Problem Set 9.

1. (The Bachet-Mordell equation) Study of the rational or integral solutions of $y^2 = x^3 - t$ for integer t goes back to Bachet who noted in 1621 that a rational solution to the equation leads to other rational solutions by intersecting the tangent line at the known solution with the curve to find additional rational points. Mordell studied the rational and integral solutions and showed the set of integer solutions is finite. Complete the following steps to prove the following theorem:

   Let t be a positive square free integer which is not congruent to 7 modulo 8. If 3 does not divide the class number of $\mathbf{Q}(\sqrt{-t})$ then there are integers satisfying $y^2 = x^3 - t$ if and only if t is of the form $t = 3z^2 \pm 1$ or $t = 3w^2 \pm 8$ for some integers z, w. If t is of this form there are four solutions if $t = 11$, and 2 solutions for $t \neq 11$ of this form.

   a) Show that if a nonzero ideal I of the maximal order $\mathcal{O}_K$ of a number field K satisfies that I^n is principal and n and the order of the Picard group of O_K are coprime, then I is principal.
   b) Let $K = \mathbf{Q}(\sqrt{-t})$. If $y^2 = x^3 - t$ with integers x, y show that in O_K the element x^3 factors as the product of the elements $y \pm \sqrt{-t}$. Prove that the principal ideals $(y + \sqrt{-t}), (y - \sqrt{-t})$ are relatively prime by studying prime ideals P containing both.
   c) Show that if $t \neq 3$ there exist integers a, b such that $y - \sqrt{-t}$ is the cube of an element of form $a + b\sqrt{-t}$ or $a/2 + b/2\sqrt{-t}$. By computing the cube, show that t must have one of the forms in the statement of the theorem above.
   d) Treat the case $t = 3$ separately by determining all units in the ring of integers and show that it is impossible to write $y - \sqrt{-3}$ as a unit times a cube of an element of the maximal order of $\mathbf{Q}(\sqrt{-3})$.
   e) Show that if t meets the conditions of the theorem, the integral solutions to the Bachet-Mordell equation with y positive are $(x, y) = (4z^2 \pm 1, z(8z^2 \pm 3))$ when $t = 3z^2 \pm 1, z > 0$ and $(x, y) = (z^2 \pm 2, z(z^2 \pm 3))$ when $t = 3z^2 \pm 8$.
   f) Show that $t = 11$ is the only square free integer that can be expressed as $3z^2 \pm 1$ and $3w^2 \pm 8$ for integers z, w.

2. Consider the cubic fields $\mathbf{K}_1, \mathbf{K}_2, \mathbf{K}_3$ generated over the rational field by a root of $x^3 - 18x - 6$, $x^3 - 36x - 78$, $x^3 - 54x - 150$ respectively. Show that these fields all have the same discriminant. Use the decomposition of primes to show that no two of these fields are isomorphic.

3. Consider the pure cubic field $K = \mathbf{Q}(\alpha)$ where $\alpha^3 = ab^2$, with $a > b \geq 1$ relatively prime square free integers. Discuss the factorization of the ideal generated by a prime number p in $\mathbf{O}_K$ according to the cases:
   a) $p \neq 3,\ p$ divides ab.
   b) p prime to ab, $p \equiv 1 \pmod 3$, $x^3 \equiv ab^2 \pmod p$ solvable.
   c) p prime to ab, $p \equiv 1 \pmod 3$, $x^3 \equiv ab^2 \pmod p$ not solvable.
   d) p prime to ab, $p \equiv -1 \pmod 3$
   e) $p = 3, ab^2 \not\equiv \pm 1 \pmod 9$
   f) $p = 3, ab^2 \equiv \pm 1 \pmod 9$

4. Let α be a root of $x^3 - 7x^2 + 14x - 7$, and let $K = \mathbf{Q}(\alpha)$. Show that K has class number 1. Show that the norm of any element of $\mathcal{O}_K$ is congruent to a cube modulo 7. Show that any rational prime which is not a cube modulo 7 remains prime in $\mathcal{O}_K$. Determine the factorization in $\mathcal{O}_K$ of all rational primes less than 100. Explain the relation of this problem to earlier Problem 2.4.