5.1 Side and diagonal numbers

Exercise 5.1. If $n \in \mathbb{N}$ is a square, show the only solutions of $x^2 - ny^2 = 1$ are $(\pm 1, 0)$. (Cf. Exercises 5.1.3, 5.1.4.)

5.2 The equation $x^2 - 2y^2 = 1$

Exercise 5.2. Check the following composition rule holds:

$$(x_1^2 - 2y_1^2)(x_2^2 - 2y_2^2) = x_3^2 - 2y_3^2$$

where

$$x_3 = x_1x_2 + 2y_1y_2, \quad y_3 = x_1y_2 + y_1x_2.$$  

Exercise 5.3. Compute $(3, 2)^4$. Use this to obtain a decimal approximation for $\sqrt{2}$. To how many digits is it accurate? (Use a calculator/computer.)

5.4 The general Pell equation and $\mathbb{Z}[\sqrt{n}]$

For everyone’s benefit, we’ll skip Exercise 5.4 from my notes.

Exercise 5.5. Find the fundamental solution $(x_0, y_0)$ to $x^2 - 5y^2 = 1$. What is the fundamental +unit of $\mathbb{Z}[\sqrt{5}]$? Compute the solutions given by the square and the cube of $(x_0, y_0)$. What rational number decimal approximations to $\sqrt{5}$ do they yield? To how many digits are they accurate? (Use a calculator.)

Exercise 5.6. Exercises 5.4.4, 5.4.5.

5.5 *Quadratic forms

Exercise 5.7. Let $Q(x, y) = x^2 + xy - y^2$. Fact (don’t prove it): the solutions to $Q(x, y) = 1$ are given by $(F_{2n+1}, F_{2n+2})$ where $F_n$ is the n-th Fibonacci number (cf. Exercise 5.8.4; $F_1 = F_2 = 1$). On the other hand, the solutions are generated by the powers of the fundamental +unit of $\mathbb{Z}[\frac{1+\sqrt{5}}{2}]$, $\epsilon = 1 + \frac{1+\sqrt{5}}{2} = \frac{3+\sqrt{5}}{2}$.  

Check that $$(\frac{3+\sqrt{5}}{2})^n = F_{2n-1} + F_{2n} \frac{1+\sqrt{5}}{2}$$ holds for $n = 1, 2, 3$.

6.1 The Gaussian integers

Exercise 6.1. Exercises 6.1.1, 6.1.2 (be precise), 6.1.3.
6.2 Divisibility and primes in $\mathbb{Z}[i]$ and $\mathbb{Z}$

**Definition 6.4.** Let $\alpha, \beta \in \mathbb{Z}[i]$. We say $\alpha$ divides $\beta$, or $\beta|\alpha$, if

$$\beta = \alpha \gamma$$

for some $\gamma \in \mathbb{Z}[i]$. We say $\alpha$ is a Gaussian prime, or prime in $\mathbb{Z}[i]$, if the only divisors of $\alpha$ are $\pm 1, \pm i, \pm \alpha$, and $\pm i\alpha$, i.e., if the only divisors of $\alpha$, up to units, are $1$ and $\alpha$.

**Exercise 6.2.** Let $\alpha \in \mathbb{Z}[i]$. Show $\alpha$ is a unit of $\mathbb{Z}[i]$ if and only if $\alpha$ is invertible in $\mathbb{Z}[i]$, i.e., $\alpha \beta = 1$ for some $\beta \in \mathbb{Z}[i]$. (Hint: use the multiplicative property of the norm.) In fact, this is the general definition of a unit in a ring: something is a unit means it’s invertible (in the ring). The units always form a multiplicative group. The units of $\mathbb{Z}$ are just $\pm 1$. The role of $\{1, -1, i, -i\}$ in $\mathbb{Z}[i]$ is exactly analogous to the role of $\pm 1$ in $\mathbb{Z}$.

The text defines $\alpha$ to be a Gaussian prime to be an element of $\mathbb{Z}[i]$ such that $\alpha$ is not a product of two elements of smaller norm. The following exercise shows our definition and the book’s are equivalent.

**Exercise 6.3.** Using the definition of Gaussian prime we gave in class, show the following is true: $\alpha$ is a Gaussian prime if and only if $\beta|\alpha$ implies $N(\beta) = 1$ or $N(\beta) = N(\alpha)$. (Cf. Exercise 6.2.1. Hint: look at the example from class.) Conclude that if $N(\alpha)$ is prime in $\mathbb{Z}$, $\alpha$ is a Gaussian prime.

**Exercise 6.4.** Show there are no elements in $\mathbb{Z}[i]$ whose norm is of the form $4n + 3$. Conclude that if $p = 4n + 3$ is prime in $\mathbb{Z}$, then $p$ is also a Gaussian prime. (Cf. Section 6.3)