Set 3.

Please study the following Problems 21-30 by February 1 (Friday).

This time, we consider problems related to decompositions of prime numbers in the integer ring of a quadratic fields.

A maximal ideal of O_K for a number field K is nothing but a non-zero prime ideal of O_K. In number theory, people usually call a maximal of O_K just a prime ideal, not putting non-zero. I will follow them.

21. Using the uniqueness of the prime factorization in $\mathbb{Z}[i]$, prove that if

$$\tan(\alpha) = 1, \quad \tan(\beta) = 3/2, \quad \tan(\gamma) = 2,$$

then α, β, γ are linearly independent over $\mathbb{Q}$.

22. Let p be a prime number and assume $p \neq 2, 3$. Using $\left(\frac{3}{p}\right) = \left(\frac{p}{3}\right) \cdot (-1)^{\frac{p-1}{2}}$ (a special case of the quadratic reciprocity law), prove the following. If $p \equiv 1, 11 \bmod 12$, (p) in $\mathbb{Z}\sqrt{3}]$ decomposes into the product of two different prime ideals. If $p \equiv 5, 7 \bmod 12$, p is a prime element in $\mathbb{Z}[\sqrt{3}]$.

23. By using the fact $\mathbb{Z}[\sqrt{3}]$ is a PID, prove that for a prime number $p \neq 2, 3$, $p = \pm(x^2 - 3y^2)$ for some $x, y \in \mathbb{Z}$ if $p \equiv 1, 11 \bmod 12$, and that p can not be expressed in that way if $p \equiv 5, 7 \bmod 12$.

24. Let p be a prime number and assume $p \neq 2$. Computing $\left(\frac{-2}{p}\right)$ and using the fact $\mathbb{Z}[\sqrt{-2}]$ is a PID, prove that $p = x^2 + 2y^2$ for some $x, y \in \mathbb{Z}$ if $p \equiv 1, 3 \bmod 8$, and that p can not be expressed in that way if $p \equiv 5, 7 \bmod 8$.

25. Let p be a prime number and assume $p \neq 2$. Computing $\left(\frac{2}{p}\right)$ and using the fact $\mathbb{Z}[\sqrt{2}]$ is a PID, prove that $p = x^2 - 2y^2$ for some $x, y \in \mathbb{Z}$ if $p \equiv 1, 7 \bmod 8$, and that p can not be expressed in that way if $p \equiv 3, 5 \bmod 8$. (You may think that $p = \pm(x^2 - 2y^2)$ appears. That is correct, but improve it to $p = x^2 - 2y^2$ by multiplying $x + y\sqrt{2}$ by the unit $1 + \sqrt{2}$ if necessary.)

26. (Problems 26 and 27 arise from the fact that the part [improve it ....] in Problem 25 does not work for $\mathbb{Z}[\sqrt{3}]$. It is because $(2 + \sqrt{3})(2 - \sqrt{3}) = 1$ whereas $(1 + \sqrt{2})(1 - \sqrt{2}) = -1$.) Let p be a prime number, and assume $p \neq 2, 3$. Prove that if $p = x^2 - 3y^2$ $(x, y \in \mathbb{Z})$, then $p \equiv 1 \bmod 12$. Prove that if $p = -(x^2 - 3y^2)$ $(x, y \in \mathbb{Z})$, then $p \equiv 11 \bmod 12$.

27. By using 22 and 26, prove that for a prime number $p \neq 2, 3$, $p = x^2 - 3y^2$ for some $x, y \in \mathbb{Z}$ if and only if $p \equiv 1 \bmod 12$.

28. Let p be a prime number and assume $p \neq 2, 5$. The quadratic reciprocity law tells that $\left(\frac{-5}{p}\right)$ is 1 if $p \equiv 1, 3, 7, 9 \bmod 20$ and is -1 if $p \equiv 11, 13, 17, 19 \bmod 20$. One thing which did not appear in Problems 21–27 is that the integer ring $\mathbb{Z}[\sqrt{-5}]$ of $\mathbb{Q}(\sqrt{-5})$ is not a PID. In Problem 28, assume $p \equiv 1, 3, 7, 9 \bmod 20$ and write $(p) = \mathfrak{p}\bar{\mathfrak{p}}$ for a prime ideal $\mathfrak{p}$ of $\mathbb{Z}[\sqrt{-5}]$. Here $\bar{\mathfrak{p}}$ is the complex conjugate of $\mathfrak{p}$. In

this Problem 28, assume further that $\mathfrak{p}$ is a principal ideal. Prove that $p = \alpha\bar{\alpha}$ for some $\alpha \in \mathbb{Z}[\sqrt{-5}]$. Prove that $p \equiv 1, 9 \bmod 20$.

29. As in Problem 28, assume $p \equiv 1, 3, 7, 9 \bmod 20$ and write $(p) = \mathfrak{p}\bar{\mathfrak{p}}$, and assume this time that $\mathfrak{p}$ is not a principal ideal. Let $\mathfrak{a} = (2, 1+\sqrt{-5})$ which is not a principal ideal. Note that by the fact the class number of $\mathbb{Q}(\sqrt{-5})$ is 2, we see that $\mathfrak{a}\mathfrak{p}$ is a principal ideal. By using the fact $(2) = \mathfrak{a}\bar{\mathfrak{a}}$ $(= \mathfrak{a}^2)$, prove that $2p = \alpha\bar{\alpha}$ for some $\alpha \in \mathbb{Z}[\sqrt{-5}]$. Prove that $p \equiv 3, 7 \bmod 20$.

30. By using Problems 28 and 29, prove that for a prime number $p \neq 2, 5$, $p = x^2 + 5y^2$ for some $x, y \in \mathbb{Z}$ if and only if $p \equiv 1, 9 \bmod 20$.