6.5 Fermat’s two square theorem

Finish the proof of the determination of which integers are sums of two squares (Theorem 6.21) with the exercise below.

Exercise 6.12. Suppose \( n = \prod p_i^{2e_i} \prod q_j^{f_j} \) where each \( p_i, q_j \) are primes of \( \mathbb{N} \) such that each \( p_i \equiv 3 \mod 4 \) and \( q_j \equiv 1, 2 \mod 4 \). (i) Show each \( p_i^{2e_i} \) and \( q_j^{f_j} \) is the norm of an element in \( \mathbb{Z}[i] \). (ii) Deduce \( n = x^2 + y^2 \) for some \( x, y \in \mathbb{Z} \).

Exercise 6.13. Find an \( n \) such that \( n = x^2 + y^2 \) in at least two distinct ways (with \( x, y > 0 \) and \( x \geq y \)). Write down all solutions (with \( x, y > 0, x \geq y \)). Using this, show there are two elements \( \alpha, \beta \in \mathbb{Z}[i] \) such that \( N(\alpha) = N(\beta) \) but \( \alpha \) and \( \beta \) do not differ by units.

6.6 Pythagorean triples

Exercise 6.14. Give an example of relatively prime \( \alpha, \beta \) in \( \mathbb{Z}[i] \) such that \( \alpha \beta \) is a square in \( \mathbb{Z}[i] \), but \( \alpha \) and \( \beta \) are not squares in \( \mathbb{Z}[i] \).

6.7 *Primes of the form \( 4n + 1 \)

Exercise 6.15. Let \( f(x) \) be any nonconstant polynomial over \( \mathbb{Z} \). Show there are infinitely many primes dividing the values of \( f(x) \). (Cf. Exercises 6.7.1—6.7.4.)

Exercise 6.16. Show that there are infinitely many primes of the form \( 4n + 3 \) (Cf. Exercises 6.3.4—6.3.6. Note that this argument is similar to the \( 4n + 1 \) case with the polynomial \( f(x) = 2x^2 + 1 \). If you like, you may try to use this idea and apply the previous exercise.)