THE INVARIANT DERIVATION AT A SUPERSINGULAR PRIME

Prerequisites. Formal groups of elliptic curves, their height, and supersingular reduction [Si1, Ch. IV and §§V.3–V.4]. The Weierstrass functions $\wp$ and σ [Si2, §I.5]. Legendre's formula $v_p(n!) = \sum_{i\ge1}\lfloor n/p^i\rfloor$, Kummer's theorem that $v_p\binom{m+n}{m}$ is the number of carries in the base-p addition of m and n, and the Lagrange inversion formula. From Chapter 12, *Complex tori, theta functions and periods*, we use the lattice $\varpi\mathbb{Z}[\mathrm{i}]$ of Problem 12.1.9. From Chapter 14, *Complex multiplication and reduction at an inert prime*: formal groups, their height and the invariant derivation (Section 14.2), and Problem 14.2.3; Section 16.3 proves the congruence $D^p \equiv \lambda D \pmod p$ stated there. Chapter 17, *The isotropic plane*, continues this one.

16.1. Gaussian moments

Let $\zeta = e^{2\pi\mathrm{i}/8}$, and for integers $a, w \ge 0$ consider the moments

$$m(a,w) := \sum_{x\in\mathbb{Z}[\mathrm{i}]^2} (x_1+\zeta x_2)^a\,(x_1-\zeta x_2)^w\,e^{-\pi(|x_1|^2+|x_2|^2)}.$$

After a normalization they are rational numbers. How divisible are they by a prime $p \equiv 3 \pmod 4$, that is, by a prime that is inert in $\mathbb{Q}(\mathrm{i})$?

Let sl be the lemniscate sine, the meromorphic function with $\mathrm{sl}(0)=0$, $\mathrm{sl}'(0)=1$ and $\mathrm{sl}'^2 = 1-\mathrm{sl}^4$, and let $\varpi := 2\int_0^1 (1-t^4)^{-1/2}\,dt$. Let $\wp$ and σ be the Weierstrass functions with $g_2 = 4$ and $g_3 = 0$, whose period lattice is $\Lambda = \varpi\mathbb{Z}[\mathrm{i}]$ (Problem 12.1.9). Let

$$F := \sigma^2\wp.$$

Problem 16.1.1. $\wp = \mathrm{sl}^{-2}$.

Problem 16.1.2. F is entire and even, $F(\mathrm{i}u) = F(u)$, and $F(u) = 1 + \frac{1}{6}u^4 + \frac{17}{2520}u^8 + O(u^{12})$.

Problem 16.1.3. Let $\vartheta_0 := \sum_{\alpha\in\mathbb{Z}[\mathrm{i}]} e^{-\pi|\alpha|^2}$. For $z\in\mathbb{C}$,

$$\sum_{\alpha\in\mathbb{Z}[\mathrm{i}]} e^{-\pi|\alpha|^2+z\alpha} = \vartheta_0\,F\Big(\frac{\varpi z}{2\pi}\Big).$$

Let $\Theta(Z_1,Z_2) := F(Z_1)F(Z_2)$ on $\mathbb{C}^2$, let $e_\pm := (1,\pm\zeta)$, and let

$$t(a,w) := \partial_s^a\partial_t^w\,\Theta(se_+ + te_-)\big|_{s=t=0}, \qquad \Theta(se_+ + te_-) = F(s+t)\,F\big(\zeta(s-t)\big).$$

Problem 16.1.4. $m(a,w) = \vartheta_0^2\,(\varpi/2\pi)^{a+w}\,t(a,w)$.

Problem 16.1.5. The numbers $t(a,w)$ are rational, $t(a,w) = t(w,a)$, and $t(a,w) = 0$ unless $a + 5w \equiv 0 \pmod 8$.

For instance $t(3,1) = 8$, $t(4,4) = 448$ and $t(8,0) = -576$. The table lists $v_{11}(t(a,w))$ for $w \le 2$ and the first nine values of $a \ge 8$ allowed by Problem 16.1.5.

Date: November 24, 2026.

$w=0$, $a=$	8	16	24	32	40	48	56	64	72
v_{11}	0	1	2	2	3	4	5	5	6
$w=1$, $a=$	11	19	27	35	43	51	59	67	75
v_{11}	0	0	1	2	2	3	4	5	5
$w=2$, $a=$	14	22	30	38	46	54	62	70	78
v_{11}	0	0	0	1	2	2	3	4	5

In this range $v_{11}(t(a,w)) = \max(\lfloor a/11 \rfloor - w, 0)$. Each derivative in the second direction seems to cost one factor of 11. By contrast, $t(8,0) = -576$ is prime to 7. This chapter treats one variable: what p divides the derivatives of a function on the lemniscate, and why F alone does not gain. The sequel, *The isotropic plane*, proves a lower bound of the shape above at every prime $p \equiv 3 \pmod 8$.

16.2. The lemniscate and its formal group

Let E be the curve $y^2 = 1 - X^4$ with origin $(0,1)$. It is a curve of genus one with good reduction at every odd prime. The map $u \mapsto (\operatorname{sl} u, \operatorname{sl}' u)$ identifies $\mathbb{C}/L$ with $E(\mathbb{C})$, where $L \subset \Lambda$ is the period lattice of sl. The function X is a parameter at the origin, $du = dX/y$ is an invariant differential, and the addition law is

$$\operatorname{sl}(u+v) = \frac{\operatorname{sl} u \, \operatorname{sl}' v + \operatorname{sl} v \, \operatorname{sl}' u}{1 + \operatorname{sl}^2 u \, \operatorname{sl}^2 v}.$$

Let $D := d/du = y\, d/dX$ be the invariant derivation, and let $\ell(X) := \int_0^X (1 - v^4)^{-1/2}\, dv$ be the logarithm, so that $\operatorname{sl}(\ell(X)) = X$.

Problem 16.2.1. $\operatorname{sl} u = u - \frac{1}{10}u^5 + \frac{1}{120}u^9 - \frac{11}{15600}u^{13} + \cdots$. Only exponents $\equiv 1 \pmod 4$ occur, $\operatorname{sl}(\mathrm{i}u) = \mathrm{i} \operatorname{sl} u$, and the lattice L satisfies $\mathrm{i}L = L$.

Problem 16.2.2. The formal group law $X \oplus X'$, defined by $\operatorname{sl} u \oplus \operatorname{sl} v = \operatorname{sl}(u+v)$, has coefficients in $\mathbb{Z}[\frac{1}{2}]$, and $X \mapsto \mathrm{i}X$ is an endomorphism of it.

Problem 16.2.3. D maps $\mathbb{Z}[\frac{1}{2}][[X]]$ into itself, and $(D^n f)(0) = n!\,[u^n]\, f(\operatorname{sl} u)$ for $f \in \mathbb{Q}[[X]]$.

Fix an odd prime p, let $\mathcal{O} := \mathbb{Z}_p[\mathrm{i}]$, and let v_p be the valuation with $v_p(p) = 1$. For $p \equiv 3 \pmod 4$, $\mathcal{O}$ is the ring of integers of the unramified quadratic extension of $\mathbb{Q}_p$. It contains ζ, since 8 divides $p^2 - 1$. We write $\hat{E}$ for the formal group of Problem 16.2.2 over $\mathcal{O}$.

Problem 16.2.4. For each $\alpha \in \mathcal{O}$ the series $[\alpha](X) := \operatorname{sl}(\alpha \ell(X))$ lies in $\mathcal{O}[[X]]$. It is the unique endomorphism of $\hat{E}$ with $[\alpha](X) = \alpha X + O(X^2)$.

When $p \equiv 3 \pmod 4$, this action of $\mathcal{O}$ makes $\hat{E}$ a formal $\mathcal{O}$-module of the kind constructed by Lubin and Tate [LT]; we use only Problem 16.2.4. For these primes E is supersingular and $\hat{E}$ has height two [Si1, Thm. V.3.1]. Indeed E is isogenous to $y^2 = x^3 - x$ by $(X, y) \mapsto (X^{-2}, -yX^{-3})$, and that curve is supersingular exactly when $p \equiv 3 \pmod 4$ [Si1, §V.4]. Section 16.3 shows what height two does to D.

16.3. The pth power of the invariant derivation

Let f be a function on E, regular at the origin, with expansion in $\mathcal{O}[[X]]$. Its derivatives $(D^n f)(0)$ are integral by Problem 16.2.3. We show that they are divisible by $p^{\lfloor n/p \rfloor}$ when $p \equiv 3 \pmod 4$. The smallest case is $p = 3$: $DX = y$, $D^2X = -2X^3$ and $D^3X = -6X^2 y$.

For a series f, let $\tau_Y f(X) := f(X \oplus Y)$, a series in two variables.

Problem 16.3.1. Modulo p, the operator D^p is a derivation of $\mathcal{O}[[X]]$.

Problem 16.3.2. Let k be a field of characteristic p, and let δ be a continuous derivation of $k[[X]]$ with $\delta\tau_Y = \tau_Y\delta$. Then $\delta = (\delta X)(0)\, D$. The operator D itself commutes with τ_Y.

Thus $D^p \equiv \lambda_p D \pmod p$, with $\lambda_p \equiv (D^p X)(0) = p!\,[u^p]\,\mathrm{sl}\,u$.

Problem 16.3.3. If $p \equiv 3 \pmod 4$, then $\lambda_p \equiv 0$, so that $D^p\,\mathcal{O}[[X]] \subseteq p\,\mathcal{O}[[X]]$.

Problem 16.3.4. Let $p \equiv 3 \pmod 4$, let $f \in \mathcal{O}[[X_1, X_2]]$, and let D_1, D_2 be the invariant derivations in the two variables. Then $(D_1^a D_2^w f)(0) \in p^{\lfloor a/p \rfloor}\mathcal{O}$.

At $p \equiv 1 \pmod 4$ there is no such gain: λ_p is then a unit, since $\lambda_p \equiv p\,[X^p]\,\ell = 4^{-m}\binom{2m}{m}$ for $p = 4m+1$ by the argument of Problem 14.2.3, and for instance $(D^5 X)(0) = -12$. Divisibilities of this kind on formal groups of any height are studied by Katz [Ka].

16.4. The higher odd levels

At $p = 3$, the integer $(D^{29}X)(0)$ is divisible exactly by 3^{10}, one more than $\lfloor 29/3 \rfloor = 9$. Where does the extra factor come from? Throughout this section $p \equiv 3 \pmod 4$ and $q := p^2$, and we write

$$E_p(n) := \sum_{\substack{i \geq 1 \\ i \text{ odd}}} \Big\lfloor \frac{n}{p^i} \Big\rfloor.$$

The answer is that D^n gains $p^{E_p(n)}$. The extra factor at p^3 comes from the coefficient of X^q in the logarithm.

Problem 16.4.1. $[X^{4m+1}]\,\ell = \binom{2m}{m}\big/\big(4^m(4m+1)\big)$, and ℓ has p-integral coefficients in all degrees less than q.

Problem 16.4.2. $p\,[X^q]\,\ell \equiv -1 \pmod p$. (For $p = 3$: $[X^9]\,\ell = 1/24$.)

By Problems 16.4.1 and 16.4.2, the truncation T of $\ell(X) + X^q/p$ to degree at most q lies in $X + X^2\mathbb{Z}_{(p)}[X]$. It is therefore a parameter on $\hat{E}$ over $\mathbb{Z}_{(p)}$, and $\mathcal{O}[[T]] = \mathcal{O}[[X]]$. In this parameter

$$\ell = T - \frac{T^q}{p} + O(T^{q+1}), \qquad g(z) := \ell^{-1}(z) = z + \frac{z^q}{p} + O(z^{q+1}),$$

where $O(\cdot)$ allows arbitrary rational coefficients. Write the group law in T again as $\oplus$, and define operators Δ_j on $\mathcal{O}[[T]]$ by $f(T \oplus Y) = \sum_{j \geq 0} (\Delta_j f)(T)\, Y^j$. They commute with each other and with D, and $\Delta_1 = D$.

Problem 16.4.3. For $f \in \mathcal{O}[[T]]$, $f(T \oplus g(z)) = \sum_{n \geq 0} (D^n f)(T)\, z^n/n!$. Consequently $D^p = p!\,\Delta_p$ and $D^q = q!\,(\Delta_q + D/p)$.

Problem 16.4.4. $\varepsilon := q!/p^{p+1}$ is a p-adic unit, and $D^q = p^p \varepsilon\, H$ with $H := D + p\Delta_q$.

Problem 16.4.5. Let A, B be commuting $\mathcal{O}$-linear operators on a torsion-free $\mathcal{O}$-module V with $(A - B)V \subseteq pV$. Then $(A^p - B^p)V \subseteq p^2 V$.

Let $e_j := E_p(p^j) = p^{j-1} + p^{j-3} + \cdots$, the sum over the exponents $j-i$ with $i \le j$ odd. Thus $e_0 = 0$, $e_1 = 1$, $e_j = p^{j-1} + e_{j-2}$, and $e_j \le p\, e_{j-1} + 1$.

Problem 16.4.6. For every $j \ge 0$, as operators on $\mathcal{O}[[T]]$,

$$D^{p^j} \equiv 0 \pmod{p^{e_j}}, \qquad H^{p^j} \equiv D^{p^j} \pmod{p^{e_j+1}}.$$

Problem 16.4.7. $D^n\, \mathcal{O}[[X]] \subseteq p^{E_p(n)}\, \mathcal{O}[[X]]$ for every $n \ge 0$.

Problems 16.4.1–16.4.7 prove the following.

Theorem 16.4.1. *Let $p \equiv 3 \pmod 4$ and $f \in \mathcal{O}[[X]]$. Then $v_p\big((D^n f)(0)\big) \ge E_p(n)$ for every $n \ge 0$. The same holds for $f \in \mathcal{O}[[X_1, X_2]]$ and $D = D_1$, the invariant derivation in the first variable.*

The method gains nothing at the even levels. In Problem 16.4.4, D^q has the factor p^p, not the p^{p+1} one would get from $\lfloor q/p \rfloor + \lfloor q/q \rfloor$. The factor H gains nothing by itself, and the next gain comes from $H^p \equiv D^p$.

16.5. One theta function

The function F of Section 16.1 is not a function on E. Does it nevertheless gain? At $p = 3$ the valuations $v_3(F^{(k)}(0))$ for $k = 4, 8, \ldots, 60$ are

$$0,\ 0,\ 1,\ 1,\ 2,\ 2,\ 4,\ 4,\ 4,\ 4,\ 4,\ 5,\ 5,\ 7,\ 7,$$

far below $\lfloor k/3 \rfloor$.

Problem 16.5.1. $(\log F)'' = 2\,\mathrm{sl}^2$.

Let $b_n := (D^n X^2)(0) = n!\,[u^n]\ \mathrm{sl}^2\, u$, an element of $\mathbb{Z}[\frac{1}{2}]$. By Problem 16.5.1,

$$\log F(u) = 2 \sum_{n \ge 0} b_n \frac{u^{n+2}}{(n+2)!}.$$

Problem 16.5.2. Let $p \equiv 3 \pmod 4$ and $m := (p-3)/4$. Then $b_{p-1} \equiv -4^{-m} \binom{2m}{m} \pmod p$. In particular b_{p-1} is a p-adic unit. (For $p = 3$: $b_2 = 2$.)

Problem 16.5.3. Let $p \equiv 3 \pmod 4$. Then $F^{(p+1)}(0) \equiv 2b_{p-1} \pmod p$. Hence F, written as a series in $X = \mathrm{sl}\, u$, does not have p-integral coefficients. (For $p = 3$: $F^{(4)}(0) = 4$.)

Thus the coefficient of u^{p+1} in $\log F$ is c_p/p with $c_p = 2b_{p-1}/\big((p+1)(p-1)!\big)$ a unit. For $p = 3, 7, 11$ this coefficient is $\frac{1}{6}, -\frac{1}{140}, \frac{1}{2475}$, so $c_p = \frac{1}{2}, -\frac{1}{20}, \frac{1}{225}$. By the Exercise below, the exponential of such a term alone has derivatives of valuation about $k/(p^2-1)$; the values above fit this, since $v_3(F^{(60)}(0)) = 7$ and $60/8 = 7.5$. We do not know whether $v_p(F^{(k)}(0)) = k/(p^2-1) + O(\log k)$ holds in general for k divisible by 4; the other derivatives vanish at 0 by Problem 16.1.2.

The first non-integral term of $\log F$ is $c_p u^{p+1}/p$, a function of one variable. To remove it one needs a second variable. The plane should be chosen so that the restriction of the theta function to each axis is integral, and the remaining factor is 1 on both axes. Chapter 17, *The isotropic plane*, shows that the directions $e_\pm$ of Section 16.1 achieve this.

Exercise. Let c be a p-adic unit, $g(u) := \exp(cu^{p+1}/p)$, and $k = (p+1)m$. Then

$$v_p\big(k!\,[u^k]\,g\big) = \frac{k}{p^2-1} + \frac{s_p(m) - s_p(k)}{p-1},$$

where s_p is the sum of base-p digits.

Hints

§16.1.

16.1.1: Both sides are even, have leading term u^{-2}, and satisfy $f'^2 = 4f^3 - 4f$.

16.1.2: $\sigma(\mathrm{i}u) = \mathrm{i}\sigma(u)$ and $\wp(\mathrm{i}u) = -\wp(u)$. For the coefficients, $(\log\sigma)'' = -\wp$ and Problem 16.1.1.

16.1.3: Write $\alpha = m + \mathrm{i}n$; the left side is a product of two Jacobi theta functions, in z and in $\mathrm{i}z$. Compare zeros and transformation laws under $z \mapsto z + 2\pi\beta$, $\beta \in \mathbb{Z}[\mathrm{i}]$. The quotient is the exponential of a polynomial of degree at most two, and the symmetry $z \mapsto \mathrm{i}z$ and evenness leave only a constant. Alternatively, use Problem 12.2.7.

16.1.4: Apply Problem 16.1.3 to each coordinate, with $z_1 = s + t$ and $z_2 = \zeta(s - t)$.

16.1.5: $F(\zeta v) = \sum_k f_{4k}(-1)^k v^{4k}$ if $F = \sum_k f_{4k} v^{4k}$. For the congruence, compare $\Theta(\zeta s e_+ - \zeta t e_-)$ with $\Theta(s e_+ + t e_-)$.

§16.2.

16.2.1: Differentiate $\mathrm{sl}'^2 = 1 - \mathrm{sl}^4$ to get $\mathrm{sl}'' = -2\,\mathrm{sl}^3$.

16.2.2: $\mathrm{sl}'\,u = \sqrt{1 - X^4}$ lies in $\mathbb{Z}[\frac{1}{2}][[X]]$.

16.2.4: By [Si1, §IV.7], $[p](X) \equiv g(X^p) \pmod p$ for a series g, so $[p^k](X) \to 0$ in the (p, X)-adic topology. Extend $n \mapsto [n]$ from $\mathbb{Z}$ to $\mathbb{Z}_p$, and use [i].

§16.3.

16.3.1: Leibniz's rule.

16.3.2: Write $\delta = g(X)\,d/dX$, apply both sides to $X \oplus Y$, and set $X = 0$.

16.3.3: Use Problem 16.2.1. Alternatively, compare D^p with its pullback by [i].

16.3.4: Problem 16.3.3 in the variable X_1.

§16.4.

16.4.1: If $p \mid 4m + 1$ and $4m + 1 < q$, then $m \equiv (3p - 1)/4 \pmod p$. Count carries in $m + m$.

16.4.2: Write $p = 4r + 3$ and $m = (q - 1)/4 = rp + 3r + 2$. Take the unit parts of the factorials in $\binom{2m}{m}$ and use Wilson's theorem.

16.4.3: In the coordinate $z = \ell(T)$, translation by $g(z')$ is $z \mapsto z + z'$. For the consequences, compare coefficients of z^p and z^q in $\sum_j (\Delta_j f)(T)\,g(z)^j$.

16.4.4: Legendre's formula.

16.4.5: Factor $A^p - B^p$.

16.4.6: Induction on j, using Problems 16.4.4 and 16.4.5; apply the latter to $H^{p^{j-1}}$ and $D^{p^{j-1}}$ divided by $p^{e_{j-1}}$.

16.4.7: Write n in base p.

§16.5.

16.5.1: $(\log\sigma)'' = -\wp$, $\wp'' = 6\wp^2 - 2$, $\wp'^2 = 4\wp^3 - 4\wp$, and Problem 16.1.1.

16.5.2: By Lagrange inversion, $[u^n]\ \mathrm{sl}^k\, u = \frac{k}{n}\,[X^{n-k}]\,(X/\ell(X))^n$. Modulo p and modulo X^p, $(X/\ell(X))^p \equiv 1$.

16.5.3: In $\exp(\log F)$, only the term $2b_{p-1}u^{p+1}/(p+1)!$ of $\log F$ has p in its denominator up to degree $p+1$. For the second statement, compare with Problem 16.3.4.

References

[Ka] N. M. Katz, *Divisibilities, congruences, and Cartier duality*, J. Fac. Sci. Univ. Tokyo Sect. IA Math. **28** (1981), 667–678.

[LT] J. Lubin and J. Tate, *Formal complex multiplication in local fields*, Ann. of Math. **81** (1965), 380–387.

[Si1] J. H. Silverman, *The Arithmetic of Elliptic Curves*, 2nd ed., Grad. Texts in Math. 106, Springer, 2009.

[Si2] J. H. Silverman, *Advanced Topics in the Arithmetic of Elliptic Curves*, Grad. Texts in Math. 151, Springer, 1994.