On p-adic unit-root formulas

Masha Vlasenko

Abstract For a multivariate Laurent polynomial $f(x)$ with coefficients in a ring R we construct a sequence of matrices with entries in R whose reductions modulo p give iterates of the Hasse–Witt operation for the hypersurface of zeroes of the reduction of $f(x)$ modulo p. We show that our matrices satisfy a system of congruences modulo powers of p. If the Hasse–Witt operation is invertible these congruences yield p-adic limit formulas, which conjecturally describe the Gauss–Manin connection and the Frobenius operator on the the slope 0 part of a crystal attached to $f(x)$. We also apply our results on congruences to integrality of formal group laws of Artin–Mazur kind.

1 Hasse–Witt matrix

Let $X/\mathbb{F}_q$ be a smooth projective variety of dimension n over a finite field with $q = p^a$ elements. The congruence formula due to Katz (see [1]) states that modulo p the zeta function of X is described as

$$Z(X/\mathbb{F}_q;T) \quad \equiv \quad \prod_{i=0}^{n} \det(1 - T \cdot \mathscr{F}^a \,|\, H^i(X,\mathscr{O}_X))^{(-1)^{i+1}} \qquad \mod p\,, \qquad (1)$$

where $H^i(X,\mathscr{O}_X)$ is the cohomology of X with coefficients in the structure sheaf $\mathscr{O}_X$ and $\mathscr{F}$ is the Frobenius map, the *p-linear* vector space map induced by $h \mapsto h^p$ on the structure sheaf (*p-linear* means $\mathscr{F}(bs+ct) = b^p\mathscr{F}(s) + c^p\mathscr{F}(t)$ for $b,c \in \mathbb{F}_q$ and $s,t \in H^i(X,\mathscr{O}_X)$). When X is a complete intersection the only interesting term in formula (1) is given by $H^n(X,\mathscr{O}_X)$. The action of $\mathscr{F}$ on this space is classically known as the *Hasse–Witt operation*.

Masha Vlasenko
Institute of Mathematics of the Polish Academy of Sciences
Śniadeckich 8, 00-656 Warsaw, Poland, e-mail: m.vlasenko@impan.pl

The following algorithm (see [2, §7.10], [1, Corollary 6.1.13] or [3, §II.1]) can be used to compute the Hasse–Witt matrix of a hypersurface $X \subset \mathbb{P}^{n+1}$ given by a homogeneous equation $f(x_0,\dots,x_{n+1})=0$ of degree $d > n+2$. One extends the Frobenius to a transformation of the exact sequence of sheaves on $\mathbb{P}^{n+1}$:

$$\begin{array}{ccccccc} 0 \to \mathscr{O}_{\mathbb{P}^{n+1}}(-d) & \xrightarrow{f} & \mathscr{O}_{\mathbb{P}^{n+1}} & \to & \mathscr{O}_X & \to 0 \\ \downarrow f^{p-1}\mathscr{F} & & \downarrow \mathscr{F} & & \downarrow \mathscr{F} & \\ 0 \to \mathscr{O}_{\mathbb{P}^{n+1}}(-d) & \xrightarrow{f} & \mathscr{O}_{\mathbb{P}^{n+1}} & \to & \mathscr{O}_X & \to 0\,. \end{array}$$

The coboundary in the resulting long exact cohomology sequence allows to identify

$$H^n(X,\mathscr{O}_X) \quad \widetilde{\to} \quad H^{n+1}(\mathbb{P}^{n+1},\mathscr{O}_{\mathbb{P}^{n+1}}(-d))\,,$$

so that the Frobenius $\mathscr{F}$ on $H^n(X,\mathscr{O}_X)$ corresponds to the map on $H^{n+1}(\mathbb{P}^{n+1},\mathscr{O}_{\mathbb{P}^{n+1}}(-d))$ induced by

$$0 \to \mathscr{O}_{\mathbb{P}^{n+1}}(-d) \xrightarrow{\mathscr{F}} \mathscr{O}_{\mathbb{P}^{n+1}}(-pd) \xrightarrow{f^{p-1}} \mathscr{O}_{\mathbb{P}^{n+1}}(-d) \to 0\,.$$

Computing Čech cohomology we find that Laurent monomials $x^{-u} = x_0^{-u_0}\dots x_{n+1}^{-u_{n+1}}$ where u runs through the set

$$U = \{u = (u_0,\dots,u_{n+1}) \,:\, u_i \in \mathbb{Z}_{\geq 1}\,, \quad \sum_{i=0}^{n+1} u_i = d\} \tag{2}$$

form a basis in $H^{n+1}(\mathbb{P}^{n+1},\mathscr{O}_{\mathbb{P}^{n+1}}(-d))$ and the Hasse–Witt matrix is given in this basis by

$$\mathscr{F}_{u,v\in U} \;=\; \text{the coefficient of } x^{pv-u} \text{ in } f(x)^{p-1}\,. \tag{3}$$

Suppose one starts from a polynomial f in characteristic 0, e.g. with coefficients in $\mathbb{Z}$. In my talk at the MATRIX institute in Creswick I presented a construction which lifts (3) to a matrix with entries in $\mathbb{Z}_p$ whose characteristic polynomial conjecturally gives the p-adic unit root part of the zeta function attached to the middle cohomology of X. The proofs and a few evidences for the conjecture can be found in the preprint [4].

2 Main results

We study a sequence of matrices which generalize (3). Let R be a commutative characteristic 0 ring, that is the natural map $R \to R\otimes\mathbb{Q}$ is an embedding. Let $f \in R[x_1^{\pm 1},\dots,x_N^{\pm 1}]$ be a Laurent polynomial in N variables. If $f(x) = \sum_u a_u x^u, a_u \in R$, the *Newton polytope* $\Delta(f) \subset \mathbb{R}^N$ is the convex hull of the finite set $\{u : a_u \neq 0\}$. Consider the set of internal integral points $J = \Delta(f)^o \cap \mathbb{Z}^N$, where $\Delta(f)^o$ denotes the topological interior of the Newton polytope. Let $g = \#J$ be the number of internal integral points in the Newton polytope, which we assume to be positive. Consider the following sequence of $g \times g$ matrices with entries in R whose rows and columns are indexed by the elements of J:

$$(\beta_m)_{u,v \in J} \;=\; \text{the coefficient of } x^{(m+1)v-u} \text{ in } f(x)^m\,. \tag{4}$$

By convention, β_0 is the identity matrix. We shall consider arithmetic properties of the sequence $\{\beta_m; m \geq 0\}$.

Let us fix a prime number p. We restrict our attention to the sub-sequence $\{\alpha_s = \beta_{p^s-1}; s \geq 0\}$. The entries of these matrices are then given by

$$(\alpha_s)_{u,v \in J} \;=\; \text{the coefficient of } x^{p^s v-u} \text{ in } f(x)^{p^s-1}\,.$$

Notice that when R/pR is a finite field and f is a homogeneous polynomial of degree d such that its reduction modulo p defines a smooth hypersurface, then U in (2) coincides with J (with $N = n+2$) and $\alpha_1 = \beta_{p-1}$ modulo p is the Hasse–Witt matrix.

Theorem 1. *Assume that the ring R is endowed with a pth power Frobenius endomorphism, that is a ring endomorphism $\sigma : R \to R$ satisfying $\sigma(a) \equiv a^p \mod p$ for all $a \in R$. Then for every s*

$$\alpha_s \;\equiv\; \alpha_1 \cdot \sigma(\alpha_1) \cdot \ldots \cdot \sigma^{s-1}(\alpha_1) \mod p\,. \tag{5}$$

If α_1 is invertible modulo p then for every $s \geq 1$ one has congruences

$$\alpha_{s+1} \cdot \sigma(\alpha_s)^{-1} \;\equiv\; \alpha_s \cdot \sigma(\alpha_{s-1})^{-1} \mod p^s \tag{6}$$

and

$$D(\alpha_s) \cdot \alpha_s^{-1} \;\equiv\; D(\alpha_{s-1}) \cdot \alpha_{s-1}^{-1} \mod p^s \tag{7}$$

for any derivation $D : R \to R$.

Congruence (5) shows that $\alpha_s \mod p$ are iterates of the Hasse–Witt operation whenever the latter is defined. It also implies that when α_1 is invertible modulo p then all α_s are invertible modulo p and hence also modulo p^s for all s. Therefore statements (6) and (7) make sense. We remark that analogous congruences also hold when one multiplies by the inverse matrices on the left, that is we can prove that $\sigma(\alpha_s)^{-1} \cdot \alpha_{s+1} \;\equiv\; \sigma(\alpha_{s-1})^{-1} \cdot \alpha_s$ and $\alpha_s^{-1} \cdot D(\alpha_s) \;\equiv\; \alpha_{s-1}^{-1} \cdot D(\alpha_{s-1}) \mod p^s$.

Our results are related to the topic of the workshop because when $\Delta(f)$ is a reflexive polytope (in this case $g = 1$), the toric hypersurface of zeroes of f can be compactified to a Calabi–Yau variety. Congruence (6) then generalizes so called Dwork's congruences (see [5, 6]) and (7) seems to be new even in the Calabi–Yau case.

Theorem 1 implies existence of the p-adic limits

$$F \;=\; \lim_{s\to\infty} \alpha_{s+1}\cdot\sigma(\alpha_s)^{-1} \tag{8}$$

and

$$\nabla_D \;=\; \lim_{s\to\infty} D(\alpha_s)\cdot\alpha_s^{-1} \quad \text{for every derivation} \quad D\in Der(R)\,. \tag{9}$$

These are $g\times g$ matrices have entries in the p-adic closure $\widehat{R} = \lim\limits_{\leftarrow} R/p^s R$. Note that $F \equiv \alpha_1 \mod p$. We are currently working on identifying the limiting matrices (8) and (9) with the Frobenius and Gauss–Manin connection on the slope 0 part of a crystal attached to the Laurent polynomial f. This fact was conjectured for homogeneous polynomials in [4] based on several examples and analogy with the congruences for expansion coefficients of differential forms stated in [7]. The progress in this project is due to our collaboration with Frits Beukers, which started at the MATRIX institute. I am also grateful to Frits for the series of extremely helpful lectures on Dwork cohomology which he gave during the first week of the program.

Matrices (4) showed up in [8] as coefficients of the logarithms of explicit coordinalizations of the Artin–Mazur formal group laws of projective hypersurfaces and complete intersections. Under certain conditions (e.g. R is the ring of integers of the unramified extension of $\mathbb{Q}_p$ of degree a and f is a homogeneous polynomial whose reduction modulo p defines a non-singular hypersurface $X/\mathbb{F}_{p^a}$) one can combine (6) with the generalized Atkin and Swinnerton-Dyer congruences in [9], which yields that the eigenvalues of $\Phi = F\cdot\sigma(F)\cdot\ldots\cdot\sigma^{a-1}(F)$ are p-adic unit eigenvalues of the Frobenius operator on the middle crystalline cohomology of X (see [4, Section 5]).

Our second result is the following integrality theorem for formal group laws attached to a Laurent polynomial. Its proof is based on explicit congruences (similar to those in Theorem 1) and Hazewinkel's functional equation lemma (see [4, Section 4]).

Theorem 2. *Let J be either the set $\Delta(f)\cap\mathbb{Z}^N$ of all integral points in the Newton polytope of f or the subset of internal integral points $\Delta(f)^\circ\cap\mathbb{Z}^N$. Assume that J is non-empty and let $g=\#J$. Consider the sequence of matrices $\beta_m\in \mathrm{Mat}_{g\times g}(R)$, $m\geq 0$ given by formula* (4) *and define a g-tuple of formal powers series $l(\tau)=(l_u(\tau))_{u\in J}$ in g variables $\tau=(\tau_v)_{v\in J}$ as*

$$l(\tau) \;=\; \sum_{m=1}^{\infty}\frac{1}{m}\,\beta_{m-1}\,\tau^m\,.$$

Consider the g-dimensional formal group law $G_f(\tau,\tau') = l^{-1}(l(\tau)+l(\tau'))$ with coefficients in $R\otimes\mathbb{Q}$.

Let p be a prime number. If R can be endowed with a pth power Frobenius endomorphism then G_f is p-integral, that is $G_f\in R_{(p)}[[\tau,\tau']]$ where $R_{(p)}=R\otimes\mathbb{Z}_{(p)}$ is the subring of $R\otimes\mathbb{Q}$ formed by elements without p in the denominator.

Note that if one can define a Frobenius endomorphism on R for every prime p then Theorem 2 implies that $G_f \in R[[\tau,\tau']]$ because the subring $\cap_p R_{(p)} \subset R \otimes \mathbb{Q}$ coincides with R. For example, rings $\mathbb{Z}$ and $\mathbb{Z}[t]$ are of this type: one can take the Frobenuis endomorphism to be the identity on $\mathbb{Z}$ and $h(t) \mapsto h(t^p)$ on $\mathbb{Z}[t]$.

Acknowledgements My work is supported by the National Science Centre of Poland, grant UMO-2016/21/B/ST1/03084. I am grateful to the European Mathematical Society and the MATRIX institute for sponsoring my participation in the program. I would like to mention that hospitality of the staff of the institute and MATRIX Family Fund made it possible for me to bring to Creswick my 3 month old daughter Helena.

References

1. N. Katz, *Une formule de congruence pour la fonction* ζ, S.G.A. 7 II, Lecture Notes in Mathematics 340, Springer, 1973
2. B. Dwork, *On the zeta function of a hypersurface II*, Annals of Math. 80 (1964), 227–299
3. N. Koblitz, *p-adic variation of the zeta function over families of varieties defined over finite fields*, Comp. Math. 31 (1975), f. 2, 119–218
4. M. Vlasenko, *Higher Hasse–Witt matrices*, arXiv:1605.06440 [math.NT]
5. A. Mellit, M. Vlasenko, *Dwork congruences for the constant terms of powers of a Laurent polynomial*, International Journal of Number Theory, vol. 12, no. 2 (2016), 313–321
6. K. Samol, D. van Straten, *Dwork congruences and reflexive polytopes*, Annales Mathématiques du Québec, vol. 39 , no. 2 (2015), 185–203
7. N. Katz, *Internal reconstruction of unit-root F-crystals via expansion-coefficients*, Annales scientifiques de l' É.N.S. 4e série, tome 18, no. 2(1985), 245–285
8. J. Stienstra, *Formal group laws arising from algebraic varieties*, American Journal of Mathematics, 109, no. 5 (1987), 907–925
9. J. Stienstra, *Formal groups and congruences for L-functions*, American Journal of Mathematics, 109, no. 6 (1987), 1111–1127