ROOTS OF UNITY FOR MANY POLYNOMIALS

Prerequisites. Valuations on $\bar{\mathbb{Q}}_\ell$ [Ne, Ch. II]; roots of unity of prime power order [Wa, Ch. 1–2]. No earlier chapter.

Chapter 67, *Twists with few congruences*, describes how the proof bounds Selmer lengths and the valuations of ratios of Hecke L-values at each prime ℓ through values of polynomials at points $(\zeta_w - 1)_w$, with the ζ_w of ℓ-power order. Suppose finitely many integral polynomials have starting points whose coordinates have valuation at least a fixed rational $\rho > 0$, and the sum of their starting valuations is bounded. Can one replace all the points by one tuple $(\zeta_w - 1)_w$ while increasing each valuation by at most a prescribed $\varepsilon > 0$? Theorem 68.2.1 gives a level depending only on the prime, the bound on the number of variables, ρ, the sum bound and ε. Problem 68.2.7 treats the first m powers simultaneously.

Throughout, ℓ is a prime, val is the valuation of $\bar{\mathbb{Q}}_\ell$ with $\mathrm{val}(\ell) = 1$ and $\mathrm{val}(0) = \infty$, $\|y\| = \ell^{-\,\mathrm{val}(y)}$, and $\bar{\mathbb{Z}}_\ell = \{y : \mathrm{val}(y) \geq 0\}$. For $h \geq 0$ put

$$\rho_h := 1/\varphi(\ell^h),$$

with Euler's function φ. For a polynomial $g = \sum_i y_i Y^i \in \bar{\mathbb{Q}}_\ell[Y]$ and a rational $\rho \geq 0$, the *Gauss valuation* is $v_\rho(g) := \min_i\big(\mathrm{val}(y_i) + \rho i\big)$, and $R_\rho(g)$ is the multiset of roots of g in $\bar{\mathbb{Q}}_\ell$ of valuation exactly ρ, counted with multiplicity; for the zero polynomial $v_\rho(0) = \infty$ and $R_\rho(0) = \varnothing$. Below, g denotes a nonzero polynomial in $\bar{\mathbb{Z}}_\ell[Y]$. "Of order ℓ^h" means of exact order ℓ^h. We write ζ_d for a root of unity of exact order d.

68.1. One variable

Given g and a point x of positive valuation, can one replace x by $\zeta - 1$, with ζ a root of unity of ℓ-power order, without making g much more divisible?

Problem 68.1.1. If $h \geq 1$ and ζ has order ℓ^h, then $\mathrm{val}(\zeta - 1) = \rho_h$. For $\ell = 3$ the radii ρ_1, ρ_2, ρ_3 are $1/2, 1/6, 1/18$; for $\ell = 2$ they are $1, 1/2, 1/4$. The ρ_h with $h \geq 1$ are distinct and tend to 0.

Problem 68.1.2. Let $0 \neq g \in \bar{\mathbb{Z}}_\ell[Y]$, and write $g = c\prod_k (Y - \alpha_k)$ in $\bar{\mathbb{Q}}_\ell[Y]$. For rational $\rho \geq 0$,

$$v_\rho(g) = \mathrm{val}(c) + \sum\nolimits_k \min\big(\mathrm{val}(\alpha_k), \rho\big).$$

Hence $v_\rho(g_1 g_2) = v_\rho(g_1) + v_\rho(g_2)$, and $\rho \mapsto v_\rho(g)$ is nondecreasing.

Problem 68.1.3. (a) If $\mathrm{val}(x) \geq \rho$, then $\mathrm{val}(g(x)) \geq v_\rho(g)$. (b) If $\mathrm{val}(y) = \rho$, then

$$\mathrm{val}(g(y)) = v_\rho(g) + \sum\nolimits_{\alpha \in R_\rho(g)} \big(\mathrm{val}(y - \alpha) - \rho\big).$$

Problem 68.1.4. Let $\ell = 3$ and $g = Y^2 + 3Y + 3$. Then $v_\rho(g) = \min(1, 2\rho)$, and for ζ of order 3^h the valuation $\mathrm{val}(g(\zeta - 1))$ is ∞ if $h = 1$ and $2\rho_h = v_{\rho_h}(g)$ if $h \geq 2$.

Date: November 26, 2026.

We bound the root counts on the radii $\rho_h \le \rho$, each weighted by ρ_h. For a rational $\rho > 0$ and an integer $h_0 \ge 1$, let $H(\rho, h_0)$ be the set of h with $1 \le h \le h_0$ and $\rho_h \le \rho$.

Problem 68.1.5. $\sum_{h \in H(\rho,h_0)} \#R_{\rho_h}(g) \cdot \rho_h \le v_\rho(g)$.

Problem 68.1.6. Let $\delta > 0$ and $\beta \ge 0$, with $\beta < \delta \sum_{h \in H(\rho,h_0)} 1/(h+1)$. If $v_\rho(g) \le \beta$, then some $h \in H(\rho, h_0)$ has $\#R_{\rho_h}(g) \cdot \rho_h \le \delta/(h+1)$.

Next, how close can the $\zeta - 1$ of a given order be to a fixed point?

Problem 68.1.7. Let $\alpha \in \bar{\mathbb{Z}}_\ell$ with $\mathrm{val}(\alpha) > 0$, and $h \ge 1$. Then

$$\sum\nolimits_\zeta \min\big(\mathrm{val}(\zeta - 1 - \alpha), 1\big) \le h + 1,$$

the sum over the ζ of order ℓ^h. For $\ell = 3$, $h = 1$ and $\alpha = \zeta_0 - 1$, with ζ_0 of order 3, the sum is $3/2$.

Problem 68.1.8. For $\ell = 3$, $h = 2$ and $\alpha = \zeta_9 - 1$, the six terms $\min(\mathrm{val}(\zeta - 1 - \alpha), 1)$, for $\zeta = \zeta_9^e$ with $e = 1, 2, 4, 5, 7, 8$, are $1, \frac{1}{6}, \frac{1}{2}, \frac{1}{6}, \frac{1}{2}, \frac{1}{6}$; their sum is $\frac{5}{2} \le h + 1$.

Problem 68.1.9. Let R be a finite multiset of elements of $\bar{\mathbb{Z}}_\ell$ of positive valuation, and $h \ge 1$. Some ζ of order ℓ^h has $\sum_{\alpha \in R} \min\big(\mathrm{val}(\zeta - 1 - \alpha), 1\big) \le \#R \cdot \rho_h(h+1)$.

Problem 68.1.10. Let $0 < \delta < 1$, $\rho > 0$ rational, and $\beta < \delta \sum_{h \in H(\rho,h_0)} 1/(h+1)$. If $v_\rho(g) \le \beta$, then for some $h \in H(\rho, h_0)$ and some ζ of order ℓ^h,

$$\mathrm{val}\big(g(\zeta - 1)\big) \le v_{\rho_h}(g) + \delta.$$

Problem 68.1.11. For rational $\rho > 0$, real $\delta > 0$ and $\beta \ge 0$, some h_0 has $\beta < \delta \sum_{h \in H(\rho,h_0)} 1/(h+1)$. For $\ell = 2$, $\rho = \delta = 1/2$ and $\beta = 1$, the least such h_0 is 18.

Problem 68.1.12. Let δ, ρ, β, h_0 be as in Problem 68.1.10. If $\mathrm{val}(x) \ge \rho$ and $\mathrm{val}(g(x)) \le \beta$, then some ζ with $\zeta^{\ell^{h_0}} = 1$ and $\mathrm{val}(\zeta - 1) \le \rho$ has $\mathrm{val}(g(\zeta - 1)) \le \mathrm{val}(g(x)) + \delta$.

68.2. Several variables and several powers

Let $\rho > 0$ be rational, and $\mathcal{V}$ and I finite sets. For $i \in I$ let $F_i \in \bar{\mathbb{Z}}_\ell[X_j : j \in \mathcal{V}]$, and let $x_i \in \bar{\mathbb{Z}}_\ell^{\mathcal{V}}$ be a point. We seek one tuple of roots of unity that works for every i.

Problem 68.2.1. Fix $j \in \mathcal{V}$, and assume $\mathrm{val}(x_{ij}) \ge \rho$ for all i (the other coordinates are only integral). Let $0 < \delta < 1$, $\beta < \delta \sum_{h \in H(\rho,h_0)} 1/(h+1)$, and $\sum_i \mathrm{val}(F_i(x_i)) \le \beta$. There is ζ with $\zeta^{\ell^{h_0}} = 1$ and $\mathrm{val}(\zeta - 1) \le \rho$ such that, if the coordinate x_{ij} is replaced by $\zeta - 1$ for every i, each $\mathrm{val}(F_i(x_i))$, and also their sum, grows by at most δ.

Problem 68.2.2. Let $0 < \delta < 1$, $\#\mathcal{V} \cdot \delta \le 1$, $\beta + 1 < \delta \sum_{h \in H(\rho,h_0)} 1/(h+1)$, $\mathrm{val}(x_{ij}) \ge \rho$ for all i, j, and $\sum_i \mathrm{val}(F_i(x_i)) \le \beta$. There are ζ_j, $j \in \mathcal{V}$, with $\zeta_j^{\ell^{h_0}} = 1$, $\mathrm{val}(\zeta_j - 1) \le \rho$, and $\mathrm{val}\big(F_i((\zeta_j - 1)_j)\big) \le \mathrm{val}(F_i(x_i)) + \#\mathcal{V} \cdot \delta$ for all i.

Problem 68.2.3. Let $\ell = 3$, $F_1 = X + Y$, $F_2 = XY + 3$, $F_3 = X^2 + 3X + 3$, with starting points $(3, 0)$, $(0, 3)$, $(0, 0)$, at which each F_i has valuation 1. For $\zeta = \zeta_{27}$, the common point $(\zeta - 1, \zeta^2 - 1)$ gives $\mathrm{val}(F_i) = \frac{1}{9}$ for $i = 1, 2, 3$.

The following theorem is proved by the problems of this section. In Theorem 68.2.1, the level h_0 depends only on $\ell, s_0, \rho, \beta, \varepsilon$.

Theorem 68.2.1. *Let $s_0 \geq 0$ be an integer, $\rho > 0$ rational, $\beta \geq 0$ and $\varepsilon > 0$. There is h_0 with the following property. Let $\mathcal{V}$, I be finite sets with $\#\mathcal{V} \leq s_0$, let $F_i \in \bar{\mathbb{Z}}_\ell[X_j : j \in \mathcal{V}]$ and $x_i \in \bar{\mathbb{Z}}_\ell^{\mathcal{V}}$ for $i \in I$, with $\mathrm{val}(x_{ij}) \geq \rho$ for all i, j and $\sum_i \mathrm{val}(F_i(x_i)) \leq \beta$. Then there are $\zeta_j \in \bar{\mathbb{Z}}_\ell$, $j \in \mathcal{V}$, with*

$$\zeta_j^{\ell^{h_0}} = 1, \quad \mathrm{val}(\zeta_j - 1) \leq \rho \quad (j \in \mathcal{V}), \qquad \mathrm{val}\big(F_i((\zeta_j - 1)_j)\big) \leq \mathrm{val}\big(F_i(x_i)\big) + \varepsilon \quad (i \in I).$$

A twist will be used through its first m powers at once, so the roots of unity must also serve for $\zeta_j^n - 1$, $1 \leq n \leq m$.

Problem 68.2.4. Let $n \geq 1$ and $x \in \bar{\mathbb{Z}}_\ell$ with $\mathrm{val}(x) \geq \rho$. Some $x' \in \bar{\mathbb{Z}}_\ell$ has $(1 + x')^n = 1 + x$ and $\mathrm{val}(x') \geq \rho/n$.

Problem 68.2.5. Let $0 < \rho < 1$, $1 \leq n \leq m$, and let ζ have ℓ-power order and $\mathrm{val}(\zeta - 1) \leq \rho/m$. Then $\mathrm{val}(\zeta^n - 1) \leq \rho$; in particular $\zeta^n \neq 1$. For $\ell = 2$, ζ of order 8, $m = n = 2$ and $\rho = 1/2$, equality holds.

Problem 68.2.6. Let $\ell = 3$ and $\Phi_3(Y) = Y^2 + Y + 1$. The values $\mathrm{val}(\Phi_3(\zeta_n^j))$ for $j = 1, 2, 3$ are $\frac{1}{3}, \frac{1}{3}, \infty$ for $n = 9$; $\frac{1}{9}, \frac{1}{9}, \frac{1}{3}$ for $n = 27$; and $\frac{1}{27}, \frac{1}{27}, \frac{1}{9}$ for $n = 81$. For $m = 3$, $\rho = 1/2$, one variable, $F(X) = \Phi_3(1 + X)$, $x = 0$ and $\beta = 1$, no root of order 9 satisfies the conclusion of Problem 68.2.7, for any $\varepsilon > 0$.

Problem 68.2.7. Let integers $s_0 \geq 0$, $m \geq 1$, a rational $\rho > 0$, $\varepsilon > 0$, a finite set I and numbers $\beta_i \geq 0$, $i \in I$, be given. There is h_0 such that, for every finite set $\mathcal{V}$ with $\#\mathcal{V} \leq s_0$, all $F_i \in \bar{\mathbb{Z}}_\ell[X_j : j \in \mathcal{V}]$ and all $x_i \in \bar{\mathbb{Z}}_\ell^{\mathcal{V}}$ satisfying $\mathrm{val}(x_{ij}) \geq \rho$ for every i, j and $\mathrm{val}(F_i(x_i)) \leq \beta_i$ for every i, some ζ_j with $\zeta_j^{\ell^{h_0}} = 1$ and $\mathrm{val}(\zeta_j - 1) \leq \rho/m$ satisfy

$$\mathrm{val}\big(F_i((\zeta_j^n - 1)_j)\big) \leq \mathrm{val}\big(F_i(x_i)\big) + \varepsilon \qquad (i \in I,\ 1 \leq n \leq m).$$

The exercises derive Theorem 68.2.1 and Problem 68.2.7 from the stated prerequisites and the divergence of the harmonic series. Chapter 67 states the polynomial input and uses Problem 68.2.7 to construct the twist and bound its powers.

In the Lean formalization. In the Lean proof [GL], Theorem 68.2.1 is `New.Selmer.exists_rootsOfUnity_ellVal_eval_le_add` (`New/Congruences/Selmer/RootsOfUnity.lean`); two one-variable steps, used in Problems 68.1.6 and 68.1.10, are `New.Selmer.exists_card_rootsOfValuation_mul_le` and `New.Selmer.exists_rootOfUnity_eval_le_gaussVal_add` in the same file; the form for powers, Problem 68.2.7, is `New.Selmer.exists_rootsOfUnity_ellVal_eval_le` (`New/Congruences/Selmer/GeneralTheorem.lean`). The truncated valuation $\max(\mathrm{val}, 0)$ is `New.ellVal`. The polynomial input and the use of the first m powers of one twist are `New.Selmer.exists_twistPolynomials` (`New/Congruences/Selmer/Line.lean`) and the proof of `New.Selmer.exists_anticyclotomic_twist` (`New/Congruences/Selmer/GeneralTheorem.lean`). The passage from a Stickelberger value to a bound on a Hecke L-value ratio uses `New.Selmer.exists_stickelbergerSystem_ellVal_ratio_le` (`New/Congruences/Selmer/LValueSystems.lean`).

Hints

Section 68.1.

68.1.1: The conjugates of $\zeta - 1$ have product $\pm\Phi_{\ell^h}(1) = \pm\ell$.

68.1.2: For $\rho = 0$ reduce modulo the maximal ideal of $\bar{\mathbb{Z}}_\ell$; for $\rho = \mathrm{val}(\pi)$ substitute $Y = \pi Z$.

68.1.3: For (b), factor g and use $\mathrm{val}(y-\alpha) = \min(\mathrm{val}(\alpha), \rho)$ when $\mathrm{val}(\alpha) \neq \rho$.

68.1.4: $g(Y) = ((1+Y)^3 - 1)/Y$.

68.1.5: By Problem 68.1.1 a root lies in at most one R_{ρ_h}; compare with Problem 68.1.2, using $v_0(g) \geq 0$.

68.1.7: The $\zeta - 1 - \alpha$ are roots of $(1+\alpha+Y)^{\ell^h} - 1$; look at its coefficient of Y and use Problem 68.1.2 with $\rho = 1$.

68.1.8: $\zeta_9^e - \zeta_9 = \zeta_9(\zeta_9^{e-1} - 1)$; Problem 68.1.1.

68.1.9: Sum Problem 68.1.7 over R and average over the $1/\rho_h$ choices of ζ.

68.1.10: Choose the radius by Problem 68.1.6 and ζ by Problem 68.1.9.

68.1.11: The harmonic series diverges.

68.1.12: Problem 68.1.3(a) and the monotonicity in Problem 68.1.2.

Section 68.2.

68.2.1: Apply Problem 68.1.10 to the product of the one-variable polynomials $g_i(Y)$ obtained by freeing the coordinate j; for each i separately, use $\mathrm{val}(g_i(\zeta - 1)) \geq v_{\rho_h}(g_i)$.

68.2.2: Induction on the number of coordinates moved, with Problem 68.2.1, keeping the running sum at most $\beta + 1$. For Theorem 68.2.1 take $\delta = \min(\varepsilon, 1)/(s_0 + 2)$ and h_0 from Problem 68.1.11 with $\beta + 1$ in place of β.

68.2.3: Factor F_1 and F_3 at the point; Problem 68.1.1.

68.2.4: The roots of $(1+Y)^n - 1 - x$ have product $\pm x$.

68.2.5: First compare m with $\varphi(\ell^h)$, where ℓ^h is the order of ζ. What is the order of ζ^n?

68.2.6: $\Phi_3(y) = (y^3 - 1)/(y - 1)$; Problem 68.1.1.

68.2.7: Theorem 68.2.1 with radius ρ/m, after the substitution $X_j \mapsto (1 + X_j)^n - 1$; Problem 68.2.4.

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/`.

[Ne] J. Neukirch, *Algebraic Number Theory*, Grundlehren Math. Wiss. 322, Springer, 1999.

[Wa] L. C. Washington, *Introduction to Cyclotomic Fields*, 2nd ed., Grad. Texts in Math. 83, Springer, 1997.