DIVISIBILITY ALONG THE CHAIN

Prerequisites. Formal power series over a commutative ring. Finite extensions of $\mathbb{Q}_p$, their valuations, and lattices over their rings of integers; the length of a module of finite length. Gaussian binomial coefficients $\begin{bmatrix} n \\ l \end{bmatrix}_Q$ [Mac, Ch. I, §2, Example 3]. From Chapter 6, *The slope method*: Theorem 6.5.1. From Chapter 8, *The chain and the square root*: Section 8.4. From Chapter 19, *Hecke nondegeneracy on the tree*: the loss, defined in Section 19.1. From Chapter 24, *Hecke operators and theta lifts*: Section 24.5, in particular Problems 24.5.3 and 24.5.4.

Theorem 8.4.2 adds gains that hold on the whole of each lattice. In the argument a lift gains more only on a sublattice spanned by images of a Hecke operator, and Chapter 19 measures the colength of such a sublattice. How does a gain on a sublattice at the start of a chain become a gain of the composite? The Hecke operator has to be moved along the chain, by Problem 24.5.4, and the coefficients that appear are complete symmetric functions. Their denominators are the price of the move. We follow the reconstruction of Adriazola [Adr, §10], with one Hecke operator in place of several.

25.1. Elementary and complete symmetric functions

Let $x = (x_1, \dots, x_n)$ be a finite family in a commutative ring. The *elementary* and *complete symmetric functions* $e_l(x)$ and $h_l(x)$ are the sums of the products $x_{i_1} \cdots x_{i_l}$ over $i_1 < \cdots < i_l$ and over $i_1 \le \cdots \le i_l$ respectively, with $e_0 = h_0 = 1$. Their generating series are

$$E_x(X) := \prod_i (1+x_iX) = \sum_{l \ge 0} e_l(x) X^l, \qquad H_x(X) := \prod_i (1-x_iX)^{-1} = \sum_{l \ge 0} h_l(x) X^l.$$

Problem 25.1.1. $E_x(X)H_x(-X) = 1$, that is, $\sum_{l=0}^{r} (-1)^l e_{r-l}(x)\, h_l(x) = 0$ for $r \ge 1$. For $x = (a, b)$, $h_2(x) = a^2 + ab + b^2$.

This is [Mac, Ch. I, (2.6)]. For families x and y write $x \sqcup y$ for the concatenated family.

Problem 25.1.2.

$$e_r(x \sqcup y) = \sum_{l=0}^{r} e_l(x)\, e_{r-l}(y), \qquad h_r(x \sqcup y) = \sum_{l=0}^{r} h_l(x)\, h_{r-l}(y).$$

The families that occur are geometric progressions.

Problem 25.1.3. For $t \ge 0$,

$$e_l(1, Q, \dots, Q^t) = Q^{l(l-1)/2} \begin{bmatrix} t+1 \\ l \end{bmatrix}_Q, \qquad h_l(1, Q, \dots, Q^t) = \begin{bmatrix} t+l \\ l \end{bmatrix}_Q.$$

For instance $h_2(1, Q) = 1 + Q + Q^2$.

Date: November 25, 2026.

These are [Mac, Ch. I, §2, Example 3]. Let q be invertible, $Q := q^2$, $g \geq 1$ and $t := g - 1$. A *block* is a family

$$x = m\,(q^t, q^{t-2}, \ldots, q^{-t}) \tag{1}$$

of g terms with ratio Q^{-1}. These are the families of Problem 24.5.3, where q^t is written $Q^{t/2}$.

Problem 25.1.4. For the block (1), $e_l(x) = m^l q^{-l(g-l)} \begin{bmatrix} g \\ l \end{bmatrix}_Q$ and $h_l(x) = m^l q^{-lt} \begin{bmatrix} t+l \\ l \end{bmatrix}_Q$.

The first formula is Problem 24.5.3.

25.2. Valuations

Let k be a finite extension of $\mathbb{Q}_p$, with ring of integers $\mathcal{O}$ and valuation v normalized by $v(p) = 1$.

Problem 25.2.1. $\begin{bmatrix} n \\ l \end{bmatrix}_Q$ is a polynomial in Q with integer coefficients and constant term 1, for $0 \leq l \leq n$. Hence $v\big(\begin{bmatrix} n \\ l \end{bmatrix}_Q\big) = 0$ if $Q \in k$ and $v(Q) > 0$.

Problem 25.2.2. Let $a \in k^\times$ and $Q \in k$ with $v(Q) = \nu > 0$. Then

$$v\big(e_l(a, aQ, \ldots, aQ^t)\big) = l\,v(a) + \nu\,\frac{l(l-1)}{2} \qquad (0 \leq l \leq t+1),$$
$$v\big(h_l(a, aQ, \ldots, aQ^t)\big) = l\,v(a) \qquad (l \geq 0).$$

So the valuation of e_l exceeds that of h_l by $\nu\,l(l-1)/2$.

Problem 25.2.3. Let x be the block (1) with $m, q \in k^\times$ and $v(q) = \nu > 0$. Then $v(h_l(x)) = l\,(v(m) - t\nu)$ and $v(e_l(x)) = l\,(v(m) - t\nu) + \nu\,l(l-1)$ for $0 \leq l \leq g$. In particular every $h_l(x)$ lies in $\mathcal{O}$ if and only if $v(m) \geq t\nu$.

For a union of blocks only a bound survives.

Problem 25.2.4. Let Z be a finite family in k whose least valuation is μ. Then $v(h_l(Z)) \geq l\mu$, with equality if exactly one member of Z has valuation μ. For $Z = (1, 1)$ and $Z = (1, -1)$ one has $h_l(Z) = l + 1$ and $h_l(Z) = (1 + (-1)^l)/2$.

Problem 25.2.5. Let $Z = x_1 \sqcup x_2$, where $x_i = m_i\,(q, q^{-1})$ are blocks with $g = 2$, and let $v(q) = \nu > 0$ and $v(m_1) = v(m_2) = 0$. Then $h_1(Z) = (m_1 + m_2)(q + q^{-1})$, so $v(h_1(Z)) = v(m_1 + m_2) - \nu$, which exceeds $-\nu$ exactly when $m_1 \equiv -m_2$ modulo the maximal ideal of $\mathcal{O}$.

25.3. Moving a Hecke operator along a chain

We use the setting of Problem 24.5.4. Let $F_0, \ldots, F_m$ be finite-dimensional k-vector spaces, let $K_j \colon F_j \to F_{j+1}$ be linear maps, and let $\mathcal{K}_j := K_{j-1} \cdots K_0$, with $\mathcal{K}_0 := 1$. Fix $r \geq 1$. For each j let $\mathcal{E}_0^{(j)} = 1, \mathcal{E}_1^{(j)}, \ldots, \mathcal{E}_r^{(j)}$ be operators on F_j, and let $x_1, \ldots, x_m$ be finite families in k with

$$\mathcal{E}_i^{(j+1)}\,K_j = K_j \sum_{l=0}^{i} e_l(x_{j+1})\,\mathcal{E}_{i-l}^{(j)} \qquad (0 \leq i \leq r,\ 0 \leq j < m). \tag{2}$$

For lifts with split kernels, Section 24.5 gives (2) with x_{j+1} a block (1), up to a unit that we take to be 1 [Adr, Props. 10.8 and 10.13]. Let $Z_j := x_1 \sqcup \cdots \sqcup x_j$. In (2)

the operators at the target are expressed through those at the source. We need the converse.

Problem 25.3.1. Let $r = 1$. Then $K_0\mathcal{E}_1^{(0)} = \big(\mathcal{E}_1^{(1)} - e_1(x_1)\big)K_0$, and $\mathcal{K}_2\mathcal{E}_1^{(0)} = \big(\mathcal{E}_1^{(2)} - h_1(Z_2)\big)\mathcal{K}_2$.

Problem 25.3.2. Let $r = 2$. Then $K_0\mathcal{E}_2^{(0)} = \big(\mathcal{E}_2^{(1)} - h_1(x_1)\,\mathcal{E}_1^{(1)} + h_2(x_1)\big)K_0$.

Problem 25.3.3. $\mathcal{E}_i^{(j)}\,\mathcal{K}_j = \mathcal{K}_j \sum_{l=0}^{i} e_l(Z_j)\,\mathcal{E}_{i-l}^{(0)}$ for $0 \le i \le r$.

Problems 25.3.3 and 25.1.1 give the following, which is Problem 24.5.4.

Theorem 25.3.1. *For $1 \le j \le m$, $\mathcal{K}_j\,\mathcal{E}_r^{(0)} = \displaystyle\sum_{l=0}^{r} (-1)^l h_l(Z_j)\,\mathcal{E}_{r-l}^{(j)}\,\mathcal{K}_j$.*

The relation for one lift has the elementary functions of a block, whose valuations exceed those of the complete functions by $\nu\, l(l-1)$ (Problem 25.2.3). The inverse relation has the complete functions, which may have denominators. The operators $\mathcal{E}_i^{(j)}$ are normalized forms of the sums $T_i^{(j)}$ over edges of type i of Section 24.5: when F_j consists of functions of lattices in a space of dimension N_j, with $N_0 < N_1 < \cdots < N_m$, one takes $\mathcal{E}_i^{(j)} = q^{-i(N_j-i)}\,T_i^{(j)}$ [Adr, §10.3].

Problem 25.3.4. With this normalization, Theorem 25.3.1 reads

$$\sum_{l=0}^{r} (-1)^l h_l(Z_j)\,q^{l(N_j-2r+l)}\,T_{r-l}^{(j)}\,\mathcal{K}_j = q^{r(N_j-N_0)}\,\mathcal{K}_j\,T_r^{(0)}.$$

Problem 25.3.5. Suppose that Z_j is a union of blocks (1) with the same t, that $v(q) > 0$, that $v(m) \ge 0$ for each block, and that $N_j \ge 2r + t - 1$. Then every coefficient $h_l(Z_j)\,q^{l(N_j-2r+l)}$ in Problem 25.3.4 lies in $\mathcal{O}$.

25.4. A gain on a sublattice

For each j let $\mathrm{Int}_j \subset F_j$ be an $\mathcal{O}$-lattice of full rank. For $w \in F_j$ let $\mathrm{ord}(w)$ be the least valuation of a coordinate of w in a basis of Int_j, with $\mathrm{ord}(0) = \infty$. For a linear map $A\colon F_i \to F_j$ let $\mathrm{gain}(A)$ be the least value of $\mathrm{ord}(Ab)$ over the members b of a basis of Int_i. For $k = \mathbb{Q}_p$, $\mathrm{gain}(A)$ is the largest integer g with $A(\mathrm{Int}_i) \subseteq p^g\mathrm{Int}_j$; so $\mathrm{gain}(A)\log p$ plays at p the role of the divisibility $-h_{\mathrm{fin}}$ of Section 8.4.

Problem 25.4.1. ord and gain do not depend on the bases. $\mathrm{ord}(Aw) \ge \mathrm{ord}(w) + \mathrm{gain}(A)$, $\mathrm{gain}(AB) \ge \mathrm{gain}(A) + \mathrm{gain}(B)$, $\mathrm{gain}(A+B) \ge \min(\mathrm{gain}(A), \mathrm{gain}(B))$, and $\mathrm{gain}(cA) = v(c) + \mathrm{gain}(A)$ for $c \in k^\times$.

Assume (2). For $1 \le j \le m$ and $0 \le i \le r$ let

$$\gamma_j(i) := \mathrm{gain}\big(\mathcal{E}_i^{(j)} K_{j-1}\big),$$

so that $\gamma_j(0) = \mathrm{gain}(K_{j-1})$ is the gain of the jth step on the whole lattice, and $\gamma_j(r)$ its gain after the Hecke operator $\mathcal{E}_r^{(j)}$ at the target. Let $c \in k^\times$ be such that $Y := c\,\mathcal{E}_r^{(0)}$ maps Int_0 into itself, and let $A := v(c)$. The gain of the jth step on the image of Y is not $A + \gamma_j(r)$. By Theorem 25.3.1 it is controlled by

$$\delta_j := \min_{0 \le l \le r} \big(v(h_l(Z_j)) + \gamma_j(r-l)\big), \qquad \mathrm{Pr}_j := \gamma_j(r) - \delta_j.$$

When $\gamma_j(r) < \infty$, we call Pr_j the *price* of the jth step; the term $l = 0$ shows that $\mathrm{Pr}_j \ge 0$, and $\delta_j = \gamma_j(r) - \mathrm{Pr}_j$.

Problem 25.4.2. For $w \in F_0$ and $1 \le j \le m$, $\operatorname{ord}\big(\mathcal{K}_j\, \mathcal{E}_r^{(0)} w\big) \ge \operatorname{ord}\big(\mathcal{K}_{j-1} w\big) + \delta_j$.

Problem 25.4.3. Let $S \subseteq \{1, \dots, m\}$, and let n_j be the number of elements of S that are at most j. For $G \in \mathrm{Int}_0$ and $0 \le j \le m$,

$$\operatorname{ord}\big(\mathcal{K}_j\, Y^{n_j} G\big) \ge \sum_{i \le j,\ i \in S} \big(A + \delta_i\big) + \sum_{i \le j,\ i \notin S} \gamma_i(0).$$

Take S to be the set of j with $A + \delta_j > \gamma_j(0)$, and $G := Y^{m-n_m} F$, which lies in Int_0 because Y preserves Int_0. Problem 25.4.3 with $j = m$ gives the following.

Theorem 25.4.1. *For every $F \in \mathrm{Int}_0$,*

$$\operatorname{ord}\big(\mathcal{K}_m\, Y^m F\big) \ge \sum_{j=1}^{m} \max\big(\gamma_j(0),\ A + \delta_j\big).$$

This is the case of one orbit of [Adr, Thm. 10.7], in which the estimates at several primes are combined. A step uses a factor of Y only when the factor pays for its price; the other factors are applied at the start, where they cost nothing. The gain holds on the image $Y^m \mathrm{Int}_0$. When Y is injective this is a sublattice of full rank, and in Theorem 6.5.1 the gain on such a sublattice is charged its colength, divided by the rank.

Problem 25.4.4. If Y is injective, then the length of $\mathrm{Int}_0 / Y^m \mathrm{Int}_0$ is m times the length of $\mathrm{Int}_0 / Y\, \mathrm{Int}_0$.

When Int_0 consists of integral forms and Y is the normalized Hecke operator of Chapter 19, the values of Y at one lattice L span the module $S(L)$ there, and the loss of Chapter 19 is its colength in $H(L)$.

25.5. Stepwise maxima overcount

Theorem 25.4.1, like [Adr, Thm. 10.7], charges each step a price; in [Adr, (10.2)] an upper bound for it is subtracted from the gain of the jth lift. Can the price be ignored, so that each step gains $\max(\gamma_j(0), A + \gamma_j(r))$ on $Y^m \mathrm{Int}_0$? We compare two chains with the same numbers $\gamma_j(i)$. Let p be any prime, $k = \mathbb{Q}_p$, $m = 2$, $r = 1$, $F_j = \mathbb{Q}_p^2$ and $\mathrm{Int}_j = \mathbb{Z}_p^2$. Let $K_0 = K_1 = K$ be a diagonal matrix, let $x_1 = (a_1)$ and $x_2 = (a_2)$ be families of one element, and let

$$Y := \mathcal{E}_1^{(0)} := \operatorname{diag}(p, 1), \qquad \mathcal{E}_1^{(j)} := Y + h_1(Z_j) \quad (j = 1, 2),$$

so that $A = 0$.

Problem 25.5.1. These data satisfy (2), and $\operatorname{length} \mathbb{Z}_p^2 / Y \mathbb{Z}_p^2 = 1$.

Problem 25.5.2. Let $K = \operatorname{diag}(1, p)$ and $a_1 = a_2 = p$. Then $\gamma_j(0) = 0$, $\gamma_j(1) = 1$ and $\Pr_j = 0$ for $j = 1, 2$, and $\operatorname{gain}(\mathcal{K}_2\, Y^2) = 2$.

Problem 25.5.3. Let $K = \operatorname{diag}(p, 1)$, $a_1 = p - 1$ and $a_2 = -2p$. Then $\gamma_j(0) = 0$, $\gamma_j(1) = 1$ and $\Pr_j = 1$ for $j = 1, 2$, and $\operatorname{gain}(\mathcal{K}_2\, Y^2) = 0$.

In both chains each step, followed by the Hecke operator at its target, gains 1, and the sum of the stepwise maxima is 2. In the second chain the composite gains nothing on $Y^2 \mathrm{Int}_0$: the Hecke operator at the target of each step is not the image of the one at the source, and $h_1(Z_j)$ is a unit. Theorem 25.4.1 gives the exact gain in both cases.

The theorem takes two inputs: the gains $\gamma_j(i)$ of a single lift followed by a Hecke operator at its target, for which Chapters 16 and 17 give models through the divisibility of theta kernels, and the colength of $Y\,\mathrm{Int}_0$, which Chapter 19 computes at one lattice. The price couples them, through the least valuation in the union Z_j of the blocks met so far (Problems 25.2.3 and 25.2.4).

Exercises.

(1) The Newton polygon of $\prod_{i=0}^{t}(1+aQ^iX)$ over k, with $a \in k^\times$ and $v(Q) > 0$, has the vertices $\big(l, l\,v(a) + v(Q)\,l(l-1)/2\big)$ for $0 \le l \le t+1$.

(2) Suppose that (2) holds with $u_{j+1}^i K_j$ in place of K_j on the right, for units $u_j \in \mathcal{O}^\times$. In terms of $E_j(X) := \sum_{i \le r} \mathcal{E}_i^{(j)} X^i$ this reads $E_{j+1}(X)K_j = K_j\,E_{x_{j+1}}(u_{j+1}X)\,E_j(u_{j+1}X)$ modulo X^{r+1}; it is the relation of Section 24.5 with the family $u_{j+1}x_{j+1}$, whose product $\prod_a(1+aX)$ is the $P(X)$ written there. Then Theorem 25.3.1 holds with $\mathcal{K}_j\mathcal{E}_r^{(0)}$ multiplied by $(u_1\cdots u_j)^r$, and with Z_j replaced by the family Z_j' of the $u_l u_{l+1}\cdots u_j\,a$ for $l \le j$ and a in x_l [Adr, Prop. 10.8]. Theorem 25.4.1 holds with δ_j computed from Z_j'. These agree with the old δ_j when Z_j has exactly one member of least valuation (Problem 25.2.4), but not in general: for p odd, $x_1 = (1)$, $x_2 = (-1)$, $u_1 = -1$ and $u_2 = 1$, one has $h_1(Z_2) = 0$ while $h_1(Z_2')$ is a unit.

Hints

§25.1.

25.1.1: Compare the product formulas.
25.1.2: $E_{x \sqcup y} = E_x E_y$.
25.1.3: Induction on t, with the rule $\begin{bmatrix} n \\ l \end{bmatrix}_Q = \begin{bmatrix} n-1 \\ l-1 \end{bmatrix}_Q + Q^l \begin{bmatrix} n-1 \\ l \end{bmatrix}_Q$ and its companion $\begin{bmatrix} n \\ l \end{bmatrix}_Q = Q^{n-l} \begin{bmatrix} n-1 \\ l-1 \end{bmatrix}_Q + \begin{bmatrix} n-1 \\ l \end{bmatrix}_Q$.
25.1.4: Problem 25.1.3 for the family $mq^{-t}(1, Q, \ldots, Q^t)$; e_l and h_l are homogeneous of degree l.

§25.2.

25.2.1: The first rule in the hint to Problem 25.1.3.
25.2.2: Problems 25.1.3 and 25.2.1.
25.2.3: Problems 25.1.4 and 25.2.1.
25.2.4: Which monomial of degree l has the least valuation?
25.2.5: Problem 25.1.2.

§25.3.

25.3.1: Apply (2) with $i = 1$ once for each step.
25.3.2: Use (2) with $i = 1$ to remove $K_0\mathcal{E}_1^{(0)}$, then Problem 25.1.1.
25.3.3: Write (2) as an identity of polynomials in X modulo X^{r+1}, as in the hint to Problem 24.5.4, and use Problem 25.1.2.
25.3.4: Multiply Theorem 25.3.1 by $q^{r(N_j - r)}$.
25.3.5: Problems 25.2.3 and 25.2.4; look at $l = 1$.

§25.4.

25.4.1: Write w in coordinates.

25.4.2: Apply Theorem 25.3.1 to w, write $\mathcal{K}_j = K_{j-1}\mathcal{K}_{j-1}$, and use Problem 25.4.1.

25.4.3: Induction on j. For $j \in S$ write $Y^{n_j} = c\,\mathcal{E}_r^{(0)}\,Y^{n_{j-1}}$ and use Problem 25.4.2.

25.4.4: $Y^i\mathrm{Int}_0/Y^{i+1}\mathrm{Int}_0 \cong \mathrm{Int}_0/Y\,\mathrm{Int}_0$.

§25.5.

25.5.1: Diagonal matrices commute.

25.5.2: Compute $\mathcal{K}_2\,Y^2$.

25.5.3: Compute $\mathcal{E}_1^{(1)}$ and $\mathcal{E}_1^{(2)}$ first.

References

[Adr] J. Adriazola, *The Alpöge proof of the Riemann hypothesis*, manuscript, revised 24 November 2026, `https://github.com/jimjamzola/RH-Alpoge-Reconstruction`.

[Mac] I. G. Macdonald, *Symmetric Functions and Hall Polynomials*, 2nd ed., Oxford Math. Monogr., Clarendon Press, Oxford, 1995.