1. (a) Let p be an odd prime. There is an isomorphism $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \to (\mathbb{Z}/p\mathbb{Z})^\times$, and this group is cyclic of order $p-1$. In particular, it has a unique subgroup H of index 2, namely the subgroup of squares in $(\mathbb{Z}/p\mathbb{Z})^\times$. By the Galois correspondence, $\mathbb{Q}(\zeta_p)/\mathbb{Q}$ has a unique quadratic subfield $K/\mathbb{Q}$ (the fixed field of H).

   Since $X^p - 1$ has distinct roots modulo q for any prime $q \neq p$, we see that any such prime q is unramified in $\mathbb{Q}(\zeta_p)$. Quite generally, if $L/E/\mathbb{Q}$ is a tower of number fields and q is unramified in L, then q is unramified in E (use that the ramification index is multiplicative in towers). It follows that any prime $q \neq p$ is unramified in K.

   We have seen in lectures that the quadratic extensions of $\mathbb{Q}$ have the form $\mathbb{Q}(\sqrt{d})$, where d is a square-free integer such that $d \neq 0, 1$. We have moreover seen that the primes ramified in $\mathbb{Q}(\sqrt{d})$ are precisely the divisors of $2d$ (if $d \equiv 2, 3 \bmod 4$) or the divisors of d (if $d \equiv 1 \bmod 4$). We see that $K = \mathbb{Q}(\sqrt{d})$, where d is the unique square-free integer which has p as its unique prime divisor and satisfies $d \equiv 1 \bmod 4$. This is $p^* = (-1)^{(p-1)/2}p$.

   (b) We make the following general observations: if L/E is an abelian extension of number fields and $P \subset \mathcal{O}_E$ is a non-zero prime ideal which is unramified in $\mathcal{O}_L$, then P splits completely in L if and only if $(P, L/E) = 1$. Indeed, P splits completely if and only if the residue degrees $f_{Q/P} = |D_{Q/P}|$ are 1. Since $D_{Q/P}$ is generated by $(P, L/E)$, this is equivalent to $(P, L/E)$ being the identity element of $\mathrm{Gal}(L/E)$. Also, if $L/M/E$ is an intermediate extension, then $(P, M/E) = (P, L/E)|_M$. This follows from the definitions.

   In our case, we see that an odd prime $q \neq p$ splits in K if and only if $(q, K/\mathbb{Q}) = (q, \mathbb{Q}(\zeta_p)/\mathbb{Q})|_K = 1$, if and only if $(q, \mathbb{Q}(\zeta_p)/\mathbb{Q}) \in H$. We proved in lectures that $(q, \mathbb{Q}(\zeta_p)/\mathbb{Q})$ corresponds in $(\mathbb{Z}/p\mathbb{Z})^\times$ to the residue class of $q \bmod p$. Thus q splits in K if and only if $q \bmod p \in H$. Since H is the subgroup of squares, this is equivalent to $(\frac{q}{p}) = 1$ (by the definition of the Legendre symbol).

   On the other hand, we proved in lectures that q splits in K if and only if the polynomial $X^2 - p^*$ has a root modulo q, if and only if $(\frac{p^*}{q}) = 1$. We see that $(\frac{q}{p}) = (\frac{p^*}{q})$, as required.

2. Let $K \subset \mathbb{Q}(\zeta_N)$ be a subfield such that $C_{K/\mathbb{Q}}|(M)$. We must show that $K \subset \mathbb{Q}(\zeta_M)$. By the Galois correspondence, this is equivalent to showing that $\mathrm{Gal}(\mathbb{Q}(\zeta_N)/K)$ contains $\mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q}(\zeta_M))$. Under the isomorphism $\mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q}) \cong (\mathbb{Z}/N\mathbb{Z})^\times$, this subgroup corresponds to the subgroup $\ker((\mathbb{Z}/N\mathbb{Z})^\times \to (\mathbb{Z}/M\mathbb{Z})^\times)$.

By the Chinese remainder theorem, it is enough to show that if $p|N$ is a prime, and the exact powers of p dividing N, M are p^a, p^b, then $\mathrm{Gal}(\mathbb{Q}(\zeta_N)/K)$ contains $\mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q}(\zeta_{Np^{b-a}}))$. If Q is a prime ideal of $\mathcal{O}_{\mathbb{Q}(\zeta_N)}$ lying above p, then $\mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q}(\zeta_{Np^{b-a}}))$ is a subgroup of $I_{Q/(p)}$. Using Sheet 3, 6(c), we see that it is in fact the subgroup of $I_{Q/(p)}$ corresponding to the upper ramification group G^b of $G = \mathrm{Gal}(\mathbb{Q}(\zeta_N)_Q/\mathbb{Q}_p)$.

It remains to interpret the condition $C_{K/\mathbb{Q}}|(M)$. This implies that the p-part of $C_{K/\mathbb{Q}}$ divides p^b, or equivalently that $(G/H)^b = \{1\}$, where $P = Q \cap \mathcal{O}_K$ and $H = \mathrm{Gal}(\mathbb{Q}(\zeta_N)_Q/K_P)$. Using the compatibility of upper ramification groups with passage to quotient, we see that this is precisely the condition $G^b \subset H$. Since H may be identified with the subgroup $I_{Q/P}$ of $\mathrm{Gal}(\mathbb{Q}(\zeta_N)/K)$, this is what we needed to show.

3. (a) We assume $E/\mathbb{Q}_p$ is a Galois, totally ramified extension of degree p, where p is an odd prime. Let $f(X) \in \mathbb{Z}_p[X]$ be the minimal polynomial of a uniformizer π_E. Then $f(X)$ is Eisenstein of degree p. Writing $f(X) = X^p + a_1X^{p-1} + \cdots + a_p$, we have $a_i \in p\mathbb{Z}_p$ and $a_p \in p\mathbb{Z}_p^\times$, hence $f'(X) = pX^{p-1} + \cdots + iX^{i-1} + a_{p-1}$, hence $f'(\pi_E) = p\pi_E^{p-1} + \cdots + i\pi_E^{i-1} + \cdots + a_{p-1}$. We observe that the values under v_E of the p terms in the sum defining $f'(\pi_E)$ are distinct modulo p, so distinct. Therefore $v_E(f'(\pi_E))$ equals the minimum of $v_E(p\pi_E^{p-1}), \ldots, v_E(a_{p-1})$. In particular, it is at most $2p-1$.

On the other hand, we have $f(X) = \prod_{\sigma\in G}(X - \sigma(\pi_E))$, where $G = \mathrm{Gal}(E/\mathbb{Q}_p)$, hence $f'(\pi_E) = \prod_{\sigma\neq 1}(\pi_E - \sigma(\pi_E))$, hence $v_E(f'(\pi_E)) = \sum_{\sigma\neq 1} i_G(\sigma)$. Let $r \geq 1$ be the maximal integer such that $G_r \neq 1$. Then $G_r = G$ is cyclic of order p, and $v_E(f'(\pi_E)) = (p-1)(r+1)$. Using the previous paragraph, we see that we must have $r = 1$, hence $G = G_1$, $G_2 = \{1\}$. It follows that the upper ramification groups are given by $G^{[0,1]} = G$, $G^{(1,\infty)} = \{1\}$, hence $C_{E/\mathbb{Q}} = (p^2)$.

(b) Let $K_1, K_2/\mathbb{Q}$ be distinct Galois extensions, abelian of degree p, ramified only at p. Then there is an embedding $\mathrm{Gal}(K_1\cdot K_2/\mathbb{Q}) \to \mathrm{Gal}(K_1/\mathbb{Q}) \times \mathrm{Gal}(K_2/\mathbb{Q}) \cong (\mathbb{Z}/p\mathbb{Z})^2$, given by sending an automorphism to its restriction to each subfield. If it is not surjective then the degree of $K_1\cdot K_2/\mathbb{Q}$ must divide p, contradicting $K_1 \neq K_2$. By Sheet 2, 7, p is the only prime which ramifies in $K_1 \cdot K_2$.

We claim that $K_1\cdot K_2/\mathbb{Q}$ is totally ramified. Let Q be a prime ideal lying above p; we must show that $I_{Q/(p)} = \mathrm{Gal}(K_1 \cdot K_2/\mathbb{Q})$. The fixed field $(K_1 \cdot K_2)^{I_{Q/(p)}}$ is a proper subfield of $K_1 \cdot K_2/\mathbb{Q}$ which is

everywhere unramified over $\mathbb{Q}$. We are given that no such proper extension exists, so we have $(K_1 \cdot K_2)^{I_{Q/(p)}} = \mathbb{Q}$, hence (by the Galois correspondence) $I_{Q/(p)} = \mathrm{Gal}(K_1 \cdot K_2/\mathbb{Q})$.

(c) The first part of the question shows that if now $G = \mathrm{Gal}(K_1 \cdot K_2/\mathbb{Q})$, then $G^{[0,1]} = G$ and $G^{(1,\infty)} = \{1\}$. Indeed, it suffices to check these equalities after projection to any order p quotient of G. On the other hand, we have shown in lectures that the quotient groups at jumps in the ramification filtration inject either into $\mathbb{F}_p^\times$ or $\mathbb{F}_p$ (i.e. either the units in the residue field or the additive group of the residue field). Neither of these groups is large enough to contain $(\mathbb{Z}/p\mathbb{Z})^2$, so we get a contradiction.

(d) We have proved that there is at most one extension, so we just need to exhibit one. On Sheet 3 we show that $\mathbb{Q}(\zeta_{p^2}/\mathbb{Q})$ is totally ramified at p, hence so is its degree p subfield.

4. We recall that the relation $\mathfrak{m} \leq \mathfrak{n}$ means $\mathfrak{m}_0|\mathfrak{n}_0$ and $\mathfrak{m}_\infty \subset \mathfrak{n}_\infty$. In particular, we have $\mathscr{I}(\mathfrak{n}_0) \subset \mathscr{I}(\mathfrak{m}_0)$ and $K_\mathfrak{n} \subset K_\mathfrak{m}$, hence $\mathscr{P}_\mathfrak{n} \subset \mathscr{P}_\mathfrak{m}$. Since $H(\mathfrak{m}) = \mathscr{I}(\mathfrak{m}_0)/\mathscr{P}_\mathfrak{m}$, by definition, we see that the inclusion $\mathscr{I}(\mathfrak{n}_0) \subset \mathscr{I}(\mathfrak{m}_0)$ induces by passage to quotient a homomorphism $H(\mathfrak{n}) \to H(\mathfrak{m})$.

   To show that this is surjective, it is enough to show that for any non-zero ideal $\mathfrak{a} \subset \mathcal{O}_K$, prime to $\mathfrak{m}_0$, we can find an element $\alpha \in K_\mathfrak{m}$ such that $\alpha\mathfrak{a}$ is a fractional ideal of $\mathcal{O}_K$ prime to $\mathfrak{n}_0$. By the Chinese remainder theorem, we can find an element $\beta \in \mathcal{O}_K \cap K_\mathfrak{m}$ such that $(\beta) = \mathfrak{a}\mathfrak{b}$, where $\mathfrak{b} \subset \mathcal{O}_K$ is a non-zero ideal prime to $\mathfrak{n}_0$. On the other hand, we know from an argument given in lectures that we can find $\gamma \in \mathcal{O}_K \cap K_\mathfrak{m}$ such that (γ) is a non-zero ideal prime to $\mathfrak{n}_0$, and for every $\tau \in \mathfrak{m}_\infty$, $\tau(\beta\gamma) > 0$. It follows that $\alpha = (\beta\gamma)^{-1}$ has the desired property (note in particular that $K_\mathfrak{m}$ is a group, so $\alpha \in K_\mathfrak{m}$ by construction).

5. Let $K = \mathbb{Q}(\sqrt{3})$. We will use class field theory to determine whether there exists a degree 3 abelian extension ramified only at the prime ideals of K above 5. Note that the polynomial $X^2 - 3$ is irreducible over $\mathbb{F}_5$, so there is a unique prime ideal $\mathfrak{p} \subset \mathcal{O}_K$ above 5, namely $5\mathcal{O}_K$. If L/K is a Galois degree 3 extension ramified only at $\mathfrak{p}$, then $\mathfrak{m}_{L/K} \leq \mathfrak{m}_r = (\mathfrak{p}^r, \mathrm{Hom}_\mathbb{Q}(K, \mathbb{R}))$ for some $r \geq 1$. We therefore need to decide whether or not there exists $r \geq 1$ such that $H(\mathfrak{m}_r)$ has order divisible by 3.

   The ideal class group H_K is trivial, and a fundamental unit is $\epsilon =$

$2+\sqrt{3}$. Therefore the ray class group $H(\mathfrak{m}_r)$ is isomorphic to the quotient of the group $(\mathcal{O}_K/\mathfrak{p}^r)^\times \times \{\pm 1\}^2$ by the subgroup generated by -1 and ϵ. We see that $\ker(H(\mathfrak{m}_r) \to H((\mathfrak{p},\emptyset)))$ has order prime to 3, so it is enough to decide whether $H((\mathfrak{p},\emptyset))$ has order divisible by 3. The group $H((\mathfrak{p},\emptyset))$ is isomorphic to the quotient of the group $(\mathcal{O}_K/\mathfrak{p})^\times$ (which is cyclic of order 24) by the subgroup generated by -1 and ϵ.

We calculate $\epsilon^2 \bmod \mathfrak{p} = 4+3+4\sqrt{3} = 2+4\sqrt{3}$ and $\epsilon^3 \bmod \mathfrak{p} = (2+4\sqrt{3})(2+\sqrt{3}) = 4+12+10\sqrt{3} = 1$, hence $\epsilon \bmod \mathfrak{p}$ has order 3. We find that $H((\mathfrak{p},\emptyset)) \cong (\mathcal{O}_K/\mathfrak{p})^\times/\langle -1,\epsilon\rangle$ is cyclic of order 4, and hence that there is no cyclic degree 3 extension of K ramified only at $\mathfrak{p}$.

6. (a) The condition that u is a non-square says exactly that $f(X) = X^2-u$ is irreducible in $K[X]$. The polynomial $f(X)$ has discriminant $4u$. If $2 \notin \mathfrak{p}$ and $u \notin \mathfrak{p}$ then $f(X)$ has distinct roots modulo $\mathfrak{p}$, and so $\mathfrak{p}$ is unramified in $L = K(\sqrt{u})$.

   Now suppose instead that $2 \in \mathfrak{p}$ and $u = b^2-4c$ for some $b, c \in \mathcal{O}_K$. Then L can also be realized as the splitting field of the polynomial $g(X) = X^2+bX+c$. This polynomial has distinct roots modulo $\mathfrak{p}$, and so $\mathfrak{p}$ is again unramified in L.

   (b) Let $K = \mathbb{Q}(\sqrt{-14})$, $L = K(\sqrt{2\sqrt{2}-1})$. To show that L/K is the Hilbert class field of K, we need to check that L/K is an abelian, everywhere unramified extension, and that $[L:K] = \#H_K$. We first calculate the structure of the group H_K using the theory of binary quadratic forms. The ring $\mathcal{O}_K$ has discriminant $-14 \times 4 = -56$, and we check by hand that there are exactly 4 reduced forms of this discriminant: they are x^2+14y^2, $2x^2+7y^2$, and $3x^2 \pm 2xy + 5y^2$. It follows that we have $H_K \cong \mathbb{Z}/4\mathbb{Z}$ or $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Recalling the characterization of reduced forms representing classes of order 2, we see that we must have $H_K \cong \mathbb{Z}/4\mathbb{Z}$ (there are 2, not 3, classes of order exactly 2).

   Let $\beta = 2\sqrt{2}-1$, and let γ be a square root of β. Let $\beta' = -2\sqrt{2}-1$, so that $\beta\beta' = -7$. Then γ is a root of the polynomial X^4+2X^2-7, which is irreducible. Indeed, this is so if and only if β is not a square in $\mathbb{Q}(\sqrt{2})$; but the prime 7 is unramified in $\mathbb{Q}(\sqrt{2})$ and factors as $7\mathcal{O}_{\mathbb{Q}(\sqrt{2})} = \mathfrak{p}\mathfrak{p}'$; after relabeling we must therefore have $\mathfrak{p} = (\beta)$, $\mathfrak{p}' = (\beta')$. In particular, β cannot be a square in this field (by unique factorization of ideals).

   Let $E = \mathbb{Q}(\gamma)$ so that $L = E \cdot K$. Then $E/\mathbb{Q}$ is not Galois, because e.g. it admits both real and complex embeddings. However, L/K

is Galois: if M/K denotes the Galois closure, and $\tau \in \mathrm{Gal}(M/K)$, then $\tau(K(\sqrt{2})) = K(\sqrt{2})$, and $\tau(\gamma)$ is a square root of $\tau(\beta)$. If $\tau(\beta) = \beta$ then $\tau(\gamma) = \pm\gamma$, so $\tau(L) = L$. If $\tau(\beta) = \beta'$, then $\tau(\gamma)$ is a square root of β', and then $(\sqrt{-7}/\tau(\gamma))^2 = -7/\beta' = \beta$, showing that $\tau(L) = L$ in this case also (note that $\sqrt{-7} \in K(\sqrt{2})$). Since τ was arbitrary, this shows that L/K is normal, hence indeed Galois as claimed.

We thus see that L/K is an abelian extension of degree 4. It remains to show that L/K is everywhere unramified. Using the first part of the exercise, we see that $K(\sqrt{2})/K$ is everywhere unramified, because it can also we written as $K(\sqrt{-7})/K$. We can write $(\beta) = \mathfrak{q}^2$ and $(\beta') = (\mathfrak{q}')^2$, where $\mathfrak{q}, \mathfrak{q}'$ are prime ideals of $K(\sqrt{-7})$ lying above $\mathfrak{p}$ and $\mathfrak{p}'$, respectively. The extension $L/K(\sqrt{2})$ is unramified at the primes above 2, because we can write $\beta = (1+\sqrt{2})^2 - 4$. It is unramified at the primes above 7, namely $\mathfrak{q}$ and $\mathfrak{q}'$, because it is unramified at $\mathfrak{q}'$ and L/K is Galois, $\mathfrak{q}$ and $\mathfrak{q}'$ being interchanged by the non-trivial element of $\mathrm{Gal}(K(\sqrt{2})/K)$. This completes the proof.

7. (a) By assumption $d < 0$ is a square-free integer such that $d \equiv 3 \bmod$. Then the associated discriminant $D = \operatorname{disc} \mathcal{O}_K$ is $4d$. The group $H_K[2]$ is an $\mathbb{F}_2$-vector space of cardinality equal to the number of reduced forms of discriminant D which have order 2 in the class group $H(\mathcal{O}_K)$; we need to show that this equals 2^μ, where μ is the number of prime divisors of d. Recall that a reduced form $ax^2 + bxy + cy^2$ has order 2 in H_K if and only if we have either $b = 0$, $a = b$, or $a = c$. There are three (distinct) kinds:

   i. $f(x, y) = ax^2 + cy^2$, with $c \geq a \geq 0$ and $\operatorname{disc} f = -4ac$.
   ii. $f(x, y) = ax^2 + axy + cy^2$, with $c \geq a \geq 0$ and $\operatorname{disc} f = a(a - 4c)$.
   iii. $f(x, y) = ax^2 + bxy + ay^2$, with $a \geq b \geq 0$ and $\operatorname{disc} f = (b - 2a)(b + 2a)$.

   We count the number of forms of each type. The squarefree integer $-d$ has 2^μ divisors, hence $2^{\mu-1}$ factorizations $-d = -ac$ with $c \geq a \geq 0$, hence there are $2^{\mu-1}$ forms of type (i).

   Forms of type (ii) correspond to factorizations $4d = a(a - 4c) = 2d_1(-2d_2)$, say (note that a and $a - 4c$ are necessarily both congruent to 2 mod 4 as d is odd), hence to factorizations $-d = d_1 d_2$. We then have $a = 2d_1$, $4c - a = 2d_2$, hence $a = 2d_1$, $c = (d_1 + d_2)/2$.

The corresponding form is reduced exactly when $c \geq a$, or equivalently $d_2 \geq 3d_1$.

Forms of type (iii) correspond to factorizations $4d = (b-2a)(b+2a) = (-2d_1)(2d_2)$, hence to factorizations $-d = d_1 d_2$. We then have $2a - b = 2d_1$, $2a + b = 2d_2$, hence $a = (d_1 + d_2)/2$ and $b = d_2 - d_1$. The corresponding form is reduced exactly when $a \geq b \geq 0$, or equivalently when $3d_1 \geq d_2$ and $d_2 \geq d_1$.

Noting that the possibility $3d_1 = d_2$ does not occur since d is square-free and $d \neq -3$, we see that the forms of type (ii) and (iii) together correspond to factorizations $-d = d_1 d_2$ with $d_2 \geq d_1$. There are $2^{\mu-1}$ of these, giving a total count of 2^μ reduced forms of discriminant D.

(b) The snake lemma shows that we have

$$\#H_K[2] = \#H_K/2H_K,$$

hence $H_K/2H_K \cong (\mathbb{Z}/2\mathbb{Z})^\mu$. By Galois theory and class field theory, this means that the maximal abelian everywhere unramified extension of K of exponent 2 has degree 2^μ. At this point it is useful to recall that the abelian extensions of $\mathbb{Q}$ of exponent 2 are in bijection with the finite subgroups $\Delta \subset \mathbb{Q}^\times/(\mathbb{Q}^\times)^2$, the bijection being given by $\Delta \mapsto \mathbb{Q}(\sqrt{\Delta})$.

If p is an odd prime, let $p^* = (-1)^{(p-1)/2}p$, so that the extension $\mathbb{Q}(\sqrt{p^*})/\mathbb{Q}$ is a quadratic extension ramified only at the prime p. Writing $p_1, \ldots, p_\mu$ for the primes dividing d, we define

$$H = K(\sqrt{p_1^*}, \ldots, \sqrt{p_\mu^*}) = \mathbb{Q}(\sqrt{d}, \sqrt{p_1^*}, \ldots, \sqrt{p_\mu^*}).$$

Then H/K is an abelian extension of degree 2^μ. It is everywhere unramified, because each extension $\mathbb{Q}_{p_i}(\sqrt{d}, \sqrt{p_i^*})/\mathbb{Q}_{p_i}(\sqrt{d})$ is unramified. It follows that H/K is the desired extension.

(c) Under the given hypotheses, $x^2 - dy^2$ is the principal form of discriminant $D = 4d$, and a prime $p \nmid 4d$ is represented by this form if and only if it splits in H. By construction, the field H is in fact abelian over $\mathbb{Q}$, and is a subfield of $\mathbb{Q}(\zeta_{-4d})$. Let $X = \mathrm{Gal}(\mathbb{Q}(\zeta_{-4d}/H)$. If $p \nmid 4d$ is a prime then p splits in $H/\mathbb{Q}$ if and only if $p \bmod -4d$ lies in X (same argument as in the solution to the first exercise on this sheet).

(d) We first list the reduced forms of discriminant $-420 = -4 \times 105 = -4 \times 3 \times 5 \times 7$. They are:

- Forms of type (i): x^2+105y^2, $3x^2+35y^2$, $5x^2+21y^2$, $7x^2+15y^2$.
- Forms of type (ii): $2x^2+2xy+53y^2$, $6x^2+6xy+19y^2$, $10x^2+10xy+13y^2$.
- Forms of type (iii): $11x^2+8xy+11y^2$.

In particular, all of these forms correspond to classes of order 2, so $H_K = H_K[2]$ and we are in the situation of part (c). By the discussion in lectures, a prime $p > 7$ is represented by some one of these forms if and only if p splits in $K = \mathbb{Q}(\sqrt{-105})$. A prime $p > 7$ is represented by a fixed form $f(x,y)$ if and only if $(p, H/\mathbb{Q}) = \phi_{H/K}([I_f])$, where $\phi_{H/K} : H_K \to \mathrm{Gal}(H/K)$ is the isomorphism of class field theory and $[I_f]$ is the ideal class corresponding to $f(x,y)$.

To interpret this concretely, let $G \subset (\mathbb{Z}/420\mathbb{Z})^\times$ be the subgroup fixing $H \subset \mathbb{Q}(\zeta_{420})$, and let $f(x,y) = 11x^2+8xy+11y^2$. This form represents the prime 11, so $(11, H/\mathbb{Q}) = \phi_{H/K}([I_f])$. Consequently another prime $p > 7$ is represented by $f(x,y)$ if and only if p mod 420 and 11 mod 420 lie in the same coset of G in $(\mathbb{Z}/420\mathbb{Z})^\times$. For example, $11+420 = 431$ is prime, and it is represented as $431 = f(-6,5)$. The other reduced forms can be treated using the same technique.