METU, Spring 2015, Math 366.

Exercise Set 6

1. Let α, β be non-zero Gaussian integers. Show that $N(\gcd(\alpha,\beta)) \mid \gcd(N(\alpha), N(\beta))$.

2. Use the arithmetic of the Gaussian integers to determine all solutions to the Diophantine equation $x^2 + y^2 = z^2$. (Hint: Show that $x + iy = u\alpha^2$ for some Gaussian integer $\alpha = m + ni$ and a unit u.)

3. Let $N = p_1 p_2 \cdots p_n$ where $p_1, p_2, \ldots, p_n$ are distinct primes of the form $4k+1$. In how many different ways can you represent N as a sum of two squares? Prove your formula by using the properties of Gaussian integers (Do not use the fact that $r_2(n)$ is a multiplicative function).

4. In how many different ways can you represent $3, 9, 27, 81, \ldots$ in the form $x^2 + 2y^2$. Do you see a pattern? Write a formula for the number of representations of 3^k in the form $x^2 + 2y^2$. Which facts do you need about the ring $\mathbb{Z}[\sqrt{-2}]$ in order to prove this formula.

5. Let a, b and c be integers such that $b^2 - 4ac = -4$ and let m be fixed positive integer. Show that the Diophantine equation $ax^2 + bxy + cy^2 = m$ has a solution if and only if the Diophantine equation $\tilde{x}^2 + \tilde{y}^2 = m$ has a solution. (Hint: A number of the form $k^2 + 1$ has no prime divisor congruent 3 modulo 4).

6. Let d be a squarefree integer and let $\alpha = \sqrt{d} + 1$ and $\beta = \sqrt{d} - 3$. Write $\alpha^3, \alpha\beta, \frac{\alpha+1}{\beta}$ and $\frac{\beta}{\alpha-2}$ in the form $r + s\sqrt{d}$ for some rational numbers r and s.

7. Let d_1 and d_2 be two distinct squarefree integers. Show that $\mathbb{Q}(\sqrt{d_1}) \neq \mathbb{Q}(\sqrt{d_2})$.

8. Prove the following facts about the conjugation in $\mathbb{Q}(\sqrt{d})$.
   - $(\alpha+\beta)' = \alpha' + \beta'$, $(\alpha\beta)' = \alpha'\beta'$, $(\alpha/\beta)' = \alpha'/\beta'$,
   - $\alpha = \alpha'$ if and only if α is rational.

9. Prove the following facts about the trace and norm maps on $\mathbb{Q}(\sqrt{d})$.
   - $Tr(\alpha+\beta) = Tr(\alpha) + Tr(\beta)$,
   - $N(\alpha\beta) = N(\alpha)N(\beta)$,
   - $N(\alpha) = 0$ if and only if $\alpha = 0$,
   - α is a root of the polynomial equation $x^2 - Tr(\alpha) + N(\alpha) = 0$.

10. Let α be a root of an irreducible polynomial $f(x) \in \mathbb{Q}[x]$ of degree three. Consider
$$\mathbb{Q}(\alpha) = \{a + b\alpha + c\alpha^2 : a, b, c \in \mathbb{Q}\}.$$
Show that $\mathbb{Q}(\alpha)$ is a field. You may start with showing that α^3 is an element of $\mathbb{Q}(\alpha)$. What about $\frac{1}{\alpha-1}$?