Mathematics W4043 Algebraic Number Theory
Final Exam

Benjamin Church (bvc2105)

April 24, 2018

1. Let K be the splitting field of $X^3 - 15$ over $\mathbb{Q}$. Consider $\mathcal{O}_K$. The Galois group is given by, $Gal(K/\mathbb{Q}) \cong S_3$ because the discriminant $\Delta = -27 \cdot 15^2$ is not a square in $\mathbb{Q}$ and $X^3 - 15$ is irreducible over $\mathbb{Q}$. Therefore, the subfields of K correspond to the subgroups of S_3. These subgroups are the three order two subgroups generated by swapping two roots which fix the fields generated by the single remaining root, $L_1 = \mathbb{Q}(\sqrt[3]{15})$ and $L_2 = \mathbb{Q}(\zeta_3 \sqrt[3]{15})$ and $L_3 = \mathbb{Q}(\zeta_3^2 \sqrt[3]{15})$. The final subgroup is generated by a 3-cycle which fixes the product of the three roots and thus corresponds to $E = \mathbb{Q}(\zeta_3) = \mathbb{Q}(\sqrt{\Delta})$.

   (a) A prime p is ramified in some field L if and only if $\mathcal{O}_L/(p)$ has nilpotents. Consider the element $x = \zeta_3^{(i-1)} \sqrt[3]{15} + p\mathcal{O}_{L_i} \in \mathcal{O}_{L_i}/p\mathcal{O}_{L_i}$. Then,
   $$x^3 = (\zeta_3^{(i-1)} \sqrt[3]{15})^3 + p\mathcal{O}_{L_i} = 15 + p\mathcal{O}_{L_i}$$
   Therefore, if $p \mid 15$ then $15 \in p\mathcal{O}_{L_i}$ so $x^3 \in p\mathcal{O}_{L_i}$. Thus, if $p \mid 15$ then p is ramified in L_i so 3 and 5 are ramified in L_1, L_2, and L_3. Finally, $E = \mathbb{Q}(\zeta_3)$ is a cyclotomic field and therefore the only prime ramified in E is 3. So 5 is only unramifieid in E and 3 is never unramified. Furthermore, $\sqrt[3]{15} \in K$ so by the same argument, 3 and 5 are ramified in K.

   (b) Consider the ideals generated by $2, 3, 5, 7$ in the ring $\mathcal{O}_K$.

   Case p = 2: First, we consider the factorization of (2) in $E = \mathbb{Q}(\zeta_3) = \mathbb{Q}(\sqrt{-3})$. Because $-3 \equiv 5 \pmod 8$, we know that 2 is inert in E i.e. $\mathfrak{p} = 2\mathcal{O}_E$ is a prime ideal. Consider the extension, $[K : E] = 3$, which is Galois because $K/\mathbb{Q}$ is Galois. Therefore, in the extension K/E, we can factor,
   $$\mathfrak{p}\mathcal{O}_K = \prod_{j=1}^{g} \mathfrak{P}_j^e$$
   where the indices are the same for each prime factor because the extension is Galois. Also, $[K : E] = efg$ where $[K : E] = 3$ and $f = [\mathcal{O}_K/\mathfrak{P}_j : \mathcal{O}_E/\mathfrak{p}]$. Now, in $\mathcal{O}_K$,
   $$\begin{aligned}(\sqrt[3]{15} - 1)(\zeta_3\sqrt[3]{15} - 1)(\zeta_3^2\sqrt[3]{15} - 1) \\ &= (\sqrt[3]{15} - 1)(\sqrt[3]{15}^2 - \sqrt[3]{15}(\zeta_3^2 + \zeta_3) + 1) \\ &= (\sqrt[3]{15} - 1)(\sqrt[3]{15}^2 + \sqrt[3]{15} + 1) = \sqrt[3]{15}^3 - 1 = 14 \in 2\mathcal{O}_K\end{aligned}$$
   however, these elements are all Galois conjugates. In particular, because the Galois group acts transitivly on the roots and each root has a stabilizer of order 2,
   $$\mathrm{N}_{\mathbb{Q}}^{K}\left(\zeta_3^k \sqrt[3]{15} - 1\right) = \prod_{\sigma \in G} \sigma(\zeta_3^k \sqrt[3]{15} - 1) = (\sqrt[3]{15} - 1)^2(\zeta_3\sqrt[3]{15} - 1)^2(\zeta_3^2\sqrt[3]{15} - 1)^2 = 14^2$$

Furthermore, $\mathrm{N}_{\mathbb{Q}}^{K}(2) = \prod_{\sigma \in G} \sigma(2) = 2^6$. Suppose that $2 \mid (\zeta_3^k \sqrt[3]{15} - 1)$ then using the multiplicativity of the norm, we must have that, $\mathrm{N}_{\mathbb{Q}}^{K}(2) \mid \mathrm{N}_{\mathbb{Q}}^{K}\left(\zeta_3^k \sqrt[3]{15} - 1\right)$. However, $2^6 \not| \, 14^2$. Therefore, $(\zeta_3^k \sqrt[3]{15} - 1) \notin 2\mathcal{O}_K$ so $2\mathcal{O}_K$ is not a prime ideal of $\mathcal{O}_K$ and thus must factor with $g > 1$ or $e > 1$. Assuming that 2 is unramified in K, the factors of 2 must be unramified in any sub extension. In particular, $e = 1$. Thus, $g > 1$ so $g = 3$ because $g \mid 3$. Therefore, three prime ideals of $\mathcal{O}_K$ lie above $\mathfrak{p}$, the inert prime (2) in E. Thus, in total, three prime ideals of $\mathcal{O}_K$ lie above 2.

Case p = 3: In the field K, we know that $(3)(5) = (15) = (\sqrt[3]{15})^3$. However, (3) and (5) are coprime so both (3) and (5) must be cubes. Because K is a splitting field over $\mathbb{Q}$, the extension $K/\mathbb{Q}$ is Galois. Therefore, (3) factors as,

$$3\mathcal{O}_K = \prod_{i=1}^{g} \mathfrak{P}_i^{e_i}$$

where for every i we have, $e_i = e$ and $f = [\mathcal{O}_K/\mathfrak{P}_i : \mathbb{F}_3]$. Thus, $efg = [K : \mathbb{Q}] = 6$. However, (3) is a cube so $3 \mid e$ since the prime factors are all distinct. Furthermore, consider the ideal (3) in $E = \mathbb{Q}(\zeta_3)$. By cyclotomic reciprocity, we know that 3 ramifies as $3\mathcal{O}_E = (\lambda)^2$. Therefore, the ramification index of a prime lying above 3 in E namely, $(\lambda) = \mathfrak{p} = \mathfrak{P}_i \cap \mathcal{O}_E$ factors as,

$$e_{K/\mathbb{Q}}(\mathfrak{P}) = e_{K/E}(\mathfrak{P}) \ e_{E/\mathbb{Q}}(\mathfrak{p})$$

since $e_{E/\mathbb{Q}}(\mathfrak{p}) = 2$ we know that $2 \mid e_{K/\mathbb{Q}}(\mathfrak{P}) = e$. Thus, both 2 and 3 divide e so $6 \mid e$ but $efg = 6$ so $e = 6$ and $g = 1$. Therefore, a single prime lies above 3 in K.

Case p = 5: Because $K/\mathbb{Q}$ is Galois, (5) factors as,

$$5\mathcal{O}_K = \prod_{i=1}^{g} \mathfrak{P}_i^{e_i}$$

where for every i we have, $e_i = e$ and $f = [\mathcal{O}_K/\mathfrak{P}_i : \mathbb{F}_5]$. Thus, $efg = [K : \mathbb{Q}] = 6$. However, (5) is a cube so $3 \mid e$. Furthermore, consider the ideal (5) in $E = \mathbb{Q}(\zeta_3)$. Because $E = \mathbb{Q}(\sqrt{-3})$ and $\left(\frac{-3}{5}\right) = -1$ we know that 5 is inert in E i.e. $\mathfrak{p} = 5\mathcal{O}_E$ is a prime ideal. Therefore, the ramification index of 5 in E with $\mathfrak{p} = \mathfrak{P}_i \cap \mathcal{O}_E$ satisfies,

$$e_{K/\mathbb{Q}}(\mathfrak{P}) = e_{K/E}(\mathfrak{P}) \ e_{E/\mathbb{Q}}(\mathfrak{p}) = e_{K/E}(\mathfrak{P})$$

However, because $\mathbb{Q} \subset E \subset K$ and $K/\mathbb{Q}$ is Galois we know that K/E is Galois and $[K : E] = 3$. Therefore, the prime $\mathfrak{p}$ in E factors in K such that,

$$e_{K/E}(\mathfrak{P}) f_{K/E}(\mathfrak{P}) g_{K/E}(\mathfrak{P}) = [K : E] = 3$$

In particular, $3 \mid e_{K/\mathbb{Q}}(\mathfrak{P}) = e_{K/E}(\mathfrak{P})$ so $e_{K/E}(\mathfrak{P}) = 3$ and $f_{K/E}(\mathfrak{P}) = g_{K/E}(\mathfrak{P}) = 1$. Therefore, only one prime of K lies above $5\mathcal{O}_E$ which is the only prime of E above 5. Therefore, only one prime in K lies above 5.

Case p = 7: First, we consider the factorization of (7) in $E = \mathbb{Q}(\zeta_3) = \mathbb{Q}(\sqrt{-3})$. Since $\left(\frac{-3}{7}\right) = 1$ we know that 7 is split in E, that is,

$$7\mathcal{O}_E = \mathfrak{p}_1 \mathfrak{p}_2$$

Because $(2+\sqrt{-3})(2+\sqrt{-3}) = 4+3 = 7$ we know that $(7) = (2+\sqrt{-3})(2-\sqrt{-3})$. However, these two ideals must be prime in E because otherwise they would factor into multiple or ramified primes either of which would contradict the unique factorization of (7) into two prime ideals. Thus, $\mathfrak{p}_1 = (2+\sqrt{-3})$ and $\mathfrak{p}_2 = (2-\sqrt{-3})$. Now, consider the extension, $[K : E] = 3$, which is Galois because $[K : \mathbb{Q}]$ is Galois. Therefore, in the extension K/E, we can factor,

$$\mathfrak{p}_i \mathcal{O}_K = \prod_{j=1}^{g} \mathfrak{P}_j^e$$

where the indeces are the same for each prime factor because the extension is Galois. Also, $[K : E] = efg$ where $[K : E] = 3$ and $f = [\mathcal{O}_K/\mathfrak{P}_j : \mathcal{O}_E/\mathfrak{p}_i]$. As before, in $\mathcal{O}_K$,

$$(\sqrt[3]{15}-1)(\zeta_3\sqrt[3]{15}-1)(\zeta_3^2\sqrt[3]{15}-1) = 14 \in 7\mathcal{O}_K \subset (2+\sqrt{-3})\mathcal{O}_K = \mathfrak{p}_1\mathcal{O}_K$$

and again,

$$\mathrm{N}_{\mathbb{Q}}^{K}\left(\zeta_3^k\sqrt[3]{15}-1\right) = \prod_{\sigma\in G}\sigma(\zeta_3^k\sqrt[3]{15}-1) = (\sqrt[3]{15}-1)^2(\zeta_3\sqrt[3]{15}-1)^2(\zeta_3^2\sqrt[3]{15}-1)^2 = 14^2$$

Furthermore, the Galois group $Gal(K/\mathbb{Q})$ restricted to act on $E = \mathbb{Q}(\sqrt{-3})$ is exactly 3 copies of $Gal(E/\mathbb{Q})$ (since E is the fixed field of the subgroup generated by a 3-cycle). Thus,

$$\mathrm{N}_{\mathbb{Q}}^{K}\left(2+\sqrt{-3}\right) = \prod_{\sigma\in G}\sigma(2+\sqrt{-3}) = (2+\sqrt{-3})^3(2-\sqrt{-3})^3 = 7^3$$

Suppose that $(2+\sqrt{-3}) \mid (\zeta_3^k\sqrt[3]{15}-1)$ then using the multiplicativity of the norm, we must have that, $\mathrm{N}_{\mathbb{Q}}^{K}\left(2+\sqrt{-3}\right) \mid \mathrm{N}_{\mathbb{Q}}^{K}\left(\zeta_3^k\sqrt[3]{15}-1\right)$. However, $7^3 \nmid 14^2$. Therefore, $(\zeta_3^k\sqrt[3]{15}-1) \notin (2+\sqrt{-3})\mathcal{O}_K$ so $(2+\sqrt{-3})\mathcal{O}_K = \mathfrak{p}_1\mathcal{O}_K$ is not a prime ideal of $\mathcal{O}_K$ and thus must factor with $g > 1$ or $e > 1$. Assuming that 7 is unramified in K, the factors of 7 must be unramified in any sub extension. In particular, $e = 1$. Thus, $g > 1$ so $g = 3$ because $g \mid 3$. Therefore, three prime ideals of $\mathcal{O}_K$ lie above each $\mathfrak{p}_i$. Thus, in total, six prime ideals of $\mathcal{O}_K$ lie above 7.

(c) To conclude that 2 and 7 are unramified in K it would suffice to calculate the discriminant of K. Given Δ_K we know that p is ramified in K if and only if $p \mid \Delta_K$. Therefore, showing that 2 and 3 do not divide Δ_K would show that neither 2 or 3 are ramified. Calculating the discriminant would require knowing a $\mathbb{Z}$-basis of $\mathcal{O}_K$. A perhaps more direct route would be to show that the principal ideals,

$$(\alpha_1) = (\sqrt[3]{15}-1), \quad (\alpha_2) = (\zeta_3\sqrt[3]{15}-1), \quad (\alpha_3) = (\zeta_3\sqrt[3]{15}-1)$$

are relatively prime and thus factor into distinct prime ideals. We can show that this condition is equivalent to both 2 and 7 being unramified by considering the products of the ideals,

$$(\alpha_1)(\alpha_2)(\alpha_3) = (\sqrt[3]{15}-1)(\zeta_3\sqrt[3]{15}-1)(\zeta_3^2\sqrt[3]{15}-1) = (14) = (2)(7)$$

Because (2) and (7) are relatively prime, they have distinct prime factors in K. Therefore, their product has nonzero multiplicity in its prime factorization if and only if the factorizations of (2) or (7) do independently i.e. at least one is ramified. However, we can show that each of the left-hand factors cannot be ramified. Using the norm,

$$\mathrm{N}(\zeta_3^k \sqrt[3]{15} - 1) = \mathrm{N}_{\mathbb{Q}}^{K}\left(\zeta_3^k \sqrt[3]{15} - 1\right) = 2^2 \cdot 7^2$$

we conclude that each left-hand factor must itself factor into a multiplicity two (either $e = 2$ or $f = 2$ or $g = 2$) product of primes lying above 2 and above 7. Because ideals (α_k) are Galois conjugates, their factorizations must have equal e, f, and g. Let $\mathfrak{p}_2$ be a divisor of (α_k) and of (2) and let $\mathfrak{p}_7$ be a divisor of (α_k) and of (7). However, 2 is inert in E so the residue field of any prime lying above 2 in K must be an extension of $\mathbb{F}_{2^2}$. Thus, $\mathrm{N}(\mathfrak{p}_2) = 2^2$ exactly since, in the field extenson K/E, $f = 1$ because $e > 1$ or $g > 1$ and $efg = 3$. Therefore, because 2 divides $\mathrm{N}(\alpha_k)$ with multiplicity exactly 2, this ideal must be divisible by exactly one prime above 2, i.e. $(\alpha_k) = \mathfrak{p}_2 \cdot \mathfrak{a}$ where $\mathfrak{a}$ is a divisor of (7). Now, if the factorization of $\mathfrak{a}$ is ramified, then because 7 divides $\mathrm{N}(\alpha_k)$ with multiplicity exactly 2, we know that $(\alpha_k) = \mathfrak{p}_2 \cdot \mathfrak{p}_7^2$. Furthermore, we know, for the decomposition of $7\mathcal{O}_K$, that $efg = 6$ and $2 \mid g$ (because it is split in E) so $ef = |D_7|$ is odd. Therefore, at most, only the 3-cycles can stabilize $\mathfrak{p}_7$. Let $\sigma \in G$ be a 3-cycle and $\tau \in G$ be the 2-cycle taking α_k to $\sigma(\alpha_k)$. Then, $\sigma(\alpha_k) = \tau(\alpha_k)$ so the ideals,

$$(\sigma(\alpha_k)) = \sigma(\mathfrak{p}_2)\sigma(\mathfrak{p}_7)^2 = (\tau(\alpha_k)) = \tau(\mathfrak{p}_2)\tau(\mathfrak{p}_7)^2$$

which implies by the uniqueness of prime factorizations of ideals that $\sigma(\mathfrak{p}_7) = \tau(\mathfrak{p}_7)$ since the Galois group preserves the prime in the base field that a given prime ideal lies above. However, τ does not stabilize $\mathfrak{p}_7$ so neither can σ which implies that $D_7 \cong \{e\}$. This implies that $ef = 1$ which contradicts the assumption that primes above 7 were ramified in the factorization of $\mathfrak{a}$ since $(a_1)(a_2)(a_3) = (2)(7)$ so every one of the 6 unique factors (since $ef = 1$ implies that $g = 6$) would necessarily appear in the left-hand factors. Thus, each (α_k) is unramified. Therefore, if they share no common factors then their product remains unramified proving that both (2) and (7) are unramified.

2. (a) We want to consider quadratic forms $Q(X, Y) = aX^2 + bXY + cY^2$ such that the discriminant, $\Delta = b^2 - 4ac = -68$ and Q is reduced i.e. $|b| \leq a \leq c$ and if $a = |b|$ or $a = c$ then $b \geq 0$. When the quadratic form is reduced, we know that $a \leq \sqrt{|\Delta|/3} \approx 4.76$. Now, $b^2 = 4ac - 68 = 4(ac - 17)$ so b must be even. However, $|b| \leq a \leq \sqrt{|\Delta|/3} \approx 4.76$ so the only possibilities are $b = -4, -2, 0, 2, 4$. We must consider each of these cases. Remembering that $0 \leq |b| \leq a \leq c$.

Let $b = -4$ then $ac = (b/2)^2 + 17 = 21$ so $(a, c) = (1, 21)$ or $(3, 7)$. However, $|b| \leq a$ so neither of these are possible reduced forms.

Let $b = -2$ then $ac = (b/2)^2 + 17 = 18$ so $(a, c) = (1, 18)$ or $(2, 9)$ or $(3, 6)$. However, $|b| \leq a$ so only $(a, b, c) = (3, -2, 6)$ is a vaild reduced form because in the case $a = 2$ then $a = |b|$ so $b \geq 0$ which is not the case here.

Let $b = 0$ then $ac = (b/2)^2 + 17 = 17$ so $(a, c) = (1, 17)$ which gives the vaild reduced form $(a, b, c) = (1, 0, 17)$.

Let $b = 2$ then $ac = (b/2)^2 + 17 = 18$ so $(a, c) = (1, 18)$ or $(2, 9)$ or $(3, 6)$. Thus,

$(a,b,c) = (2,2,9)$ and $(3,2,6)$ are vaild reduced forms but $a \neq 1$ since $|b| \leq a$.

Let $b = 4$ then $ac = (b/2)^2 + 17 = 21$ so $(a,c) = (1,21)$ or $(3,7)$. However, $|b| \leq a$ so neither of these are possible reduced forms.

Therefore, the only reduced quadratic forms with $\Delta = -68$ presented as (a,b,c) are: $(3,-2,6)$, $(1,0,17)$, $(3,2,6)$, and $(2,2,9)$.

(b) Let $K = \mathbb{Q}(\sqrt{-17})$. Because $-17 \equiv 3 \pmod 4$ we know that $\mathcal{O}_K = \mathbb{Z}[\sqrt{-17}]$. I claim that,

$$\begin{aligned}(5) &= 5\mathbb{Z} \oplus 5\sqrt{-17}\mathbb{Z}\\ (2, 1+\sqrt{-17}) &= 2\mathbb{Z} \oplus (1+\sqrt{-17})\mathbb{Z}\\ (3, 1+\sqrt{-17}) &= 3\mathbb{Z} \oplus (1+\sqrt{-17})\mathbb{Z}\\ (3, 1-\sqrt{-17}) &= 3\mathbb{Z} \oplus (1-\sqrt{-17})\mathbb{Z}\end{aligned}$$

are representatives of the entire ideal class group of $\mathbb{Q}(\sqrt{-17})$ and are all prime ideals. I must justify the $\mathbb{Z}$-bases I wrote down, prove that these ideals are members of distinct ideal classes, show that there are at most 4 elements in $Cl(K)$, and prove that all these ideals are prime.

First, there is an injection from the ideal class group into the set of strong equivalence classes of forms with discriminant, $\Delta_K = 4d = -68$. We have shown there are only four such strong equivalence classes which implies that $|Cl(K)| \leq 4$.

Consider the factorization of the primes less than Minkowski's Bound,

$$c_1 = \left(\frac{4}{\pi}\right)^{r_2} \frac{n!}{n^n}\sqrt{|\Delta_K|} = \frac{4}{\pi}\frac{1}{2}\sqrt{68} \approx 5.25$$

We know that there must be an ideal in each class with norm less than c_1 and thus its prime factors must lie above 2 or 3 or 5. First, $\left(\frac{-17}{5}\right) = \left(\frac{3}{5}\right) = -1$ so 5 is inert in K and thus, $I_1 = (5)$ is a prime ideal of $\mathcal{O}_K$. Also, $\mathcal{O}_K = \mathbb{Z}[\sqrt{-17}] = \mathbb{Z} \oplus \sqrt{-17}\mathbb{Z}$ so the basis for (5) is obvious. Computing the quadratic form of I_1,

$$q_1(X,Y) = \frac{\mathrm{N}_{\mathbb{Q}}^{K}\left(5X + 5\sqrt{-17}Y\right)}{\mathrm{N}(5)} = \frac{5^2X^2 + 5^2 \cdot 17Y^2}{5^2} = X^2 + 17Y^2$$

Noting that, $-17 \equiv 3(\mathrm{mod}4)$, we conclude that 2 is ramified in K so $(2) = (2, 1+\sqrt{-17})^2$. See Appendix for tedious calculations. Therefore, $(2, 1+\sqrt{-17})$ is a prime ideal since $\mathrm{N}(2) = 2^2$ so $\mathrm{N}(2, 1+\sqrt{-17}) = 2$ and thus, $(2, 1+\sqrt{-17})$ cannot be a product of primes and thus must be prime itself. The elements of $(2, 1+\sqrt{-17})$ are exactly those of the form $a + b\sqrt{-17}$ such that $a \equiv b \pmod 2$. Clearly, every element of this form is in $(2, 1+\sqrt{-17})$. Furthermore,

$$2(x + y\sqrt{-17}) + (1+\sqrt{-17})(z + w\sqrt{-17}) = (2x + z - 17w) + (2y + z + w)\sqrt{-17}$$

and therefore, $a = (2x + z - 17w)$ and $b = (2y + z + w)$ so $a \equiv z + w \pmod{2}$ and $b \equiv z + w \pmod{2}$ so every element satisfies the condition. Thus, we arrive at the basis,

$$(2, 1 + \sqrt{-17}) = 2\mathbb{Z} \oplus (1 + \sqrt{-17})\mathbb{Z}$$

which represents every element of this form via, $a + b\sqrt{-17} = 2k + (1 + \sqrt{-17})b$ where $k = \frac{1}{2}(a-b)$. Finally, we compute the quadratic form associated with $I_2 = (2, 1+\sqrt{-17})$.

$$q_2(X,Y) = \frac{\mathrm{N}^K_{\mathbb{Q}}\left(2X + (1 + \sqrt{-17})Y\right)}{\mathrm{N}(I_2)} = \frac{4X^2 + 4XY + 18Y^2}{2} = 2X^2 + 2XY + 9Y^2$$

Now, because $\left(\frac{-17}{3}\right) = \left(\frac{1}{3}\right) = 1$ we know that 3 is split in K. I claim that,

$$(3) = (3, 1 + \sqrt{-17})(3, 1 - \sqrt{-17}) = I_3^+ I_3^-$$

as before, see Appendix for the factorization. The elements of $(3, 1 \pm \sqrt{-17})$ are exactly those of the form $a + b\sqrt{-17}$ such that $a \equiv \pm b \pmod{3}$. Clearly, every element of this form is in $(3, 1 \pm \sqrt{-17})$. Furthermore,

$$3(x + y\sqrt{-17}) + (1 \pm \sqrt{-17})(z + w\sqrt{-17}) = (3x + z \mp 17w) + (3y \pm z + w)\sqrt{-17}$$

and therefore, $a = (3x + z \mp 17w)$ and $b = (3y \pm z + w)$ so $a \equiv z \pm w \pmod{3}$ and $b \equiv \pm z + w \pmod{2}$ so $a \equiv \pm b \pmod{3}$. Thus, we arrive at the basis,

$$(3, 1 \pm \sqrt{-17}) = 3\mathbb{Z} \oplus (1 \pm \sqrt{-17})\mathbb{Z}$$

which represents every element of this form via, $a+b\sqrt{-17} = 3k+(1\pm\sqrt{-17})(\pm b)$ where $k = \frac{1}{3}(a \mp b)$. Now, both of these ideals are not the entire ring so they must have norms greater than 1. However, $\mathrm{N}(3) = 3^2$ which implies that $\mathrm{N}^K_{\mathbb{Q}}\left(I_3^+\right) = \mathrm{N}^K_{\mathbb{Q}}\left(I_3^{-2}\right) = 3$. Thus, both ideals must be prime otherwise they would factor as a product of prime ideals and could not have prime norm. Finally, we compute the quadratic form associated with $I_3^\pm = (3, 1 \pm \sqrt{-17})$.

$$q_3^\pm(X,Y) = \frac{\mathrm{N}^K_{\mathbb{Q}}\left(3X + (1 \pm \sqrt{-17})Y\right)}{\mathrm{N}(I_3^\pm)} = \frac{9X^2 \pm 6XY + 18Y^2}{3} = 3X^2 \pm 2XY + 6Y^2$$

Now, I will show that no two of the forms,

$$\begin{aligned} q_1(X,Y) &= X^2 + 17Y^2 \\ q_2(X,Y) &= 2X^2 + 2XY + 9Y^2 \\ q_3(X,Y) &= 3X^2 + 2XY + 6Y^2 \end{aligned}$$

are weakly equivalent except for q_3^+ and q_3^- which are clearly equivalent under $X \mapsto -X$. It suffices to find, for each form, a number which can only be represented by that form. I claim that,

$q_1(X,Y)$ is the only form to represent 1
$q_2(X,Y)$ is the only form to represent 2
$q_3(X,Y)$ is the only form to represent 3

First, the easy step, $q_1(1,0) = 1$ and $q_2(1,0) = 2$ and $q_3(1,0) = 3$. Second, $q_2(X,Y) = 2X^2 + 2XY + 9Y^2 = (X+Y)^2 + X^2 + 8Y^2 \neq 1,3$ because all the terms are positive and $1,3 < 8$ forcing $Y = 0$ but $q_2(X,0) = 2X^2 \neq 1,3$ because they are odd. Also, $q_3^{\pm}(X,Y) = (X \pm Y)^2 + 2X^2 + 5Y^2 \neq 1,2$ because all the terms are positive which forces $Y = 0$ since $5 > 1,2$ and then $q_3^{\pm}(X,Y) = 3X^2 \neq 1,2$ because $3 \nmid 1,2$. Finally, $q_1(X,Y) = X^2 + 17Y^2 \neq 2,3$ because $17 > 2,3$ so $Y = 0$ but 2 and 3 are not squares so $q_1(X,0) = X^2 \neq 2,3$. Therefore, no two of these forms can be weakly equivalent because otherwise they would represent the same sets of integers. By Lemma **??**, this implies that I_1, I_2, and I_3 are distinct in the class group.

Furthermore, $I_2^2 = (2)$ but we have shown that $I_2 \not\sim I_1 = (5)$ so I_2 cannot be principal. Therefore, I_2 has order 2 in the class group. However, we have shown that I_1 and I_2 and I_3^+ are representatives of distinct ideal classes. Thus, $|Cl(K)| > 2$ but $|Cl(K)| \leq 4$ and $Cl(K)$ contains an element of order 2. Therefore, $Cl(K)$ must be a group of order 4 else it would have order 3 and could not have an element of order 2. We have found three distinct representatives, namely, I_1, I_2, and I_3^+. There must exist a representative of the missing class with norm less than $c_1 \approx 5.25$. However, the only ideal of norm 1 is $\mathcal{O}_K = (1) \sim I_1$. Every ideal of norm 2 is a prime which lies above 2 and thus equals I_2. There are exactly two ideals of norm 3 both lying above 3, namely, I_3^+ and I_3^-. Every ideal of norm 4 is a product of primes lying above 2 and thus equal to $I_2^2 = (2) \sim I_1$. Finally, there are no ideals of norm 5 because 5 is inert so no primes except (5) lie above it but $\mathrm{N}(5) = 5^2$. Therefore, every ideal with norm less than c_1 is in the class of either I_1 or I_2 or I_3^+ except for possibly I_3^-. Thus, I_3^- must be a representative of the missing ideal class.

3. (a) Define,

$$\log_p(x) = \sum_{i=1}^{\infty} (-1)^{i-1} \frac{x^i}{i}$$

Suppose that $x \in p\mathbb{Z}_p$. Let $S_n = \sum_{i=1}^{n} (-1)^{i-1} \frac{x^i}{i}$. Now, for $n > m$, consider,

$$|S_n - S_m|_p = \left| \sum_{i=m+1}^{n} (-1)^{i-1} \frac{x^i}{i} \right|_p \leq \max \left\{ \left| \frac{x^{m+1}}{m+1} \right|_p, \cdots, \left| \frac{x^n}{n} \right|_p \right\} \leq p^{-m+\log_p(m)}$$

which holds by the ultrametric inequality. This is because $v_p(i) \leq \log_p(i)$ and $v_p(x) \geq 1$ since $x \in p\mathbb{Z}_p$ and $\forall y \in \mathbb{Z}_p$ we know that $v_p(y) \geq 0$. Thus, $v_p(\frac{x^i}{i}) \geq i - \log_p(i)$ which is a positive increasing function for $i > 1$. Furthermore, $p^{-m+\log_p(m)} \to 0$ as $m \to \infty$ so the difference $|S_n - S_m|_p \to 0$ for sufficiently large m and any $n > m$. Thus, S_n is Cauchy so it converges to an element of $\mathbb{Q}_p$ because $\mathbb{Q}_p$ is a complete metric space. However, we have shown that $_p(\frac{x^i}{i}) \geq i - \log_p(i) \geq 0$ so the valuation of every term in the sequence is positive. Therefore, $v_p(S_n) \geq 0$ because the p-adic integers are closed under addition. Alternatively, we know that $v_p(x+y) \geq \min\{v_p(x), v_p(y)\} \geq 0$ so by induction, we know that $v_p(S_n) \geq 0$. This implies that $v_p(\log_p(x)) = \lim\limits_{n\to\infty} v_p(S_n) \geq 0$ so $\log_p(x) \in \mathbb{Z}_p$ because it has positive valuation.

We know that $\ln(x)$ is an analytic function on $\mathbb{R}$ with the property that,

$$\ln((1+x)(1+y)) = \ln(1+x) + \ln(1+y)$$

Furthermore, the Taylor series of $f(x) = \ln(1+x)$ at $x = 0$ is given by,

$$T(x) = \sum_{i=1}^{\infty} (-1)^{i-1} \frac{x^i}{i}$$

because,

$$f^{(n)}(x) = (-1)^{n-1} \frac{(n-1)!}{(1+x)^n} \quad \text{so} \quad \frac{f^{(n)}(0)}{n!} x^n = (-1)^{n-1} \frac{x^n}{n}$$

On the interval $x \in (-1, 1)$ this series converges absolutely to $\ln(1+x)$. Now, for $x, y \in (-\frac{1}{4}, \frac{1}{4})$ we have $|x + y + xy| \le 1$ so the series converge,

$$\begin{aligned}&\ln((1+x)(1+y)) - \ln(1+x) - \ln(1+y) \\ &\qquad = \left(\sum_{i=1}^{\infty} (-1)^{i-1} \frac{(x+y+xy)^i}{i} \right) - \left(\sum_{i=1}^{\infty} (-1)^{i-1} \frac{x^i}{i} \right) - \left(\sum_{i=1}^{\infty} (-1)^{i-1} \frac{y^i}{i} \right) = 0\end{aligned}$$

Because the convergence is absolute, we can rearrange this sum without altering its limit. As formal power series, we denote,

$$\sum_{i,j} C_{i,j} x^i y^j = \left(\sum_{i=1}^{\infty} (-1)^{i-1} \frac{(x+y+xy)^i}{i} \right) - \left(\sum_{i=1}^{\infty} (-1)^{i-1} \frac{x^i}{i} \right) - \left(\sum_{i=1}^{\infty} (-1)^{i-1} \frac{y^i}{i} \right)$$

Absolute convergence implies that,

$$\sum_{i,j} C_{i,j} x^i y^j = \left(\sum_{i=1}^{\infty} (-1)^{i-1} \frac{(x+y+xy)^i}{i} \right) - \left(\sum_{i=1}^{\infty} (-1)^{i-1} \frac{x^i}{i} \right) - \left(\sum_{i=1}^{\infty} (-1)^{i-1} \frac{y^i}{i} \right) = 0$$

However, any smooth function can be represented as a power series in exactly one way. Therefore, $C_{i,j} = 0$ identically. Therefore, the formal power series is also identically zero. Now, take $x, y \in p\mathbb{Z}_p$. Then, $x + y + xy \in p\mathbb{Z}_p$ so $\log_p((1+x)(1+y)) = \log_p(1 + x + y + xy)$ converges. However,

$$\begin{aligned}&\log_p((1+x)(1+y)) - \log_p(1+x) - \log_p(1+y) \\ &\qquad = \left(\sum_{i=1}^{\infty} (-1)^{i-1} \frac{(x+y+xy)^i}{i} \right) - \left(\sum_{i=1}^{\infty} (-1)^{i-1} \frac{x^i}{i} \right) - \left(\sum_{i=1}^{\infty} (-1)^{i-1} \frac{y^i}{i} \right) \\ &\qquad = \sum_{i,j} C_{i,j} x^i y^j = 0\end{aligned}$$

Thus, $\log_p((1+x)(1+y)) = \log_p(1+x) + \log_p(1+y)$.

(b) First, note that,

$$\binom{2n}{n} = \frac{(2n)!}{n!^2} = \frac{1}{n!} \frac{(2n)!}{n!} = \frac{2^n}{n!} \cdot \frac{1 \cdot 2 \cdots 2n}{2 \cdot 4 \cdots 2n} = \frac{2^n}{n!} (1 \cdot 3 \cdot 5 \cdots 2n - 1) = \frac{2^n (2n-1)!!}{n!}$$

We will now apply the theorem that a sequence, $a_n \in \mathbb{Z}_p$ satisfies

$$\sum_{n=1}^{\infty} a_n \text{ converges} \iff \lim_{n \to \infty} a_n = 0$$

Therefore, for $x \in 1 + p\mathbb{Z}_p$ let $x = z + 1$ with $z \in \mathbb{Z}_p$ and take,

$$a_n = \frac{(-1)^{n-1}}{n}\binom{2n-2}{n-1}\left(\frac{x-1}{4}\right)^n = (-1)^{n-1}\frac{2^{n-1}(2n-3)!!}{n!}\frac{z^n}{2^{2n}} = (-1)^{n-1}\frac{(2n-3)!!}{2^{n+1}n!}z^n$$

Now, $v_p(a_n) = v_p((2n-3)!!) + nv_p(z) - v_p(2^{n+1}) - v_p(n!) \geq n - \frac{n}{p-1}$ where $v_p(2^{n+1}) = 0$ because p is odd and $v_p(z) \geq 1$ because $z \in p\mathbb{Z}_p$. Also, $v_p(n!) \leq \frac{n}{p-1}$ which can be demonstrated by decomposing, the valuation into the set of elements that give at least one factor plus the set of elements that give at lest two factors and so on. A given element k appears in this sum exactly $v_p(k)$ of times. Thus,

$$\begin{aligned} v_p(n!) &= |\{k \leq n \mid v_p(k) \geq 1\}| + |\{k \leq n \mid v_p(k) \geq 2\}| + \cdots + |\{k \leq n \mid v_p(k) \geq r)\}| \\ &\leq \frac{n}{p} + \frac{n}{p^2} + \cdots + \frac{n}{p^r} \leq \frac{n}{p}\left(1 + \frac{1}{p} + \frac{1}{p^2} + \cdots + \frac{1}{p^r}\right) \leq \frac{n}{p}\cdot\frac{1}{1-\frac{1}{p}} = \frac{n}{p-1} \end{aligned}$$

Therefore, $v_p(a_n) \geq \frac{p-2}{p-1}n \to \infty$ because $p > 2$. Thus, $|a_n|_p = p^{-v_p(a_n)} \to 0$. Therefore, the sum,

$$\sum_{n=1}^{\infty} a_n = \sum_{n=1}^{\infty}\frac{(-1)^{n-1}}{n}\binom{2n-2}{n-1}\left(\frac{x-1}{4}\right)^n$$

converges. Likewise,

$$y = 1 + 2\sum_{n=1}^{\infty} a_n = 1 + 2\sum_{n=1}^{\infty}\frac{(-1)^{n-1}}{n}\binom{2n-2}{n-1}\left(\frac{x-1}{4}\right)^n$$

exists. Furthermore, we have shown that $v_p(a_n) \geq 0$ for all $n \geq 1$. Thereore, because $v_p(x+y) \geq \min\{v_p(x), v_p(y)\} \geq 0$ the sum must have positive valuation and thus is an element of $\mathbb{Z}_p$. Therefore, because $1, 2 \in \mathbb{Z}_p$ we know that $y \in Z_p$.

(c) We know that $\sqrt{x}$ is an anylitic function on $\mathbb{R}$ with the property that,

$$\sqrt{x}^2 = x$$

Furthermore, the taylor series of $f(x) = \sqrt{x}$ at $x = 1$ is given by,

$$\begin{aligned} T(x) &= \sum_{n=0}^{\infty}(-1)^{n-1}\frac{(2n-3)!!}{2^n n!}(x-1)^n = 1 + 2\sum_{n=1}^{\infty}(-1)^{n-1}\frac{(2n-3)!!}{2^{n+1}n!}(x-1)^n \\ &= 1 + 2\sum_{n=1}^{\infty}\frac{(-1)^{n-1}}{n}\binom{2n-2}{n-1}\left(\frac{x-1}{4}\right)^n \end{aligned}$$

because,

$$f^{(n)}(x) = (-1)^{n-1}\frac{(2n-3)!!}{2^n\, x^{n-1/2}} \quad \text{so} \quad \frac{f^{(n)}(1)}{n!}(x-1)^n = (-1)^{n-1}\frac{(2n-3)!!}{2^n n!}(x-1)^n$$

On the interval $x \in (0, 2)$ this series converges absolutely to $\sqrt{x}$. Therefore,

$$\sqrt{x}^2 - x = \left(1 + 2\sum_{n=1}^{\infty}\frac{(-1)^{n-1}}{n}\binom{2n-2}{n-1}\left(\frac{x-1}{4}\right)^n\right)^2 - x = 0$$

Because the convergence is absolute, we can rearage this sum without altering its limit. As formal power series, we denote,

$$\sum_{i,j} C_{i,j} x^i y^j = \left(1 + 2\sum_{n=1}^{\infty} \frac{(-1)^{n-1}}{n} \binom{2n-2}{n-1} \left(\frac{x-1}{4}\right)^n\right)^2 - x$$

Absolute convergence implies that,

$$\sum_{i,j} C_{i,j} x^i y^j = \sqrt{x}^2 - x = 0$$

However, any smooth function can be represented as a power series in exactly one way. Therefore, $C_{i,j} = 0$ identically. Therefore, the formal power series is also identically zero. Now, take $x \in 1 + p\mathbb{Z}_p$. Then, we know that the sum converges absolutely, so,

$$\begin{aligned} y^2 - x &= \left(1 + 2\sum_{n=1}^{\infty} \frac{(-1)^{n-1}}{n} \binom{2n-2}{n-1} \left(\frac{x-1}{4}\right)^n\right)^2 - x \\ &= \sum_{i,j} C_{i,j} x^i y^j = 0 \end{aligned}$$

Thus, $y^2 = x$.

4. Let $K_p = \mathbb{Q}(\zeta_p)$ with $n = [\mathbb{Q}(\zeta_p) : \mathbb{Q}] = p - 1$ and for $q \neq p$ let $D_q \subset Gal(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ be the decomposition group at q. In particular, by Dedekind prime factorization, write,

$$q\mathcal{O}_{K_p} = \prod_{i=1}^{g} \mathfrak{p}_i^{e_i}$$

where for all i we have $e_i = e$ and $f_i = [\mathcal{O}_{K_p}/\mathfrak{p}_i : \mathbb{F}_q] = f$ because the extension is Galois. Then, by taking norms, we know that $n = efg$. The decomposition group of each prime is, $D_q \cong D_{\mathfrak{p}_i} = \{\sigma \in Gal(K/\mathbb{Q}) \mid \sigma(\mathfrak{p}_i) = \mathfrak{p}_i\}$ and satisfies, by the Orbit-Stabilizer theorem, $|D_q| = |D_{\mathfrak{p}_i}| = |G|/|\text{Orb}(\mathfrak{p}_i)| = n/g = ef$.

Define $c : \mathbb{N} \to \mathbb{C}^\times$ by $c(1) = 1$ and for $n > 1$ take $c(n) = 1$ if $p \not| n$ and every prime $q \mid n$ satisfies $|D_q| = 2$. Otherwise let $c(n) = 0$.

(a) c is a multiplicative function. Suppose that $c(a) = c(b) = 1$ then every prime factor q of a and of b satisfies $|D_q| = 2$. However, these are all of the prime factors of ab so $c(ab) = 1 = c(a)c(b)$. Also, if $c(a) = 0$ then there exists some $q \mid a$ such that $|D_q| \neq 2$. Therefore, $q \mid ab$ and $|D_q| \neq 2$ so $c(ab) = 0 = c(a)c(b)$. The case with $c(b) = 0$ is identical. Finally, if $a = 1$ then $c(1 \cdot b) = c(b) = c(1)c(b)$ since $c(1) = 1$. Thus, c is multiplicative.

(b) Define the function,

$$D(s) = \sum_{n=1}^{\infty} \frac{c(n)}{n^s}$$

Observing that $|c(n)| \leq 1$, consider the sum of absolute values where $\sigma = \text{Re}(s)$,

$$\sum_{n=1}^{\infty} \left|\frac{c(n)}{n^s}\right| \leq \sum_{n=1}^{\infty} \frac{1}{|n^s|} = \sum_{n=1}^{\infty} \frac{1}{n^\sigma} = \zeta(\sigma)$$

For $\text{Re}(s) = \sigma > 1$, we know that $\zeta(\sigma)$ converges so the sum,

$$\sum_{n=1}^{\infty} \left| \frac{c(n)}{n^s} \right|$$

is a bounded monotonically increasing sequence and is therefore convergent. Thus, $D(s)$ converges absolutely on the half-plane, $\text{Re}(s) > 1$.

(c) To show that $D(s)$ cannot extend to a continuous function on $(1-\epsilon, \infty)$ for any $\epsilon > 0$ it suffices to show that $D(s)$ has a pole at $s = 1$ because if $D(s)$ were continuous on $(1-\epsilon, \infty)$ then it would be continuous on $[1-\epsilon/2, 1]$ which is compact. In that case, $D(s)$ must be bounded on $[1-\epsilon/2, 1]$ and, in particular, cannot have a pole at $s = 1$.

Let $A = \{q \in \mathbb{Z}^+ \mid q \neq p \text{ and } |D_q| = 2\}$ and note that $\forall q \in A : c(q) = 1$. Therefore,

$$\sum_{p \in A} \frac{1}{p^s} \leq \sum_{n=1}^{\infty} \frac{c(n)}{n^s}$$

To prove that $D(s)$ has a pole at $s = 1$, it suffices to prove that A has nonzero Dirichlet density. This follows because if

$$0 < \lim_{s \to 1^+} \frac{\sum_{p \in A} \frac{1}{p^s}}{\log\left(\frac{1}{s-1}\right)} \leq \lim_{s \to 1^+} \frac{\sum_{n=1}^{\infty} \frac{c(n)}{n^s}}{\log\left(\frac{1}{s-1}\right)}$$

then there would exist $C \in \mathbb{R}^+$ such that $D(s) = \sum_{n=1}^{\infty} \frac{c(n)}{n^s} \sim C \log\left(\frac{1}{s-1}\right)$ which implies that $D(s)$ has a pole at $s = 1$.

By cyclotomic reciprocity, since $q \neq p$, we know that q is unramified so $e = 1$ and $f = \text{ord}_p(q)$, the multiplicative order of $q \in \mathbb{F}_p$, i.e. the least positive integer such that $q^f \equiv 1 \pmod{p}$. Therefore, $|D_q| = ef = \text{ord}_p(q)$ so $|D_q| = 2$ if and only if $q^2 \equiv 1 \pmod{p}$ and $q \not\equiv 1 \pmod{p}$. However, $p \mid q^2 - 1$ if and only if $p \mid q - 1$ or $p \mid q + 1$. Thus, $\text{ord}_p(q) = 2$ if and only if $q \equiv -1 \pmod{p}$. Therefore, the primes in A are exactly those primes that can be written in the form $q = pk - 1$. Since p and -1 are coprime, by Dirichlet's theorem on primes in an arithmetic progression, the set A has Dirichlet density equal to $\frac{1}{\phi(p)} = \frac{1}{p-1} > 0$ which proves the proposition.

Lemmas

Lemma 0.1. *If $I \sim J$ are equivalent ideals in $\mathcal{O}_K$ where $K = \mathbb{Q}(\sqrt{-d})$ the quadratic forms q_I and q_J given by $q_I(X, Y) = \frac{\text{N}_{\mathbb{Q}}^K(b_1X + b_2Y)}{\text{N}(I)}$ where $\{b_1, b_2\}$ is a $\mathbb{Z}$-basis of I, are weakly equvalent.*

Proof. Let $I = b_1\mathbb{Z} \oplus b_2\mathbb{Z}$ and $J = c_1\mathbb{Z} \oplus c_2\mathbb{Z}$ where these are $\mathbb{Z}$-bases. Suppose that $I \sim J$ so there exist $\alpha, \beta \in \mathcal{O}_K \backslash \{0\}$ such that $\alpha I = \beta J$. Thus, $\alpha b_1, \alpha b_2 \in \beta J$ so there exist $r, s, t, u \in \mathbb{Z}$ such that $\alpha b_1 = \beta(rc_1 + tc_2)$ and $\alpha b_2 = \beta(sc_1 + uc_2)$. Note that, $\alpha I = \beta J$ implies $\text{N}(\alpha)\text{N}(I) = \text{N}(\beta)\text{N}(J)$

which is equivalent to, $\mathrm{N}^K_{\mathbb{Q}}(\alpha)\,\mathrm{N}(I) = \mathrm{N}^K_{\mathbb{Q}}(\beta)\,\mathrm{N}(J)$. Now consider,

$$\begin{aligned}
q_J(rX+sY, tX+uY) &= \frac{\mathrm{N}^K_{\mathbb{Q}}\left((rX+sY)c_1 + (tX+uY)c_2\right)}{\mathrm{N}(J)} = \frac{\mathrm{N}^K_{\mathbb{Q}}\left(\beta(rc_1+tc_2)X + \beta(sc_1+uc_2)Y\right)}{\mathrm{N}^K_{\mathbb{Q}}(\beta)\,\mathrm{N}(J)} \\
&= \frac{\mathrm{N}^K_{\mathbb{Q}}\left(\alpha b_1 X + \alpha b_2 Y\right)}{\mathrm{N}(J)} = \frac{\mathrm{N}^K_{\mathbb{Q}}\left(b_1X+b_2Y\right)\mathrm{N}^K_{\mathbb{Q}}(\alpha)}{\mathrm{N}(J)\mathrm{N}^K_{\mathbb{Q}}(\beta)} = \frac{\mathrm{N}^K_{\mathbb{Q}}\left(b_1X+b_2Y\right)\mathrm{N}^K_{\mathbb{Q}}(\alpha)}{\mathrm{N}(I)\mathrm{N}^K_{\mathbb{Q}}(\alpha)} \\
&= \frac{\mathrm{N}^K_{\mathbb{Q}}\left(b_1X+b_2Y\right)}{\mathrm{N}(I)} = q_I(X,Y)
\end{aligned}$$

However, we can swap I and J and repeat the argument to write $q_I(r'X+s'Y, t'X+u'Y) = q_J(X,Y)$. Therefore, the transformation matrix,

$$g = \begin{pmatrix} r & s \\ t & u \end{pmatrix} \in \mathrm{GL}(2,\mathbb{Z})$$

must be invertible. Therefore, the forms q_I and q_J are weakly equivalent. In particular, they represent the same integers because either form can be written in terms of the other. □

Addendum

Lemma 0.2. *In $K = \mathbb{Q}(\sqrt{-17})$, the following hold,*

$$(2) = (2, 1+\sqrt{-17})^2$$

$$(3) = (3, 1+\sqrt{-17})(3, 1-\sqrt{-17})$$

Proof. Using the basis derived in 2(b), write, $(2, 1+\sqrt{-17}) = 2\mathbb{Z} \oplus (1+\sqrt{-17})\mathbb{Z}$, then any element of $(2, 1+\sqrt{-17})^2$ can be generated by sums of elements of the form,

$$\begin{aligned}
(2a+b+b\sqrt{-17})(2c+d+d\sqrt{-17}) &= (4ac+2ad+2bc+bd-17bd) + (2ad+2bc+bd+bd)\sqrt{-17} \\
&= 2(2ac+ad+bc-8bd) + 2(ad+bc+bd)\sqrt{-17} \in (2)
\end{aligned}$$

Therefore, $(2, 1+\sqrt{-17})^2 \subset (2)$. Also,

$$2 = [-11+3\sqrt{-17}][1+\sqrt{-17}] + [4-4\sqrt{-17}][-1+\sqrt{-17}] \in (2, 1+\sqrt{-17})^2$$

Thus, $(2) \subset (2, 1+\sqrt{-17})^2$ so $(2) = (2, 1+\sqrt{-14})^2$.

Likewise, using the basis derived in 2(b), write, $(3, 1 \pm \sqrt{-17}) = 3\mathbb{Z} \oplus (1+\sqrt{-17})\mathbb{Z}$, then any element of $(3, 1+\sqrt{-17})(3, 1-\sqrt{-17})$ can be generated by sums of elements of the form,

$$\begin{aligned}
(3a+b+b\sqrt{-17})(3c+d-d\sqrt{-17}) &= (9ac+3ad+3bc+bd+17bd) + (-3ad+3bc+bd-bd)\sqrt{-17} \\
&= 3(3ac+ad+bc+6bd) + 3(-ad+bc)\sqrt{-17} \in (3)
\end{aligned}$$

Therefore, $(3, 1+\sqrt{-17})(3, 1-\sqrt{-17}) \subset (3)$. Also,

$$3 = 3 \cdot [3 - [1-\sqrt{-17}]] + [1+\sqrt{-17}] \cdot (-3) \in (3, 1+\sqrt{-17})(3, 1-\sqrt{-17})$$

Thus, $(3) \subset (3, 1+\sqrt{-17})(3, 1-\sqrt{-17})$ so $(3) = (3, 1+\sqrt{-17})(3, 1-\sqrt{-17})$. □