DIVISIBILITY OF THE COMPOSITE LIFT

Prerequisites. Chapter 33: the parameters, the field E and its places (Section 33.2), the scales and ranks (Section 33.3), the weights κ and the prime sums s_{fin} (Section 33.4), and the source forms, twists and integral vacuum (Chapter 34). Chapter 43: chain data and the composite lift $B_{\vartheta,\Psi}$. The stage bound of one lift, Theorem 50.4.4, is used here and proved in Chapter 50, which follows; its shape in the plane is Theorem 16.3.1. The colength of Chapter 5, Section 5.4, in the form of Chapter 18, Section 18.6; the elementary divisor theorem, Theorem 48.5.1, is stated in Section 48.5. The step at a full mark, Theorem 53.4.1, and the case of the level prime, Theorem 52.4.1, are used here and proved in Chapters 53 and 52, which follow. Modules over a valuation ring; $\mathbb{C}_p$, with $|p|_p = p^{-1}$.

Theorem A needs a valuation bound for the composite lift $B_{\vartheta,\Psi}$ at every prime p. The divisibility predicted at p is a number $\mathrm{gain}(p)$. It holds up to an error, on a submodule of colength at most the error times $D_X = \dim_{\mathbb{C}} S$, and the errors, weighted by $\log p$, add up to at most $U = fa\log^3 b$. We follow the four cases of the proof.

- Read from the proof: the expansion of a chain datum into a weak one (Theorem 48.3.4), inputs (i) and (ii) of Section 48.3, and the colength estimate for one marked prime (from Theorem 48.5.1, itself read from the proof).
- Developed in the chapters that follow: the bound for one lift at a prime $p < x_1$ with $\chi_K(p) \neq 1$, input (iii) of Section 48.3, is Theorem 50.4.4, and Chapter 49 treats the count behind it; the primes above an exceptional prime, the existence of a full mark and the valuation bound at a full mark are in Chapter 53 (Theorem 53.4.1); the level prime is Chapter 52 (Theorem 52.4.1).
- Derived here from these: Theorems 48.7.1 and 48.7.2.

48.1. The gain at a prime

We use q_0, d, K, χ_K, q_1, E, Φ, f, $[\nu]$, Φ_a, Φ_b, the weight κ and s_{fin} as in Chapter 33; recall that $a/x_1 \le \kappa(\sigma) \le b \le a$ and that q_1 is q_0 times a product of powers of 2 and 3. For a natural number p, let $c_p = 1/2$ if $p = d$ and $c_p = 1$ otherwise, and let I_p be the set of integers $e \ge 1$ such that $p = d$, or $\chi_K(p) = -1$ and e is odd. For $y \in \mathbb{R}$ and $\sigma \in \Phi$, with $z_+ = \max(z, 0)$, the *local prime sum* and the *gain* are

$$s_{\mathrm{fin},p}(y,\sigma) = c_p \sum_{e\in I_p} \Big(\frac{y}{p^e} - \kappa([-p^e]\sigma)\Big)_+, \qquad \mathrm{gain}(p) = m\Big(\sum_{\tau\in\Phi_a} s_{\mathrm{fin},p}(a,\tau) + k\sum_{\sigma\in\Phi} s_{\mathrm{fin},p}(\kappa(\sigma),\sigma)\Big).$$

The first sum records the a columns of height one at each a-place; the second counts the local term at $\kappa(\sigma)$ with multiplicity k at every place.

Problem 48.1.1. Every prime dividing q_1 splits in K. Hence a prime $p \neq d$ with $\chi_K(p) \neq 1$ is prime to q_1, and $[-p^e]$ is the place of the class of $-p^e$.

Date: November 26, 2026.

Problem 48.1.2. Let $p \neq d$ be inert in K, $\tau \in \Phi_a$, and suppose that $\kappa([-p^e]\tau) = w$ for every positive odd integer e. Then $s_{\mathrm{fin},p}(a,\tau) = \sum_{e\geq 1,\ e\ \mathrm{odd}} (a/p^e - w)_+$, the first sum of Theorem 16.3.1 without the integer parts. Evaluated at $p = 13$, $a = 13^4$ and $w = 1$, the sum is 2208.

Problem 48.1.3. $\mathrm{gain}(p) = 0$ if $\chi_K(p) = 1$ or $p \geq x_1$.

Problem 48.1.4. Let p be prime and $y \leq a$. The terms of $s_{\mathrm{fin}}(y,\sigma)$ with ν a power of p add up to $2\, s_{\mathrm{fin},p}(y,\sigma)\log p$.

Let Π be the set of primes $p < x_1$ with $\chi_K(p) \neq 1$. Summing over primes, $2\sum_{p\in\Pi} \mathrm{gain}(p)\log p = m\sum_{\tau\in\Phi_a} s_{\mathrm{fin}}(a,\tau) + mk\sum_{\tau\in\Phi} s_{\mathrm{fin}}(\kappa(\tau),\tau)$; the contribution of the powers of p to the right-hand side is $2\,\mathrm{gain}(p)\log p$.

48.2. Collisions

In this section p is a prime. For a set $\Phi' \subseteq \Phi$, a *collision outside* Φ' is a pair (τ, e) with $e \in I_p$ and $\tau, [-p^e]\tau \in \Phi_a \smallsetminus \Phi'$; the *collision sum* is

$$C_p(\Phi') = \sum_{(\tau,e)\ \text{collision outside}\ \Phi'} \frac{a}{p^e}.$$

Let o_p be the order of the image of $[-p]$ in $(\mathbb{Z}/q_0)^\times$, and r_p the least integer $h \geq 0$ with $m \leq p^h$. The prime p is *exceptional* if $\chi_K(p) = -1$, $p \not\equiv \pm 1 \pmod m$, and o_p is odd with $o_p \leq r_p$. The *unit of loss* at p is

$$L_p = f(\log b)^2\, \frac{a}{p} \cdot \begin{cases} m & \text{if } m \mid p-1 \text{ or } m \mid p+1, \\ 1 & \text{otherwise.} \end{cases}$$

Problem 48.2.1. Let $\chi_K(p) \neq 1$ and let (τ, e) be a collision outside some Φ'. Then $p \neq d$, e is odd, and $o_p \mid e$; in particular o_p is odd.

Problem 48.2.2. Let $q_0 = 18480$ and let p be a prime not dividing q_0. If o_p is odd, then $p \equiv -1 \pmod{240}$ and $o_p \in \{1,3,5,15\}$. For $d = 138599$, the inert prime 13 has $o_{13} = 20$. Among the primes inert in $\mathbb{Q}(\sqrt{-138599})$, the least with o_p odd is 479, with $o_{479} = 15$, and the least with $o_p = 1$ is 55439.

Problem 48.2.3. Let $o \geq 0$ be an integer. If every collision (τ, e) outside Φ' has $e \geq o$, then $C_p(\Phi') \leq 2fa/p^o$.

From Chapter 33 we use $(\log b)^2 \geq 15$ and $m \geq 2$.

Problem 48.2.4. Let $p < x_1$ be a prime with $\chi_K(p) \neq 1$ that is not exceptional. Then $m\, C_p(\varnothing) \leq L_p$.

Problem 48.2.5. Let p be exceptional with $o_p = 1$, and let $h_0 = \#(\mathbb{Z}/q_0)^\times$. Then $\#\Phi_a = f/h_0$ and $m\, C_p(\varnothing) \geq mfa/(h_0 p)$, which exceeds L_p when $m > h_0(\log b)^2$.

So at an exceptional prime the unit of loss need not pay for the collisions; Section 48.4 obtains the valuation bound there on a submodule.

48.3. The chain of lifts

Fix a prime p and a ring map $\eta\colon \mathbb{C} \to \mathbb{C}_p$; $\mathcal{O}_\eta$ is the ring of Chapter 34.

Definition 48.3.1. At a point g of the finite adelic group, the *gauge* $\|\omega\|_g$ of a Weyl vector ω is the largest absolute value of a coordinate of $g^{-1}\cdot\eta(\omega)$, where at τ the adelic matrix acts in the Weyl representation through the extension to finite adeles of $u \mapsto \eta(\Phi_\tau(\bar{u}))$, and Φ_τ is the embedding of E selected by the CM type. A form φ *has valuation at least* c, for a real number c, if $\|\varphi(g)\|_g \le p^{-c}$ for every g; it is *integral* if it has valuation at least 0.

With $S \supseteq S_{\mathrm{ram}}$ the source forms and the ramified ones (Chapter 34), let $S_\eta \subseteq S$ be the $\mathcal{O}_\eta$-module of integral source forms and $S_{\mathrm{ram},\eta} = S_\eta \cap S_{\mathrm{ram}}$.

The translations $\mathfrak{t} = (\mathfrak{t}_j)_{j\ge 0} \in \mathcal{T}$ and the translated vacua $v_j(\mathfrak{t})$ are those of Definition 43.4.2.

Definition 48.3.2. For a twist ϑ, a finitely supported $\Psi\colon \mathcal{T} \to \mathbb{C}$ is a *weak chain datum* for ϑ if: for every $\mathfrak{t}$ in its support and every j, the entries of $\alpha\mathfrak{t}_j$ are integral at every finite place not dividing $N\mathrm{Nm}\,Q_\vartheta$ (with α as in Chapter 33); every value $\Psi(\mathfrak{t})$ is integral under every ring map $\mathbb{C} \to \mathbb{C}_\ell$ for every prime $\ell \nmid \mathrm{Nm}\,Q_\vartheta$; if $Q_\vartheta = \varnothing$, then $\sum_{\mathfrak{t}} |\sigma(\Psi(\mathfrak{t}))| \le \exp(x^{60})$ for every automorphism σ of $\mathbb{C}$; and $\sum_{\mathfrak{t}} \Psi(\mathfrak{t}) \bigotimes_{j<m} v_j(\mathfrak{t})$ is fixed by the levels of $X_0, \dots, X_{m-1}$.

Definition 48.3.3. The *restricted chain* of a weak chain datum Ψ for ϑ is $R_{\vartheta,\Psi} := \sum_{\mathfrak{t}} \Psi(\mathfrak{t})\, \Theta^{\mathfrak{t}}_{m-1} \cdots \Theta^{\mathfrak{t}}_0$, followed by restriction to Y_m, where the jth lift $\Theta^{\mathfrak{t}}_j$ is built from ϑ and has the datum $v_j(\mathfrak{t})$.

Away from N the proof uses the following expansion, which we take from it [GL].

Theorem 48.3.4. *For every twist ϑ and every chain datum Ψ for ϑ there is a weak chain datum Ψ' for ϑ with $B_{\vartheta,\Psi}\varphi = R_{\vartheta,\Psi'}\varphi$ for all $\varphi \in S$.*

We use three inputs. In (i) and (ii), let Ψ' be a weak chain datum for ϑ and suppose $p \nmid \mathrm{Nm}\,Q_\vartheta$.

(i) If $p \ne N$ and $p \ne d$, then $R_{\vartheta,\Psi'}$ maps S_η to integral forms.

(ii) Let $p \ne N$. If $p \nmid M$, then for every $\mathfrak{t}$ in the support of Ψ' and every $j \ge 0$ the datum $v_j(\mathfrak{t})$ is a standard datum of denominator 1 (Definition 50.4.1). If $\rho_0, \rho_1, \dots$ are real numbers such that, for every $\mathfrak{t}$ in the support of Ψ' and every $j \ge 0$, the datum $v_j(\mathfrak{t})$ multiplies gauges by at most $p^{-\rho_j}$ (Definition 50.4.2, for the lift j built from ϑ), then $R_{\vartheta,\Psi'}$ maps S_η to forms of valuation at least $\sum_{j<m} \rho_j$.

(iii) Let $\mathcal{D}_j(\Phi')$, for $j \ge 0$ and $\Phi' \subseteq \Phi$, be the stage bound of Definition 50.1.1. By Theorem 50.4.4: if $\chi_K(p) \ne 1$, then for every twist, every $j \ge 0$ and every standard datum φ of denominator 1 on $\mathrm{Hom}(X_j, X_{j+1})$, φ multiplies gauges by at most $p^{-\mathcal{D}_j(\varnothing)}$; and if $p < x_1$ and $\chi_K(p) \ne 1$, then for every $0 \le j < m$ and every $\Phi' \subseteq \Phi$,

$$\mathcal{D}_j(\Phi') \ge \frac{\mathrm{gain}(p)}{m} - C_p(\Phi') + c_p\, \#(\Phi_a \cap \Phi')\, \frac{a}{x_1} - \frac{f a (\log b)^2}{mp}.$$

Inputs (i) and (ii) are read from the proof. Input (iii) is proved in Chapter 50: its first part from the bound on jets along products of minors, Theorem 17.5.1, applied to the theta series of a standard datum, with four statements read from the proof; its second part by comparing the predicted divisibility of the diagram of the lift

with the prime sums that define gain(p). Here $\gamma_p = 1/(p-1) - \rho(d,p)$, which is $p/(p^2-1)$ at an inert prime and $1/(2d-2)$ at $p=d$ (Problem 49.1.1), is the credit of one box in the stage bound. A prime $p < x_1$ divides neither M nor N, since $p_0, p_1 \geq b^{10}$ and $N > M$ (Chapter 33).

Problem 48.3.1. Let $\mathcal{V}_0, \dots, \mathcal{V}_m$ be finite-dimensional $\mathbb{C}_p$-spaces with sup norms in fixed bases, let $\Theta_j^{\mathfrak{t}} \colon \mathcal{V}_j \to \mathcal{V}_{j+1}$ satisfy $\|\Theta_j^{\mathfrak{t}} u\| \leq p^{\rho_j}\|u\|$ for $\mathfrak{t}$ in a finite set, and let $\Psi(\mathfrak{t}) \in \mathbb{C}_p$ have $|\Psi(\mathfrak{t})|_p \leq 1$. Then $\big\|\sum_{\mathfrak{t}} \Psi(\mathfrak{t})\Theta_{m-1}^{\mathfrak{t}} \cdots \Theta_0^{\mathfrak{t}} u\big\| \leq p^{\rho_0+\cdots+\rho_{m-1}}\|u\|$.

Problem 48.3.2. Let $p < x_1$ be prime with $\chi_K(p) \neq 1$, $p \nmid \operatorname{Nm} Q_\vartheta$, and Ψ a chain datum for ϑ. For $\varphi \in S_\eta$, $B_{\vartheta,\Psi}\varphi$ has valuation at least gain$(p) - L_p - m\,C_p(\varnothing)$.

Let $p \nmid \operatorname{Nm} Q_\vartheta$ and let Ψ be a chain datum for ϑ. If $p < x_1$ is non-split and not exceptional, then by Problems 48.2.4 and 48.3.2, $B_{\vartheta,\Psi}$ has valuation at least gain$(p) - 2L_p$ on S_η. If $p \neq N$ and either $\chi_K(p) = 1$ or $p \geq x_1$, then $p \neq d$, as $d < x_1$ by Chapter 33; by (i), $B_{\vartheta,\Psi}$ maps S_η to integral forms, and gain$(p) = 0$.

48.4. Exceptional primes

Let p be inert in K. Each place σ, represented by the embedding Φ_σ, gives through η a prime v_σ of E above p; for every positive odd integer e, $v_{[-p^e]\sigma} = \bar{v}_\sigma$, the complex conjugate prime (Problem 53.1.1). Let $p < x_1$ be exceptional. A *mark* is a set $\mathfrak{M}$ of primes of E above p, each of the form v_τ with $\tau \in \Phi_a$, such that $\bar{v} \notin \mathfrak{M}$ for $v \in \mathfrak{M}$. It is *full* if it contains v_τ or $\bar{v}_\tau$ for each $\tau \in \Phi_a$; a full mark exists for every exceptional $p < x_1$ (Problem 53.1.5). Let $\Phi_{\mathfrak{M}} = \{\sigma \in \Phi : v_\sigma \in \mathfrak{M}\}$.

Problem 48.4.1. If $\mathfrak{M}$ is a full mark, then $C_p(\Phi_{\mathfrak{M}}) = 0$.

For $v \in \mathfrak{M}$ let $a_v = a \cdot \#\{\tau \in \Phi_a : v_\tau = v\}$, let T_v be the Hecke operator at the split pair $v, \bar{v}$ of the double coset of $\operatorname{diag}(p1_{r_p}, 1)$ (p is a uniformizer at v, as p is unramified in E), and let $Y_v = p^{a_v} T_v$ on S. Let $Y_{\mathfrak{M}}$ be the product of the Y_v, $v \in \mathfrak{M}$, in a fixed order. By Theorem 53.4.1, for a full mark $\mathfrak{M}$, a weak chain datum Ψ' for ϑ with $p \nmid \operatorname{Nm} Q_\vartheta$, and $\varphi \in S_\eta$, the form $R_{\vartheta,\Psi'}(Y_{\mathfrak{M}}^m \varphi)$ has valuation at least gain$(p) - 2L_p$. Let $j_p = \lceil 2mfa/p \rceil$.

Problem 48.4.2. Under the hypotheses of Problem 48.3.2, $B_{\vartheta,\Psi}(p^{j_p}\varphi)$ has valuation at least gain$(p) - L_p$ for $\varphi \in S_\eta$.

Problem 48.4.3. Let $p < x_1$ be exceptional, $\mathfrak{M}$ a full mark, $p \nmid \operatorname{Nm} Q_\vartheta$, and Ψ a chain datum for ϑ. On $S' = Y_{\mathfrak{M}}^m S_\eta + p^{j_p} S_\eta$, $B_{\vartheta,\Psi}$ has valuation at least gain$(p) - 2L_p$.

How large is S' in S_η? We use the colength of Chapter 5 and the phrase "onto modulo p^u up to colength c" as defined in Chapter 18. The proof applies Theorem 48.5.1 (Section 48.5) at the marked primes and obtains: for a mark $\mathfrak{M}$, $v \in \mathfrak{M}$ and every integer $u \geq 0$, Y_v is onto S_η modulo p^u up to colength $\big(12a_v/(mp) + u/(m^2 f)\big) D_X$.

Problem 48.4.4. Let $\mathcal{O}$ be a commutative ring, $p \in \mathcal{O}$, $\mathcal{L}$ a submodule of an $\mathcal{O}$-module $\mathcal{W}$, and Y_1, Y_2 $\mathcal{O}$-linear endomorphisms of $\mathcal{W}$ that are onto $\mathcal{L}$ modulo p^u up to colengths c_1 and c_2. Then $Y_1 Y_2$ is onto $\mathcal{L}$ modulo p^u up to colength $c_1 + c_2$.

Problem 48.4.5. For a mark $\mathfrak{M}$, $\sum_{v \in \mathfrak{M}} a_v \leq af$ and $\#\mathfrak{M} \leq f$, and

$$m \sum_{v \in \mathfrak{M}} \Big(\frac{12 a_v}{mp} + \frac{j_p}{m^2 f} \Big) \leq \frac{14fa + p/m}{p} \leq L_p.$$

So $Y^m_{\mathfrak{M}}$ is onto S_η modulo p^{j_p} up to colength L_pD_X: there is an integer $0 \le l \le L_pD_X$ such that the colength of S' in S_η divides p^l.

48.5. The theorem on elementary divisors

This section states the theorem that Section 48.4 applies at the marked primes. It is read from the proof [GL] and is not proved here; Chapter 18 computes its model at one vertex of the tree (Theorem 18.5.1), and "onto modulo p^u up to colength" is defined in Section 18.6. The letters of this section are its own and are used in no other section: here X, Z and I are finite sets, U is an endomorphism, η, η' are elements of $X \times \mathcal{C}$, ω is a coset, $\rho(\gamma)$ and D are matrices, and β is a family of exponents, not the diagram of the data.

In this chapter N_0, n, r_0, D and θ are local to the following theorem. Let $N_0 \ge 1$, let W' be a commutative local ring with maximal ideal $\mathfrak{m}$, and let O be a valuation domain of characteristic 0. In the setting of the theorem, a *Frobenius cycle* of length N_0 from W' to O consists of a prime p, a power $P \ge 5$ of p, ring homomorphisms $\iota_s\colon W' \to O$ for $s \in \mathbb{Z}/N_0$, a parity, even or odd, for each s, and an element $\varpi \in O$, such that $\varpi^2 = p$; p divides $\iota_{s+1}(w) - \iota_s(w)^P$ in O for all s and all $w \in W'$; the parities of s and $s+1$ differ for every s; and $W'/\mathfrak{m}$ has $q := P^{N_0}$ elements. Fix integers $n \ge 1$ (the rank), $\mu \ge 0$ (the degree in each letter s) and $r_0 \ge 0$. Let $\mathcal{B}$ be the set of families $\beta = (\beta_s)_{s\in\mathbb{Z}/N_0}$ of maps $\beta_s\colon \{0,\dots,n-1\} \to \mathbb{Z}_{\ge 0}$ with $\sum_i \beta_s(i) = \mu$ for each s. For $\gamma \in \mathrm{GL}_n(W')$ put $\gamma_s = \iota_s(\gamma)$ if s is even and $\gamma_s = \iota_s((\gamma^{-1})^{\mathsf{T}})$ if s is odd, and let $\rho(\gamma)$ be the $\mathcal{B}\times\mathcal{B}$ matrix whose (β,β') entry is the product over s of the coefficients of z^{β_s} in $\prod_i \bigl(\sum_j (\gamma_s)_{ji} z_j\bigr)^{\beta'_s(i)}$. The *depth* $\mathrm{dp}(\beta)$ is the sum of $\beta_s(i)$ over the pairs (i,s) with s even and $i \ge r_0$, or s odd and $i < r_0$; and D is the diagonal matrix with entries $p^{\mathrm{dp}(\beta)}$. Let $\mathcal{K}_{r_0} \subseteq \mathrm{GL}_n(W')$ consist of the matrices whose (i,j) entry lies in $\mathfrak{m}$ whenever $i < r_0 \le j$, and let $\mathcal{C} = \mathrm{GL}_n(W')/\mathcal{K}_{r_0}$, the set of left cosets.

For the theorem take finite sets X and Z. *Edge coordinates* on (X,Z) are maps $\pi\colon X\times\mathcal{C} \to X$, $\gamma\colon X\times\mathcal{C} \to \mathrm{GL}_n(W')$, $\gamma'\colon \mathcal{C} \to \mathrm{GL}_n(W')$ and $\upsilon\colon X\times\mathcal{C} \to \mathrm{GL}_Z(O)$, such that $\gamma'(\omega)^{-1}\mathcal{K}_{r_0} = \omega$ for every $\omega \in \mathcal{C}$, and $\eta = \eta'$ whenever $\eta,\eta' \in X\times\mathcal{C}$ satisfy $\pi(\eta) = \pi(\eta')$ and $\gamma(\eta)^{\mathsf{T}}(\gamma(\eta')^{\mathsf{T}})^{-1} \in \mathcal{K}_{r_0}$. For a finite set I and a bijection $J = (J_1, J_2)\colon I \to \mathcal{B}\times Z$, the *edge Hecke operator* $\mathcal{A}$ is the O-linear endomorphism of $(O^I)^X$ given by

$$(\mathcal{A}F)(\lambda)_i = \sum_{\omega\in\mathcal{C}} \sum_{i'\in I} \upsilon(\lambda,\omega)_{J_2 i,\, J_2 i'} \bigl(\rho(\gamma(\lambda,\omega))\, D\, \rho(\gamma'(\omega))\bigr)_{J_1 i',\, J_1 i}\, F(\pi(\lambda,\omega))_{i'}.$$

For $n = 2$ and $r_0 = 1$ the cosets $\mathcal{C}$ correspond to the lines of the residue plane, as the sources of Problem 18.1.1 do.

Theorem 48.5.1. *Let a Frobenius cycle of length $N_0 \ge 1$ from a commutative local ring W' to a valuation domain O of characteristic 0 be given, with prime p, power P and $q = P^{N_0}$ as above, and suppose that p is not a unit in O. Let n, μ, r_0 be integers and θ a real number with, for the natural logarithm,*

$$0 < r_0, \quad 2r_0 \le n, \quad 0 < \theta \le 1, \quad \mu^4 \le q, \quad \Bigl(\frac{N_0 n \log q}{\theta}\Bigr)^5 P^{3r_0} \le \mu.$$

Let X, Z and I be finite sets ($\mathcal{C}$ is finite), $J\colon I \to \mathcal{B}\times Z$ a bijection, edge coordinates on (X,Z) with edge Hecke operator $\mathcal{A}$, $\mathcal{M}$ an O-module, $\psi\colon (O^I)^X \to \mathcal{M}$ an O-linear map and U an endomorphism of $\mathcal{M}$ with $U\psi = \psi\mathcal{A}$. Then for every integer

$u \geq 0$, U is onto $\mathcal{L} = \psi\big((O^I)^X\big)$ modulo p^u up to colength

$$\big(3\,c_{\mathrm{div}} + \theta u\big)\,\#X\,\#I, \qquad c_{\mathrm{div}} = N_0\mu\Big(\frac{1}{P^{2r_0}} + \frac{r_0^2}{nP}\Big).$$

The bound has a part $\theta u\,\#X\,\#I$, a share θ of the bound $u\,\#X\,\#I$ that every endomorphism keeping $\mathcal{L}$ satisfies, as $\mathcal{L}$ is generated by $\#X\,\#I$ elements, and a part $3c_{\mathrm{div}}\#X\,\#I$ that does not depend on u. It bounds a colength, not the individual elementary divisors. Theorem 18.5.1 is its model, not a case of it:

Problem 48.5.1. A Frobenius cycle has even length N_0. Under the hypotheses on n, μ, r_0, θ of Theorem 48.5.1, $\mu > P^{3r_0}$ and $N_0 > 12r_0$. For $N_0 = 14$, $n = 2$, $r_0 = 1$, $\theta = 1/2$, $P = 5^{100}$ and $\mu = 5^{350}$ these hypotheses hold.

48.6. The level prime and the sum of the errors

At the level prime N, which is at least x_1, the gain is 0. Let S_N be the module of Definition 52.3.1. By Theorem 52.4.1 there is an integer $0 \leq l \leq mfb\,D_X$ such that the colength of S_N in S_η divides N^l, and for every twist ϑ, every chain datum Ψ for ϑ and every $\varphi \in S_{\mathrm{ram}} \cap S_N$, the form $B_{\vartheta,\Psi}\varphi$ has valuation at least $-2mfb$. The elements of S_N are forms on X_0, not all of them source forms; at $p = N$ the module of Theorem 48.7.1 is $S' = S_N \cap S_\eta$.

The *allowed loss* is

$$\mathrm{loss}(p) = \begin{cases} 2L_p & \text{if } p < x_1 \text{ is prime and } \chi_K(p) \neq 1, \\ 2mfb & \text{if } p = N, \\ 0 & \text{otherwise.} \end{cases}$$

Problem 48.6.1. Let $m \geq 2$, $p \geq 2$, and $p \equiv \pm 1 \pmod m$. Then $p = mc - 1$ or $p = mc + 1$ for an integer c with $1 \leq c \leq p$ and $m \leq 2p/c$.

Let $T_0 = 4fa(\log b)^2 \log x_1$.

Problem 48.6.2. For a prime $p < x_1$ with $\chi_K(p) \neq 1$ there is an integer $1 \leq c \leq p$ with $p \in \{mc - 1, c, mc + 1\}$ and $\mathrm{loss}(p)\log p \leq T_0/c$.

The term of N is also at most T_0: the scale inequalities of Chapter 33 give $2mfb\log N \leq T_0$ (they give $\log N \leq 30\,m\log b$ and $m \leq 2\sqrt{x}$, and imply $(\log b)\log x_1 \geq 60$). In sums over natural numbers we set $\log 0 = 0$.

Problem 48.6.3. For every finite set A of natural numbers, $\sum_{p\in A}\mathrm{loss}(p)\log p \leq 4T_0(1 + \log x_1)$.

Problem 48.6.4. If $(\log x_1)^6 \leq \log b$ and $\log x_1 \geq 3$, then $4T_0(1 + \log x_1) \leq U$.

Both hypotheses of Problem 48.6.4 hold for the data of Chapter 33.

48.7. The theorem

The four kinds of primes are: $p \neq N$ split or at least x_1, with S_η and $l = 0$ (Section 48.3); $p < x_1$ non-split and not exceptional, with S_η and $l = 0$ (Section 48.3); $p < x_1$ exceptional, with S' (Section 48.4); and $p = N$, with $S' = S_N \cap S_\eta$ and the integer l of Theorem 52.4.1 (Section 48.6). These four cases give the following theorem for ramified inputs.

Theorem 48.7.1. *Let p be prime and $\eta\colon \mathbb{C} \to \mathbb{C}_p$ a ring map. There are an integer $l \geq 0$ with $l \leq \operatorname{loss}(p)\, D_X$ and an $\mathcal{O}_\eta$-submodule $S' \subseteq S$ whose colength in S_η divides p^l, such that, for every twist ϑ, every chain datum Ψ for ϑ with $p \nmid \operatorname{Nm} Q_\vartheta$, and every $\varphi \in S' \cap S_{\mathrm{ram}}$, the form $B_{\vartheta,\Psi}\varphi$ has valuation at least* $\operatorname{gain}(p) - \operatorname{loss}(p)$.

Intersecting S' with $S_{\mathrm{ram},\eta}$ keeps the bound on its colength, now in $S_{\mathrm{ram},\eta}$. The definition of loss gives its nonnegativity and vanishing, and Problems 48.6.3 and 48.6.4 bound its weighted sum. This gives the theorem of this chapter.

Theorem 48.7.2. *There are real numbers* $\operatorname{err}(p)$, $p \in \mathbb{N}$, *with the following properties.*

(a) $\operatorname{err}(p) \geq 0$ *for every p.*
(b) *If $p \neq N$, and $\chi_K(p) = 1$ or $x_1 \leq p$, then* $\operatorname{err}(p) = 0$.
(c) $\sum_{p \in A} \operatorname{err}(p) \log p \leq U$ *for every finite set A of natural numbers.*
(d) *For every prime p and every ring map $\eta\colon \mathbb{C} \to \mathbb{C}_p$ there are an integer $l \geq 0$ with $l \leq \operatorname{err}(p)\, D_X$ and an $\mathcal{O}_\eta$-submodule $S' \subseteq S_{\mathrm{ram},\eta}$ whose colength in $S_{\mathrm{ram},\eta}$ divides p^l, such that for every twist ϑ, every chain datum Ψ for ϑ with $p \nmid \operatorname{Nm} Q_\vartheta$, and every $\varphi \in S'$, the form $B_{\vartheta,\Psi}\varphi$ has valuation at least* $\operatorname{gain}(p) - \operatorname{err}(p)$.

Its proof takes err = loss. The dimension in (d) is that of all source forms, while the colength is measured in the integral ramified ones; the module S' depends on p and η and serves every twist of level prime to p and every chain datum for that twist.

Theorem 48.7.2 is the divisibility input to Theorem A: Chapter 42 combines (c) and (d) with the seesaw identity of Chapter 43 and further inputs to bound the index of finite families in the images $A_s(S_{\mathrm{ram}}^{\mathrm{int}})$ of the integral ramified source forms under the normalized translates. Chapters 49 and 50 prove input (iii), Chapter 52 treats the level prime and Chapter 53 the exceptional primes; Chapter 51 bounds the size of the composite lift, against which Theorem A sets this divisibility.

In the Lean formalization. In the Lean proof [GL], Theorem 48.7.2 is `New.Data.exists_err_gaugeLe_compositeLift` and Theorem 48.7.1 is `New.Data.exists_colengthDvd_gaugeLe_compositeLift`, in `New/UpperBound/Divisibility/LocalDivisibility.lean`. The definitions are `Data.gain`, `Data.localPrimeSum`, `Data.loss` (L_p), `Data.allowedLoss` (loss), `Data.IsExceptional`, `Data.IsMarked`, `Data.IsFullMark`, `Data.IsWeakChainDatum` and `Data.restrictedChain`. The inputs read in the text are `Data.IsChainDatum.exists_isWeakChainDatum_compositeLift_eq` (Theorem 48.3.4), `Data.IsWeakChainDatum.gaugeLe_restrictedChain_one` (i), `Data.IsWeakChainDatum.translateDatum_mem_standardData` and `Data.IsWeakChainDatum.gaugeLe_restrictedChain_of_mem_raises` (ii), and `Data.IsMarked.isOntoUpToColength_scaledHeckeOperator`. Theorem 48.5.1 is `FrobeniusCycle.elementary_divisors`, with the hypotheses `IsLargeDegree`, in `New/UpperBound/ElementaryDivisors/ElementaryDivisorTheorem.lean`.

Hints

§48.1.

48.1.1: Show $d \equiv q_0/2 - 1 \pmod{q_0}$, so $d \equiv -1$ modulo 8 and modulo each odd prime dividing q_0. Then quadratic reciprocity.

48.1.2: I_p is the set of odd $e \geq 1$, and $c_p = 1$.
48.1.3: If $\chi_K(p) = 1$, I_p is empty. If $p \geq x_1$, compare y/p^e with a/x_1.
48.1.4: Compute $1 - \chi_K(p^e)$ in the three cases inert, ramified, split. For $p^e > a$ the term of $s_{\mathrm{fin},p}$ vanishes.

§48.2.

48.2.1: τ and $[-p^e]\tau$ have class 1 modulo q_0. For $p = d$, compute $-d^e$ modulo q_0 separately for even and odd e, using $4 \mid q_0$ and the congruence for d in the hint to Problem 48.1.1.
48.2.2: Decompose $(\mathbb{Z}/18480)^\times$ by the Chinese remainder theorem and find its elements of odd order. Use a prime search for the two minima.
48.2.3: At each of the f places, a geometric series of ratio at most $1/2$.
48.2.4: Two cases, according as $p \equiv \pm 1 \pmod m$ (Problem 48.2.3 with $o = 1$) or not; in the second, Problem 48.2.1 and $m \leq p^{r_p}$.
48.2.5: Every $(\tau, 1)$ with $\tau \in \Phi_a$ is a collision.

§48.3.

48.3.1: The sup norm is ultrametric.
48.3.2: Theorem 48.3.4; then (ii) and (iii) with $\Phi' = \varnothing$.

§48.4.

48.4.1: The relation $v_{[-p^e]\sigma} = \bar{v}_\sigma$.
48.4.2: Problem 48.2.3 with $o = 1$.
48.4.3: The ultrametric inequality.
48.4.4: A product of two matrices.
48.4.5: Each $\tau \in \Phi_a$ induces one prime. Bound j_p by $2mfa/p + 1$.

§48.5.

48.5.1: Go once around $\mathbb{Z}/N_0$. For the size, $N_0 n \log q/\theta > 1$; for the example, $\log 5 < 2$.

§48.6.

48.6.1: $mc \leq p + 1 \leq 2p$.
48.6.2: Problem 48.6.1, or $c = p$.
48.6.3: Each $c \leq x_1$ serves at most the four numbers N, $mc - 1$, c, $mc + 1$; give N the value $c = 1$.
48.6.4: Compare $16\,t(1 + t)$ with t^6.

References

[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/`.