Set 2.

Please study the following Problems 11–20 by January 25 (Friday).

This time, we consider integer solutions of algebraic equations by thinking about the friends ($\mathbb{Z}[\sqrt{2}]$, $\mathbb{Z}[\sqrt{-2}]$, $\cdots$) of $\mathbb{Z}$.

In Problems 11-16, we consider integer solutions of algebraic equations like $x^3 = y^2 + 2$. Let m be an even integer such that $m < 0$ and such that m is not divisible by r^2 for any integer $r > 1$. It is known that the integer ring of $\mathbb{Q}(\sqrt{m})$ is $\mathbb{Z}[\sqrt{m}]$.

11. Prove that if p is a prime number which divides m, then $(p, \sqrt{m})$ is a maximal ideal of $\mathbb{Z}[\sqrt{m}]$. (Hint for the proof. Recall that for an ideal I of a commutative ring R, I is a maximal ideal if and only if R/I is a field. By using $\mathbb{Z}[\sqrt{m}] \cong \mathbb{Z}[T]/(T^2 - m)$, where T corresponds to $\sqrt{m}$ in this isomorphism, prove that $\mathbb{Z}[\sqrt{m}]/(p, \sqrt{m})$ is isomorphic to the field $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$.)

In Problems 12-13, let a be an integer and assume that any prime divisor of a is a prime divisor of m. We consider integer solutions of $x^3 = y^2 - a^2 m$ by using the method explained in the course.

12. Assume $x, y \in \mathbb{Z}$, $x^3 = y^2 - a^2 m$. Prove that $(y + a\sqrt{m}) = I^3$ for some non-zero ideal I of $\mathbb{Z}[\sqrt{m}]$.

13. Assume $x, y \in \mathbb{Z}$, $x^3 = y^2 - a^2 m$ and assume that the class number of $\mathbb{Q}(\sqrt{m})$ is not divisible by 3. Prove that $y + a\sqrt{m} = \alpha^3$ for some $\alpha \in \mathbb{Z}[\sqrt{m}]$. (You can use the fact $\mathbb{Z}[\sqrt{m}]^\times = \{\pm 1\}$.)

14. By using the fact the class number of $\mathbb{Q}(\sqrt{-2})$ is 1, prove that all integer solutions of $x^3 = y^2 + 2$ are given by $(x, y) = (3, \pm 5)$.

(Remark. Fermat gave all integer solutions of $x^3 = y^2 + 2$, and also all integer solutions of $x^3 = y^2 + 4$ explained in the course.)

15. By using the fact the class number of $\mathbb{Q}(\sqrt{-6})$ is 2, prove that all integer solutions of $x^3 = y^2 + 54$ are given by $(x, y) = (7, \pm 17)$.

16. By using the fact the class number of $\mathbb{Q}(\sqrt{-14})$ is 4, prove that all integer solutions of $x^3 = y^2 + 56$ are given by $(x, y) = (18, \pm 76)$.

In Problems 17-20, we consider integer solutions of algebraic equations like $x^2 - 2y^2 = \pm 1$.

17. Prove that there is a bijection between the two sets $\mathbb{Z}[\sqrt{2}]^\times$ and $\{(x, y) \in \mathbb{Z} \times \mathbb{Z} \mid x^2 - 2y^2 = \pm 1\}$ given by $x + y\sqrt{2} \leftrightarrow (x, y)$ $(x, y \in \mathbb{Z})$.

18. For $x + y\sqrt{2} \in \mathbb{Z}[\sqrt{2}]^\times$ $(x, y \in \mathbb{Z})$, prove that $x + y\sqrt{2} > 1$ if and only if $x > 0$ and $y > 0$. Using the fact $(x, y) = (1, 1)$ is the smallest integer solution of $x^2 - y^2 = \pm 1$ such that $x > 0$ and $y > 0$, prove that $1 + \sqrt{2}$ is the smallest element of $\mathbb{Z}[\sqrt{2}]^\times$ which is > 1.

19. By using Problems 17 and 18, prove that $\mathbb{Z}[\sqrt{2}]^\times = \{\pm(1 + \sqrt{2})^n \mid n \in \mathbb{Z}\}$.

20. Prove that $\mathbb{Z}[\sqrt{3}]^\times = \{\pm(2 + \sqrt{3})^n \mid n \in \mathbb{Z}\}$.