HOMEWORK 15

Due date:
Ex: M.2, page 411 of Artin's book.

For a reference, we record the Minkowski bound below.

Theorem 0.1. *Let F be a number field with $[F:\mathbb{Q}]=n$. Let $\mathcal{O}_F$ be the ring of integers of F. Let $2s$ be the number of non-real embeddings of $F\hookrightarrow\mathbb{C}$. Then in each ideal class of $\mathcal{O}_F$, there is an ideal $\mathfrak{a}$ such that*

$$\mathrm{Nm}(\mathfrak{a})\le B_F$$

with

$$B_F=\frac{n!}{n^n}\left(\frac{4}{\pi}\right)^s|\Delta_F|^{1/2}.$$

Here Δ_F is the discriminant of F.

Problem 1. *Let F be a number field and let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_F$. Show that there exists an integer prime $p\in\mathfrak{p}$. Show that $\mathrm{Nm}(\mathfrak{p})$ is a power of p.*

Problem 2. *Let m be a square-free integer such that $m\equiv 1 \bmod 4$. Let $F=\mathbb{Q}(\sqrt{m})$. Then $\mathcal{O}_F=\mathbb{Z}[\alpha]$ with $\alpha=\frac{-1+\sqrt{m}}{2}$. Let $p\in\mathbb{Z}$ be a prime integer. Determine how the ideal $p\mathcal{O}_F$ decomposes in $\mathcal{O}_F$. Determine primes p such that $p\mathcal{O}_F$ remains prime in $\mathcal{O}_F$.*

Answer: it depends on $(\frac{m}{p})$, namely, where m is a square or not in $\mathbb{F}_p^\times$. As a very special case of the above problem. For $F=\mathbb{Q}(\sqrt{-7})$. Determine how $2\mathcal{O}_F$ decomposes into product of prime ideals.

Problem 3. *Show that $\mathcal{O}_F$ is a PID for $F=\mathbb{Q}(\sqrt{-m})$ and $m=7,11,43$.*

Problem 4. *Determine the class group of $\mathbb{Q}(\sqrt{m})$ for $m=-19,-21,-47,15,-26$..*

Answer: the class group is 1 if $m=-19$; $C_2\times C_2$ if $m=-21$; C_5 for $m=-47$; C_2 if $m=15$; C_6 if $m=-26$.

See some examples of class numbers in Page 399 of Artin's book. You are encouraged to prove everything in the table (13.8.1) of page 399. For $m=15$, we have $\mathrm{Cl}(\mathbb{Q}(\sqrt{15}))\cong C_2$. For $m=-26$, its class group is C_6. Find generators for each class group.

Problem 5. *Consider $F=\mathbb{Q}(\alpha)$, where α is a root of $f=x^5-x+1$. It is known that the discriminant of f is 19×151 and f has only one real root and thus there are 4 non-real embeddings $F\hookrightarrow\mathbb{C}$. Show that F is a PID.*

Problem 6. *Find all integral solutions of the Diophantine equations*

(1)
$$y^2=x^3-2.$$

(2)
$$y^2=x^3-74.$$

Some useful facts. The class group of $\mathbb{Q}(\sqrt{-2})$ is trivial. The ideal class group of $\mathbb{Q}(\sqrt{-74})$ is cyclic of order 10.

Also, try the equation $y^2=x^3-7$. It is hard. The solutions are $(2,\pm1),(32,\pm181)$. Here is the issue. If we factorize $y^2+7=(y+\sqrt{-7})(y-\sqrt{-7})$, we cannot guarantee that $(y+\sqrt{-7})$ and $(y-\sqrt{-7})$ are coprime. Actually, they are not. Try to explain the equality $181^2+7=32^3=2^{15}$ in the ring $\mathcal{O}_F$ where $F = \mathbb{Q}(\sqrt{-7})$. How does $181 + \sqrt{-7}$ decompose into products of primes? Keep in mind that we know the ring $\mathcal{O}_F$ is a UFD. Answer:

$$181 + \sqrt{-7} = -\left(\frac{1+\sqrt{-7}}{2}\right)^{14}\left(\frac{1-\sqrt{-7}}{2}\right).$$

Moreover, try the equation $y^2 = x^3 - 26$. It is known that the class group of $\mathbb{Q}(-\sqrt{26})$ is C_6. Thus this one is hard if you want to repeat the usual process. (Solutions for $y^2 = x^3 - 26$ are $(3, \pm 1)$ and $(35, \pm 207)$.)

The following is a relatively general result regarding the equation $y^2 = x^3 - d$. In particular, it generalizes the cases in the above problem.

Problem 7. *Let $d > 1$ be square free and $d \equiv 1$ or $2 \bmod 4$. Assume that the class number of $\mathbb{Q}(\sqrt{-d})$ is not divisible by 3. Then $y^2 = x^3 - d$ has an integral solution iff d is of the form $3t^2 \pm 1$. The solutions are then $(t^2 + d, \pm t(t^2 - 3d))$.*

You should be able to prove this result on your own. But of course, you could find a proof anywhere else. If $d \equiv 3 \bmod 4$, the result is a little bit harder. The reason is, in this case, the integer ring is $\mathbb{Z}[\alpha]$ with $\alpha = \frac{-1+\sqrt{-d}}{2}$, which is not $\mathbb{Z}[\sqrt{-d}]$.

You might be wondering if the same method as above could be used to solve equations of the form $y^2 = x^3 + d$ for $d > 0$. Actually it is very hard and the reason is that the units of $\mathcal{O}_F$ is infinite if $F = \mathbb{Q}(\sqrt{d})$ if $d > 0$ is square free. Here is one example. We know that $(x, y) = (5, 12)$ is an integral solution of this equation $y^2 = x^3 + 19$. Try to think about what would happen if you want to use the method covered in class to solve it. We know that the ring $\mathbb{Z}[\sqrt{19}]$ is a PID. The units of $\mathbb{Z}[\sqrt{19}]$ are of the form $\pm(170 - 39\sqrt{19})^n$.

Equations of the type $y^2 = x^3 + k$ is called Mordell equation, which always have finitely many integral solutions. However, they could have infinitely many rational solutions. Example: The equation $y^2 = x^3 - 2$ has rational solutions $(x, y) = (1.29, 0.383)$ (Check this with a calculator). If you want to learn more about these equations, search the key word "elliptic curves".

Problem 8. *Let F be a number field. Show that there exists a finite extension L/F such that for each ideal $\mathfrak{a} \subset \mathcal{O}_F$, the ideal $\mathfrak{a}\mathcal{O}_L$ is principal.*

See this link for a proof.

The class group can be defined in a different way, which is given in next problem. We first introduce the terminorlogy *fractional ideal*. Let F be a number field and let $\mathcal{O}_F$ be its ring of integers. A fractional ideal of $\mathcal{O}_F$ is a nonzero $\mathcal{O}_F$-submodule $\mathfrak{a}$ of F such that $d\mathfrak{a} = \{dx : x \in \mathfrak{a}\}$ is an ideal of $\mathcal{O}_F$ for some $d \in \mathcal{O}_F$. More formally, a fractional ideal is a subset $\mathfrak{a} \subset F$ such that: (1) $\mathfrak{a}$ is an abelian group under addition; (2) $ax \in \mathfrak{a}$ for any $a \in \mathcal{O}_F, x \in \mathcal{O}_F$; and (3) there exists a $d \in \mathcal{O}_F$ such that $d\mathfrak{a} \subset \mathcal{O}_F$. Note that these conditions imply that $d\mathfrak{a}$ is an ideal of $\mathcal{O}_F$. Note that a fractional ideal is not necessary in $\mathcal{O}_F$. On the other hand, an ideal $\mathfrak{a} \subset \mathcal{O}_F$ is also a fractional ideal. To distinguish fractional ideals and ideals in $\mathcal{O}_F$, an ideal $\mathfrak{a} \subset \mathcal{O}_F$ is called an **integral ideal** of $\mathcal{O}_F$ to emphasize it is in $\mathcal{O}_F$. For two fractional ideals $\mathfrak{a}, \mathfrak{b}$, we define

$$\mathfrak{a} \cdot \mathfrak{b} = \left\{\sum a_i b_i | a_i \in \mathfrak{a}, b_i \in \mathfrak{b}\right\}.$$

Problem 9.
(1) *Let $\mathfrak{a}$ be a fractional ideal, show that one can decompose $\mathfrak{a} = \mathfrak{p}_1^{e_1} \dots \mathfrak{p}_k^{e_k}$ with $\mathfrak{p}_i$ prime and $e_i \in \mathbb{Z}$.*
(2) *Let $I(\mathcal{O}_F)$ be the set of all fractional ideals. Show that $I(\mathcal{O}_F)$ is an abelian group with respect to the ideal production.*
(3) *Show that $I(\mathcal{O}_F)$ is a free abelian group with generators of all prime ideals of $\mathcal{O}_F$.*
(4) *For any $a \in F^\times$, show that $(a) := \{ax : x \in \mathcal{O}_F\}$ is a fractional ideal. Thus there is a homomorphism*
$$F^\times \to I(\mathcal{O}_F)$$
defined by $a \mapsto (a)$. A fractional ideal of the form (a) for some $a \in F^\times$ is called a principal fractional ideal.

(5) *Let $P(\mathcal{O}_F)$ be the subgroup of all principal fractional ideals. Show that the quotient $I(\mathcal{O}_F)/P(\mathcal{O}_F)$ is isomorphic to $\mathrm{Cl}(\mathcal{O}_F)$.*

Problem 10. *Let $d \in \{19, 43, 67, 163\}$ and let $K = \mathbb{Q}(\sqrt{-d})$. Show that $\mathcal{O}_K$ is not an Euclidean domain.*

Note that $\mathcal{O}_K$ is a PID since $\mathcal{O}_K$ has class number 1. For the case when $d = 19$, this is Problem 4. Other cases can be checked in the same way. This problem gives us several examples of PID which are not ED. Hint: By contradiction. Suppose $\mathcal{O}_K$ is an ED. Let $\lambda : \mathcal{O}_K \to \mathbb{N}$ is a size function. This means that for any $a, b \in \mathcal{O}_K$, $b \neq 0$, we can write $a = bq + r$ with $b, r \in \mathcal{O}_K$ and $r = 0$ or $\lambda(r) < \lambda(b)$. Take $x \in \mathcal{O}_K - \mathcal{O}_K^\times - \{0\}$ such that $\lambda(x) = \min\left\{\lambda(y) : y \in \mathcal{O}_K - \mathcal{O}_K^\times - \{0\}\right\}$ is minimal. Then for any $a \in \mathcal{O}_K$, we have $a = qx + r$ with $r = 0$ or $\lambda(r) < \lambda(x)$. The assumption shows that $r \in \mathcal{O}_K^\times \cup \{0\}$. We have $\mathcal{O}_K^\times = \{\pm 1\}$. This shows that there is a principal ideal $I = (x)$ such that $\mathrm{Nm}(I) = |\mathcal{O}_K/I| = 2$ or 3. The rest is easy.

1. For your Winter Break

The next several problems might be hard. You don't have to submit solutions of them. But try them in the Winter break.

Problem 11. *Let p be a prime number of the form $4n - 1$ for some positive integer n. Show that $\mathbb{Q}(\sqrt{-p})$ has class number 1 iff $m^2 + m + n$ is prime for all m with $0 \le m \le n - 2$.*

Since $\mathbb{Q}(\sqrt{-163})$ has class number 1, we get that $m^2 + m + 41$ is prime for all m with $m = 0, 1, \ldots, 39$, which was observed by Euler.

Problem 12. *Let α be a root of $x^3 - x - 4$ and let $F = \mathbb{Q}(\alpha)$. Show that $\mathcal{B} = \left\{1, \alpha, \frac{\alpha+\alpha^2}{2}\right\}$ is an integral basis of $\mathcal{O}_F$. Moreover, show that F has class number 1.*

2. Ramanujan constant $e^{\pi\sqrt{163}}$

The number $e^{\pi\sqrt{163}}$ is called the Ramanujan constant, and its numerical value is

$$262537412640768743.99999999999925007259 72...$$

As you can see, it is almost an integer. There is a deep reason behind it. See this link for some discussions. One reason related to this is the field $\mathbb{Q}(\sqrt{-163})$ has class number 1. It is related to j-invariants of elliptic curves, Kronecker jugendtraum (Hilbert's 12th problem). Recall that, we know that every finite abelian extension of $\mathbb{Q}$ is contained in certain cyclotomic field $\mathbb{Q}(\zeta_N)$. In other words, one can obtain every finite abelian extension of $\mathbb{Q}$ by adjoining the roots of polynomials of the form $x^N - 1 = 0$. The Hilbert 12th problem asks the following question: given a number field F, to obtain all finite abelian extension of F, what are the algebraic numbers (or roots of what kind polynomials) should we adjoin to F? For general F, there is no answer yet. But for fields like $\mathbb{Q}(\sqrt{-d})$ with $d > 0$ (or its generalizations called CM fields), there is an answer to it. This is Shimura-Taniyama's celebrated complex multiplication theory for abelian varieties (which are generalizations of elliptic curves). See this wikipedia page if you can.

A good reference for this is D. Cox' book "Primes of the form $x^2 + ny^2$". You can find a copy of it here.