THE SLOPE METHOD

Prerequisites. Linear algebra over $\mathbb{R}$ and $\mathbb{C}$: the spectral theorem, the Hilbert–Schmidt norm $\|A\|_{\mathrm{HS}}^2 = \mathrm{tr}(A^*A)$, exterior powers, and Hadamard's inequality $|\det(v_1,\dots,v_n)| \le \|v_1\|\cdots\|v_n\|$. Lattices in a Euclidean space [Ne, Ch. I, §4]. Dedekind domains, the absolute norm of a fractional ideal, ramification indices and residue degrees, the Frobenius element of an unramified prime, and the product formula [Ne, Ch. I and Ch. III]. Legendre's formula $v_p(n!) = \sum_{e\ge1}\lfloor n/p^e\rfloor$, Stirling's formula, and the von Mangoldt function Λ. No earlier chapter is used; one remark in Section 6.4 points to Chapter 16. The next chapter, *The slope inequality in the mean*, continues this one with many maps into one target.

6.1. Divisibility against size

How can a divisibility statement bound a sum over primes? Chebyshev's answer uses one integer [Ch]. Let $\theta(x) := \sum_{p\le x}\log p$.

Problem 6.1.1. Every prime p with $n < p \le 2n$ divides $\binom{2n}{n}$, and $\binom{2n}{n} \le 4^n$. Hence $\theta(2n) - \theta(n) \le n\log 4$.

The principle is the following. If a nonzero integer Δ is divisible by p^{e_p} for each prime p in a set S, then

$$\sum_{p\in S} e_p \log p \le \log|\Delta|. \tag{1}$$

For $\Delta = n!$ both sides of (1) are known exactly.

Problem 6.1.2. $\log n! = \sum_{r\le n}\Lambda(r)\lfloor n/r\rfloor$.

By Stirling's formula the left side is $n\log n - n + O(\log n)$. Without the floor function the right side would be $n\sum_{r\le n}\Lambda(r)/r$. The fractional parts contribute $\sum_{r\le n}\Lambda(r)\{n/r\}$, which by Chebyshev's bounds is of size n, the size of the term $-n$ on the left. So the identity cannot see $\psi(n) - n$, where $\psi(x) := \sum_{r\le x}\Lambda(r)$. To do better one needs an object whose exponent at p^e is a smooth function of p^e, such as the ramp $(x/p^e - 1)_+$, where $t_+ := \max(t, 0)$, and whose size is known with an error much smaller than its linear term.

The integer Δ will be a minor of a matrix.

Problem 6.1.3. Let $A \in M_r(\mathbb{Z})$ with $\det A \ne 0$, and suppose that the jth column A_j is divisible by the positive integer g_j. Then

$$g_1\cdots g_r \le |\det A| \le \|A_1\|\cdots\|A_r\|.$$

For the columns $(6, 6)$ and $(10, 20)$ the three numbers are 60, 60 and $60\sqrt{10}$.

The same principle holds over a number field K, where the product formula accounts for the size of a number at every place. At a finite place v write $\mathcal{O}_v$, $\mathfrak{p}_v$ and q_v for the valuation ring, its maximal ideal and the size of its residue field, and let $|x|_v := q_v^{-\,\mathrm{ord}_v\, x}$. At an archimedean place use the usual modulus. Let $n_v := 2$

Date: November 25, 2026.

at complex places and $n_v := 1$ at the other places. Then $\sum_v n_v \log|c|_v = 0$ for $c \in K^\times$. Hence, if $\delta \in K^\times$ satisfies $|\delta|_v \le \exp(b_v - g_v)$ at every place, where b_v and g_v are real and vanish for almost all v, then

$$\sum_v n_v g_v \le \sum_v n_v b_v. \tag{2}$$

Typically δ is a minor of a matrix, b_v bounds it through the sizes of the entries, and g_v records an improvement from a congruence. The minor is chosen once over K, but the basis in which one proves the congruence may vary with v.

6.2. A minor of a jet evaluation map

Where does a minor with many prime factors come from? One source is Frobenius. Let $K = \mathbb{Q}(\mathrm{i})$, so that a prime $p \equiv 3 \pmod 4$ is inert and $\mathbb{Z}[\mathrm{i}]/p$ is the field with p^2 elements.

Problem 6.2.1. If $p \equiv 3 \pmod 4$ and $u \in \mathbb{Z}[\mathrm{i}]$, then $\bar{u} \equiv u^p \pmod p$.

Thus complex conjugation is the Frobenius at every inert prime. Let $u_1, \dots, u_I \in \mathbb{Z}[\mathrm{i}]$, let $\mathcal{T} \subset \mathbb{Z}^2_{\ge 0}$ be a finite set of s exponents, and let $J \ge 1$. On the span of the monomials $X^a Y^b$, $(a,b) \in \mathcal{T}$, consider the jet evaluation map

$$\mathrm{ev}\colon f \longmapsto \big((\partial_X^j f)(u_i, \bar{u}_i)\big)_{1 \le i \le I,\ 0 \le j < J}.$$

Its matrix has entries in $\mathbb{Z}[\mathrm{i}]$. Let $g := X^p - Y$.

Problem 6.2.2. Let $p \equiv 3 \pmod 4$. For $f \in \mathbb{Z}[\mathrm{i}][X,Y]$, $u \in \mathbb{Z}[\mathrm{i}]$ and integers $j, k \ge 0$, the number $\big(\partial_X^j (g^k f)\big)(u, \bar{u})$ is divisible by p^k.

Problem 6.2.3. Let $p \equiv 3 \pmod 4$, and suppose that $(a-p, b+1) \in \mathcal{T}$ whenever $(a,b) \in \mathcal{T}$ and $a \ge p$. Then every $s \times s$ minor of the matrix of ev is divisible by p^{N_p}, where $N_p := \sum_{(a,b)\in\mathcal{T}} \lfloor a/p \rfloor$. The set $\mathcal{T} = \{(a,b) : a + 2b \le N\}$ satisfies the hypothesis for every p.

Let $\beta := \max(1, |u_1|, \dots, |u_I|)$, $D := \sum_{\mathcal{T}} (a+b)$ and $A_* := \max(\{1\} \cup \{a : (a,b) \in \mathcal{T}\})$. An entry in the column of $X^a Y^b$ has absolute value at most $A_*^{J-1} \beta^{a+b}$, so every $s \times s$ minor has absolute value at most $s!\, A_*^{s(J-1)} \beta^D$. With Problem 6.2.3, the inequality (2) for one nonzero minor proves the following.

Theorem 6.2.1. *Suppose that* ev *is injective, and let P be a set of primes $p \equiv 3 \pmod 4$ for which $\mathcal{T}$ satisfies the hypothesis of Problem 6.2.3. Then*

$$\sum_{p \in P} \log p \sum_{(a,b)\in\mathcal{T}} \left\lfloor \frac{a}{p} \right\rfloor \le D \log \beta + \log s! + s(J-1) \log A_*.$$

Over a function field this is the mechanism of Stepanov's proof of the Riemann hypothesis for curves [Bom].

6.3. Normed spaces and slopes

The minor δ of Section 6.2 is the top exterior power of a linear map, written in chosen bases. To let the bases vary with the place, one puts norms on the spaces.

Let K be a number field, with the conventions of Section 6.1. A *normed space* over K is a finite-dimensional K-vector space V with a norm on each $V_v := V \otimes_K K_v$: a Euclidean or Hermitian norm at each archimedean place, and at each finite place

the sup norm of a full $\mathcal{O}_v$-lattice L_v, the *unit lattice*. Almost everywhere L_v is the $\mathcal{O}_v$-span of a fixed basis. Subspaces carry the restricted norms, quotients the quotient norms, the dual $V^\vee$ the dual norms, and exterior powers the induced norms. For $e \neq 0$ in V let $h(e) := \sum_v n_v \log\|e\|_v$, and for a nonzero linear map $\varphi\colon V \to F$ of normed spaces let

$$h(\varphi) := \sum_v n_v \log\|\varphi\|_v,$$

with the operator norms, and $h_\infty(\varphi)$ for the sum over the archimedean places alone. For $r = \dim V > 0$ and a generator ω of $\det V := \wedge^r V$, let

$$\deg V := -h(\omega), \qquad \mu(V) := \deg V/r.$$

By the product formula $\deg V$ does not depend on ω. These are the *degree* and the *slope* of V. We follow Bost [Bo1] and do not divide by $[K : \mathbb{Q}]$.

Problem 6.3.1. Over $\mathbb{Q}$, the lattice $L := V \cap \bigcap_p L_p$ has $L \otimes \mathbb{Z}_p = L_p$ for every p, and $\deg V = -\log \operatorname{covol}(L)$.

So over $\mathbb{Q}$ a normed space is a Euclidean lattice.

Problem 6.3.2. Let $\tau \in \mathbb{C}$ with $\operatorname{Im}\tau > 0$, and give $\mathbb{C} = \mathbb{R}^2$ its usual norm. Then the Euclidean lattice $\mathbb{Z}+\mathbb{Z}\tau$ has $\deg(\mathbb{Z}+\mathbb{Z}\tau) = -\log \operatorname{Im}\tau$. If $M \subseteq L$ is a sublattice of index N, then $\deg M = \deg L - \log N$. Multiplying the norm of L by $c > 0$ subtracts $r \log c$ from $\deg L$.

Problem 6.3.3. If $U \subseteq V$ is a subspace, then $\deg V = \deg U + \deg(V/U)$.

The domain of the slope method is a lattice of sections of a line bundle, or of automorphic forms. The simplest case is the projective line. For $D \geq 0$ let E_D be the lattice of homogeneous polynomials $f \in \mathbb{Z}[x, y]$ of degree D, with

$$\|f\|^2 := \int_{\mathbb{C}} \frac{|f(z,1)|^2}{(1+|z|^2)^D} \, \frac{dA(z)}{\pi(1+|z|^2)^2}.$$

This is the L^2 norm of a section of $\mathcal{O}(D)$ for the Fubini–Study metric and the Fubini–Study probability measure.

Problem 6.3.4. The monomials are orthogonal, and $\|x^a y^{D-a}\|^2 = a!\,(D-a)!/(D+1)!$.

Problem 6.3.5. $\mu(E_D) = D/4 + O(\log D)$.

Problem 6.3.5 is the simplest case of the arithmetic Hilbert–Samuel theorem [GS2, Thm. 8].

Problem 6.3.6. Let $\mathfrak{a}$ be a fractional ideal of K, with unit lattices $\mathfrak{a}\mathcal{O}_v$ and $\|x\|_v = |x|_v$ at the archimedean places. Then $\deg \mathfrak{a} = -\log N\mathfrak{a}$. Replacing every unit lattice L_v of V by $\mathfrak{a}L_v$ lowers $\mu(V)$ by $\log N\mathfrak{a}$.

To compare slopes over fields of different degrees, one normalizes by the degree, and many authors also use squared norms. Let

$$\mu^\sharp := \frac{2}{[K:\mathbb{Q}]}\,\mu, \qquad h^\sharp := \frac{2}{[K:\mathbb{Q}]}\,h.$$

For a prime $\mathfrak{p}$ of K above p, with ramification index $e_\mathfrak{p}$, let $c_\mathfrak{p} := 2e_\mathfrak{p} \log N\mathfrak{p}/[K:\mathbb{Q}]$.

Problem 6.3.7. $\sum_{\mathfrak{p}|p} c_{\mathfrak{p}} = 2\log p$. If every unit lattice $L_{\mathfrak{p}}$, $\mathfrak{p} \mid p$, is replaced by $p^{-e}L_{\mathfrak{p}}$, then $\mu^\sharp$ increases by $2e\log p$.

So a divisibility by p^e at every place above p is worth $2e\log p$ in the normalized slopes.

6.4. The height inequality for an image

How does a linear map compare the slopes of its source and target? Let $\varphi\colon V \to F$ be an injective map of normed spaces with image U, and let $r = \dim V > 0$. On determinant lines it induces $\wedge^r\varphi\colon \det V \to \det U$.

Problem 6.4.1. $\sum_v n_v \log\|\wedge^r\varphi\|_v = r\big(\mu(V)-\mu(U)\big)$, and $\|\wedge^r\varphi\|_v \le \|\varphi\|_v^r$ at every place.

Summing local bounds gives the following.

Theorem 6.4.1. *Suppose that* $\log\|\wedge^r\varphi\|_v \le b_v - g_v$ *at every place, with* $b_v = g_v = 0$ *almost everywhere. Then*

$$\sum_v n_v g_v \le \sum_v n_v b_v + r\big(\mu(U) - \mu(V)\big).$$

In particular $\mu(V) \le \mu(U) + h(\varphi) \le \mu_{\max}(F) + h(\varphi)$, *where* $\mu_{\max}(F)$ *is the supremum of the slopes of the nonzero subspaces of* F.

The last inequality is the slope inequality of Bost [Bo1], [Bo2, Prop. 4.5]. For $V = F = K$ with the standard norms and φ the multiplication by δ, Theorem 6.4.1 is (2).

Over $\mathbb{Q}$ the local norms at the primes are divisibilities.

Problem 6.4.2. Let L and M be Euclidean lattices and $\varphi\colon L_{\mathbb{Q}} \to M_{\mathbb{Q}}$ nonzero. Then $\|\varphi\|_p = p^{-e}$ for the largest integer e with $\varphi(L) \subseteq p^e(M \otimes \mathbb{Z}_{(p)})$. In particular $\sum_p \log\|\varphi\|_p \le 0$ when $\varphi(L) \subseteq M$, with every divisibility of the values making it smaller.

When the ranks agree, an identity replaces the inequality.

Problem 6.4.3. Suppose that $\dim L_{\mathbb{Q}} = \dim M_{\mathbb{Q}}$, that φ is injective, and that $\varphi(L) \subseteq M$. Then

$$\deg M - \deg L = \log[M : \varphi(L)] - \log|\det \varphi_{\mathbb{R}}|,$$

where $\det\varphi_{\mathbb{R}}$ is computed in orthonormal bases.

Where do divisible values and controlled norms come from together? The simplest example is the ath derivative at 0 of a polynomial with integer coefficients, which is divisible by $a!$, on a space of polynomials with a Gaussian norm. For $f \in \mathbb{C}[z]$ let

$$\|f\|^2 := \frac{1}{\pi}\int_{\mathbb{C}} |f(z)|^2 e^{-|z|^2}\, dA(z).$$

Problem 6.4.4. The monomials are orthogonal, and $\|z^a\|^2 = a!$.

Problem 6.4.5. Let $a < D$, let L be the lattice of polynomials in $\mathbb{Z}[z]$ of degree less than D with the norm above, and let $\varphi(f) := f^{(a)}(0) \in \mathbb{Z}$, with $\mathbb{Z}$ the standard lattice. Then $\sum_p \log\|\varphi\|_p = -\log a!$ and $h_\infty(\varphi) = \frac{1}{2}\log a!$.

By Problem 6.1.2 the gain $\log a!$ at the finite places is a sum over primes, and the cost at infinity is half of it. In the applications the function is a theta function with complex multiplication, and at a supersingular prime the divisibility that one proves is only about $a\sum_{e\ \mathrm{odd}} p^{-e}$ of the $v_p(a!) \approx a\sum_{e\geq 1} p^{-e}$ (Chapter 16, Theorem 16.4.1).

6.5. Divisibility of a pairing as a change of lattice

In the applications the values of the map are periods, that is, values of a bilinear pairing. Let $P\colon V\times W\to K$ be a bilinear pairing of normed spaces, with unit lattices L_v and R_v, and let $\varphi_P\colon V\to W^\vee$ be the induced map.

Problem 6.5.1. At a finite place, if $P\neq 0$, then $\|\varphi_P\|_v = q_v^{-k}$ for the largest k with $P(L_v,R_v)\subseteq \mathfrak{p}_v^k$. Multiplying the norms of W at the archimedean places by constants $\lambda_v>0$ adds $\sum_v n_v\log\lambda_v$ to $\mu(W^\vee)$ and subtracts it from $h(\varphi_P)$.

So only $h(\varphi_P)+\mu(W^\vee)$ is independent of the normalization of W. To estimate P at different places one may use different factorizations.

Problem 6.5.2. Suppose that $P(x,w) = c_v\,P'_v(A_{m,v}\cdots A_{1,v}\,x,\ C_{m,v}\cdots C_{1,v}\,w)$ at a place v, where $c_v\in K_v^\times$, the intermediate spaces carry norms and P'_v has the bilinear operator norm. Then

$$\log\|\varphi_P\|_v \leq \log|c_v|_v + \log\|P'_v\|_v + \sum_{j=1}^{m}\bigl(\log\|A_{j,v}\|_v + \log\|C_{j,v}\|_v\bigr).$$

At a finite place, an inclusion $A_{j,v}L_{j-1}\subseteq \mathfrak{p}_v^k L_j$, where L_{j-1} and L_j are the unit lattices of the source and the target of $A_{j,v}$, contributes $-k\log q_v$, for every integer k.

Thus local gains add along a chain of maps, while the slopes of V and $W^\vee$ enter only once. Now record a gain as a change of the unit lattice of V.

Problem 6.5.3. Let v be finite, let $L'_v\subseteq L_v$ be a full sublattice, and let k be an integer with $P(L'_v,R_v)\subseteq\mathfrak{p}_v^k$. Replace L_v by $N_v := \mathfrak{p}_v^{-k}L'_v$. Then the new norm of φ_P at v is at most 1, and $\deg V$ increases by $\log q_v\bigl(k\dim V - \mathrm{length}_{\mathcal{O}_v}(L_v/L'_v)\bigr)$.

Problem 6.5.3 and Theorem 6.4.1 prove the following.

Theorem 6.5.1. *Let $P\colon V\times W\to K$ be a pairing with φ_P injective and $r=\dim V>0$. For each finite place v let $L'_v\subseteq L_v$ be a full sublattice and k_v an integer with $P(L'_v,R_v)\subseteq\mathfrak{p}_v^{k_v}$, where $L'_v=L_v$ and $k_v=0$ almost everywhere. Then*

$$\sum_{v\nmid\infty} k_v\log q_v \leq h_\infty(\varphi_P) + \mu_{\max}(W^\vee) - \mu(V) + \frac{1}{r}\sum_{v\nmid\infty}\log[L_v:L'_v].$$

For $V=W=K$ with the standard norms, $P(x,y)=cxy$ with $0\neq c\in\mathcal{O}_K$, $L'_v=L_v$ and $k_v=\mathrm{ord}_v(c)$, this is the product formula for c, with equality. The left side is the unknown sum over primes. The right side involves $\mu_{\max}$ of the target, so a single map sees only the part of the target that contains its image; the sequel removes this by using many maps.

Hints

§6.1.

6.1.1: Write $\binom{2n}{n} = (2n)!/(n!)^2$. For the size, expand $(1+1)^{2n}$.
6.1.2: Count the multiples of p^e up to n.
6.1.3: Divide each column by g_j.

§6.2.

6.2.1: The binomial theorem modulo p.
6.2.2: Problem 6.2.1 and the Leibniz rule.
6.2.3: Write $a = kp+t$ with $0 \le t < p$, and consider the polynomials $X^t Y^b g^k$.

§6.3.

6.3.1: For almost all p, L_p is the $\mathbb{Z}_p$-span of a fixed basis of V, and every L_p lies between p^k and p^{-k} times that span for some k. Then take $\omega = e_1 \wedge \cdots \wedge e_r$ for a basis (e_j) of L.
6.3.2: A fundamental domain of M is a union of N translates of one for L.
6.3.3: At a finite place, extend a basis of the saturated lattice $U_v \cap L_v$. At an archimedean place, use an orthogonal complement.
6.3.4: Use polar coordinates and $t = |z|^2$. The result is a Beta integral.
6.3.5: Compute $\deg E_D$ from Problem 6.3.4, then use Stirling's formula.
6.3.6: Take $\omega = x \in \mathfrak{a}$, and use $\sum_{v|\infty} n_v \log|x|_v = \log|N_{K/\mathbb{Q}}(x)|$.
6.3.7: $\sum_{\mathfrak{p}|p} e_{\mathfrak{p}} f_{\mathfrak{p}} = [K:\mathbb{Q}]$, where $N\mathfrak{p} = p^{f_{\mathfrak{p}}}$.

§6.4.

6.4.1: The norm of a map of lines is $\|(\wedge^r \varphi)\omega\|_v / \|\omega\|_v$. For the second statement use Hadamard's inequality at the archimedean places, and at a finite place a basis of the unit lattice.
6.4.2: The unit ball of $M \otimes \mathbb{Q}_p$ is $M \otimes \mathbb{Z}_p$.
6.4.3: Compute $\deg \varphi(L)$ in two ways.
6.4.4: Polar coordinates.
6.4.5: Problems 6.4.2 and 6.4.4.

§6.5.

6.5.1: The local norm of φ_P is the supremum of $|P(x,w)|_v$ over unit vectors.
6.5.2: Operator norms are submultiplicative.
6.5.3: Compare the top exterior powers of L_v, L'_v and N_v.

References

[Bo1] J.-B. Bost, *Périodes et isogénies des variétés abéliennes sur les corps de nombres (d'après D. Masser et G. Wüstholz)*, Séminaire Bourbaki, Exp. 795, Astérisque **237** (1996), 115–161.

[Bo2] J.-B. Bost, *Algebraic leaves of algebraic foliations over number fields*, Publ. Math. IHÉS **93** (2001), 161–221.

[Bom] E. Bombieri, *Counting points on curves over finite fields (d'après S. A. Stepanov)*, Séminaire Bourbaki, Exp. 430, Lecture Notes in Math. 383, Springer, 1974, 234–241.

[Ch] P. L. Chebyshev, *Mémoire sur les nombres premiers*, J. Math. Pures Appl. **17** (1852), 366–390.

[GS2] H. Gillet and C. Soulé, *An arithmetic Riemann–Roch theorem*, Invent. Math. **110** (1992), 473–543.

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