Number Theory, Lecture 11

The Gaussian integers

Jan Snellman[1]

[1]Matematiska Institutionen
Linköpings Universitet

TEKNISKA HÖGSKOLAN
LINKÖPINGS UNIVERSITET

Summary

1. **Definition**
   - Norm
   - Units,irreducibles, primes
2. **Division algorithm**
   - Division algorithm in $\mathbb{Z}$
   - Rationalizing denominators
   - Greatest common divisor
   - Euclidean Algorithm
3. **Unique factorization**
   - Irreducibles are primes
4. **Gaussian primes**
5. **Sums of two squares**
6. **Pythagorean triples**
7. **Congruences**
   - Representatives, transversals
   - Fermat and euler

Definition

- $z = a + ib \in \mathbb{C}$
- conjugate $\overline{z} = a - ib$
- norm $N(z) = z\overline{z} = a^2 + b^2$

Lemma

$N(zw) = N(z)N(w)$

Proof.

$\overline{zw} = \overline{z}\overline{w}$ □

Definition

$\mathbb{Z}[i] = \{ a + ib | a, b \in \mathbb{Z} \}$

Lemma

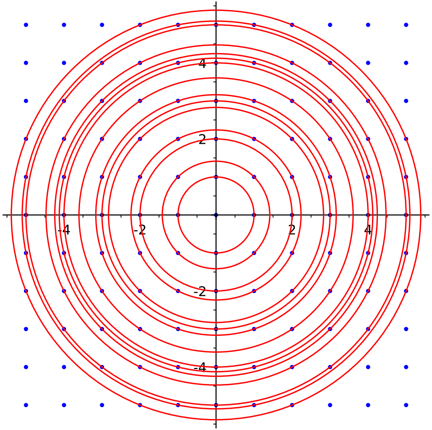
- *$\mathbb{Z}[i]$ subring of $\mathbb{C}$*
- *Not a subfield ($1/2 \notin \mathbb{Z}[i]$)*
- *Integral domain (no zero-divisors)*
- *Principal ideal domain*
- *Euclidean domain*

Lemma

If $N(\alpha) = n$ then $v_p(n)$ is even for all $p \equiv 3 \mod 4$. If n is a positive integer such that $v_p(n)$ is even for all $p \equiv 3 \mod 4$, then n is the norm of some $\alpha \in \mathbb{Z}[i]$.

Proof.

If $\alpha = a + ib$ then $n = N(\alpha) = a^2 + b^2$ is a sum of two squares. Thus, every prime congruent to 3 mod 4 occurse with even multiplicity; the converse also holds. □


4
2
-2
-4
-4
-2
2
4

Definition

$\alpha, \beta \in \mathbb{Z}[i]$

- $\alpha | \beta$ iff exists $\gamma \in \mathbb{Z}[i]$ s.t. $\beta = \gamma\alpha$
- α is a unit if $\alpha | 1$
- α, β are associate if $\alpha | \beta$ and $\beta | \alpha$
- α is irreducible if any divisor is a unit or associate to α
- α is a (Gaussian) prime if $\alpha | \beta_1 \beta_2$ implies that $\alpha | \beta_1$ or $\alpha | \beta_2$ (or both)

$\mathbb{Q}[i]$

Definition

$\mathbb{Q}[i] = \{ a + bi | a, b \in \mathbb{Q} \}$

Lemma

- *$\mathbb{Z}[i]$ subring of $\mathbb{Q}[i]$, which is a subfield of $\mathbb{C}$, and a quadratic field extension of $\mathbb{Q}$*
- *$\mathbb{Q}[i]$ is the field of fractions of $\mathbb{Z}[i$ in the same way that $\mathbb{Q}$ is for $\mathbb{Z}$, namely, it is the smallest field containing $\mathbb{Z}[i]$*
- *So, if $\alpha, \beta \in \mathbb{Z}[i]$, with $\beta \neq 0$, then it is always true that $\frac{\alpha}{\beta} \in \mathbb{Q}[i]$, but $\frac{\alpha}{\beta} \in \mathbb{Z}[i]$ if and only if $\beta | \alpha$*

Example

$$\frac{2+3i}{1-i} = \frac{(2+3i)(1+i)}{(1+i)(1-i)} = \frac{-1+5i}{2} = \frac{-1}{2} + \frac{5}{2}i \in \mathbb{Q}[i] \setminus \mathbb{Z}[i],$$

so $1-i \not| 2+3i$.

On the other hand,

$$\frac{3-i}{1-i} = \frac{(3-i)(1+i)}{(1+i)(1-i)} = \frac{4+2i}{2} = 2+i \in \mathbb{Z}[i],$$

so $1-i | 3-i$.

Lemma

$\alpha | \beta$ *implies that* $N(\alpha) | N(\beta)$

Proof.

Follows from multiplicativity of the norm. □

Corollary

- *$N(\alpha) = 1$ iff α is a unit iff $\alpha \in \{\pm 1, \pm i\}$*
- *if $N(\alpha)$ is a (rational) prime, then α is irreducible.*

Proof.

- $1 = N(1) = N(\alpha \frac{1}{\alpha}) = N(\alpha)N(\frac{1}{\alpha})$, so since $N(\alpha)$ and $N(\frac{1}{\alpha})$ are positive integers, they are both 1.
- If $\alpha = \beta\gamma$ with $N(\beta), N(\gamma) > 1$, then $N(\alpha) = N(\beta)N(\gamma)$, a contradiction.

$\square$

Lemma

$u, v \in \mathbb{Z}[i]$ are associate iff $u = \alpha v$ for some unit $\alpha \in \mathbb{Z}[i]$, i.e. if $u \in \{\pm v, \pm iv\}$

Proof.

Obvious. □

Lemma

If $u, v \in \mathbb{Z}[i]$ are associate, then $N(u) = N(v)$.

Example

If $\alpha = 3 + 4i$ then $N(\alpha) = N(\overline{\alpha}) = 3^2 + 4^2 = 25$, yet $\alpha \not| \overline{\alpha}$ since

$$\frac{3-4i}{3+4i} = \frac{(3-4i)^2}{25} = \frac{9-16-24i}{25} = \frac{-7}{25} + \frac{-24}{25}i \not\in \mathbb{Z}[i]$$

Example

- $7/3 \in \mathbb{Q}$
- $7/3 = 2 + 1/3$
- $7 = 2 * 3 + 1$
- Quotient 2, remainder 1
- $a = bq + r$, $0 \leq r < b$
- $q = \lfloor a/b \rfloor$, $r = a - bq$
- Can also choose q to be closest integer to a/b, and $|r| \leq b/2$
- $8/3 = 2 + 2/3 = 3 - 1/3$
- $8 = 2 * 3 + 2 = 3 * 3 - 1$

Theorem (Division algorithm)

If $\alpha, \beta \in \mathbb{Z}[i]$, $\beta \neq 0$, *then exists (not necessarily unique)* $\gamma, \rho \in \mathbb{Z}[i]$ *such that*

1. $\alpha = \gamma\beta + \rho$,
2. $N(\rho) < N(\beta)$, *(in fact, can achieve* $N(\rho) \leq \frac{1}{2}N(\beta)$*)*

Proof.

Calculate $\frac{\alpha}{\beta} = \frac{r}{t} + \frac{s}{t}i \in \mathbb{Q}[i]$ as before. Let u, v be closest integers to $\frac{r}{t}$ and $\frac{s}{t}$. Let $\gamma = u + iv$, $\rho = \alpha - \gamma\beta$. □

Example

$$\frac{1+8i}{2-4i} = \frac{(1+8i)(2+4i)}{20} = \frac{-30+20i}{20} = \frac{-3}{2} + i$$

If we take $\gamma = -1 + i$ then $\rho = -1 + 2i$, with norm 5.

If we take $\gamma = -2 + i$ then $\rho = 1 - 2i$, also with norm 5.

Theorem

Let $\alpha, \beta \in \mathbb{Z}[i]$. For $\gamma \in \mathbb{Z}[i]$, the following are equivalent:

1. $\gamma|\alpha$, $\gamma|\beta$ *(so γ is a common divisor of α and β) and if* $\rho|\alpha$, $\rho|\beta$ *then* $\rho|\gamma$
2. $\gamma|\alpha$, $\gamma|\beta$ *and if* $\rho|\alpha$, $\rho|\beta$ *then* $N(\rho) \leq N(\gamma)$
3. $\gamma = u\alpha + v\beta$ *for some* $u, v \in \mathbb{Z}[i]$, *and if* $\rho = f\alpha + g\beta$ *for some* $f, g \in \mathbb{Z}[i]$ *then* $\gamma|\rho$
4. $\gamma = u\alpha + v\beta$ *for some* $u, v \in \mathbb{Z}[i]$, *and if* $\rho = f\alpha + g\beta$ *for some* $f, g \in \mathbb{Z}[i]$ *then* $N(\rho) \leq N(\gamma)$

Proof.

Same as for the integers, with $|\cdot|$ replaced by $N(\cdot)$. □

Definition

In this case, we say that γ is a greatest common divisor of α and β.

Lemma

Any two gcd's of α, β are associate.

Proof.

Obvious. □

Definition

$\alpha, \beta \in \mathbb{Z}[i]$ are relatively prime if $\gcd(\alpha, \beta) = 1$ (or a unit); equivalently, iff

$$u\alpha + v\beta = 1$$

is solvable in $\mathbb{Z}[i]$.

Lemma

If $\alpha = \gamma\beta + \rho$ *with* $N(\rho) < N(\beta)$*, then* $\gcd(\alpha, \beta) = \gcd(\beta, \rho)$

Theorem (Euclidean algorithm)

Iterate the above, then you'll get a greatest common divisor. Collect terms, and you'll get a Bezout expression.

Note that this works even though quotients and remainders are not unique.

Example

$$
\begin{aligned}
11 + 3i &= (1 - i)(1 + 8i) + 2 - 4i \\
1 + 8i &= (-1 + i)(2 - 4i) + 1 - 2i \\
2 - 4i &= 2(1 - 2i) + 0
\end{aligned}
$$

so

$$
\begin{aligned}
\gcd(11 + 3i, 1 + 8i) = 1 - 2i = (1)(1 + 8i) + (1 - i)(2 - 4i) = \\
= (1)(1 + 8i) + (1 - i)((11 + 3i) + (-1 + i)(1 + 8i)) = \\
= (1 - i)(11 + 3i) + (1 + (1 - i)(-1 + i))(1 + 8i)
\end{aligned}
$$

Lemma

If $\alpha, \beta, \gamma \in \mathbb{Z}[i]$, $\alpha | \beta\gamma$, $\gcd(\alpha, \beta) = 1$, *then* $\alpha | \gamma$.

Proof.

Since $\alpha | \beta\gamma$ we can write $\beta\gamma = \alpha w$ for some $w \in \mathbb{Z}[i]$. Furthermore, since $\gcd(\alpha, \beta) = 1$,

$$1 = u\alpha + v\beta,$$

so

$$\gamma = \gamma u \alpha + \gamma v \beta = \alpha \gamma u + \alpha w v = \alpha(u\gamma + wv)$$

□

Lemma

If $\alpha \in \mathbb{Z}[i]$ is irreducible, then it is prime.

Proof.

Suppose that $\alpha | ab$. Since α is irreducible, $\gcd(\alpha, a) = 1$, so by the previous lemma $\alpha | b$. □

Lemma

If $\alpha \in \mathbb{Z}[i]$ is prime, then it is irreducible.

Proof.

Suppose, towards a contradiction, that $\alpha = ab$ with $N(a), N(b) < N(\alpha)$. Then $\alpha | ab$ but $\alpha \not| a$, $\alpha \not| b$. □

Theorem

Every $\alpha \in \mathbb{Z}[i]$ can be written as a (finite) product of (Gaussian) primes.

Proof.

If α is irreducible, it is prime, and we are done.
If $\alpha = ab$ with $N(a), N(b) < N(\alpha)$, then by induction we can write a, b as products of prime. Combine. □

Theorem (Unique factorization)

If $0 \neq \alpha \in \mathbb{Z}[i]$, then

$$\alpha = \pi_1 \cdots \pi_s$$

where the π_i's are Gaussian primes. If furthermore

$$\alpha = q_1 \cdots q_t$$

is another factorization of α into Gaussian primes, then $t = s$, and there is some permutation $\sigma \in S_s$ such that $q_j = \epsilon_j \pi_{\sigma(j)}$ for $1 \leq j \leq s$, with $N(\epsilon_j) = 1$.

Proof.

Similar to the integers. □

Example

Note that a (rational) prime p need not be a Gaussian prime. For instance,

$$5 = (1+2i)(1-2i) = (2-i)(2+i)$$

Here, $(1+2i)$ and $2-i$ are associate, as is $1-2i$ and $2+i$, so the two factorizations are (essentially) the same.

Example

Let $\alpha = 3 + 4i$. Then $N(\alpha) = 9 + 16 = 25 = 5^2$. Thus, either α is a prime, or $\alpha = uv$ with $N(u) = N(v) = 5$.
What can have norm 5? By exhaustive search, we find

$$1 + 2i, 1 - 2i, -1 + 2i, -1 - 2i, 2 + i, 2 - i, -2 + i, -2 - i$$

and that

$$3 + 4i = -(1 - 2i)^2$$

Theorem

- *Any* $\alpha \in \mathbb{Z}[i]$ *with even norm is divisible by* $1 + i$
- 2 *is not a Gaussian prime*

Proof.

- Suppose that $N(a + ib) = (a + ib)(a - ib) = a^2 + b^2 = 2c$. Since $(1 + i)(1 - i) = 2$, we have

$$(a + ib)(a - ib) = (1 + i)(1 - i)c = (1 + i)^2 ic$$

  Since $N(1 + i) = 2$, $1 + i$ is a Gaussian prime. By unique factorization, $1 + i$ divides $a + ib$ or $a - ib$.
  But if $1 + i$ divides $a - ib$ then $1 - i$ divides $a + ib$, and $1 + i$ is associate to $1 - i$.
- $2 = (1 + i)(1 - i)$.

□

Lemma

Let π be a Gaussian prime. Then $\pi | p$ for some unique rational prime p.

Proof.

Put $N(\pi) = \pi\overline{\pi} = n$, and factor into rational primes, $n = p_1 \cdots p_r$. Then

$$\pi | p_1 p_2 \cdots p_r \quad \implies \quad \pi | p_j \text{ some } p_j$$

But $\pi\alpha \in \mathbb{Z}[i]$ iff $\alpha = \overline{\pi}c$, $c \in \mathbb{Z}$; if $\pi\overline{\pi}c = p$ is prime, then $c = \pm 1$. □

Theorem

A rational prime p factors in $\mathbb{Z}[i]$ iff it is a sum of two squares.

Proof.

- Suppose $p = \alpha\beta \in \mathbb{Z}[i]$, α, β non-units. Then $N(p) = p^2 = N(\alpha\beta) = N(\alpha)N(\beta)$. Hence $N(\alpha) = N(\beta) = p$. Write $\alpha = a + ib$, then $p = N(a + ib) = a^2 + b^2$, so p is a sum of two squares.
- Suppose $p = a^2 + b^2$, $a, b \in \mathbb{Z}$. Put $\alpha = a + ib$. Then

$$p = (a + ib)(a - ib) = \alpha\overline{\alpha}$$

is a non-trivial factorization of p.

□

Corollary

Any rational prime $p \equiv 3 \mod 4$ *is a Gaussian prime.*

Proof.

Recall that such a rational prime can not be written as the sum of two squares. □

Corollary

A rational prime $p \equiv 1 \mod 4$ has exactly two non-associate Gaussian prime factors in $\mathbb{Z}[i]$.

Proof.

We know that

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

where $a + ib$ and $a - ib$ have prime norm, and hence are Gaussian primes. We claim that they are not associate.

1. If $a + ib = 1(a - ib)$ then $b = 0$, hence $p = a^2$, contradicting p rational prime.
2. If $a + ib = -(a - ib)$ then $a = 0$.
3. If $a + ib = i(a - ib) = b + ia$ then $a = b$, hence $p = a^2 + b^2 = 2a^2$, a contradiction.
4. If $a + ib = -i(a - ib) = -b - ia$ then $a = -b$ so $p = a^2 + b^2 = 2b^2$, a contradiction.

□

Corollary

Let p be a rational prime.

- *If* $p = 2$ *then* $p = 2 = -(1+i)^2$
- *If* $p \equiv 1 \mod 4$ *then* $p = \pi\overline{\pi}$, *where* π *and* $\overline{\pi}$ *are not associate.*
- *If* $p \equiv 3 \mod 4$ *then* p *is (also) a Gaussian prime.*

Theorem

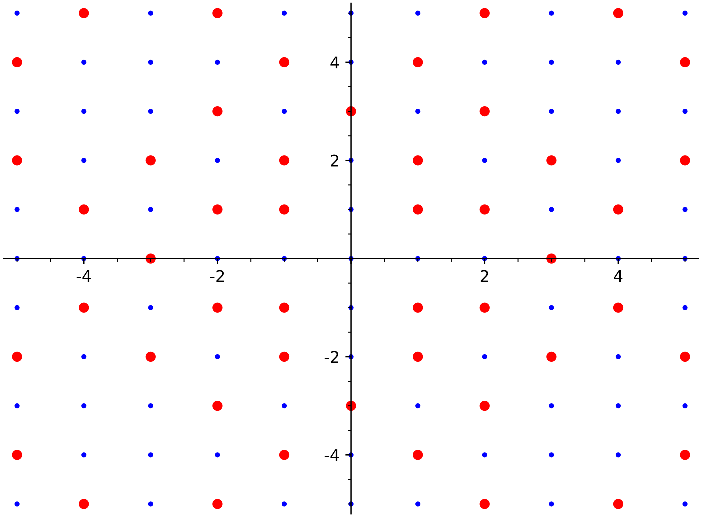
Every Gaussian prime α is associate to either

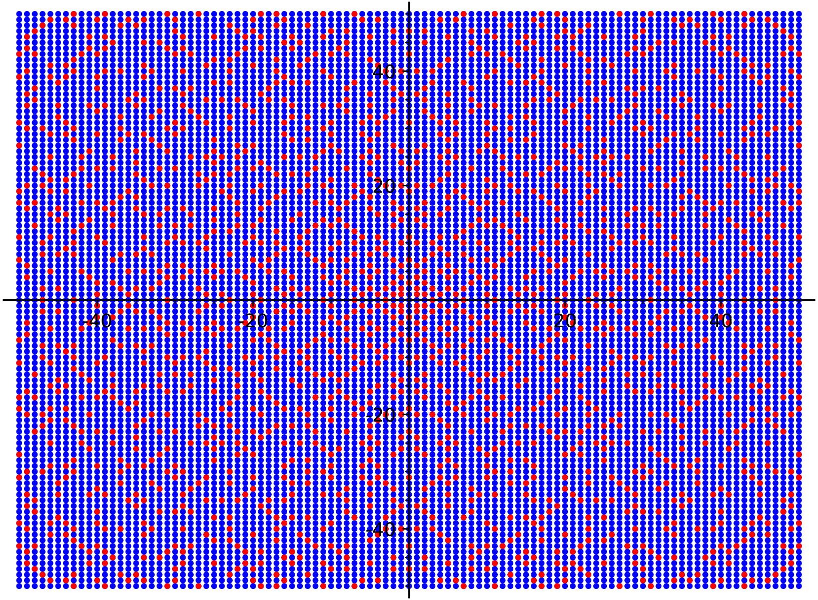
1. $1+i$
2. π *or* $\overline{\pi}$, *where* $N(\pi) = p$ *is a rational prime,* $p \equiv 1 \mod 4$,
3. p, *where* p *is a rational prime,* $p \equiv 3 \mod 4$.

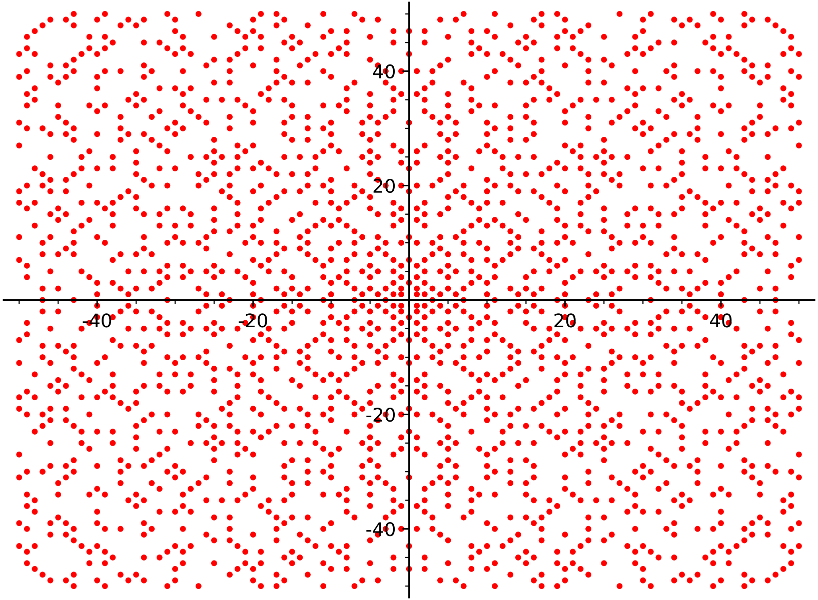
Proof.

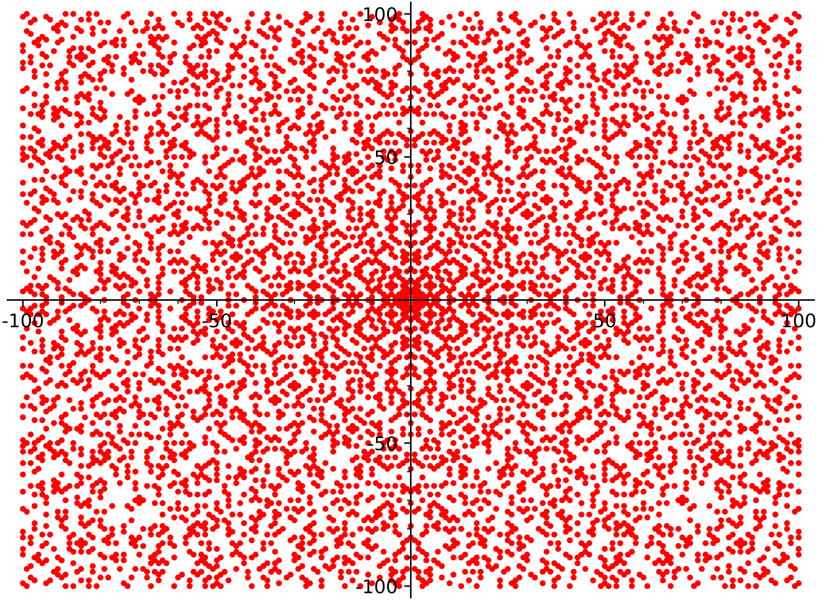
- Every Gaussian prime α is a factor of some rational prime p
- Either $p = 2$, $p \equiv 1 \mod 4$, or $p \equiv 3 \mod 4$
- We now know how these rational primes factor in $\mathbb{Z}[i]$

□


4
2
-2
-4
-4
-2
2
4


40
20
-20
-40
-40
-20
20
40


40
20
-40
-20
20
40
-20
-40


100
50
-50
-100
-100
-50
50
100

Theorem

If a rational prime p is a sum of two squares, say $p = a^2 + b^2$, then it is so expressible in an essentially unique way: a^2 and b^2 are uniquely determined (up to ordering).

Proof.

- $p = a^2 + b^2 = (a + ib)(a - ib)$
- $N(a + ib) = N(a - ib) = p$, so $a + ib$, $a - ib$ are Gaussian primes
- Suppose that $p = c^2 + d^2 = (c + id)(c - id)$.
- By unique factorization, $a + ib = u(c + id)$, u unit, or $a + ib = u(c - id)$.
- In the first case, if $u = 1$, then $c = -a$ and $d = -b$, so $c^2 = a^2$ and $d^2 = b^2$

□

Theorem

Let the positive integer n have prime factorization

$$n = 2^m \prod_{j=1}^{s} p_j^{e_j} \prod_{k=1}^{t} q_k^{f_k}$$

where the p_j*'s are primes* $\equiv 1 \mod 4$, *the* q_k*'s are primes* $\equiv 3 \mod 4$, *and all* f_k*'s are even.*
Then the number of ways of writing n as a sum of two squares, counting signs and order, is

$$4 \prod_j (e_j + 1)$$

Proof.

- Count the ways to factor $n = u^2 + v^2 = (u+iv)(u-iv)$ in $\mathbb{Z}[i]$
- $2^m = i^m(1-i)^{2m}$
- $p_j = (a_j + ib_j)(a_j - ib_j)$, product non-associate Gaussian primes
- So $n = \epsilon(1-i)^{2m} \prod_{j=1}^{s}(a_j + ib_j)(a_j - ib_j) \prod_{k=1}^{t} q_k^{f_k}$
- The factor $u + iv$ is, by unique factorization of the form $\epsilon_0(1-i)^w \prod_{j=1}^{s}(a_j + ib_j)^{g_j}(a_j - ib_j)^{h_j} \prod_{k=1}^{t} \ell_k$ with $0 \le w \le 2m$, $0 \le g_j \le e_j$, $0 \le h_j \le e_j$, $0 \le \ell_k \le f_k$
- $u - iv = \overline{u+iv} = \overline{\epsilon_0}(1-i)^w \prod_{j=1}^{s}(a_j - ib_j)^{g_j}(a_j + ib_j)^{h_j} \prod_{k=1}^{t} \ell_k$
- $n = (u+iv)(u-iv) = 2^w \prod_{j=1}^{s} p_j^{g_j + h_j} \prod_{k=1}^{t} q_k^{2\ell_k}$
- So $w = m$, $g_j + h_j = e_j$, $2\ell_k = f_k$, ϵ_0 unit
- So $e_j + 1$ choices for g_j, 4 choices for ϵ_0.

□

Example

$$n = 5^2 = (2+i)^2(2-i)^2$$

Possible factors $u + iv$ are

$$(2+i)^2 = 3+4i,\ i(2+i)^2 = -4+3i,\ i^2(2+i)^2 = -3-4i,\ i^3(2+i)^2 = 4-3i,$$
$$(2+i)(2-i) = 5$$
$$(2-i)^2 = 3-4i$$

and 6 more, yielding $n = (\pm 5)^2 + 0^2 = (\pm 3)^2 + (\pm 4)^2 = (\pm 4)^2 + (\pm 3)^2$.

Example

$$13 = (2+3i)(2-3i),$$

with factors

$$2+3i, -3+2i, -2-3i, 3-2i, 2-3i, 3+2i, -2+3i, -3-2i$$

Hence

$$5^2 * 13 = (2+i)^2(2-i)^2(2+3i)(2-3i),$$

one possible factor is

$$(2+i)^2(2+3i) = (3+4i)(2+3i) = -6+17i$$

so

$$5^2 * 13 = (-6)^2 + 17^2.$$

Theorem

Let $4F(n)$ denote the number of ways of writing n as a sum of squares. Then F is a multiplicative function, with values on prime powers given by

- $F(2^m) = 1$,
- *if* $q \equiv 3 \mod 4$ *then* $F(q^{2f}) = 1$ *and* $F(q^{2f+1}) = 0$
- *if* $p \equiv 1 \mod 4$ *then* $F(p^e) = e + 1$

Recall:

Definition

- Solutions (in integers) to $a^2 + b^2 = c^2$ are called Ptyhagorean triples (PT)
- If $\gcd(a, b, c) = 1$ then primitive Pythagoreant triple (PPT)

Lemma

- *If (a, b, c) PPT, then $\gcd(a, b) = 1$, a, b different parity, c odd*
- *Assume a odd, b even, then given by parametrization*

$$a = u^2 - v^2, \qquad b = 2uv, \qquad c = u^2 + v^2$$

with $u > v > 0$, $\gcd(u, v) = 1$, u, v different parity.

Let us prove this once again, now using Gaussian integers!

Sketch of proof

- $c^2 = a^2 + b^2 = (a+ib)(a-ib)$
- First show $\gcd(a+ib, a-ib) = 1 \in \mathbb{Z}[i]$. Let δ be common divisor.
- δ divides $a+ib, a-ib$, hence $2a$ and $2ib$, hence $2b$.
- δ is relatively prime to $2 = -i(1+i)^2$ since
  1. $1+i$ prime
  2. $1+i$ divides δ iff $N(\delta)$ is even
  3. $\delta^2|c^2$ so $N(\delta)^2|c^4$; however, c is odd.
  4. So $\gcd(\delta, 1+i) = 1$, hence $\gcd(\delta, 2) = 1$
- So $\delta|2a \implies \delta|a$, and $\delta|2b \implies \delta|b$.
- Since $\gcd(a,b) = 1 \in \mathbb{Z}$, by Bezout, $1 = ra + sb$, thus by Bezout in $\mathbb{Z}[i]$, $\gcd(a,b) = 1 \in \mathbb{Z}[i]$.

Proof (contd)

- Hence $\delta = 1$, and $\gcd(a + ib, a - ib) = 1$.
- $c^2 = a^2 + b^2 = (a + ib)(a - ib)$, with $\gcd(a + ib, a - ib) = 1$. By unique factorization, $a + ib = \varepsilon(u + iv)^2$, with ε unit.
- Also true that $a - ib$ is a square, up to a unit.
- $-1 = i^2$ can be absorbed, so can take $\varepsilon \in \{1, i\}$.
- $\varepsilon = 1$ gives $a + ib = u^2 - v^2 + 2uvi$, $\varepsilon = i$ gives $a + ib = i(u^2 - v^2) + 2uv$.
- Convention: a odd, so take first case.
- Easy check: $u > v$, different parity, relatively prime.

Let us study a similar Diophantine equation.

Theorem

The integer solutions to

$$a^2 + b^2 = c^3$$

with $\gcd(a, b) = 1$ *are parametrized by*

$$a = m^3 - 3mn^2, \qquad b = 3m^2 n - n^3, \qquad c = m^2 + n^2$$

with $\gcd(m, n) = 1$, m, n *different parity.*

Proof.

Sketch of proof

- $c^3 = a^2 + b^2 = (a + ib)(a - ib)$
- $a + ib$ is a perfect cube, so

$$a+ib = (m+in)^3 = m^3+3m^2ni-3mn^2-in^3 = m^3-3mn^2+(3m^2n-n^3)i$$

□

- Yet another Diophantine (Rosen 14.3.8):

$$y^3 = x^2 + 1 = (x + i)(x - i)$$

- $x + i, x - i$ relatively prime
-
$$x + i = (r + si)^3 = r^3 - 3rs^2 + i(3r^2 s - s^3)$$
- $x = r(r^2 - 3s^2)$, $1 = s(3r^2 - s^2)$
- So $s = 1$ or $s = -1$
- If $s = 1$ then $1 = 3r^2 - 1$, $3r^2 = 2$, impossible
- If $s = -1$ then $1 = -3r^2 + 1$, $3r^2 = 0$, $r = 0$, $x = 0$, $y = 1$

Definition

$\alpha, \beta, \gamma \in \mathbb{Z}[i]$, $\gamma \neq 0$.

$$\alpha \equiv \beta \mod \gamma$$

if and only if

$$\gamma | (\alpha - \beta)$$

Example

$$(3+4i)(3-4i) = 25$$

so $(3+4i)|25$, and

$$7+2i \equiv 32+2i \mod 3+4i$$

Lemma

- *For fixed* γ*, equivalence relation on* $\mathbb{Z}[i]$
- *Congruence, i.e. if* $\alpha_1 \equiv \alpha_2 \mod \gamma$*,* $\beta_1 \equiv \beta_2 \mod \gamma$*, then* $\alpha_1 + \beta_1 \equiv \alpha_2 + \beta_2 \mod \gamma$*, and* $\alpha_1 \beta_1 \equiv \alpha_2 \beta_2 \mod \gamma$*.*

Example

$$2 + 5i \equiv i \mod 1 + 2i$$

so

$$(2 + 5i)^{16} \equiv i^{16} \equiv 1 \mod 1 + 2i$$

Lemma

If $a, b, n \in \mathbb{Z}$ then $a|b$ in $\mathbb{Z}[i]$ iff $a|b$ in $\mathbb{Z}$.
Similarly, $a \equiv b \mod n$ in $\mathbb{Z}[i]$ iff $a \equiv b \mod n$ in $\mathbb{Z}$.

Definition

$\frac{\mathbb{Z}[i]}{(\gamma)}$ is the set of congruence classes $[\alpha]$ mod γ, made into a ring by the well-defined operations

$$[\alpha] + [\beta] = [\alpha + \beta]$$
$$[\alpha][\beta] = [\alpha\beta]$$

Lemma

- $\frac{\mathbb{Z}[i]}{(\gamma)}$ *is a field if and only if* γ *is a Gaussian prime*
- $\frac{\mathbb{Z}[i]}{(\gamma)}$ *is finite*

Example

$\gamma = (1+i)(2+3i) = -1+5i$ is composite, so $\mathbb{Z}[i]/(\gamma)$ has zero-divisors, and is not a field. That does not mean that all elements are non-invertible:

$$\gcd(5\sqrt{-1}-1, 2\sqrt{-1}+3) = -1$$

and

$$1 = (-\sqrt{-1}-2)(5\sqrt{-1}-1) + (3\sqrt{-1})(2\sqrt{-1}+3)$$

so

$$(2\sqrt{-1}+3)(3\sqrt{-1}) \equiv 1 \mod 5\sqrt{-1}-1$$

CRT

Theorem

If $u, v, \alpha, \beta \in \mathbb{Z}[i]$, *with* α, β *relatively prime, then the system of congruences*

$$\begin{aligned} x &\equiv u \mod \alpha \\ x &\equiv v \mod \beta \end{aligned}$$

is solvable, and soln unique mod $\alpha\beta$.

Example

$$
\begin{aligned}
x &\equiv 7\sqrt{-1}+5 \mod 17\sqrt{-1}+13 \\
x &\equiv 13\sqrt{-1}+11 \mod 23\sqrt{-1}+19
\end{aligned}
$$

has solution $x = 126\sqrt{-1} + 624$.

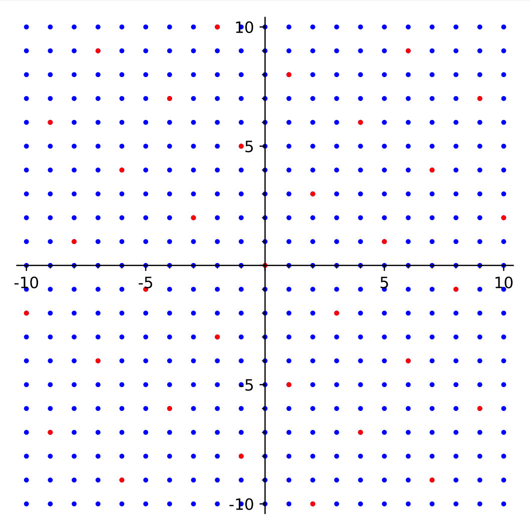
Theorem

Let $\alpha \in \mathbb{Z}[i] \setminus \{0\}$

1. *The congruence class* $[0]$ *forms a lattice in* $\mathbb{Z}[i]$, *the class* $[\beta]$ *is the translate* $\beta + [0]$
2. *Let* $H = \{ s\alpha + ti\alpha | 0 \le s, t \le 1 \} \cap \mathbb{Z}[i]$. *Then* H *constitute a complete set of residues for* $\mathbb{Z}[i]$ *mod* α. *Removing lattice points on the edges* $s = 1$ *and* $t = 1$ *that are congruent mod* α *to other lattice points in* H *we get a reduced set of residues*
3. $\mathbb{Z}[i]/(\alpha)$ *has* $N(\alpha)$ *elements*

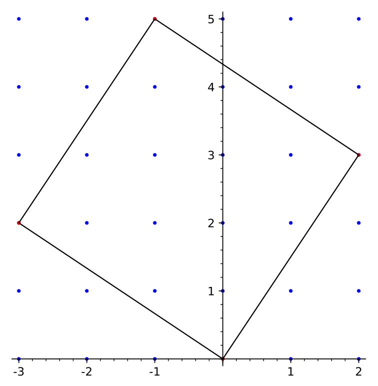
Example

$\alpha = 2 + 3i$, multiples of α in red:



Example

We zoom in on the fundamental region:



$N(2+3i) = 4+9 = 13$ and there are 12 interior lattice points, none on the edges, the 4 vertices all congruent, we pick 0.

Theorem

If $\pi, \alpha \in \mathbb{Z}[i]$, with π a Gaussian prime, $\alpha \neq 0$, then

$$\alpha^{N(\pi)-1} \equiv 1 \mod \pi$$

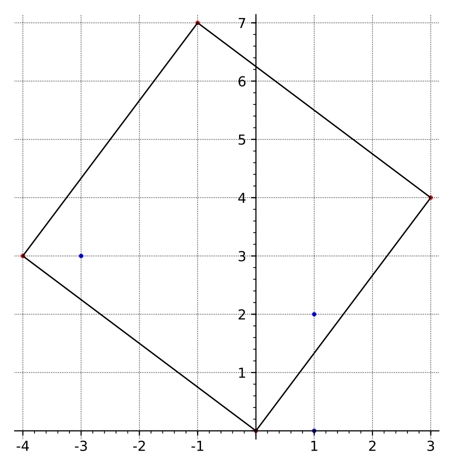
Proof.

Similar to the proof for the integers: choose a complete, reduced set of residues for $\mathbb{Z}[i]$ modulo π, multiply the non-zero classes together. Also scale this set by α and then multiply together. Equate, and pull out the factor $\alpha^{N(\pi)-1}$. □

Example

Take $\alpha = 1 + 2i$, $\pi = 3 + 4i$. Then $N(\pi) = 25$, and $\gcd(\alpha, \pi) = 1$, so

$$(1 + 2i)^{24} \equiv 1 \equiv 1 + i(3 + 4i) \equiv -3 + 3i \mod 3 + 4i$$



Definition

For $\alpha \in \mathbb{Z}[i] \setminus \{0\}$, $\phi_{\mathbb{Z}[i]}(\alpha) = \left| \left(\frac{\mathbb{Z}[i]}{(\alpha)} \right)^{\times} \right|$

Lemma

$\phi_{\mathbb{Z}[i]}(\cdot)$ *is multiplicative; it's value on powers of Gaussian primes is*

$$\phi_{\mathbb{Z}[i]}(\pi^k) = N(\pi)^{k-1} (N(\pi) - 1)$$

Theorem

For $\alpha, \beta \in \mathbb{Z}[i] \setminus \{0\}$*, with* $\gcd(\alpha, \beta) = 1$,

$$\beta^{\phi_{\mathbb{Z}[i]}(\alpha)} \equiv 1 \mod \alpha$$

Example

$\phi(5) = 4$, but

$\phi_{\mathbb{Z}[i]}(5) = \phi_{\mathbb{Z}[i]}((1+2i)(1-2i)) = (N(1+2i)-1)(N(1-2i)-1) = 16.$

Hence

$$(2+3i)^{16} \equiv 1 \mod 5,$$

so

$$(2+3i)^{33} \equiv 2+3i \mod 5,$$