2.$$

For $\alpha, \beta \in \mathbb{Z}[i]$, we have $N(\alpha\beta) = N(\alpha)N(\beta)$.

Back to primes: Is 2 prime in $\mathbb{Z}[i]$?

Suppose we have

$$(a + bi)(c + di) = 2.$$

Taking N of both sides, we get

$$(a^2 + b^2)(c^2 + d^2) = 4.$$

Possibilities:

$a^2 + b^2 = 1$

$a^2 + b^2 = 2$

$a^2 + b^2 = 4$

Define

$$N : \mathbb{Z}[i] \to \mathbb{Z}_{\geqslant 0} \quad \text{by} \quad a + bi \mapsto a^2 + b^2.$$

For $\alpha, \beta \in \mathbb{Z}[i]$, we have $N(\alpha\beta) = N(\alpha)N(\beta)$.

Back to primes: Is 2 prime in $\mathbb{Z}[i]$?

Suppose we have

$$(a + bi)(c + di) = 2.$$

Taking N of both sides, we get

$$(a^2 + b^2)(c^2 + d^2) = 4.$$

Possibilities:

- $a^2 + b^2 = 1$: In this case, $a + bi$ is a unit.
- $a^2 + b^2 = 2$
- $a^2 + b^2 = 4$

Define

$$N : \mathbb{Z}[i] \to \mathbb{Z}_{\geqslant 0} \quad \text{by} \quad a + bi \mapsto a^2 + b^2.$$

For $\alpha, \beta \in \mathbb{Z}[i]$, we have $N(\alpha\beta) = N(\alpha)N(\beta)$.

Back to primes: Is 2 prime in $\mathbb{Z}[i]$?

Suppose we have

$$(a + bi)(c + di) = 2.$$

Taking N of both sides, we get

$$(a^2 + b^2)(c^2 + d^2) = 4.$$

Possibilities:

$a^2 + b^2 = 1$: In this case, $a + bi$ is a unit.

$a^2 + b^2 = 2$

$a^2 + b^2 = 4$: In this case, $c + di$ is a unit.

Define

$$N : \mathbb{Z}[i] \to \mathbb{Z}_{\geqslant 0} \quad \text{by} \quad a + bi \mapsto a^2 + b^2.$$

For $\alpha, \beta \in \mathbb{Z}[i]$, we have $N(\alpha\beta) = N(\alpha)N(\beta)$.

Back to primes: Is 2 prime in $\mathbb{Z}[i]$?

Suppose we have

$$(a + bi)(c + di) = 2.$$

Taking N of both sides, we get

$$(a^2 + b^2)(c^2 + d^2) = 4.$$

Possibilities:

$a^2 + b^2 = 1$: In this case, $a + bi$ is a unit.
$a^2 + b^2 = 2$: Potentially nontrivial factors?
$a^2 + b^2 = 4$: In this case, $c + di$ is a unit.

Define
$$N : \mathbb{Z}[i] \to \mathbb{Z}_{\geqslant 0} \quad \text{by} \quad a + bi \mapsto a^2 + b^2.$$
For $\alpha, \beta \in \mathbb{Z}[i]$, we have $N(\alpha\beta) = N(\alpha)N(\beta)$.

Back to primes: Is 2 prime in $\mathbb{Z}[i]$?

Suppose we have
$$(a + bi)(c + di) = 2.$$
Taking N of both sides, we get
$$(a^2 + b^2)(c^2 + d^2) = 4.$$
Possibilities:

$a^2 + b^2 = 1$: In this case, $a + bi$ is a unit.

$a^2 + b^2 = 2$: Potentially nontrivial factors?

$a^2 + b^2 = 4$: In this case, $c + di$ is a unit.

Are there non-trivial solutions to $a^2 + b^2 = 2$?

Define

$$N : \mathbb{Z}[i] \to \mathbb{Z}_{\geqslant 0} \quad \text{by} \quad a + bi \mapsto a^2 + b^2.$$

For $\alpha, \beta \in \mathbb{Z}[i]$, we have $N(\alpha\beta) = N(\alpha)N(\beta)$.

Back to primes: Is 2 prime in $\mathbb{Z}[i]$?

Suppose we have

$$(a + bi)(c + di) = 2.$$

Taking N of both sides, we get

$$(a^2 + b^2)(c^2 + d^2) = 4.$$

Possibilities:

$a^2 + b^2 = 1$: In this case, $a + bi$ is a unit.
$a^2 + b^2 = 2$: Potentially nontrivial factors?
$a^2 + b^2 = 4$: In this case, $c + di$ is a unit.

Are there non-trivial solutions to $a^2 + b^2 = 2$? Yes! For example, $1 + i$.

Define

$$N : \mathbb{Z}[i] \to \mathbb{Z}_{\geqslant 0} \quad \text{by} \quad a + bi \mapsto a^2 + b^2.$$

For $\alpha, \beta \in \mathbb{Z}[i]$, we have $N(\alpha\beta) = N(\alpha)N(\beta)$.

Back to primes: Is 2 prime in $\mathbb{Z}[i]$?

Suppose we have

$$(a + bi)(c + di) = 2.$$

Taking N of both sides, we get

$$(a^2 + b^2)(c^2 + d^2) = 4.$$

Possibilities:

$a^2 + b^2 = 1$: In this case, $a + bi$ is a unit.

$a^2 + b^2 = 2$: Potentially nontrivial factors?

$a^2 + b^2 = 4$: In this case, $c + di$ is a unit.

Are there non-trivial solutions to $a^2 + b^2 = 2$? Yes! For example, $1 + i$. Does $1 + i$ divide 2?

Define

$$N : \mathbb{Z}[i] \to \mathbb{Z}_{\geqslant 0} \quad \text{by} \quad a + bi \mapsto a^2 + b^2.$$

For $\alpha, \beta \in \mathbb{Z}[i]$, we have $N(\alpha\beta) = N(\alpha)N(\beta)$.

Back to primes: Is 2 prime in $\mathbb{Z}[i]$?

Suppose we have

$$(a + bi)(c + di) = 2.$$

Taking N of both sides, we get

$$(a^2 + b^2)(c^2 + d^2) = 4.$$

Possibilities:

$a^2 + b^2 = 1$: In this case, $a + bi$ is a unit.
$a^2 + b^2 = 2$: Potentially nontrivial factors?
$a^2 + b^2 = 4$: In this case, $c + di$ is a unit.

Are there non-trivial solutions to $a^2 + b^2 = 2$? Yes! For example, $1 + i$. Does $1 + i$ divide 2? Compute:

$$\frac{2}{1 + i}$$

Define

$$N : \mathbb{Z}[i] \to \mathbb{Z}_{\geqslant 0} \quad \text{by} \quad a + bi \mapsto a^2 + b^2.$$

For $\alpha, \beta \in \mathbb{Z}[i]$, we have $N(\alpha\beta) = N(\alpha)N(\beta)$.

Back to primes: Is 2 prime in $\mathbb{Z}[i]$?

Suppose we have

$$(a + bi)(c + di) = 2.$$

Taking N of both sides, we get

$$(a^2 + b^2)(c^2 + d^2) = 4.$$

Possibilities:

$a^2 + b^2 = 1$: In this case, $a + bi$ is a unit.

$a^2 + b^2 = 2$: Potentially nontrivial factors?

$a^2 + b^2 = 4$: In this case, $c + di$ is a unit.

Are there non-trivial solutions to $a^2 + b^2 = 2$? Yes! For example, $1 + i$. Does $1 + i$ divide 2? Compute:

$$\frac{2}{1 + i} = \frac{2(1 - i)}{2}$$

Define

$$N : \mathbb{Z}[i] \to \mathbb{Z}_{\geqslant 0} \quad \text{by} \quad a + bi \mapsto a^2 + b^2.$$

For $\alpha, \beta \in \mathbb{Z}[i]$, we have $N(\alpha\beta) = N(\alpha)N(\beta)$.

Back to primes: Is 2 prime in $\mathbb{Z}[i]$?

Suppose we have

$$(a + bi)(c + di) = 2.$$

Taking N of both sides, we get

$$(a^2 + b^2)(c^2 + d^2) = 4.$$

Possibilities:

$a^2 + b^2 = 1$: In this case, $a + bi$ is a unit.
$a^2 + b^2 = 2$: Potentially nontrivial factors?
$a^2 + b^2 = 4$: In this case, $c + di$ is a unit.

Are there non-trivial solutions to $a^2 + b^2 = 2$? Yes! For example, $1 + i$. Does $1 + i$ divide 2? Compute:

$$\frac{2}{1+i} = \frac{2(1-i)}{2} = 1 - i.$$

Define
$$N : \mathbb{Z}[i] \to \mathbb{Z}_{\geqslant 0} \quad \text{by} \quad a + bi \mapsto a^2 + b^2.$$
For $\alpha, \beta \in \mathbb{Z}[i]$, we have $N(\alpha\beta) = N(\alpha)N(\beta)$.

Back to primes: Is 2 prime in $\mathbb{Z}[i]$?

Suppose we have
$$(a + bi)(c + di) = 2.$$
Taking N of both sides, we get
$$(a^2 + b^2)(c^2 + d^2) = 4.$$
Possibilities:

$a^2 + b^2 = 1$: In this case, $a + bi$ is a unit.

$a^2 + b^2 = 2$: Potentially nontrivial factors?

$a^2 + b^2 = 4$: In this case, $c + di$ is a unit.

Are there non-trivial solutions to $a^2 + b^2 = 2$? Yes! For example, $1 + i$. Does $1 + i$ divide 2? Compute:
$$\frac{2}{1 + i} = \frac{2(1 - i)}{2} = 1 - i.$$
So since $1 + i$ isn't a unit, nor is it a unit multiple of 2, we have 2 is not prime in $\mathbb{Z}[i]$!!

Theorem

Let p be an odd prime. Then there are integers a, b satisfying

$$a^2 + b^2 = p$$

if and only if $p \equiv_4 1$.

Theorem

Let p be an odd prime. Then there are integers a, b satisfying

$$a^2 + b^2 = p$$

if and only if $p \equiv_4 1$.

Proof. Show $a^2 + b^2 = p$ implies $p \equiv_4 1$ by direct computation. For the reverse, see Ch. 24. $\square$

Theorem
Let p be an odd prime. Then there are integers a, b satisfying
$$a^2 + b^2 = p$$
if and only if $p \equiv_4 1$.

Proof. Show $a^2 + b^2 = p$ implies $p \equiv_4 1$ by direct computation. For the reverse, see Ch. 24. □

Ex. There are no integer solutions to $a^2 + b^2 = 3$. So, using the same idea as last time, suppose we have
$$(a + bi)(c + di) = 3.$$

Theorem
Let p be an odd prime. Then there are integers a, b satisfying
$$a^2 + b^2 = p$$
if and only if $p \equiv_4 1$.

Proof. Show $a^2 + b^2 = p$ implies $p \equiv_4 1$ by direct computation. For the reverse, see Ch. 24. □

Ex. There are no integer solutions to $a^2 + b^2 = 3$. So, using the same idea as last time, suppose we have
$$(a + bi)(c + di) = 3.$$
Taking N of both sides, we get
$$(a^2 + b^2)(c^2 + d^2) = 9.$$

Theorem

Let p be an odd prime. Then there are integers a, b satisfying

$$a^2 + b^2 = p$$

if and only if $p \equiv_4 1$.

Proof. Show $a^2 + b^2 = p$ implies $p \equiv_4 1$ by direct computation. For the reverse, see Ch. 24. $\square$

Ex. There are no integer solutions to $a^2 + b^2 = 3$. So, using the same idea as last time, suppose we have

$$(a + bi)(c + di) = 3.$$

Taking N of both sides, we get

$$(a^2 + b^2)(c^2 + d^2) = 9.$$

Possibilities:

$a^2 + b^2 = 1$

$a^2 + b^2 = 3$

$a^2 + b^2 = 9$

Theorem

Let p be an odd prime. Then there are integers a, b satisfying

$$a^2 + b^2 = p$$

if and only if $p \equiv_4 1$.

Proof. Show $a^2 + b^2 = p$ implies $p \equiv_4 1$ by direct computation. For the reverse, see Ch. 24. $\square$

Ex. There are no integer solutions to $a^2 + b^2 = 3$. So, using the same idea as last time, suppose we have

$$(a + bi)(c + di) = 3.$$

Taking N of both sides, we get

$$(a^2 + b^2)(c^2 + d^2) = 9.$$

Possibilities:

$a^2 + b^2 = 1$: In this case, $a + bi$ is a unit.

$a^2 + b^2 = 3$

$a^2 + b^2 = 9$

Theorem
Let p be an odd prime. Then there are integers a, b satisfying
$$a^2 + b^2 = p$$
if and only if $p \equiv_4 1$.

Proof. Show $a^2 + b^2 = p$ implies $p \equiv_4 1$ by direct computation. For the reverse, see Ch. 24. □

Ex. There are no integer solutions to $a^2 + b^2 = 3$. So, using the same idea as last time, suppose we have
$$(a + bi)(c + di) = 3.$$
Taking N of both sides, we get
$$(a^2 + b^2)(c^2 + d^2) = 9.$$
Possibilities:

$a^2 + b^2 = 1$: In this case, $a + bi$ is a unit.

$a^2 + b^2 = 3$

$a^2 + b^2 = 9$: In this case, $c + di$ is a unit.

Theorem
Let p be an odd prime. Then there are integers a, b satisfying

$$a^2 + b^2 = p$$

if and only if $p \equiv_4 1$.

Proof. Show $a^2 + b^2 = p$ implies $p \equiv_4 1$ by direct computation. For the reverse, see Ch. 24. $\square$

Ex. There are no integer solutions to $a^2 + b^2 = 3$. So, using the same idea as last time, suppose we have

$$(a + bi)(c + di) = 3.$$

Taking N of both sides, we get

$$(a^2 + b^2)(c^2 + d^2) = 9.$$

Possibilities:

$a^2 + b^2 = 1$: In this case, $a + bi$ is a unit.

$a^2 + b^2 = 3$: No solutions.

$a^2 + b^2 = 9$: In this case, $c + di$ is a unit.

Theorem

Let p be an odd prime. Then there are integers a, b satisfying

$$a^2 + b^2 = p$$

if and only if $p \equiv_4 1$.

Proof. Show $a^2 + b^2 = p$ implies $p \equiv_4 1$ by direct computation. For the reverse, see Ch. 24. □

Ex. There are no integer solutions to $a^2 + b^2 = 3$. So, using the same idea as last time, suppose we have

$$(a + bi)(c + di) = 3.$$

Taking N of both sides, we get

$$(a^2 + b^2)(c^2 + d^2) = 9.$$

Possibilities:

- $a^2 + b^2 = 1$: In this case, $a + bi$ is a unit.
- $a^2 + b^2 = 3$: No solutions.
- $a^2 + b^2 = 9$: In this case, $c + di$ is a unit.

So 3 is a prime in $\mathbb{Z}[i]$.

We say $\beta \in \mathbb{Z}[i]$ is prime if the only divisors of β are of the form u or $u\beta$, where u is a unit (one of $\{\pm 1, \pm i\}$).

We say $\beta \in \mathbb{Z}[i]$ is prime if the only divisors of β are of the form u or $u\beta$, where u is a unit (one of $\{\pm 1, \pm i\}$).

Looking for primes so far:

1. If $n \in \mathbb{Z}$ is composite in $\mathbb{Z}$, then it is composite in $\mathbb{Z}[i]$.

We say $\beta \in \mathbb{Z}[i]$ is prime if the only divisors of β are of the form u or $u\beta$, where u is a unit (one of $\{\pm 1, \pm i\}$).

Looking for primes so far:

1. If $n \in \mathbb{Z}$ is composite in $\mathbb{Z}$, then it is composite in $\mathbb{Z}[i]$.
2. If $p \in \mathbb{Z}$ is prime in $\mathbb{Z}$, then either
   (a) $p = 2$, which is not prime in $\mathbb{Z}[i]$; (we checked)

We say $\beta \in \mathbb{Z}[i]$ is prime if the only divisors of β are of the form u or $u\beta$, where u is a unit (one of $\{\pm 1, \pm i\}$).

Looking for primes so far:

1. If $n \in \mathbb{Z}$ is composite in $\mathbb{Z}$, then it is composite in $\mathbb{Z}[i]$.
2. If $p \in \mathbb{Z}$ is prime in $\mathbb{Z}$, then either
   (a) $p = 2$, which is not prime in $\mathbb{Z}[i]$; (we checked)
   (b) $p \equiv_4 -1$, in which case p is prime in $\mathbb{Z}[i]$; (prove using norms)

We say $\beta \in \mathbb{Z}[i]$ is prime if the only divisors of β are of the form u or $u\beta$, where u is a unit (one of $\{\pm 1, \pm i\}$).

Looking for primes so far:

1. If $n \in \mathbb{Z}$ is composite in $\mathbb{Z}$, then it is composite in $\mathbb{Z}[i]$.
2. If $p \in \mathbb{Z}$ is prime in $\mathbb{Z}$, then either
   (a) $p = 2$, which is not prime in $\mathbb{Z}[i]$; (we checked)
   (b) $p \equiv_4 -1$, in which case p is prime in $\mathbb{Z}[i]$; (prove using norms)
   (c) $p \equiv_4 1$, in which case there are $a, b \in \mathbb{Z}$ with $a^2 + b^2 = p$

We say $\beta \in \mathbb{Z}[i]$ is prime if the only divisors of β are of the form u or $u\beta$, where u is a unit (one of $\{\pm 1, \pm i\}$).

Looking for primes so far:

1. If $n \in \mathbb{Z}$ is composite in $\mathbb{Z}$, then it is composite in $\mathbb{Z}[i]$.
2. If $p \in \mathbb{Z}$ is prime in $\mathbb{Z}$, then either
   (a) $p = 2$, which is not prime in $\mathbb{Z}[i]$; (we checked)
   (b) $p \equiv_4 -1$, in which case p is prime in $\mathbb{Z}[i]$; (prove using norms)
   (c) $p \equiv_4 1$, in which case there are $a, b \in \mathbb{Z}$ with $a^2 + b^2 = p$, so that $a + ib \neq u, pu$ for any unit u

We say $\beta \in \mathbb{Z}[i]$ is prime if the only divisors of β are of the form u or $u\beta$, where u is a unit (one of $\{\pm 1, \pm i\}$).

Looking for primes so far:

1. If $n \in \mathbb{Z}$ is composite in $\mathbb{Z}$, then it is composite in $\mathbb{Z}[i]$.
2. If $p \in \mathbb{Z}$ is prime in $\mathbb{Z}$, then either
   (a) $p = 2$, which is not prime in $\mathbb{Z}[i]$; (we checked)
   (b) $p \equiv_4 -1$, in which case p is prime in $\mathbb{Z}[i]$; (prove using norms)
   (c) $p \equiv_4 1$, in which case there are $a, b \in \mathbb{Z}$ with $a^2 + b^2 = p$, so that $a + ib \neq u, pu$ for any unit u and

$$(a + ib)(a - ib) = a^2 + b^2$$

We say $\beta \in \mathbb{Z}[i]$ is prime if the only divisors of β are of the form u or $u\beta$, where u is a unit (one of $\{\pm 1, \pm i\}$).

Looking for primes so far:

1. If $n \in \mathbb{Z}$ is composite in $\mathbb{Z}$, then it is composite in $\mathbb{Z}[i]$.
2. If $p \in \mathbb{Z}$ is prime in $\mathbb{Z}$, then either
   (a) $p = 2$, which is not prime in $\mathbb{Z}[i]$; (we checked)
   (b) $p \equiv_4 -1$, in which case p is prime in $\mathbb{Z}[i]$; (prove using norms)
   (c) $p \equiv_4 1$, in which case there are $a, b \in \mathbb{Z}$ with $a^2 + b^2 = p$, so that $a + ib \neq u, pu$ for any unit u and

$$(a + ib)(a - ib) = a^2 + b^2 = p$$

We say $\beta \in \mathbb{Z}[i]$ is prime if the only divisors of β are of the form u or $u\beta$, where u is a unit (one of $\{\pm 1, \pm i\}$).

Looking for primes so far:

1. If $n \in \mathbb{Z}$ is composite in $\mathbb{Z}$, then it is composite in $\mathbb{Z}[i]$.
2. If $p \in \mathbb{Z}$ is prime in $\mathbb{Z}$, then either
   (a) $p = 2$, which is not prime in $\mathbb{Z}[i]$; (we checked)
   (b) $p \equiv_4 -1$, in which case p is prime in $\mathbb{Z}[i]$; (prove using norms)
   (c) $p \equiv_4 1$, in which case there are $a, b \in \mathbb{Z}$ with $a^2 + b^2 = p$, so that $a + ib \neq u, pu$ for any unit u and
   $$(a + ib)(a - ib) = a^2 + b^2 = p,$$
   i.e. p is not prime in $\mathbb{Z}[i]$.

We say $\beta \in \mathbb{Z}[i]$ is prime if the only divisors of β are of the form u or $u\beta$, where u is a unit (one of $\{\pm 1, \pm i\}$).

Looking for primes so far:

1. If $n \in \mathbb{Z}$ is composite in $\mathbb{Z}$, then it is composite in $\mathbb{Z}[i]$.
2. If $p \in \mathbb{Z}$ is prime in $\mathbb{Z}$, then either
   (a) $p = 2$, which is not prime in $\mathbb{Z}[i]$; (we checked)
   (b) $p \equiv_4 -1$, in which case p is prime in $\mathbb{Z}[i]$; (prove using norms)
   (c) $p \equiv_4 1$, in which case there are $a, b \in \mathbb{Z}$ with $a^2 + b^2 = p$, so that $a + ib \neq u, pu$ for any unit u and
   $$(a + ib)(a - ib) = a^2 + b^2 = p,$$
   i.e. p is not prime in $\mathbb{Z}[i]$.

Proposition

An integer n is prime in $\mathbb{Z}[i]$ if and only if n is a prime in $\mathbb{Z}$ satisfying $n \equiv_4 1$.

We say $\beta \in \mathbb{Z}[i]$ is prime if the only divisors of β are of the form u or $u\beta$, where u is a unit (one of $\{\pm 1, \pm i\}$).

Looking for primes so far:

1. If $n \in \mathbb{Z}$ is composite in $\mathbb{Z}$, then it is composite in $\mathbb{Z}[i]$.
2. If $p \in \mathbb{Z}$ is prime in $\mathbb{Z}$, then either
   (a) $p = 2$, which is not prime in $\mathbb{Z}[i]$; (we checked)
   (b) $p \equiv_4 -1$, in which case p is prime in $\mathbb{Z}[i]$; (prove using norms)
   (c) $p \equiv_4 1$, in which case there are $a, b \in \mathbb{Z}$ with $a^2 + b^2 = p$, so that $a + ib \neq u, pu$ for any unit u and

$$(a + ib)(a - ib) = a^2 + b^2 = p,$$

   i.e. p is not prime in $\mathbb{Z}[i]$.

Proposition

An integer n is prime in $\mathbb{Z}[i]$ if and only if n is a prime in $\mathbb{Z}$ satisfying $n \equiv_4 1$.

Are there any more?

Theorem (Gaussian Prime Theorem)

The Gaussian primes can be described as follows:

(i) *(ramified) 1 + i is a Gaussian prime.*

(ii) *(inert) Let* p *be a prime in* $\mathbb{Z}$ *with* $p \equiv -1 \pmod 4$*. Then* p *is a Gaussian prime.*

(iii) *(split) Let* p *be a prime in* $\mathbb{Z}$ *with* $p \equiv 1 \pmod 4$*. Then* $p = a^2 + b^2$ *for* $a, b \in \mathbb{Z}_{>0}$*, and* $a + bi$ *is a Gaussian prime.*

Moreover, every Gaussian prime is equal to a unit times a Gaussian prime of the form (i), (ii), or (iii).