Algebraic number theory
Solutions to exercise sheet for chapter 4

Nicolas Mascot (n.a.v.mascot@warwick.ac.uk),
Aurel Page (a.r.page@warwick.ac.uk)

TAs: Chris Birkbeck (c.d.birkbeck@warwick.ac.uk),
George Turcas (g.c.turcas@warwick.ac.uk)

Version: April 2, 2017

Exercise 1 (30 points)**.** *Let* $K = \mathbb{Q}(\sqrt{-155})$*.*

1. (3 points) *Write down without proof the ring of integers, the discriminant and the signature of* K*.*

   The signature of K is $(0,1)$. Since $-155 = -5 \cdot 31$ is squarefree and $-155 \equiv 1 \bmod 4$, the ring of integers of K is $\mathbb{Z}_K = \mathbb{Z}[\omega]$ where $\omega = \frac{1+\sqrt{-155}}{2}$, and $\operatorname{disc} K = -155$.

2. (10 points) *Describe a set of prime ideals of* $\mathbb{Z}_K$ *whose classes generate the class group of* K*. For each of these prime ideals, give the residue degree and ramification index.*

   The Minkowski bound is $M_K = \frac{2! \cdot 4}{2^2 \cdot \pi}\sqrt{155} \approx 7.9 < 8$, so the class group of K is generated by the classes of the primes of norm less than or equal to 8. Such ideals must be above $2, 3, 5$ or 7.

   - Since $-155 \equiv 5 \bmod 8$, the ideal $\mathfrak{p}_2 = 2\mathbb{Z}_K$ is a prime ideal with residue degree 2 and ramification index 1.
   - Since $-155 \equiv 1 \bmod 3$, we have $3\mathbb{Z}_K = \mathfrak{p}_3\mathfrak{p}_3'$ where $\mathfrak{p}_3$ and $\mathfrak{p}_3'$ are prime ideals with residue degree 1 and ramification index 1.
   - Since 5 divides -155, the prime 5 is ramified in K and we have $5\mathbb{Z}_K = \mathfrak{p}_5^2$ where $\mathfrak{p}_5$ is a prime ideal with residue degree 1 and ramification index 2.
   - We have $-155 \equiv 6 \bmod 7$. The squares modulo 7 are 0, $(\pm 1)^2 = 1$, $(\pm 2)^2 = 4$ and $(\pm 3)^2 \equiv 2 \bmod 7$, so -155 is not a square modulo 7 and $\mathfrak{p}_7 = 7\mathbb{Z}_K$ is a prime ideal with residue degree 2 and ramification index 1.

To conclude, the class group $\mathrm{Cl}(K)$ is generated by the classes of $\mathfrak{p}_2$, $\mathfrak{p}_3$, $\mathfrak{p}_3'$, $\mathfrak{p}_5$ and $\mathfrak{p}_7$. (It is already possible to reduce this set of primes, but you will get full marks for this set as well as correctly justified smaller ones.)

3. (8 points) *Factor the ideal* $(\frac{5+\sqrt{-155}}{2})$ *into primes.*

   We first compute the norm of $\alpha = \frac{5+\sqrt{-155}}{2} \in \mathbb{Z}_K$. We have $(2\alpha-5)^2+155=0$ which we can rewrite $4\alpha^2-20\alpha+180=0$ and simply $\alpha^2-5\alpha+45=0$. Since $\alpha \notin \mathbb{Q}$ we obtain the minimal polynomial $X^2-5X+45$ of α which is also its characteristic polynomial and hence $N_{\mathbb{Q}}^K(\alpha)=45$ (you can compute the norm with the method of your choice). The integral ideal $\mathfrak{a}=(\alpha)$ therefore has norm $45=3^2\cdot 5$. Given the decomposition of 3 and 5 in K, $\mathfrak{a}$ equals $\mathfrak{p}_5$ times a product of two prime ideals above 3. Since $\alpha \notin 3\mathbb{Z}_K = \mathfrak{p}_3\mathfrak{p}_3'$, we have $\mathfrak{a}=\mathfrak{p}_5\mathfrak{p}_3^2$ or $\mathfrak{a}=\mathfrak{p}_5{\mathfrak{p}_3'}^2$. After possibly swapping $\mathfrak{p}_3$ and $\mathfrak{p}_3'$ we may assume that $\mathfrak{a}=\mathfrak{p}_5\mathfrak{p}_3^2$.

4. (10 points) *Prove that* $\mathrm{Cl}(K) \cong \mathbb{Z}/4\mathbb{Z}$.

   The prime ideals $\mathfrak{p}_2 = 2\mathbb{Z}_K$ and $\mathfrak{p}_7 = 7\mathbb{Z}_K$ are principal, so their ideal classes are trivial. Moreover $\mathfrak{p}_3\mathfrak{p}_3' = 3\mathbb{Z}_K$ so $[\mathfrak{p}_3][\mathfrak{p}_3'] = 1$ and $[\mathfrak{p}_3]$ is in the subgroup generated by $[\mathfrak{p}_3']$. Since $(\alpha)=\mathfrak{p}_5\mathfrak{p}_3^2$ we have $1=[\mathfrak{p}_5][\mathfrak{p}_3]^2$ and $[\mathfrak{p}_5]=[\mathfrak{p}_3]^{-2}=[\mathfrak{p}_3']^2$ is in the subgroup generated by $[\mathfrak{p}_3']$. We have therefore proved that $\mathrm{Cl}(K)$ is generated by $[\mathfrak{p}_3']$, and we must determine its order. We have $[\mathfrak{p}_3']^4=[\mathfrak{p}_5]^2=[\mathfrak{p}_5^2]=[5\mathbb{Z}_K]=1$, so the order of $[\mathfrak{p}_3']$ divides 4: it must be $1, 2$ or 4.

   Let $x+y\omega \in \mathbb{Z}_K$ be an element of norm ± 5. Then

   $$N_{\mathbb{Q}}^K(x+y\omega) = \left(x+\frac{y}{2}\right)^2 + \frac{155}{4}y^2 = 5 \text{ since it must be positive,}$$

   so $y^2 = 20/155 < 1$, so $y=0$. But $x^2=5$ has no solution in $\mathbb{Z}$, so there is no integral element of norm ± 5 in K. The integral ideal $\mathfrak{p}_5$ of norm 5 is therefore not principal, so $[\mathfrak{p}_3']^2=[\mathfrak{p}_5]\neq 1$. So the order of $[\mathfrak{p}_3']$ does not divide 4 and must therefore be 4.

   This proves that $\mathrm{Cl}(K)$ is generated by an element of order 4, i.e. $\mathrm{Cl}(K)\cong\mathbb{Z}/4\mathbb{Z}$.

Exercise 2 (35 points)**.** *Let* $d \neq 0, 1$ *be a squarefree integer and let* $K=\mathbb{Q}(\sqrt{d})$.

1. (15 points) *Let* $n \in \mathbb{Z}$. *Prove that if neither* n *nor* $-n$ *are squares modulo* d, *then no integral ideal in* K *of norm* n *is principal.*

   - If $d \not\equiv 1 \bmod 4$: we have $\mathbb{Z}_K = \mathbb{Z}[\sqrt{d}]$. Let $\mathfrak{a}$ be a principal integral ideal of norm n. Then $\mathfrak{a} = (x+y\sqrt{d})$ with $x, y \in \mathbb{Z}$. We have

     $$N_{\mathbb{Q}}^K(x+y\sqrt{d}) = x^2-dy^2.$$

     Let $a \in \{\pm n\}$ be the norm of $x+y\sqrt{d}$. Reducing modulo d, we get $x^2 \equiv a \bmod d$, so one of $\pm n$ must be a square modulo d. By contraposition, if neither n not $-n$ are squares modulo d, then no integral ideal in K of norm n is principal.

- If $d \equiv 1 \bmod 4$: we have $\mathbb{Z}_K = \mathbb{Z}[\omega]$ where $\omega = \frac{1+\sqrt{d}}{2}$. Since d is odd, there exists $u \in \mathbb{Z}$ such that $2u \equiv 1 \bmod d$. Let $\mathfrak{a}$ be a principal integral ideal of norm n. Then $\mathfrak{a} = (x + y\omega)$ with $x, y \in \mathbb{Z}$. We have

$$N_{\mathbb{Q}}^{K}(x + y\omega) = \left(x + \frac{y}{2}\right)^2 - \frac{d}{4}y^2 = x^2 + xy + \frac{1-d}{4}y^2 = x^2 + xy + Dy^2,$$

where $1 - d = 4D$ and $D \in \mathbb{Z}$. Let $a \in \{\pm n\}$ be the norm of $x + y\omega$. Reducing modulo d, we have $(1-d)u^2 \equiv 4Du^2 \equiv D \bmod d$. We get

$$(x + uy)^2 \equiv (x + uy)^2 - d(uy)^2 \equiv x^2 + xy + Dy^2 \equiv a \bmod d,$$

so one of $\pm n$ must be a square modulo d. By contraposition, if neither n not $-n$ are squares modulo d, then no integral ideal in K of norm n is principal.

2. (3 points) *From now on $d = 105$. Write down without proof the ring of integers, the discriminant and the signature of K.*

The signature of K is $(2, 0)$. We have $d = 105 = 3 \cdot 5 \cdot 7$ is squarefree and $d \equiv 1 \bmod 4$, so $\mathbb{Z}_K = \mathbb{Z}[\omega]$ where $\omega = \frac{1+\sqrt{d}}{2}$, and $\operatorname{disc} K = d = 105$.

3. (10 points) *Find an element of norm -6 and an element of norm -5 in $\mathbb{Z}_K$.*

Let $x, y \in \mathbb{Z}$. We have $N_{\mathbb{Q}}^{K}(x + y\sqrt{d}) = x^2 - 105y^2$, so $10 + \sqrt{d} \in \mathbb{Z}_K$ has norm -5. We have $N_{\mathbb{Q}}^{K}(x + y\omega) = x^2 + xy - 26y^2$, so $4 + \omega$ has norm -6.

4. (7 points) *Prove that* $\mathrm{Cl}(K) \cong \mathbb{Z}/2\mathbb{Z}$.

The Minkowski bound is $M_K = \frac{2!}{2^2}\sqrt{105} \cong 5.12 < 6$, so the class group is generated by the classes of primes of norm up to 5. Such primes must be above 2, 3 or 5.

- We have $105 \equiv 1 \bmod 8$, so $2\mathbb{Z}_K = \mathfrak{p}_2\mathfrak{p}_2'$ where p_2 and $\mathfrak{p}_2'$ are prime ideals of norm 2.
- Since 3 divides 105, we have $3\mathbb{Z}_K = \mathfrak{p}_3^2$ where $\mathfrak{p}_3$ is a prime ideal of norm 3.
- Since 5 divides 105, we have $5\mathbb{Z}_K = \mathfrak{p}_5^2$ where $\mathfrak{p}_5$ is a prime ideal of norm 5.

The class group $\mathrm{Cl}(K)$ is therefore generated by the classes of $\mathfrak{p}_2$, $\mathfrak{p}_3$ and $\mathfrak{p}_5$ since $[\mathfrak{p}_2'] = [\mathfrak{p}_2]^{-1}$. We also have $[\mathfrak{p}_3]^2 = 1$ and $[\mathfrak{p}_5]^2 = 1$.

Since $(4 + \omega)$ is an integral ideal of norm 5, it must equal $\mathfrak{p}_5$, so $[\mathfrak{p}_5] = 1$. Since $\mathfrak{a} = (10 + \sqrt{d})$ is an integral ideal of norm 6, we must have $\mathfrak{a} = \mathfrak{p}_2\mathfrak{p}_3$ or $\mathfrak{a} = \mathfrak{p}_2'\mathfrak{p}_3$, and after possibly swapping $\mathfrak{p}_2$ and $\mathfrak{p}_2'$ we may assume $\mathfrak{a} = \mathfrak{p}_2\mathfrak{p}_3$. We get $1 = [\mathfrak{a}] = [\mathfrak{p}_2][\mathfrak{p}_3]$, so that $[\mathfrak{p}_2] = [\mathfrak{p}_3]^{-1} = [\mathfrak{p}_3]$ and $\mathrm{Cl}(K)$ is generated by $[\mathfrak{p}_3]$. Since $[\mathfrak{p}_3]^2 = 1$, this generator has order 1 or 2.

The squares modulo 5 are 0, $(\pm 1)^2 = 1$ and $(\pm 2)^2 = 4$ so neither 3 nor $-3 \equiv 2 \bmod 5$ are squares modulo 5. Since 5 divides d, they are also not squares modulo d. By 1., the ideal $\mathfrak{p}_3$ is not principal, so $[\mathfrak{p}_3]$ has order 2 and $\mathrm{Cl}(K) \cong \mathbb{Z}/2\mathbb{Z}$.

Exercise 3 (35 points)**.** We consider the equation

$$y^2 = x^3 - 6, \quad x, y \in \mathbb{Z}. \tag{1}$$

1. (3 points) *Write down without proof the ring of integers, signature and discriminant of $K = \mathbb{Q}(\sqrt{-6})$.*

   The signature of K is $(0, 1)$. Since $-6 = -2 \cdot 3$ is squarefree and $-6 \equiv 2 \bmod 4$, we have $\mathbb{Z}_K = \mathbb{Z}[\sqrt{-6}]$ and $\operatorname{disc} K = -24$.

2. (10 points) *Determine the class group of K.*

   The Minkowski bound is $M_K = \frac{2!}{2^2}\frac{4}{\pi}\sqrt{24} \approx 3.12$, so the class group of K is generated by the classes of prime ideals of norm up to 3. Such a prime ideal must be above 2 or 3. Since 2 and 3 both divide -24 we have $2\mathbb{Z}_K = \mathfrak{p}_2^2$ where $\mathfrak{p}_2$ is a prime ideal of norm 2, and $3\mathbb{Z}_K = \mathfrak{p}_3^2$ where $\mathfrak{p}_3$ is a prime ideal of norm 3. Moreover, $\sqrt{-6} \in \mathbb{Z}_K$ has norm 6 and therefore generates the ideal $\mathfrak{p}_2\mathfrak{p}_3$, so that $[\mathfrak{p}_2][\mathfrak{p}_3] = 1$: we obtain that $[\mathfrak{p}_3]$ belongs to the subgroup generated by $[\mathfrak{p}_2]$, so that $\mathrm{Cl}(K)$ is generated by $[\mathfrak{p}_2]$. We have $[\mathfrak{p}_2]^2 = 1$ so $[\mathfrak{p}_2]$ has order 1 or 2. If $\mathfrak{p}_2$ is principal, then a generator must be an element of $\mathbb{Z}_K$ of norm ± 2. The norm of a generic element $a + b\sqrt{-6}$ of $\mathbb{Z}_K$ ($a, b \in \mathbb{Z}$) is $a^2 + 6b^2 > 0$, so if $\mathfrak{p}_2$ is principal then there exists $a, b \in \mathbb{Z}$ such that

   $$a^2 + 6b^2 = 2.$$

   But this implies $b^2 \leq 2/6 = 1/3 < 1$, so $b = 0$, and $a^2 = 2$ has no solution in $\mathbb{Z}$. The ideal $\mathfrak{p}_2$ is therefore not principal, its ideal class has order 2, and $\mathrm{Cl}(K) \cong \mathbb{Z}/2\mathbb{Z}$.

3. (10 points) *Let $(x, y) \in \mathbb{Z}^2$ be a solution of (1). Prove that $(y + \sqrt{-6})$ and $(y - \sqrt{-6})$ are coprime.*

   Let $\mathfrak{p}$ be a prime ideal dividing both $(y+\sqrt{-6})$ and $(y-\sqrt{-6})$. Then $y+\sqrt{-6} \in \mathfrak{p}$ and $y-\sqrt{-6} \in \mathfrak{p}$, so their difference $2\sqrt{-6}$ is in $\mathfrak{p}$ and $\mathfrak{p}$ divides $(2\sqrt{-6})$. Taking norms, we have $N(\mathfrak{p}) \mid 24$ so $\mathfrak{p}$ is a prime ideal above 2 or 3.

   - If $\mathfrak{p}$ is above 2: then $\mathfrak{p} = \mathfrak{p}_2 = (2, \sqrt{-6})$, and since $\sqrt{-6} \in \mathfrak{p}_2$ we get $y = y + \sqrt{-6} - \sqrt{-6} \in \mathfrak{p}_2$. Since $y \in \mathbb{Z}$ we get $y \in \mathfrak{p}_2 \cap \mathbb{Z} = 2\mathbb{Z}$, and using the equation (1) x is also even. We write $y = 2z$ and $x = 2t$ with $t, z \in \mathbb{Z}$. We obtain
     $$4z^2 = 8t^3 - 6.$$
     Reducing modulo 4 gives $0 \equiv 2 \bmod 4$, which is impossible. So $\mathfrak{p}_2$ is not a common divisor of $(y + \sqrt{-6})$ and $(y - \sqrt{-6})$.
   - If $\mathfrak{p}$ is above 3: then $2y = y + \sqrt{-6} + y - \sqrt{-6} \in \mathfrak{p}$, and $2y \in \mathbb{Z}$, so $2y \in \mathbb{Z} \cap \mathfrak{p} = 3\mathbb{Z}$. Since 2 is coprime to 3, this implies that $y \in 3\mathbb{Z}$. Let $z \in \mathbb{Z}$ be such that $y = 3z$. From (1) and reducing modulo 3 we see that x must be divisible by 3, and we write $x = 3t$ with $t \in \mathbb{Z}$. The equation (1) becomes
     $$9z^2 = 27t^3 - 6.$$

Reducing modulo 9 we obtain $0 = 3 \bmod 9$, which is impossible. So $\mathfrak{p}$ is not a common divisor of $(y + \sqrt{-6})$ and $(y - \sqrt{-6})$.

We have thefore proved that $(y+\sqrt{-6})$ and $(y-\sqrt{-6})$ have no common prime divisor: they are coprime.

4. (4 points) *Prove that there exists an ideal $\mathfrak{a}$ such that $(y + \sqrt{-6}) = \mathfrak{a}^3$.*

   In the prime factorization of the ideal $(x^3) = (x)^3$, all prime ideals appear with exponents that are multiples of 3. We also have $(x^3) = (y^2 + 6) = (y + \sqrt{-6})(y - \sqrt{-6})$, and the primes appearing in the factorisations of $(y + \sqrt{-6})$ and $(y - \sqrt{-6})$ are disjoint, so their exponents are also multiples of 3. This exactly means that $(y + \sqrt{-6})$ is the cube of an ideal: there exists an integral ideal $\mathfrak{a}$ such that $\mathfrak{a}^3 = (y + \sqrt{-6})$.

5. (3 points) *Prove that $\mathfrak{a}$ is principal.*

   We have $[\mathfrak{a}]^3 = 1$ and the class number of K is 2, which is coprime to 3, so $[\mathfrak{a}] = 1$ and $\mathfrak{a}$ is principal.

6. (2 points) *Using without proof the fact that $\mathbb{Z}_K^\times = \{\pm 1\}$, prove that $y + \sqrt{-6}$ is a cube in $\mathbb{Z}_K$.*

   Let $\alpha \in \mathbb{Z}_K$ be such that $\mathfrak{a} = (\alpha)$. Then $(y + \sqrt{-6}) = (\alpha^3)$, so there exists $u \in \mathbb{Z}_K^\times$ such that $y + \sqrt{-6} = u\alpha^3$. Since the only units of $\mathbb{Z}_K$ are ± 1 and they are cubes, $y + \sqrt{-6}$ is a cube in $\mathbb{Z}_K$.

7. (3 points) *Prove that (1) has no solution.*

   Let $(x, y) \in \mathbb{Z}^2$ be a solution. Let $a, b \in \mathbb{Z}$ be such that $y+\sqrt{-6} = (a+b\sqrt{-6})^3$. Expanding, we get $y+\sqrt{-6} = a^3+3a^2b\sqrt{-6}-18ab^2-6b^3\sqrt{-6} = a(a^2-18b^2)+3b(a^2-2b^2)\sqrt{-6}$. From the coefficient of $\sqrt{-6}$ we get $3b(a^2 - 2b^2) = 1$, but 1 is not a multiple of 3 so this is impossible. The equation (1) therefore has no solution.

UNASSESSED QUESTIONS

Exercise 4. Let $K = \mathbb{Q}(\sqrt{-231})$.

1. *Write down without proof the ring of integers, the discriminant and the signature of K.*

   The signature of K is $(0, 1)$. Since $-231 = -3 \cdot 7 \cdot 11$ is squarefree and $-231 \equiv 1 \bmod 4$, we have $\mathbb{Z}_K = \mathbb{Z}[\omega]$ with $\omega = \frac{1+\sqrt{-231}}{2}$ and $\operatorname{disc} K = -231$.

2. *Compute the decompositions of* $2, 3, 5$ *and* 7 *in* K.

   - Since $-231 \equiv 1 \bmod 8$, we have $2\mathbb{Z}_K = \mathfrak{p}_2\mathfrak{p}_2'$ where $\mathfrak{p}_2$ and $\mathfrak{p}_2'$ are prime ideals of norm 2.
   - Since 3 divides -231, the prime 3 is ramified in K and $3\mathbb{Z}_K = \mathfrak{p}_3^2$ where $\mathfrak{p}_3$ is a prime ideal of norm 3.

- We have $-231 \equiv 4 \equiv 2^2 \bmod 5$, so $5\mathbb{Z}_K = \mathfrak{p}_5\mathfrak{p}_5'$ where $\mathfrak{p}_5$ and $\mathfrak{p}_5'$ are prime ideals of norm 5.
- Since 7 divides -231, the prime 7 is ramified in K and $7\mathbb{Z}_K = \mathfrak{p}_7^2$ where $\mathfrak{p}_7$ is a prime ideal of norm 7.

3. *Prove that for every element $z \in \mathbb{Z}_K$ such that $|N_{\mathbb{Q}}^K(z)| \leq 57$, we have $z \in \mathbb{Z}$.*

   Let $z \in \mathbb{Z}_K$. We can write $z = x + y\omega$ with $x, y \in \mathbb{Z}$. We have
   $$|N_{\mathbb{Q}}^K(z)| = N_{\mathbb{Q}}^K(z) = \left(x + \frac{y}{2}\right)^2 + \frac{231}{4}y^2 = x^2 + xy + 58y^2.$$
   If $|N_{\mathbb{Q}}^K(z)| \leq 57$ then $y^2 \leq \frac{4 \cdot 57}{231} = \frac{228}{231} < 1$, so $y = 0$ and $z = x \in \mathbb{Z}$.

4. *Let $\mathfrak{p}_2$ be a prime of $\mathbb{Z}_K$ above 2. Prove that the class of $\mathfrak{p}_2$ in $\mathrm{Cl}(K)$ has order 6.*

   The ideal classes of the two prime ideals above 2 are inverse of each other and hence have the same order. The element $2 + \omega \in \mathbb{Z}_K$ has norm $64 = 2^6$, and $2 + \omega \notin 2\mathbb{Z}_K = \mathfrak{p}_2\mathfrak{p}_2'$, so we have $2 + \omega = \mathfrak{p}_2^6$ or $2 + \omega = {\mathfrak{p}_2'}^6$. In both cases we get $[\mathfrak{p}_2]^6 = [\mathfrak{p}_2']^6 = 1$, and the order of $[\mathfrak{p}_2]$ can be 1, 2, 3 or 6.

   If the order m of $[\mathfrak{p}_2]$ is not 6, then $\mathfrak{p}_2^m$ is principal and has norm $2^m \leq 57$, so its generator z must be in $\mathbb{Z}$ by the previous question. The only element $z \in \mathbb{Z}$ such that $N_{\mathbb{Q}}^K(z) \in \{2, 2^2, 2^3\}$ is $z = 2$, but the ideal $(2) = \mathfrak{p}_2\mathfrak{p}_2'$ is not equal to any $\mathfrak{p}_2^m$. So $[\mathfrak{p}_2]$ has order 6.

5. Let $\mathfrak{p}_7$ be a prime of $\mathbb{Z}_K$ above 7. Prove that the class of $\mathfrak{p}_7$ in $\mathrm{Cl}(K)$ has order 2.

6. Prove that $[\mathfrak{p}_7]$ does not belong to the subgroup of $\mathrm{Cl}(K)$ generated by $[\mathfrak{p}_2]$. *Hint: prove that if it did, then $\mathfrak{p}_7\mathfrak{p}_2^3$ would be principal.*

7. Compute the prime factorisations of the ideals $(\frac{3+\sqrt{-231}}{2})$ and $(\frac{7+\sqrt{-231}}{2})$.

8. Prove that $\mathrm{Cl}(K) \cong \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Exercise 5. *Let $d > 0$ be a squarefree integer, let $K = \mathbb{Q}(\sqrt{-d})$ and let $\operatorname{disc} K$ be the discriminant of K. Let p be a prime that splits in K and let $\mathfrak{p}$ be a prime ideal above p.*

1. *Prove that for all integers $i \geq 1$ such that $p^i < |\operatorname{disc} K|/4$, the ideal $\mathfrak{p}^i$ is not principal. Hint: consider the cases $\operatorname{disc} K = -d$ and $\operatorname{disc} K = -4d$ separately.*

   Let i be as above. Since p is split, $N(\mathfrak{p}) = p$, and by uniqueness of factorisation the ideal $\mathfrak{p}^i$ is not divisible by (p).

   - If $\operatorname{disc} K = -4d$, then $\mathbb{Z}_K = \mathbb{Z}[\sqrt{-d}]$. The norm of a generic element $z = x + y\sqrt{-d} \in \mathbb{Z}_K$ is
     $$x^2 + dy^2.$$
     If $\mathfrak{p}^i$ is principal, let z be a generator. Then the norm of z is p^i, giving $x^2 + dy^2 = p^i$, so $y^2 \leq p^i/d < 1$, so $y = 0$. But then $z \in \mathbb{Z}$ has norm $z^2 = p^i$, so z is divisible by p. But this is impossible since $\mathfrak{p}^i$ is not divisible by (p).

- If $\operatorname{disc} K = -d$, then $\mathbb{Z}_K = \mathbb{Z}[\alpha]$ with $\alpha = \frac{1+\sqrt{-d}}{2}$. The norm of a generic element $z = x + y\alpha$ is

$$\left(x + \frac{y}{2}\right)^2 + d\left(\frac{y}{2}\right)^2.$$

If $\mathfrak{p}^i$ is principal, let z be a generator. Then the norm of z is p^i, so $y^2 \leq 4p^i/d < 1$, so $y = 0$ and as before z is divisible by p, which is impossible.

2. *What does this tell you about the class number of K?*

The number of i as in the previous question is

$$\left\lfloor \frac{\log(|\operatorname{disc} K|/4)}{\log p} \right\rfloor$$

so, accounting for the trivial class, we have

$$h_K \geq 1 + \left\lfloor \frac{\log(|\operatorname{disc} K|/4)}{\log p} \right\rfloor.$$

3. *Using without proof the fact that there exists infinitely many squarefree positive numbers of the form $8k+7$ for $k \in \mathbb{Z}_{>0}$, prove that for every $X > 0$ there exists a number field K such that $h_K > X$.*

Let d be squarefree of the form $8k + 7$. Then $-d < 0$ is squarefree and $-d \equiv 1 \bmod 8$. Let $K = \mathbb{Q}(\sqrt{-d})$. Then $\operatorname{disc} K = -d$ and 2 is split in K. By the previous part we have $h_K \geq 1 + \left\lfloor \frac{\log(d/4)}{\log 2} \right\rfloor$, which tends to ∞ as $d \to \infty$. Using an infinite sequence of such d we obtain $h_K \to \infty$.