Math 3527 (Number Theory 1)

Lecture #27

Modular Arithmetic in $\mathbb{Z}[i]$:

- Visualizing Residue Classes in $\mathbb{Z}[i]$ Modulo α
- Counting Residue Classes in $\mathbb{Z}[i]$ Modulo α

This material represents §4.4.1 from the course notes.

Residue Classes, I

The goal of this lecture is to study the residue classes in $\mathbb{Z}[i]$ modulo α: more specifically, we want to know how many residue classes there are and how to write them all down.

- As we showed previously, the collection of possible remainders r with $N(r) \leq \frac{1}{2}N(\beta)$ do give all the residue classes.
- However, the quotient and remainder arising in the division algorithm are not guaranteed to be unique: there can be more than one possible r such that $\alpha \equiv r \pmod{\beta}$ and $N(r) < \frac{1}{2}N(\beta)$.

It turns out that it is much easier to understand the modular arithmetic in $\mathbb{Z}[i]$ from a geometric point of view.

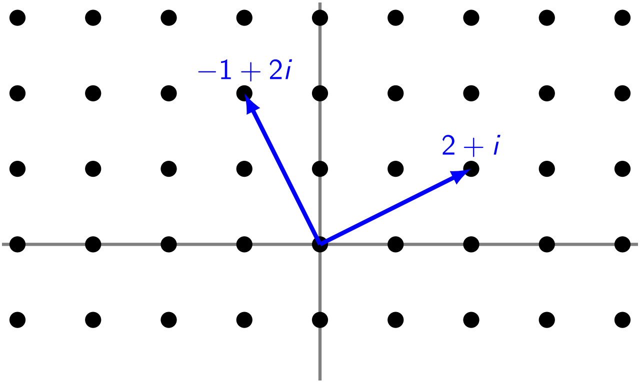
Residue Classes, II

It turns out that it is much easier to understand the modular arithmetic in $\mathbb{Z}[i]$ from a geometric point of view.

In the complex plane, the Gaussian integers form the set of lattice points, the points whose coordinates are both integers. We can also view Gaussian integers as vectors in this lattice, since the additive structure of $\mathbb{Z}[i]$ agrees with the additive structure of vectors in the plane.

Residue Classes, III

Here is a plot of the Gaussian integers as a lattice, and the two vectors $\beta = 2 + i$ and $i\beta = -1 + 2i$:



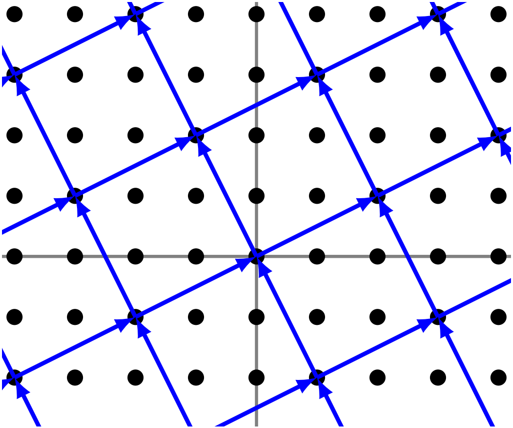
Residue Classes, IV

Now consider the multiples of a given Gaussian integer β: every multiple is of the form $(x + iy)\beta = x\beta + y(i\beta)$, so it is an integer linear combination of β and $i\beta$.

Thus, drawing all of the $\mathbb{Z}[i]$-multiples of β is the same as drawing all of the vectors that can be obtained by an integer number of "steps" each in the direction of β or $i\beta$, which produces a square tiling of the plane.

Residue Classes, V

Here are the $\mathbb{Z}[i]$-multiples of $\beta = 2 + i$ with marked vectors $\beta = 2 + i$ and $i\beta = -1 + 2i$.



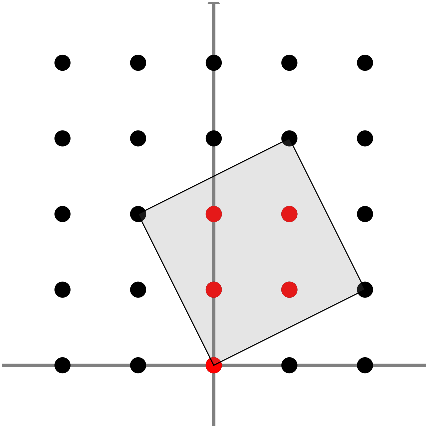
Residue Classes, VI

Using this geometric interpretation, we can give a method for finding residue class representatives:

- Geometrically, two Gaussian integers will be congruent modulo β if and only if they are located in the same position within two different squares.
- Thus, if we take the collection of lattice points inside any one of these squares, it will yield a fundamental region for the Gaussian integers modulo β.
- The elements in the fundamental region will be unique representatives for the residue classes modulo β.

Residue Classes, VII

Example: Here is a fundamental region for $\mathbb{Z}[i]$ modulo $\beta = 2 + i$ and a marked set of representatives 0, i, $2i$, $1 + i$, $1 + 2i$:



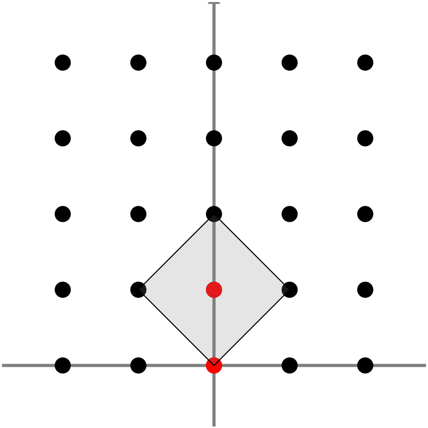
Residue Classes, VIII

As shown in the figures, there is a fundamental region for $\mathbb{Z}[i]$ modulo $2+i$ containing the 5 points 0, i, $2i$, $1+i$, and $1+2i$.

- Hence, every element of $\mathbb{Z}[i]$ is congruent modulo $2+i$ to 0, i, $2i$, $1+i$, or $1+2i$.
- We conclude that there are 5 residue classes modulo $2+i$. (Recall that we showed this earlier using a different approach.)

Residue Classes, IX

Example: Here is a fundamental region for $\mathbb{Z}[i]$ modulo $\beta = 1 + i$ and a marked set of representatives 0, i:



Number of Residue Classes, I

In the examples above, we showed that there were 5 residue classes modulo $2+i$ and 2 residue classes modulo $1+i$. Notice that $N(2+i)=5$ and that $N(1+i)=2$.

In general, it turns out that there are exactly $N(\beta)$ residue classes modulo β for any nonzero β. We will prove this fact using (of all things) a theorem from elementary geometry!

Number of Residue Classes, I

In the examples above, we showed that there were 5 residue classes modulo $2+i$ and 2 residue classes modulo $1+i$. Notice that $N(2+i)=5$ and that $N(1+i)=2$.

In general, it turns out that there are exactly $N(\beta)$ residue classes modulo β for any nonzero β. We will prove this fact using (of all things) a theorem from elementary geometry!

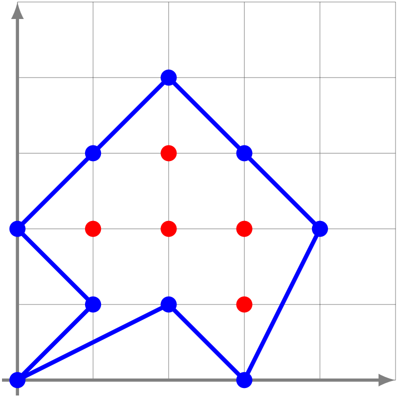
Theorem (Pick's Theorem)

If R is a polygon in the plane whose vertices are all lattice points, then the area of R is given by the formula $A = I + \frac{1}{2}B - 1$, where I is the number of lattice points in the interior of R and B is the number of lattice points on the boundary of R.

A <u>boundary point</u> is a point on one of the sides of R, while an <u>interior point</u> is a point not on one of the sides of R.

Number of Residue Classes, II

Pick's Theorem is easiest to see with an example: this polygon has 9 boundary points and 5 interior points, and by drawing triangles around it, one can verify its area is $\frac{17}{2} = 5 + \frac{9}{2} - 1$:



Number of Residue Classes, III

We can use Pick's theorem to give an easy computation of the number of residue classes in $\mathbb{Z}[i]$ modulo β:

Theorem (Number of Residue Classes in $\mathbb{Z}[i]$ Mod β)

If β is a nonzero Gaussian integer, the number of distinct residue classes in $\mathbb{Z}[i]$ modulo β is equal to $N(\beta)$.

Number of Residue Classes, III

We can use Pick's theorem to give an easy computation of the number of residue classes in $\mathbb{Z}[i]$ modulo β:

Theorem (Number of Residue Classes in $\mathbb{Z}[i]$ Mod β)

If β is a nonzero Gaussian integer, the number of distinct residue classes in $\mathbb{Z}[i]$ modulo β is equal to $N(\beta)$.

Examples:

- The number of residue classes in $\mathbb{Z}[i]$ modulo $3+4i$ is $N(3+4i)=25$.
- The number of residue classes in $\mathbb{Z}[i]$ modulo $7-7i$ is $N(7-7i)=98$.
- The number of residue classes in $\mathbb{Z}[i]$ modulo $42+16i$ is $N(42+16i)=2020$.

Number of Residue Classes, IV

Proof:

- Consider a fundamental region for $\mathbb{Z}[i]$ modulo β.
- By our geometric arguments above, every Gaussian integer has a unique representative modulo β that lies in the square whose vertices are 0, β, $i\beta$, and $\beta + i\beta$ in the complex plane.
- Each interior point of this square yields one residue class.
- The boundary points of the square come in pairs (on opposite edges) each yielding one residue class, except for the four vertices ($0, \beta, i\beta, \beta + i\beta$) which are all equivalent.
- So there are $I + \dfrac{B-4}{2} + 1 = I + \dfrac{1}{2}B - 1$ total residue classes.
- But by Pick's Theorem, this is precisely the area of the fundamental region. Since this region is a square with side length $|\beta|$, the area is simply $|\beta|^2 = N(\beta)$.

Number of Residue Classes, V

To list all of the residue classes modulo $\beta \in \mathbb{Z}[i]$, we need only give a list of $N(\beta)$ inequivalent residue classes, which must therefore be exhaustive. (To generate this list, we can draw a fundamental region for $\mathbb{Z}[i]$ modulo β.)

Number of Residue Classes, V

To list all of the residue classes modulo $\beta \in \mathbb{Z}[i]$, we need only give a list of $N(\beta)$ inequivalent residue classes, which must therefore be exhaustive. (To generate this list, we can draw a fundamental region for $\mathbb{Z}[i]$ modulo β.)

Example: Find representatives for the residue classes modulo $2 + 2i$ in $\mathbb{Z}[i]$.

- We have $N(2 + 2i) = 8$ so there are 8 residue classes.
- It is then not hard to verify that the 8 values 0, 1, 2, 3, i, $1 + i$, $2 + i$, and $3 + i$ are all pairwise distinct modulo $2 + 2i$. Thus, these are representatives of all of the residue classes.

Summary

We described a way to visualize and enumerate the residue classes in $\mathbb{Z}[i]$ modulo α geometrically as the distinct points in a fundamental region in the complex plane.

We then proved that there are exactly $N(\alpha)$ different residue classes modulo α.

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