Problem Set 9

Due: April 24th, 5pm

1 Demonstrations

For problems in this section, you still need to give complete mathematical reasoning to support your answers. I should be able to follow and understand your work, but it doesn't have to be organized into a formal proof.

1. (3 points) In this problem we show that a prime can be written in the form $x^2 + 3y^2$ if $p \equiv 1 \pmod 3$. Assume that $p \equiv 1 \pmod 3$.
   (a) Show that there exists x, r such that $x^2 + 3 = r \cdot p$.
   (b) Let L be the lattice with basis matrix $\begin{pmatrix} p & x \\ 0 & 1 \end{pmatrix}$. Show that there exists non zero $(a, b) \in L$ such that $a^2 + 3b^2 < 2.3p$. (*Hint:* Modify the argument given in by using the convex body given by $\{(a, b) \colon a^2 + 3b^2 \leq 2.3p\}$.)
   (c) Show that $a^2 + 3b^2 = p$. (*Hint:* Show that for (a, b) in the previous part $a^2 + 3b^2$ is either p or $2p$. Rule out the latter case by considering the equation modulo 3.)

2 Formal proofs

For each problem in this section, you must give a complete and rigorous proof. Your arguments should be clear, logically ordered, and written in full sentences.

In particular, state all assumptions explicitly and define all notation. Justify every nontrivial step.

2. (1 point) Let $b = 1 + 2i \in \mathbb{Z}[i]$.
   (a) Draw the lattice $\Lambda = \{qb : q \in \mathbb{Z}[i]\}$ in the complex plane.
   (b) If $a = 5 + 3i$, find the closest lattices point to a in Λ, and verify that the distance from a to this lattice point is less than $\sqrt{N(b)}$.
3. (2 points) Give a geometric argument to prove the division algorithm in $\mathbb{Z}[i]$. That is, for any $a, b \in \mathbb{Z}[i]$ with $b \neq 0$, there exist $q, r \in \mathbb{Z}[i]$ such that $a = qb + r$ and $N(r) < N(b)$, where $N(a + bi) = a^2 + b^2$ is the norm function on $\mathbb{Z}[i]$. (*Hint:* Adapt the computation

of the previous problem to find a lattice point qb that is close to a, use this to find r and make a geometric argument to show that $N(r) < N(b)$.)

3 Explorations

In this section, I'm looking for answers that are supported by evidence, but you don't have to prove your answers. Please **include all code snippets** when using computational tools, failure to do so may result in loss of points.

4. (1 point) Consider $\mathbb{Z}[\sqrt{-d}] \subseteq \mathbb{C}$ for some positive integer d, when $d = 1$ we get the Gaussian integers. Does the argument given for the division algorithm in $\mathbb{Z}[i]$ also work for $\mathbb{Z}[\sqrt{-d}]$ for any other d?

5. (2 points) Which primes $p \leq 50$ can be written as $x^2 + 5y^2$ for some integers x, y? What about $x^2 + 7y^2$? For each case, make a conjecture about which primes can be written in the given form.