MAT415 Final Assessment Solutions

December 23, 2020

Problem 1. *This problem has two parts.*

a) Compute the class number of $\mathbb{Q}(\sqrt{-35})$.

b) Find all integer solutions to $a^3 = b^2 + 35$.

Solution. (a) Note that $-35 \equiv 1 \pmod 4$. Therefore $\mathbb{Z}[\frac{1+\sqrt{-35}}{2}]$ is the rings of integers in $K = \mathbb{Q}(\sqrt{-35})$. The discriminant is -35 and the norm form is $N(\frac{a+b\sqrt{-35}}{2}) = \frac{1}{4}(a^2 + 35b^2)$ where $a \equiv b \pmod 2$. We will use Minkowski's bound. Recall that the Minkowski bound is given by:

$$M_K := \frac{n!}{n^n}\left(\frac{4}{\pi}\right)^{r_2}\sqrt{|\Delta_K|}.$$

In our case, $M_K = \frac{2!}{2^2}\left(\frac{4}{\pi}\right)^1\sqrt{35} \sim 3.77$. Thus we only need to factor $(2), (3)$. Let $\theta = \frac{1+\sqrt{-35}}{2}$ be the generator of the ring of integers. It has minimal polynomial given by $x^2 - x + 9$. It is irreducible modulo 2 and factors as $x(x-1)$ modulo 3. Therefore we find.

$$(2) = (2, \theta^2 - \theta + 9) = \mathfrak{p}_2$$
$$(3) = (3, \theta)(3, \theta + 1) = \mathfrak{p}_3\,\mathfrak{p}_3'$$

Therefore, the class group is generated by $\mathfrak{p}_3$. There are no elements of norm 3 in $\mathcal{O}_K$, so $\mathfrak{p}_3$ is not principal. To compute its order, note that $N(1 + \sqrt{-35}) = 36 = 9 \times 4$. Together with the fact that $1 + \sqrt{-35} = 2\theta \in \mathfrak{p}_3$ and that 3 does not divide $1 + \sqrt{-35}$ in $\mathcal{O}_K$, we find $(1 + \sqrt{-35}) = \mathfrak{p}_2^2\,\mathfrak{p}_3^2$. This means that $[p_3]$ has order 2.

Therefore, K has class number 2, $\mathrm{Cl}(\mathcal{O}_K) \cong \mathbb{Z}/2\mathbb{Z}$, and the generator can be taken to be either of the two prime factors of the ideal (3).

(b) Since 35 is squarefree, a and b must be coprime. Since 35 is odd, they must have different parities. If a were even, then we would have $b^2 \equiv 5 \pmod 8$, which is impossible since the quadratic residues modulo 8 are $0, 1, 4$. Thus, a and b are coprime with a odd and b even.

Let's now work over $K = \mathbb{Q}(\sqrt{-35})$. If a, b is a solution to the equation $a^3 = b^2 + 35$, we have

$$(a)^3 = (b - \sqrt{-35})(b + \sqrt{-35}).$$

We claim that the ideals $(b - \sqrt{-35})$ and $(b + \sqrt{-35})$ are coprime. Indeed, if a prime ideal $\mathfrak{p}$ divides both $(b - \sqrt{-35})$ and $(b + \sqrt{-35})$, then $\mathfrak{p}\,|(a)^3$ (and thus (a)) and also $\mathfrak{p}\,|(2b)$. Since a is odd, we have that $\mathfrak{p} \not| (2)$ (lest it contain 1), and thus $\mathfrak{p}\,|(b)$. But this would contradict the fact that a and b are coprime. Thus, the ideals $(b - \sqrt{-35})$ and $(b + \sqrt{-35})$ are coprime.

It follows by unique factorisation into prime ideals that $(b-\sqrt{-35}) = \mathfrak{a}^3$ and $(b+\sqrt{-35}) = \mathfrak{b}^3$ for some ideals $\mathfrak{a}, \mathfrak{b}$ of $\mathcal{O}_K$.

As $[\mathfrak{a}]^3 = [\mathfrak{b}]^3 = 1$ in $\mathrm{Cl}(\mathcal{O}_K)$, and as the class number of $\mathcal{O}_K$ is 2, we conclude that $\mathfrak{a}$ and $\mathfrak{b}$ are principal ideals.

By assignment 1, the only units of $\mathcal{O}_K$ are ± 1. It follows in particular that

$$b+\sqrt{-35} = \left(\frac{x+y\sqrt{-35}}{2}\right)^3 = \frac{x^3-105xy^2}{8} + \frac{y(3x^2-35y^2)}{8}\sqrt{-35}$$

for some integers x and y having the same parity. In particular, we see that

$$y(3x^2-35y^2) = 8.$$

Thus, y can be one of $\pm 1, \pm 2, \pm 4, \pm 8$. We already know that x has the same parity as y, so if y is one of ± 4 or ± 8, the left hand side of the equation above is divisible by 16 which gives a contradiction. If $y = \pm 2$, we have $3x^2 - 35(4) = \pm 4$ and since x is even (because it has the same parity as y), say $x = 2x'$, we have $3(x')^2 - 35 = \pm 1$, thus $(x')^2 = 12$ or $34/3$ and so x' isn't an integer, which is a contradiction. If $y = 1$, we have $3x^2 = 43$ which is a contradiction since $3 \not| 43$. The only possible solutions are thus $(x, y) = (\pm 3, -1)$. Plugging these back in, we find that these give $b = \pm 36$. Plugging this back into the original equation gives that $a = 11$.

Therefore, $(a, b) = (11, \pm 36)$ are the only integer solutions to the Diophantine equation $a^3 = b^2 + 35$.

□

Problem 2. *Prove that all primes $p \equiv 1 \pmod 3$ can be written as $a^2 + ab + b^2$.*

Solution. The idea is to interpret $a^2 + ab + b^2$ as a norm in a quadratic field with class number 1. Showing that all primes $p \equiv 1 \pmod 3$ can be written in the form $a^2 + ab + b^2$ then reduces to showing that all primes $p \equiv 1 \pmod 3$ are not inert in this quadratic field.

Consider the field $K = \mathbb{Q}(\sqrt{-3})$. Note that $-3 \equiv 1 \pmod 4$. Therefore $\mathbb{Z}[\frac{1+\sqrt{-3}}{2}]$ is the rings of integers in $K = \mathbb{Q}(\sqrt{-3})$. The discriminant is -3. Recall that the Minkowski bound is given by:

$$M_K := \frac{n!}{n^n}\left(\frac{4}{\pi}\right)^{r_2}\sqrt{|\Delta_K|}.$$

In our case, $M_K = \frac{2!}{2^2}\left(\frac{4}{\pi}\right)^1\sqrt{3} \sim 1.10$. Therefore, K has class number 1.

Now, let $\theta = \frac{1+\sqrt{-3}}{2}$ be the generator of $\mathcal{O}_K = \mathbb{Z}[\theta]$. The norm form is given by:

$$N(a+b\theta) = (a+b\theta)(a+b\overline{\theta}) = a^2 + ab + b^2.$$

Since K has class number 1, it thus suffices to show that all primes $p \equiv 1 \pmod 3$ are not inert in $\mathcal{O}_K$. By Kummer's factorisation theorem, since $|\mathcal{O}_K/\mathbb{Z}[\sqrt{-3}]| = 2$ and since we are only interested in primes $p \equiv 1 \pmod 3$, we can work in $\mathbb{Z}[\sqrt{-3}]$ to determine the splitting type of primes $p \equiv 1 \pmod 3$ in $\mathcal{O}_K$. Now, $\sqrt{-3}$ has minimal polynomial $x^2 + 3$. It thus suffices to show that $x^2 + 3$ has a root modulo p for any prime congruent to 1 modulo 3.

This is equivalent to showing that -3 is a quadratic residue for all primes congruent to 1 modulo 3. We can do this using quadratic reciprocity. We have

$$\left(\frac{-3}{p}\right) = \left(\frac{-1}{p}\right)(-1)^{\frac{p-1}{2}\frac{3-1}{2}}\left(\frac{p}{3}\right) = (-1)^{\frac{p-1}{2}}(-1)^{\frac{p-1}{2}} = 1.$$

Therefore, we conclude that all primes $p \equiv 1 \pmod 3$ can be written as $a^2 + ab + b^2$. □

Problem 3. *This problem has three parts.*

a) Compute the ring of integers and the discriminant of $K = \mathbb{Q}(\sqrt{2}, \sqrt{-3})$

b) Describe the prime factorisations of (6) *and* (19) *in* $\mathcal{O}_K$*.*

c) Find generators for $\mathcal{O}_K^\times$*.*

Solution. (a) Note that $K = \mathbb{Q}(\sqrt{2}, \sqrt{-3})$ is equal to the compositum $\mathbb{Q}(\sqrt{2})\mathbb{Q}(\sqrt{-3})$ of $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt{-3})$. Note that $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt{-3})$ are both Galois, $\mathbb{Q}(\sqrt{2}) \cap \mathbb{Q}(\sqrt{-3}) = \mathbb{Q}$, and that the discriminant of $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt{-3})$ (namely 8 and -3) are coprime.

Futhermore, letting $\theta = \sqrt{2}$ and $\omega = \frac{1+\sqrt{-3}}{2}$, we have that $\{1, \theta\}$ and $\{1, \omega\}$ are integral bases for $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt{-3})$ respectively.

By Propositon 2.42 and remark 2.44 of Baker, this implies that $\{1, \theta, \omega, \theta\omega\}$ is an integral basis of $K = \mathbb{Q}(\sqrt{2}, \sqrt{-3})$ and that the discriminant of K is $8^2 \times -3^2 = 576$.

(b) Since $(6) = (2)(3)$, it suffices to factor $(2), (3), (19)$. Consider

$$\gamma := \theta + \omega = \sqrt{2} + \frac{1+\sqrt{-3}}{2} \in \mathcal{O}_K.$$

The minimal polynomial of γ is $x^4 - 2x^3 - x^2 + 2x + 7$. The discriminant of γ is thus 69696. This means that:

$$|\mathcal{O}_K/\mathbb{Z}[\gamma]| = \sqrt{\frac{\Delta_{K/\mathbb{Q}}(\gamma)}{\Delta_K}} = \sqrt{\frac{69696}{576}} = 11.$$

Since, $2, 3, 19 \not| 11$, we can apply Kummer's factorisation theorem.

Modulo 2, $x^4 - 2x^3 - x^2 + 2x + 7$ factors as $(x^2 + x + 1)^2$ and so

$$(2) = (2, \gamma^2 + \gamma + 1)^2.$$

Modulo 3, $x^4 - 2x^3 - x^2 + 2x + 7$ factors as $(x^2 + 2x + 2)^2$ and so

$$(3) = (3, \gamma^2 + 2\gamma + 2)^2.$$

Modulo 19, $x^4 - 2x^3 - x^2 + 2x + 7$ factors as $(x^2 + 3x + 5)(x^2 + 14x + 9)$ and so

$$(19) = (19, \gamma^2 + 3\gamma + 5)(19, \gamma^2 + 14\gamma + 9).$$

(c) Since K is totally imaginary, by Dirichlet's unit theorem we have $\mathcal{O}_K^\times \equiv W_K \times \mathbb{Z}$, where W_K are the roots of unity of K. Computing explicitly, we find that $W_K \cong \{1, \omega^1, \omega^2, \omega^3, \omega^4, \omega^5\} \cong \mathbb{Z}/6\mathbb{Z}$ where $\omega = \frac{1+\sqrt{-3}}{2}$ as above. So we just need to find a fundamental unit for $\mathcal{O}_K^\times$. Proceeding as in Assignment 4, we find that $\epsilon = 1 + \sqrt{2}$ is a fundamental unit of $\mathbb{Q}(\sqrt{2})$. In particular, $\epsilon = 1 + \sqrt{2}$ is not a root of unity. We claim that ϵ is a fundamental unit. Indeed, K is a CM field (a totally imaginary quadratic extension of totally real field which in our case is $\mathbb{Q}(\sqrt{2})$). Thus by pg. 90 of Milne, we know that $W_K \times \mathcal{O}_{\mathbb{Q}(\sqrt{2})}^\times$ has index 2 or 1 in $\mathcal{O}_K^\times$ according to whether there exists a unit u of $\mathcal{O}_K$ such that $u = -\overline{u}$ or not. Such a unit would necessarily have the form $(a + b\sqrt{2})(\sqrt{-3})$. But such an element has norm:

$$N((a + b\sqrt{2})(\sqrt{-3})) = (a^2 - 2b^2)^2(-3)^2$$

and therefore cannot be a unit!

Therefore, $\mathcal{O}_K^\times = W_K \times \mathcal{O}_{\mathbb{Q}(\sqrt{2})}^\times$ and we see that the unit group $\mathcal{O}_K^\times$ is generated by the order 6 element $\omega = \frac{1+\sqrt{-3}}{2}$ and the fundamental unit $1+\sqrt{2}$.

□

Problem 4. *Find a quadratic field whose class number is divisible by* 1024. *(Hint:* $1024 = 2^{10}$*).*

Solution. The idea is to show to produce enough linearly independent 2-torsion elements in the class group. In a quadratic field, primes that divide the discriminant ramify. Furthermore, since the degree is 2, primes that ramify must ramify as $(p) = \mathfrak{p}^2$ for some prime ideal $\mathfrak{p}$. These $\mathfrak{p}$ (if not trivial) represent a source of 2-elements in the class group!

Now, let's use this insight to write down a quadratic field whose class number is divisble by 2^{10}. Let $p_1, p_2, \ldots, p_{11}$ be the first 11 prime numbers congruent to 1 modulo 4. Let d be the product of the 11 prime numbers and consider the field $K = \mathbb{Q}(\sqrt{-d})$. Since $-d \equiv 3 \pmod 4$, the ring of integers of K is given by $\mathcal{O}_K = \mathbb{Z}[\sqrt{-d}]$. The the discriminant is $-4d$ and the norm form is $N(a+b\sqrt{-d}) = a^2 + db^2$.

Now, fix an $1 \leq i \leq 11$. Since $p_i | -4d = \Delta_{K/\mathbb{Q}}$, we have $(p_i) = \mathfrak{p}_i^2$ for some prime ideal $\mathfrak{p}_i$ of $\mathcal{O}_K$. Now, there is no element in $\mathcal{O}_K$ with norm p_i. Indeed, if $N(a+b\sqrt{-d}) = a^2 + db^2 = p_i$, then since $p_i < d$, we would need $b = 0$ which would give $a^2 = p_i$. Since this is impossible (p_i is not a square), we find that there are no elements of norm p_i in $\mathcal{O}_K$. Thus, $[\mathfrak{p}_i]$ has order 2 in $\mathrm{Cl}(K)$.

Now, we claim that the ideals $[\mathfrak{p}_1], [\mathfrak{p}_2], \ldots, [\mathfrak{p}_{10}]$ are linearly independent in the $\mathbb{F}_2$ vector space $\mathrm{Cl}_2(K)$ (this is notation for 2-torsion elements in the class group). That is, there is no non-trivial subcollection of them whose product is principal. Indeed, suppose towards a contradiction that $\mathfrak{p}_{i_1} \cdots \mathfrak{p}_{i_l} = (a+b\sqrt{-d})$, for some $l \leq 10$. Then, $N(a+b\sqrt{-d}) = a^2 + db^2 = p_{i_1} \cdots p_{i_l}$. As before, since $p_{i_1} \cdots p_{i_l} < d$, we must have $b = 0$ and thus $a^2 = p_{i_1} \cdots p_{i_l}$ which is impossible since $p_{i_1} \cdots p_{i_l}$ is squarefree. Therefore, the ideals $[\mathfrak{p}_1], [\mathfrak{p}_2], \ldots, [\mathfrak{p}_{10}]$ are linearly independent in the $\mathbb{F}_2$-vector space $\mathrm{Cl}_2(K)$.

This means that there are at least 2^{10} elements in the Sylow 2-subgroup of $\mathrm{Cl}(K)$ and therefore that 1024 divides the class number of K.

Another solution which is a bit more high-tech would be to use Gauss' description of 2-torsion in the narrow class group of quadratic fields as given in his *Disquitiones Arithmeticae*.

Theorem 1 (Gauss's genus theory, 1801)**.** *Let K be a quadratic field, $\Delta_{K/\mathbb{Q}}$ its discriminant and $\mathrm{Cl}_2^+[K]$ the 2-torsion in its narrow class group. Let $\omega(\Delta_{K/\mathbb{Q}})$ denote the number of distinct prime factors of $\Delta_{K/\mathbb{Q}}$. Then the 2-torsion in the narrow class group of K is given by*

$$\mathrm{Cl}_2^+[K] \cong \left(\frac{\mathbb{Z}}{2\mathbb{Z}}\right)^{\omega(\Delta_{K/\mathbb{Q}})-1}.$$

For imaginary quadratic fields, there are no units of negative norm and so the class group is isomorphic to the narrow class group. Thus, we see that any imaginary quadratic field $\mathbb{Q}(\sqrt{d})$ with $d < 0$ and with the property that d has 11 distinct prime factors also works. □

Problem 5 (Exercise 4.46 on Pg. 106-7)**.** *Let L/K be a Galois extension of number fields with Galois group G. Suppose $\mathfrak{q}$, $\mathfrak{q}'$ are prime ideals of $\mathcal{O}_L$ lying over $\mathfrak{p}$, and assume that $\mathfrak{p}$ is unramified in L. If $\mathfrak{q}' = \sigma\,\mathfrak{q}$ with $\sigma \in G$, show that*

$$\mathrm{Frob}_{\mathfrak{q}'/\mathfrak{p}} = \sigma\,\mathrm{Frob}_{\mathfrak{q}/\mathfrak{p}}\,\sigma^{-1}.$$

Solution. From Baker, we know that $\mathrm{Frob}_{\mathfrak{q}'/\mathfrak{p}}$ is the unique element of the Galois group which has the property that

$$\sigma(x) \equiv x^{N(\mathfrak{p})} \pmod{\mathfrak{q}'}$$

for all $x \in \mathcal{O}_L$ and where $N(\mathfrak{p})$ the cardinality of the residue field $|k|$.

Now, fix an element σ of the Galois group. Let $x \in \mathcal{O}_L$. By the definition of $\mathrm{Frob}_{\mathfrak{q}/\mathfrak{p}}$, we have $\mathrm{Frob}_{\mathfrak{q}/\mathfrak{p}}\,\sigma^{-1}(x) - (\sigma^{-1}(x))^{N(\mathfrak{p})} \in \mathfrak{q}$. Applying σ and noting that $\sigma\,\mathfrak{q} = \mathfrak{q}'$, we find $\sigma\,\mathrm{Frob}_{\mathfrak{q}/\mathfrak{p}}\,\sigma^{-1}(x) - x^{N(\mathfrak{p})} \in \mathfrak{p}'$. Therefore, we have shown that

$$\sigma\,\mathrm{Frob}_{\mathfrak{q}/\mathfrak{p}}\,\sigma^{-1}(x) \equiv x^{N(\mathfrak{p})} \pmod{\mathfrak{q}'}$$

for all $x \in \mathcal{O}_L$. Since $\mathrm{Frob}_{\mathfrak{q}'/\mathfrak{p}}$ is the unique element of G satisfying this identity, we conclude that $\mathrm{Frob}_{\mathfrak{q}'/\mathfrak{p}} = \sigma\,\mathrm{Frob}_{\mathfrak{q}/\mathfrak{p}}\,\sigma^{-1}$ as required. □

Problem 6 (Exercise 5.10 on Pg. 118)**.** *Verify the following identities in $\mathbb{Z}_p$:*

(1) $\frac{1}{1-p} = 1 + p + p^2 + \cdots + p^n + \cdots$

(2) $-1 = (p-1) + (p-1)p + \cdots + (p-1)p^n + \cdots$

Solution. (a) This identity is formal and holds in any ring where the infinite sum $1 + p + p^2 + \cdots + p^n + \cdots$ makes sense. In our case, this infinite sum makes sense. Indeed, the sum converges absolutely because the p-adic norm of the number p is strictly less than 1. Indeed, $|p|_p = \frac{1}{p} < 1$.

(b) This identity follows form the identity in part (a) by multiplying both sides by $(p-1)$.

□