Problem Set #11

Exercise 1: (∗) 12 points

Questions are linked one to the others, lot of the times so always remember what you have proven.

1. Prove that the norm is multiplicative.
2. If \( \beta | \alpha \) in \( \mathbb{Z}[i] \) then \( N(\beta) | N(\alpha) \) in \( \mathbb{Z} \).
3. Prove that the unit of \( \mathbb{Z}[i] \) are precisely the elements of norm 1 and then \( \pm 1, \pm i \).
4. Let \( \alpha \in \mathbb{Z}[i] \), \( \alpha \) is a Gaussian prime if and only if \( \beta | \alpha \) implies \( N(\beta) = 1 \) or \( N(\beta) = N(\alpha) \).
5. Let \( \alpha \in \mathbb{Z}[i] \), \( \alpha \). If \( N(\alpha) \) is prime then \( \alpha \) is a Gaussian prime.
6. Let \( \alpha \in \mathbb{Z}[i] \) be a non-zero, non-unit. Then \( \alpha \) factors into a finite product of Gaussian primes. (Do as we have done for \( \mathbb{Z}! \))
7. Let \( p \in \mathbb{N} \) be prime. Then \( p \) is also prime in \( \mathbb{Z}[i] \) if and only if \( p \) is not the sum of two squares.
8. Suppose \( p \in \mathbb{N} \) is prime in \( \mathbb{Z} \) but factors as \( p = \alpha \beta \), where \( \alpha, \beta \) are non-units in \( \mathbb{Z}[i] \). Show \( \beta = \bar{\alpha} \).
9. Suppose \( p \in \mathbb{N} \) is prime and \( p = a^2 + b^2 \). Then \( \alpha = a + ib \) and \( \bar{\alpha} = a - ib \) are prime in \( \mathbb{Z}[i] \).
10. Suppose \( \alpha = \mu \beta + \rho \) where \( N(\rho) < N(\beta) \). Then \( \rho = 0 \) iff \( \beta | \alpha \). (Same as in \( \mathbb{Z} \))
11. Suppose \( \alpha = \mu \beta + \rho \) wher \( N(\rho) < N(\beta) \). If \( \rho = 0, \beta \) is a gcd for \( \alpha \) and \( \beta \). If not, a gcd for \( \beta \) and \( \rho \) is also a gcd for \( \alpha \) and \( \beta \) (and vice versa). (Same as in \( \mathbb{Z} \))
12. Let \( \pi, \beta \in \mathbb{Z}[i] \) and \( u \) be a unit of \( \mathbb{Z}[i] \). Show that \( \pi | u \beta \) if and only if \( \pi | \beta \).
13. Let \( \pi \) be a prime in \( \mathbb{Z}[i] \). If \( \pi | \alpha \beta \) then \( \pi | \alpha \) or \( \pi | \beta \). (Same as in \( \mathbb{Z} \))
14. Suppose \( \pi \) and \( \pi' \) are primes of \( \mathbb{Z}[i] \). Show \( \pi | \pi' \) implies \( \pi = u \pi' \) where \( u \) is a unit of \( \mathbb{Z}[i] \).
15. Let \( \alpha \neq 0 \) be a non-unit in \( \mathbb{Z}[i] \). Suppose \( \alpha = \pi_1 \ldots \pi_m \) and \( \alpha = \pi'_1 \ldots \pi'_n \) are two factorizations of \( \alpha \) into Gaussian prime \( \pi_i \) and \( \pi'_j \). Then \( m = n \), and up to a reordering of \( \pi'_j \)'s, we have

\[
\pi_i = u_i \pi'_i
\]

(Same as in \( \mathbb{Z} \)) for each \( i \), where \( u_i \) is a unit in \( \mathbb{Z}[i] \).
16. The Gaussian primes, up to units, are precisely the following:

(a) prime \( p \in \mathbb{N} \) not of the form \( x^2 + y^2 \),
(b) \( \alpha = a + bi \) where \( N(\alpha) \) is prime in \( \mathbb{N} \).

(Use the Unicity of the factorization in prime element proved in the previous question.)

Exercise 2: (⋆⋆) 5 points
Show that for any \( c > 2 \) there are only finitely many pairs of integers \( a, b \) with

\[ |\sqrt{2} - \frac{a}{b}| < \frac{1}{b^c} \]

Exercise 3: (⋆) 3 points
Let \( p \) be prime and suppose \( u^2 \equiv -1 \mod p \), (so \( p \equiv 1 \mod 4 \)). Let \([a_0, ..., a_n]\) be the continued fraction expansion of \( \frac{u}{p} \), and let \( i \) be the largest integer with \( k_i \leq \sqrt{p} \). Show that \( |\frac{h_i}{k_i} - \frac{u}{p}| < \frac{1}{k_i \sqrt{p}} \) and \( |h_i p - k_i u| < \sqrt{p} \). Setting \( x = k_i \) and \( y = h_i p - u k_i \), show that \( p|x^2 + y^2| \) and \( x^2 + y^2 < 2p \), so \( x^2 + y^2 = p \).

\(^1\) (⋆) = easy, (⋆⋆) = medium, (⋆⋆⋆) = challenge