THE BOUND IS ATTAINED

Prerequisites. Chapter 15, *The invariant derivation at a supersingular prime*: the lemniscate curve with parameter X, the lemniscate sine sl, the ring $\mathcal{O} = \mathbb{Z}_p[\mathrm{i}]$, the invariant derivation D, and Problems 15.2.2 and 15.2.3 (Section 15.2); the function E_p, the parameter T, the unit ε, the operator H, Problems 15.4.4 and 15.4.6, and Theorem 15.4.1 (Section 15.4). For the last section: the shape of the bound in Theorem 16.3.1, and the sparse sets of Chapter 4. Legendre's formula for $v_p(n!)$. The field $\mathbb{C}_p$, its valuation v with $v(p) = 1$, and its valuation ring.

19.1. The least valuation

Chapter 15 proves a lower bound for the divisibility of derivatives on the lemniscate. Is it the truth, or does every function gain more? Throughout this section and the next, $p \equiv 3 \pmod 4$ is a prime, $q := p^2$, $\mathcal{O} = \mathbb{Z}_p[\mathrm{i}]$, and $D = d/du$ is the invariant derivation, so that $(D^n g)(0) = n!\,[u^n]\,g(\mathrm{sl}\,u)$ for $g \in \mathcal{O}[[X]]$ (Problem 15.2.3). Recall Theorem 15.4.1: for $g \in \mathcal{O}[[X]]$ and every $n \geq 0$,

$$v_p\big((D^n g)(0)\big) \;\geq\; E_p(n) = \sum_{i \geq 1,\ i \text{ odd}} \Big\lfloor \frac{n}{p^i} \Big\rfloor .$$

Let $\mu(n)$ be the least value of $v_p((D^n g)(0))$ over $g \in \mathcal{O}[[X]]$. How far is $\mu(n)$ from $E_p(n)$?

Problem 19.1.1. $\mu(0) = 0$. For $n \geq 1$ the least value $\mu(n)$ exists and is attained by a power X^i with $1 \leq i \leq n$: $\mu(n) = \min_{1 \leq i \leq n} v_p\big(n!\,[u^n]\,\mathrm{sl}^i\,u\big)$.

Problem 19.1.2. For $p = 3$: $\mu(11) = 4$, while $E_3(11) = 3$.

So the bound of Theorem 15.4.1 is not attained in every degree. The rest of this section shows that μ is superadditive; Section 19.2 computes it at the powers of q.

Problem 19.1.3. Let $g \in \mathcal{O}[[X]]$, and write $g(X \oplus X') = \sum_{i,j} a_{ij} X^i X'^j$ with the group law $\oplus$ of Problem 15.2.2. Then $a_{ij} \in \mathcal{O}$, and for all $n, n' \geq 0$

$$(D^{n+n'} g)(0) = \sum_{i,j} a_{ij}\,(D^n X^i)(0)\,(D^{n'} X^j)(0).$$

Problem 19.1.4. $\mu(n + n') \geq \mu(n) + \mu(n')$ for all $n, n' \geq 0$.

Problem 19.1.5. Let $\phi\colon \mathbb{N} \to \mathbb{R}_{\geq 0}$ be superadditive, and let $\gamma' \geq 0$. If $\phi(N) \leq \gamma' N$ for infinitely many N, then $\phi(n) \leq \gamma' n$ for every $n \geq 0$.

19.2. The powers of q

Let

$$\gamma_p := \frac{p}{p^2 - 1} = \frac{1}{p} + \frac{1}{p^3} + \frac{1}{p^5} + \cdots .$$

Problem 19.2.1. $E_p(n) \leq \gamma_p n$ for every $n \geq 0$, and $E_p(q^j) = \gamma_p(q^j - 1)$ for every $j \geq 0$.

Date: November 26, 2026.

In the degrees q^j the function X itself attains the bound.

Problem 19.2.2. $v_p\big((D^{q^j}X)(0)\big) = E_p(q^j)$ for every $j \geq 0$. (For $p = 3$: $(D^9X)(0) = 3024$, of valuation 3; and $v_3((D^{81}X)(0)) = 30$.)

Problem 19.2.3. $v_p\big([u^{q^j}]\ \mathrm{sl}\, u\big) = -(q^j-1)/(q-1)$ for every $j \geq 0$. (For $p = 3$: $[u^9]\ \mathrm{sl}\, u = 1/120$; for $p = 7$: $v_7([u^{49}]\ \mathrm{sl}\, u) = -1$.)

Thus $\mu(q^j) = E_p(q^j) = \gamma_p(q^j - 1)$. Problems 19.1.4, 19.1.5 and 19.2.2, with Theorem 15.4.1, prove the following.

Theorem 19.2.1. *Let $p \equiv 3 \pmod 4$. For every $n \geq 0$,*

$$E_p(n) \ \leq\ \mu(n) \ \leq\ \gamma_p n,$$

and $\mu(q^j) = E_p(q^j)$, attained by $g = X$, for every $j \geq 0$.

Problem 19.2.4. $0 \leq \gamma_p n - E_p(n) < h + 2$, where h is the number of positive odd integers i with $p^i \leq n$. Hence $\mu(n) = \gamma_p n + O(\log n)$.

So γ_p is the exact rate, and Theorem 15.4.1 loses at most a logarithm in every degree. A computation of $\mu(n)$ by Problem 19.1.1 gives, for instance,

$p = 3$, n	9	10	11	20	27	40	80	81
$E_3(n)$	3	3	3	6	10	14	28	30
$\mu(n)$	3	3	4	7	10	14	29	30
$3n/8$	3.375	3.75	4.125	7.5	10.125	15	30	30.375

For $p = 7$ one finds $\mu(n) = E_7(n)$ for $n \leq 54$, and $\mu(55) = 8 > E_7(55) = 7$. We have checked $E_p(n) \leq \mu(n) \leq \gamma_p n$ by machine for $p = 3, 7$ and $n \leq 100$.

19.3. Curves with complex multiplication by $\mathbb{Q}(\sqrt{-d})$

The proof works with curves whose complex multiplication is by $K = \mathbb{Q}(\sqrt{-d})$ for a prime $d \equiv 7 \pmod 8$, and with every prime p, split, inert or ramified in K. The lemniscate is not among these curves, since $\mathbb{Q}(\mathrm{i})$ is not of this form; it serves here as the simplest case. Let q_p be the norm of a prime of K above p: $q_p = p^2$ if p is inert and $q_p = p$ otherwise. Let $\pi_p := \sqrt{-d}$ if $p = d$ and $\pi_p := p$ otherwise. In valuations and congruences we use its image under a chosen ring homomorphism $\eta\colon \mathbb{C} \to \mathbb{C}_p$; then $c_p := v(\pi_p)$ is $\frac{1}{2}$ if $p = d$ and 1 otherwise. Put

$$\rho_p := \frac{c_p}{q_p - 1}, \qquad \gamma_p := \frac{1}{p-1} - \rho_p.$$

For the lemniscate at $p \equiv 3 \pmod 4$ we used $\gamma_p = p/(p^2-1)$; by Problem 19.3.1 the two agree at inert primes.

Problem 19.3.1. $\gamma_p = 0,\ p/(p^2-1),\ 1/(2(p-1))$ according as p is split, inert or ramified in K. The inert value is the rate γ_p of Section 19.2.

Let $\Lambda \subset \mathbb{C}$ be a lattice with $\mathcal{O}_K\Lambda \subseteq \Lambda$, let $t \in \mathbb{C}$ with $t \notin \Lambda$, $2t \in \Lambda$, and $\omega t, \bar\omega t \notin \Lambda$ for $\omega = (1 + \sqrt{-d})/2$, and let $a_1 \in \mathbb{C}$ with $a_1^2 = 12\wp(t)$; assume the normalization $g_2(\Lambda) = 12\wp(t)^2 - 4$. Let $y(z)$ be the Taylor series at 0 of $\frac{1}{2}\big(\wp'(z+t) - a_1(\wp(z+t) - \wp(t))\big)$, with η applied to its coefficients; it begins with z. Let $\mathfrak{o}$ be the valuation ring of $\mathbb{C}_p$, and $\mathfrak{o}[[y]]$ the ring of series $\Psi(y(z))$ with $\Psi \in \mathfrak{o}[[W]]$. The proof establishes the following.

Theorem 19.3.1. *Let $d \equiv 7 \pmod 8$ be prime, Λ, t, a_1 as above, p a prime and $\eta\colon \mathbb{C} \to \mathbb{C}_p$ a ring homomorphism. For every $n \geq 0$ there is $g \in \mathfrak{o}[[y]]$ with*

$$v\big(n!\,[z^n]g\big) \;\leq\; \gamma_p n.$$

In the Lean formalization. In the Lean proof [GL] this is `CMLattice.katz_divisibility_limit`, in `New/Derivatives/Sharpness/OneCurve.lean` of the readable edition, stated with norms: $|n!\,[z^n]g| \geq (p^{-\gamma_p})^n$. The Lean proof establishes it as in Sections 19.1 and 19.2: the greatest norm of $n!\,[z^n]g$ over $g \in \mathfrak{o}[[y]]$ is attained by a power of y, it is submultiplicative in n, and a lemma of Fekete's type (Problem 19.1.5, in multiplicative form) carries a bound at the degrees q_p^j to all degrees. At those degrees it uses, in place of Problem 19.2.2, the part y_1 of y in degrees $\equiv 1 \pmod{q_p - 1}$: the coefficient $[z^{q_p^j}]\,y_1$ has valuation $-(q_p^j - 1)\rho_p$, as in Problem 19.2.3. It proves this by rescaling: for some ϖ of valuation ρ_p the series $y_1(\varpi z)/\varpi$ is integral and congruent to $\sum_{j\geq 0} z^{q_p^j}$ modulo π_p.

The proof uses Theorem 19.3.1 in many variables, along a linear form whose coefficients are units.

Problem 19.3.2. Return to the lemniscate of Section 19.1, with $p \equiv 3 \pmod 4$ and $\mathcal{O} = \mathbb{Z}_p[\mathrm{i}]$. Let $g \in \mathcal{O}[[X]]$, let $\beta_j \in \mathcal{O}^\times$ for j in a finite set J, and let $F\big((u_j)_{j\in J}\big) := g\big(\mathrm{sl}(\sum_{j\in J} \beta_j u_j)\big)$. For every multi-index ν,

$$\nu!\,[u^\nu]\,F = \beta^\nu\,(D^{|\nu|}g)(0),$$

so that $v_p(\nu!\,[u^\nu]\,F) = v_p\big((D^{|\nu|}g)(0)\big)$; for every ν there is such a g for which this value is at most $\gamma_p|\nu| = p|\nu|/(p^2-1)$.

19.4. Many places

In the proof the one-copy variables are indexed by the infinite places $\tau \in \Phi$ of the CM field E, each with its weight $\kappa(\tau)$, as in Chapter 33. For a prime p let $\mathcal{I}_p$ be the set of odd $e \geq 1$ if p is inert, of all $e \geq 1$ if $p = d$, and empty if p splits. For $e \in \mathcal{I}_p$ the *partner* of τ is $[-p^e]\tau$. The divisibility predicted at p for a derivative of order κ_0 in the variable of τ is

$$s_{\mathrm{fin},p}(\kappa_0, \tau) = v(\pi_p) \sum_{e\in\mathcal{I}_p} \Big(\frac{\kappa_0}{p^e} - \kappa([-p^e]\tau)\Big)_+,$$

the part at p of the prime sum of Chapter 33, divided by $2\log p$, without the cutoff at a. Each term has the shape of the bound in Theorem 16.3.1, with the weight of the partner in the place of w.

Problem 19.4.1. For real $\kappa_0 \geq 0$, $s_{\mathrm{fin},p}(\kappa_0, \tau) \leq \gamma_p\kappa_0$, with equality if κ vanishes at all partners of τ. Hence $\sum_\tau s_{\mathrm{fin},p}(\kappa(\tau), \tau) \leq \gamma_p \sum_\tau \kappa(\tau)$.

Setting all partner weights to zero in $s_{\mathrm{fin},p}(\kappa_0, \tau)$ gives $\gamma_p\kappa_0$. By Theorem 19.3.1, a larger linear rate cannot hold as a divisibility bound for every series on one curve. In independent variables the least valuations add.

Problem 19.4.2. Use the lemniscate, the prime $p \equiv 3 \pmod 4$, the ring $\mathcal{O}$ and the function μ of Section 19.1. For $n, n' \geq 0$, the least value of $v_p\big((D_1^n D_2^{n'} g)(0)\big)$ over $g \in \mathcal{O}[[X_1, X_2]]$, with D_1, D_2 the invariant derivations in the two variables, is $\mu(n) + \mu(n')$.

If $e \in \mathcal{I}_p$ and both $\kappa(\tau)$ and $\kappa([-p^e]\tau)$ are positive, then $s_{\mathrm{fin},p}(\kappa(\tau),\tau) < \gamma_p\kappa(\tau)$: a partner lowers the prediction. By Problem 4.1.4, for a prime $p \le kt$ with $p \nmid q_1$ and for $0 < i < j < l_0(s)$, the places τ, $[-p]^i\tau$, $[-p]^j\tau$ are not all in Φ_b. Call (τ, e) a *near pair* if $e \in \mathcal{I}_p$, $2e < l_0(s)$, and both τ and its partner lie in Φ_b. For each nonsplit prime $p \le k$, the proof uses the sparsity of Φ_b (Chapter 4) to show that distinct near pairs have distinct starts and distinct ends, and that no end is a start.

Problem 19.4.3. Let Γ be an abelian group, $\xi \in \Gamma$, $\mathcal{B} \subseteq \Gamma$ and $L \ge 1$, such that for no $x \in \Gamma$ and $0 < i < j < L$ are x, $\xi^i x$, $\xi^j x$ all in $\mathcal{B}$. Call (x, e) near if $0 < 2e < L$ and $x, \xi^e x \in \mathcal{B}$. Then two near pairs with the same start, or with the same end, are equal, and the end of a near pair is never the start of one.

For every degree vector in the range of Theorem 63.5.1, the proof chooses one nonzero scalar c_{att} for all primes. For each modulus and p-adic place in that theorem, some Taylor coefficient on twelve copies, normalized as in the theorem, has valuation at most $\sum_{\tau\in\Phi} s_{\mathrm{fin},p}(\kappa(\tau),\tau)$. This sum also enters the divisibility bound for the composite lift in Chapter 48. The proof uses Theorem 19.3.1 in several variables and the sparsity of Φ_b (Problem 19.4.3). Chapter 63 takes this up: the version at many places, on twelve copies of the variables.

Hints

§19.1.

19.1.1: Write $g = \sum_i a_i X^i$ with $a_i \in \mathcal{O}$; $\mathrm{sl}^i u$ begins with u^i. Use the ultrametric inequality.

19.1.2: $\mathrm{sl}^i u$ has only exponents $\equiv i \pmod 4$, and $[u^{11}]\,\mathrm{sl}^3 u = 11/200$. As a numerical check, $(D^{11}X^3)(0) = 2195424$.

19.1.3: Expand $g(\mathrm{sl}(u + w))$ in two ways and compare the coefficients of $u^n w^{n'}$.

19.1.4: Problem 19.1.3.

19.1.5: Treat $n = 0$ separately. For $n > 0$, write $N = sn + s'$ with $0 \le s' < n$.

§19.2.

19.2.1: Geometric series.

19.2.2: Start with $(DX)(0) = 1$. For the induction step take $j \ge 1$. $X \in \mathcal{O}[[T]]$; $D^{q^j} = (p^p\varepsilon)^{q^{j-1}} H^{q^{j-1}}$ by Problem 15.4.4; compare $H^{q^{j-1}}$ with $D^{q^{j-1}}$ by Problem 15.4.6 at level $2j - 2$.

19.2.3: Legendre's formula for $v_p(q^j!)$.

19.2.4: Write $\gamma_p n - E_p(n)$ as a sum over odd i of $n/p^i - \lfloor n/p^i \rfloor$, and bound the terms with $p^i > n$ by a geometric series.

§19.3.

19.3.2: $(D^n g)(0) = n!\,[w^n]\,g(\mathrm{sl}\, w)$, and the multinomial theorem; Theorem 19.2.1.

§19.4.

19.4.1: Compare each summand with its value when the partner has weight zero.

19.4.2: As in Problem 19.1.1, the least value is attained by a monomial $X_1^i X_2^j$.

19.4.3: For a common end $\xi^e x = \xi^{e'} x'$ with $e < e'$, consider x', $\xi^{e'-e}x'$, $\xi^{e'}x'$.

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/`.