THE LOCAL LOSS AND THE SPARSE PLACES

Prerequisites. Local fields: decomposition groups, the degree $[E_v : \mathbb{Q}_\ell] = e_v f_v$, Frobenius elements [SLF, Ch. I, IV]; Legendre's formula $\mathrm{val}_\ell(n!) = \sum_{i\ge1} \lfloor n/\ell^i \rfloor$. From Chapter 33: Definition 33.3.1 (the sparse set Φ_b, $l_0(s)$), Problems 33.1.1, 33.1.2, 33.2.1 and 33.5.4, and the budget B of Definition 33.4.1; the construction of Φ_b in Chapter 4. Theorem 31.4.1. From Chapter 65: coefficient rings $\mathcal{O}$ and normalized lengths (Section 65.4), Definitions 65.4.6, 65.4.7 and 65.4.1. p-adic Hodge theory enters only through three results stated in the text.

The clearing bound cl_ℓ of Definition 65.4.1, which controls the denominators of projections onto lifts in Chapter 65, contains the term loc_ℓ, counted per unit of rank; a main summand of rank r' pays $r'\mathrm{loc}_\ell$ (Problem 65.4.1): the price of asking that the cocycles produced by a congruence be crystalline above ℓ. Why is this price the valuation of one integer, and why is the sum of $\mathrm{loc}_\ell \log \ell$ over all primes ℓ only of size $f(m/k)\, b \log b$, far below B? The bound at one place above ℓ is taken from the proof. What this sheet proves is the arithmetic around it: the sum over the places and rows, the integer whose valuation is the loss, the sparse places that keep the small primes cheap, and the sum over ℓ. For a prime ℓ and a positive integer n we write $\mathrm{val}_\ell(n)$ for the exponent of ℓ in n, the valuation val at ℓ.

66.1. The loss at one place

We use the data and the notation of Chapter 33: the field E with f infinite places, the scales, m, r, $k = r + 1 - m$, $t = 5r$, $M = p_0 p_1$, the gap $\Delta = 2r^8$, so $\Delta/2 = r^8$.

Definition 66.1.1. Let Int_b be the product of the integers i with $\max(0, b - 30(\Delta/2)^3) < i \le b + 30(\Delta/2)^3$. For a prime ℓ put

$$\mathrm{crys}_\ell := \mathrm{val}_\ell\big((2b)!\,\mathrm{Int}_b^{(\Delta/2)^3}\big), \qquad \mathrm{defect}_\ell := 10^6\,\frac{m}{k}\,\big(b\ \mathrm{val}_\ell(M) + \mathrm{crys}_\ell\big),$$

and $\mathrm{loc}_\ell := 4f\,\mathrm{defect}_\ell$.

Fix a prime ℓ, an isomorphism $\iota\colon \mathbb{C} \simeq \overline{\mathbb{Q}}_\ell$, and $G_{\mathbb{Q}_\ell} := \mathrm{Gal}(\overline{\mathbb{Q}}_\ell/\mathbb{Q}_\ell)$. For a place $v \mid \ell$ of E choose an embedding $\jmath\colon E \to \overline{\mathbb{Q}}_\ell$ inducing v, and let $\Gamma_v \subseteq G_{\mathbb{Q}_\ell}$ be the subgroup fixing $\jmath(E)$, the Galois group of the completion E_v; thus $[G_{\mathbb{Q}_\ell} : \Gamma_v] = [E_v : \mathbb{Q}_\ell]$. In the proof of the denominators theorem, a congruence produces cocycles that obey the relations among the $U_i(g) - 1$; by Theorem 31.4.1 such a cocycle is the second coordinate of an integral cocycle on a lattice. It need not be crystalline above ℓ. The failure is priced on the dual side, and a finite model shows why the price is the same on both sides.

Problem 66.1.1. Let $F_1 \times F_2 \to \mathbb{Q}/\mathbb{Z}$ be a perfect pairing of finite abelian groups and $F_0 \subseteq F_1$ a subgroup. Its orthogonal $F_0^\perp \subseteq F_2$ has index $\#F_0$. For $F_1 = F_2 = \mathbb{Z}/9$ with $\langle y_1, y_2\rangle = y_1 y_2/9$ and F_0 generated by 3, $F_0^\perp = \{0, 3, 6\}$, of index 3: one equation costs length 1 on either side.

Date: November 26, 2026.

For a lattice with continuous action of Γ_v, write $Z_f(\cdot)$ for its integral crystalline cocycles. The proof uses three results of p-adic Hodge theory. (i) *Local duality in index form.* Let L, L' be potentially crystalline $\mathbb{Z}_\ell$-lattices with Γ_v-action in perfect equivariant duality $L' \times L \to \mathbb{Z}_\ell(1)$, let $n \geq 1$, red: $L \to L/\ell^n L$, and let $\mathcal{Q}$ be a group of maps $\Gamma_v \to L'$ whose cup products modulo ℓ^n with $\mathrm{red} \circ y$ for all $y \in Z_f(L)$, and with all members of a group $\mathcal{S}$ of continuous cocycles $\Gamma_v \to L/\ell^n L$, are coboundaries. Then $[\mathcal{S} : \mathcal{S} \cap \mathrm{red}\, Z_f(L)]$ divides $[Z_f(L') : Z_f(L') \cap \mathcal{Q}]$. The finite statement behind it is local Tate duality [SGC, II, §5.2, Thm. 2], [ADT, I.2.3]; the crystalline subgroups are exact annihilators of each other [BK, Prop. 3.8]. *Status*: classical in these forms; the integral form stated is read from the proof. (ii) *Bloch–Kato.* For a potentially crystalline $\mathbb{Z}_\ell$-lattice L with Γ_v-action, $Z_f(L)$ is a finite free $\mathbb{Z}_\ell$-module of rank $\mathrm{rk}_{\mathbb{Z}_\ell} L + [G_{\mathbb{Q}_\ell} : \Gamma_v] \cdot n^-$, where n^- is the number of negative Hodge–Tate jumps of L at the inclusion $\mathbb{Q}_\ell \subset \mathbb{C}_\ell$, counted with multiplicity [BK, §3]. *Status*: classical; the integral form is read from the proof. (iii) The bound (1) below. It rests on integral p-adic Hodge theory [Ki], [BMS, §4], and is read from the proof.

Definition 66.1.2. Let $\mathcal{O}$ be a coefficient ring, $\mathcal{C}$ a class of $\mathcal{O}$-lattices with continuous Γ_v-action, and L' such a lattice. In this sheet let $\mathcal{C}^\perp(L')$ be the $\mathcal{O}$-module of maps $c\colon \Gamma_v \to L'$ such that for every $\tilde{L} \in \mathcal{C}$, every $n \geq 0$, every pairing $\langle\,,\rangle\colon \tilde{L} \times L' \to \mathbb{Z}/\ell^n(1)$ obtained from an $\mathcal{O}$-linear form $\psi\colon \tilde{L} \otimes L' \to \mathcal{O}(1)$ whose coboundary $g \mapsto g\psi - \psi$ is ℓ^n times an integral crystalline cocycle, followed by a $\mathbb{Z}_\ell$-linear map $\mathcal{O} \to \mathbb{Z}_\ell$ and reduction modulo ℓ^n, and every $y \in Z_f(\tilde{L})$, the cochain $(g,h) \mapsto \langle y(g), g\,c(h)\rangle$, with values in the roots of unity of $\overline{\mathbb{Q}}_\ell$, is the coboundary of a continuous cochain $\Gamma_v \to \overline{\mathbb{Q}}_\ell^\times$. The *dual defect* of L' for $\mathcal{C}$ is the length of $Z_f(L')/(Z_f(L') \cap \mathcal{C}^\perp(L'))$. The *dual defect at* v of a lattice L is the dual defect of its Tate dual $L^*(1)$, in normalized length.

Let R be main-summand-like for (t', HT) (Definition 65.4.7). The *rows* at v are a Γ_v-stable $\mathcal{O}$-lattice L_0 in R, of rank r' and jumps HT, and the characters $\mathcal{O}(-e) = \chi_{\mathrm{cyc}}^{-e}$ for $0 \leq e < t'$, of rank 1. Let $\mathcal{C}$ be a class adapted to the rows: its lattices have jumps among those of the rows, and it consists of crystalline lattices or, when $\ell \in \{p_0, p_1\}$, of lattices of a fixed tame type. The proof shows: given R and v, for all large $\mathcal{O}$, for every choice of the rows at v over $\mathcal{O}$ and every class $\mathcal{C}$ of $\mathcal{O}$-lattices adapted to them, every row L in $\mathcal{C}$ has dual defect at v at most

$$[G_{\mathbb{Q}_\ell} : \Gamma_v]\ \mathrm{rk}(L)\, \mathrm{defect}_\ell / t_L, \qquad t_L = 1 \text{ for } L = L_0, \quad t_L = t \text{ for a character.} \quad (1)$$

Problem 66.1.2. $\sum_{v|\ell} [G_{\mathbb{Q}_\ell} : \Gamma_v] = [E : \mathbb{Q}] = 2f$. In $\mathbb{Q}(i)$ (a model, with 1 in place of f) the pairs (e_v, f_v) are $(1,2)$ above 3 and $(1,1), (1,1)$ above 5; the sum is 2 both times.

Problem 66.1.3. Let $r' \geq 1$ and $0 \leq t' \leq t$. The bounds (1) for the main row and the t' character rows, summed over the rows and the places $v \mid \ell$, total at most $4fr'\,\mathrm{defect}_\ell = r'\mathrm{loc}_\ell$.

In the proof these dual defects, added over the rows and the places above ℓ, bound what the crystalline relations above ℓ cost, and Problem 66.1.3 is the bound used for the sum. This is the term $r'\mathrm{loc}_\ell$ of the bound $\mathrm{sel} + 2t'\,\mathrm{ram} + r'\mathrm{loc}_\ell + \varepsilon_\ell + n_\ell \leq r'\mathrm{cl}_\ell$ of Problem 65.4.1.

66.2. The crystalline loss of one prime

Why the factorial and the interval? Each supplies one property of crys_ℓ that the local estimates need.

Problem 66.2.1. $\lfloor 2b/\ell \rfloor \le \mathrm{crys}_\ell$, so $2b < \ell(\mathrm{crys}_\ell + 1)$. If ℓ divides an integer of the interval of Definition 66.1.1, then $\mathrm{crys}_\ell \ge (\Delta/2)^3$.

Problem 66.2.2. Formally take $\Delta/2 = 1$ and $b = 32$ (no data have these values). The integer of Definition 66.1.1 is $64! \prod_{3 \le i \le 62} i$, and its valuations at $\ell = 2, 3, 5, 31, 61, 67$ are $119, 58, 28, 4, 2, 0$.

The bound (1) is proved by cases, which we only describe. If the class is tame (so $\ell \in \{p_0, p_1\}$), the cost is paid by the term $b\ \mathrm{val}_\ell(M)$, as $\mathrm{val}_\ell(M) \ge 1$. Otherwise the class is crystalline, the allowed jumps lie in a low window around 0 and in far windows of bounded width starting near $\pm b$ (at thick letters, Section 66.3) or near $\pm\lfloor a/x_1 \rfloor$, and there are three cases: $\ell \le kt$, where the thick letters are sparse (Section 66.3); $\ell > kt$ with $\mathrm{crys}_\ell \ge (\Delta/2)^3$; and $\ell > kt$ with $\mathrm{crys}_\ell < (\Delta/2)^3$. In the first two a power of ℓ bounded through $\lfloor 2\mathrm{crys}_\ell/(kt) \rfloor$ kills the quotient defining the dual defect, and (ii) bounds the number of generators. In the third, by Problem 66.2.1, ℓ divides no integer of the interval, so no nonzero multiple of ℓ lies near 0 or near the starts of the far windows, and the following estimate, read from the proof, applies. In this sheet let $\lambda, \lambda_0, \lambda_1 \ge 1$ be integers, $[-\lambda_0, \lambda_0]$ the low window and λ_1 the width of the far windows. At an unramified place with $\ell \ge 5$, group the embeddings of $\mathcal{O}$ by the root of unity of order $\ell^{f_v} - 1$ that they give (the letters of the chart of E_v), and attach to each such letter i a start fs_i and a sign $\mathrm{sg}_i = \pm 1$. Suppose $\mathrm{fs}_i + \lambda_1 + \lambda_0 \le (\ell - 3)\lambda$ and $6(\lambda + \lambda_0 + \lambda_1) < \mathrm{fs}_i$, and that ℓ divides no nonzero integer within $6(\lambda + \lambda_0 + \lambda_1)$ of 0 or $\pm\mathrm{fs}_i$. Let $\mathcal{C}$ be the class of crystalline lattices with jumps in given sets $\mathcal{J}$, and let L' be crystalline with jumps in sets $\mathcal{J}'$, where over each letter i the set $\mathcal{J}$ lies in $[-\lambda_0, \lambda_0] \cup -\mathrm{sg}_i[\mathrm{fs}_i, \mathrm{fs}_i + \lambda_1]$ and $\mathcal{J}'$ lies in $[-\lambda_0, \lambda_0] \cup \mathrm{sg}_i[\mathrm{fs}_i, \mathrm{fs}_i + \lambda_1]$. Then the dual defect of L' for $\mathcal{C}$ vanishes if no member of $\mathcal{J}$ or of $\mathcal{J}'$ lies in $[-\lambda, 0)$, or if $\mathcal{J}'$ lies in $[-\lambda_0, 0]$; and if at most n_{low} jumps of L' lie in $[-\lambda_0, \lambda_0]$ at each embedding, it is at most $11 f_v (n_{\mathrm{low}}(\lambda + 1) + \mathrm{rk}(L')(\lambda_1 + 1))$ in normalized length.

Problem 66.2.3. For $\ell = 101$, $\lambda = \lambda_0 = \lambda_1 = 1$ and one start $\mathrm{fs}_1 = 42$, the numerical hypotheses of this estimate hold: $44 \le 98$, the radius $6(\lambda + \lambda_0 + \lambda_1) = 18$ is less than 42, and no nonzero multiple of 101 lies within 18 of 0 or ± 42.

66.3. Thick letters

For $\ell \le kt$ no estimate uses ℓ large, and what keeps the loss small is the position of the places of weight b. Fix $\jmath\colon E \to \overline{\mathbb{Q}}_\ell$. For $g \in G_{\mathbb{Q}_\ell}$ let $\sigma_g := \iota^{-1} \circ g^{-1} \circ \jmath$, a complex embedding of E, with place $[\sigma_g] \in \Phi$. For a complex embedding σ its sign $s_\sigma = \pm 1$ for the CM type (as in Definition 65.4.6) is given by $\sigma(\sqrt{-d}) = s_\sigma \sqrt{-d}$, with $K \subset \mathbb{C}$ as in Chapter 33; if $\zeta \in \mathbb{C}$ is the image of ζ_{q_1} under the fixed embedding $E \to \mathbb{C}$ over K, the class of $[\sigma]$ in $(\mathbb{Z}/q_1)^\times$ is the u with $\sigma(\zeta_{q_1}) = \zeta^{s_\sigma u}$.

Definition 66.3.1. The embeddings σ_g, $g \in G_{\mathbb{Q}_\ell}$, are the *letters* over $\jmath$. A letter is *thick* if its place lies in Φ_b.

Problem 66.3.1. Let $\zeta_\jmath := \jmath(\zeta_{q_1})$, $h, n \ge 0$, and $g, g' \in G_{\mathbb{Q}_\ell}$ with $(g'g^{-1})(\zeta_\jmath^{\ell^h}) = \zeta_\jmath^{\ell^{h+n}}$. For every $q' \mid q_1$ prime to ℓ, the class of $[\sigma_g]/[\sigma_{g'}]$ modulo q' is $s_{\sigma_g} s_{\sigma_{g'}}\, \ell^n$.

For $\ell = 2$ and 31 in place of q', the powers of ℓ form the cycle $1, 2, 4, 8, 16$, which does not contain -1.

A lift $\mathrm{Fr}_\ell \in G_{\mathbb{Q}_\ell}$ of the Frobenius of the residue field raises every root of unity of order prime to ℓ to its ℓ-th power. So the letters $\sigma_{\mathrm{Fr}_\ell^n g}$, $n \in \mathbb{Z}$, form a cycle along which the classes of the places move by $\pm\ell^{-1}$ modulo the prime-to-ℓ part of q_1. The sparse condition of Definition 33.3.1(3) is designed for this cycle.

Problem 66.3.2. Let $\ell \le kt$, let ℓ^h be the largest power of ℓ dividing q_1, and let $1 \le i, j \le \lfloor \log_\ell(\Delta/2)^3 \rfloor$. Then $\lfloor \log_\ell(\Delta/2)^3 \rfloor \le 12s$, so $i + j < l_0(s)$. If $g_0, g_1, g_2 \in G_{\mathbb{Q}_\ell}$, $g_2 g_0^{-1}$ raises $\zeta_j^{\ell^h}$ to the power ℓ^{i+j}, $g_2 g_1^{-1}$ raises it to the power ℓ^j, and σ_{g_0}, σ_{g_2} are thick, then σ_{g_1} is not thick.

So along the cycle no three thick letters occur at two successive gaps of at most $\lfloor \log_\ell(\Delta/2)^3 \rfloor$, the gaps used by the local estimate for $\ell \le kt$.

Problem 66.3.3. In the cycle of Problem 66.3.1, call a set of elements of the cycle allowed if it contains no σ, τ, ρ with $\tau/\sigma \equiv \pm 2^i$, $\rho/\sigma \equiv \pm 2^j$ and $0 < i < j < 5$. Then $\{1, 2\}$ is allowed, $\{1, 2, 8\}$ is not, and an allowed set has at most 2 letters. With the true size $l_0(s) \ge 81$ in place of 5, no nonempty set is allowed: a cycle of length 5 is far shorter than any that data produce.

Which far window a thick letter uses depends on its sign. For $\ell \nmid q_1 d$ the field $E \subseteq \mathbb{Q}(\zeta_{q_1 d})$ is unramified at ℓ, and $\ell \ge 13$ since every prime below 13 divides q_0; there the proof reads the sign of each letter separately. For $\ell \mid q_1 d$ the proof needs that the thick letters have one sign, and this has two cases.

Problem 66.3.4. If $\ell \mid q_1$, then $s_{\sigma_g} = s_{\sigma_{g'}}$ for all $g, g' \in G_{\mathbb{Q}_\ell}$; in particular two thick letters have the same sign.

Problem 66.3.5. $d^2 \equiv 1$ and $d \not\equiv \pm 1 \pmod{q_0}$, so $d^n \not\equiv -1 \pmod{q_0}$ for every $n \ge 0$. Hence two thick letters over $\ell = d$ have the same sign. For $q_0 = 18480$ and $d = 9239$, $d^2 \bmod q_0 = 1$.

66.4. The sum over the primes

The number defect_ℓ is $10^6(m/k)$ times a combination of valuations at ℓ of two integers, M^b and $(2b)!\,\mathrm{Int}_b^{(\Delta/2)^3}$. Summed with weights $\log \ell$, valuations give back logarithms.

Problem 66.4.1. For an integer $n \ge 1$ and a finite set A of primes, $\sum_{\ell \in A} \mathrm{val}_\ell(n) \log \ell \le \log n$. For the integer of Problem 66.2.2 the sum over $\ell \le 67$ is $401.34123\ldots$, its logarithm.

Problem 66.4.2. $\mathrm{Int}_b \le (b + 30(\Delta/2)^3)^{60(\Delta/2)^3}$. For data,

$$b \log M + \log\Big((2b)!\,(b + 30(\Delta/2)^3)^{60(\Delta/2)^6}\Big) \le 26\, b \log b.$$

Problem 66.4.3. For every finite set A of primes, $\sum_{\ell \in A} \mathrm{defect}_\ell \log \ell \le 26 \cdot 10^6\,(m/k)\, b \log b$.

Since $26 \le e^{180}$, Problem 66.4.3 gives the following theorem; Problems 66.4.1–66.4.3 prove it.

Theorem 66.4.1. *For all data and every finite set A of primes,*

$$\sum_{\ell \in A} \mathrm{loc}_\ell \log \ell \le 4 \cdot 10^6 e^{180} \, f \, \frac{m}{k} \, b \log b.$$

The proof states the theorem with the constant e^{180}, which it obtains by a general comparison of the sizes of the data.

Problem 66.4.4. The right side of Theorem 66.4.1 is at most $16 \cdot 10^6 e^{180} \, B/(\log b)^2$.

So the local loss uses a fraction $O((\log b)^{-2})$ of the budget B. Proved here: Problems 66.1.3 and 66.2.1, the spacing and signs of thick letters, and Theorem 66.4.1. Taken as given: local duality, the Bloch–Kato rank, and the bound (1) at one place with its case analysis. Problem 65.4.4 adds Theorem 66.4.1 to the bounds for the other terms of cl_ℓ, summed with weights $\log \ell$, to fit the budget B.

In the Lean formalization. In the Lean proof [GL] (`grh/src/`; the prefixes `New.Selmer`, `New.Lift` and `New.Period` are omitted), Definition 66.1.1 is `crystallineLoss`, `defectBound` (`New/Congruences/LocalLoss/Basic.lean`) and `localDefectBound` (`New/Congruences/FirstOrder/TraceRelations.lean`). The cocycles that obey the relations and their graph are `ribetCocyclesIn` and `ribetCocycles.exists_graph_subrepresentation` (`LocalLoss/Basic.lean`). Definition 66.1.2 is `dualDefect` (`Lib/ClassField/LocalDuality/CrystallineDuality.lean`), where (i) is `IsPotentiallyCrystalline.relIndex_dvd_of_orthogonal`; (ii) is `crysCocycles.finrank_eq` (`Lib/PadicHodge/BlochKato.lean`); the frame behind (iii) is in `Lib/PadicHodge/Kisin/`. The bound (1) is `summand_defect_le_at_place` (`LocalLoss/CrystallineDefect.lean`); its case analysis is `normLength_dualDefect_le_of_crystallineSizes` (`LocalLoss/CrystallineCocycles.lean`) and, for a tame class, `normLength_dualDefect_le_defectBound_of_isTameType` with `two_mul_tame_exponent_le_defectBound`; the estimate before Problem 66.2.3 is `KummerChart.dualDefect_eq_zero_and_dualDefect_le` (`New/Congruences/Lifting/CupOrthogonalityBounds.lean`); the letters, their thickness and signs as the local estimates use them are `eventually_exists_lettersReadThick`. The dual defects summed over rows and places are bounded by $r' \mathrm{loc}_\ell$ in `eventually_exists_inClass_sum_dualDefect_le`, and $r' \mathrm{loc}_\ell$ is a term of `liftValuationBound` (`FirstOrder/DenominatorBound.lean`). Problem 66.1.3 is `sum_index_mul_defectBound_le`, whose step `h_degrees` proves the form with $\le$ of Problem 66.1.2, stated here with equality. Problem 66.2.1 is `two_mul_lt_mul_crystallineLoss_succ` and `cube_le_crystallineLoss_of_dvd`, its first inequality being a step in the proof of the former. Problem 66.3.1 is `placeClass_eq_cmSign_mul_pow`; Problem 66.3.2 is `notMem_bPlaces_of_short_arc`, with the bound on the gaps from `notMem_bPlaces_of_coefficientEmbedding_eq_pow`. Problems 66.3.4 and 66.3.5 are the two branches of `cmSign_eq_of_mem_bPlaces`, whose branch $\ell \mid q_1$ does not use that the letters are thick, with `New.Parameters.d_pow_ne_neg_one` (`New/Reduction/Data/FieldsAndPlaces.lean`) for the first assertion of Problem 66.3.5. Problem 66.4.1 is `sum_padicValNat_mul_log_le`, the first part of Problem 66.4.2 is `prod_Ioc_natB_le_pow`, and Theorem 66.4.1 is `sum_localDefectBound_mul_log_le` (`New/Congruences/FitTwistsExist.lean`).

The comparison of sizes that gives e^{180} is `New.Data.le_of_hasLogBound`, and the sum of the clearing bounds is `sum_clearingBound_add_padicValNat_le`. The constant 26, Problems 66.1.1, 66.2.2, 66.2.3, 66.3.3 and 66.4.4, and the numerical examples in Problems 66.1.2, 66.3.1, 66.3.5 and 66.4.1 are ours.

Hints

§66.1.

66.1.1: The pairing identifies F_2 with the dual of F_1; describe $F_0^{\perp}$ in these terms.

66.1.2: The places above ℓ correspond to the double cosets of the embeddings; use $\sum_v e_v f_v = [E : \mathbb{Q}]$ [SLF, Ch. I, §4, Prop. 10] and $[E_v : \mathbb{Q}_\ell] = e_v f_v$ [SLF, Ch. II, §3]. -1 is a square modulo 5, not modulo 3.

66.1.3: Sum first over the places, by Problem 66.1.2.

§66.2.

66.2.1: Legendre's formula for $(2b)!$; the integer divides Int_b.

66.2.2: Legendre's formula, plus the multiples of ℓ in $[3, 62]$.

§66.3.

66.3.1: Write $g(y) = y^{u_g}$ on roots of unity of order q_1 in $\overline{\mathbb{Q}}_\ell$, for $g \in G_{\mathbb{Q}_\ell}$, and compare $\sigma_g(\zeta_{q_1})$ with $\sigma_{g'}(\zeta_{q_1})$.

66.3.2: $r \le 3x^5$ and $2^s = m^{22} \ge x^{11}$; then Problem 33.2.1 and Problem 66.3.1.

66.3.3: For three letters, read their exponents relative to one of them. For the last assertion, σ, τ, ρ need not be distinct.

66.3.4: Consider $\theta_K = (1 + \sqrt{-d})/2$ and Problem 33.1.2.

66.3.5: $d+1$ is an odd multiple of $q_0/2$. For the second assertion, $d \nmid q_1$, and every element of $G_{\mathbb{Q}_d}$ raises the roots of unity of order q_1 to a power d^n; use Problem 66.3.1 with $q' = q_0$ and the class of Φ_b modulo q_0.

§66.4.

66.4.1: Factor n.

66.4.2: Count the factors. Then Problem 33.5.4, $(2b)! \le (2b)^{2b}$, and $(\Delta/2)^6 = r^{48}$, which is tiny compared with b by Definition 33.3.1.

66.4.3: Problem 66.4.1 for $n = M^b$ and $n = (2b)!\,\mathrm{Int}_b^{(\Delta/2)^3}$.

66.4.4: $B = fxb\log^3 b/(mk)$ and $m \le 2\sqrt{x}$.

References

[ADT] J. S. Milne, *Arithmetic Duality Theorems*, 2nd ed., BookSurge, 2006.

[BK] S. Bloch and K. Kato, *L-functions and Tamagawa numbers of motives*, in: The Grothendieck Festschrift I, Progr. Math. 86, Birkhäuser, 1990, 333–400.

[BMS] B. Bhatt, M. Morrow and P. Scholze, *Integral p-adic Hodge theory*, Publ. Math. IHÉS **128** (2018), 219–397.

[GL] L. Sernau, *GRH for Dirichlet L-functions, in Lean 4*, a shorter rewriting of the Lean proof, text by Claude, `https://github.com/lsernau/grh-lean`, commit `72fead1`, readable edition `grh/`.

[Ki] M. Kisin, *Crystalline representations and F-crystals*, in: Algebraic Geometry and Number Theory, Progr. Math. 253, Birkhäuser, 2006, 459–496.

[SGC] J.-P. Serre, *Galois Cohomology*, Springer, 1997.

[SLF] J.-P. Serre, *Local Fields*, Grad. Texts in Math. 67, Springer, 1979.