DRINFEL′D-VLĂDUŢ AND IHARA-VLĂDUŢ

JEROEN SIJSLING

CONTENTS

SUMMARY

Let, as always in our seminar, $C|\mathbf{F}_q$ be a curve. Our first purpose is to prove the Drinfel′d-Vlăduţ theorem, bounding the deviation of $C(\mathbf{F}_q)$ from $q+1$ as $g(C)$ grows. We follow the treatment of Serre in [Ser85], although the original 1983 paper is also a nice read considering its two-page conciseness: see [VD83] for an English translation.

Up next is a result proved by Ihara and, later, Vlăduţ (in [TVZ82]), a special case of a converse to the Drinfel′d-Vlăduţ theorem, namely for $q = p^2$ with p prime, which can be proved using some theory of modular curves. Some references for this part are [Edi97] and [Ser85].

1. DRINFEL′D-VLĂDUŢ

Let C be a curve over a finite field $\mathbf{F}_q$: as usual, we suppose it is smooth, complete and geometrically connected. Recall from Jos′ talk that by the rationality of the zeta function and the Riemann hypothesis, there exist $2g$ algebraic integers α_k of absolute value $q^{1/2}$ (the *eigenvalues of Frobenius*, occuring as reciprocals of the roots of the numerator of the zeta function) such that for all n

$$\#C(\mathbf{F}_{q^n}) = q^n + 1 - \sum_{k=1}^{2g} \alpha_k^n, \tag{1}$$

and that because of the functional equation for the zeta function, the α_k come in complex conjugate pairs. For such a curve C, we will by O_d^C denote the number of effective F_q-rational divisors indecomposable over $\mathbf{F}_q$, or, equivalently, the number Frob$_q$-orbits of length d of geometric points of C, or, again equivalently, the number of points of the scheme C with residue field $\mathbf{F}_q^d$. Then obviously

$$\#C(\mathbf{F}_{q^n}) = \sum_{d|n} dO_d^C. \tag{2}$$

We will now fix our q and let n be equal to 1. Our goal is to investigate how big the ″error term″ in (1) can get as we take the lim sup over all curves defined over $\mathbf{F}_q$. More precisely, for a curve C over $\mathbf{F}_q$, we introduce the quantity

$$\operatorname{dev}(C) = \frac{\#C(\mathbf{F}_q) - (q+1)}{g(C)}$$

and consider the limit

$$A(q) = \limsup_{C|\mathbf{F}_q} \operatorname{dev}(C) = \lim_{g\to\infty} \sup_{\substack{C|\mathbf{F}_q \text{ of} \\ \text{genus } g}} \operatorname{dev}(C).$$

The equality of limits holds because of

Proposition 1.1. *Let q be a prime power. Then there are only finitely many curves defined over $\mathbf{F}_q$ of a fixed genus g up to $\mathbf{F}_q$-isomorphism.*

Note that this Proposition also implies that $A(q)$ is the lim sup of $\frac{\#C(\mathbf{F}_q)}{g(C)}$, and that we certainly need our hypotheses on smoothness and completeness for it to hold.

Sketch of proof of Proposition 1.1. There are many high-powered ways to do this: one can invoke the existence of a moduli space and finiteness of twists, use Jacobians and Honda-Tate theory, or try to reason as in the theorem of Hermite in algebraic number theory, using lattices in special spaces. A more elementary sketch runs as follows.

Lenny has already proved that every curve of genus zero over our field $\mathbf{F}_q$ has a rational point, hence is isomorphic to $\mathbf{P}^1_{\mathbf{F}_q}$, so $g = 0$ has been dealt with. For $g = 1$, it follows from the fact that there are only finitely many elliptic curves rational over $\mathbf{F}_q$ (this is obvious from the fact that an elliptic curve over a field k admits a Weierstrass equation with coefficients in k), and the fact that every genus one curve over a finite field is elliptic: using either our Hasse-Weil bound or group cohomology, one can show that it always has a rational point.

For higher genus, the problem is that we have no way of explicitly describing a general curve of high genus over $\mathbf{F}_q$. However, we know that the Riemann-Roch theorem holds over arbitrary fields, not just algebraically closed ones. Now we use the following well-known consequence of Riemann-Roch:

Let $C|k$ be a curve of genus ≥ 2 with canonical line bundle ω_C. Then $\omega_C^{\otimes 3}$ is very ample.

Because ω_C is defined over $\mathbf{F}_q$, this means that there exists an embedding of our C into $\mathbf{P}^{l(\omega_C^{\otimes 3})}_{\mathbf{F}_q} = \mathbf{P}^{5g-5}_{\mathbf{F}_q}$, realizing it as a curve of degree $\deg(\omega_C^{\otimes 3}) = 6g - 6$. This is not quite enough, because the curve need not be a complete intersection, but one can project the curve birationally to a suitable hyperplane defined over a bounded finite extension of $\mathbf{F}_q$ without changing the degree; we may have to take a finite extension as the original curve can have many points over $\mathbf{F}_q$, but it is quite plausible that the degree of this extension can be bounded uniformly. Projecting further, one obtains a curve in $\mathbf{P}^2$ birational to the original curve and of degree $6g - 6$. This curve is very likely to be singular, but this is irrelevant, as every birational equivalence class of curves contains only one non-singular curve. Because the curve is defined over a finite extension of $\mathbf{F}_q$, the equation defining it has coefficients this same finite extension (an elementary form of Galois descent). But there are only finitely many possible choices for these coefficients. □

By the Riemann hypothesis, $A(q)$ is at most $2q^{1/2}$, since for any curve C, $\operatorname{dev}(C)$ is bounded by this quantity. But it is very plausible that this bound can be improved. Indeed, $\operatorname{dev}(C)$ can only be equal to this bound if q is a square and all the α_k equal $-q^{1/2}$. And in that case, considering that

$$\#C(\mathbf{F}_q) = 1 + q + 2gq^{1/2}$$

should be at least

$$\#C(\mathbf{F}_{q^2}) = 1 + q^2 - 2gq$$

one obtains $g(C) \leq \frac{1}{2}(q - q^{1/2})$, yielding a finite supply of curves only. Below, we will refine this approach to obtain Drinfel'd-Vlăduţ.

In [Ser85], it is shown that for q a square, the *Segre curve*

$$x^{q^{1/2}+1} + y^{q^{1/2}+1} + z^{q^{1/2}+1} = 0$$

over $\mathbf{F}_q$ is an example of a curve with $\operatorname{dev}(C) = 2q^{1/2}$. Since the genus of these curves grows with q, this also shows why the finite field $\mathbf{F}_q$ needs to be fixed in our considerations.

Now for some precise results. We can renumber our eigenvalues α_k in such a way that for $k = 1, \dots, g$, the α_k can be written as

$$\alpha_k = q^{1/2} e^{i\varphi_k}$$

and $\alpha_{g+1}, \dots, \alpha_{2g}$ are the complex conjugates of $\alpha_1, \dots, \alpha_g$. Then clearly

$$\#C(\mathbf{F}_{q^n}) = q^n + 1 - q^{n/2} \sum_{i=1}^{g} 2\cos n\varphi_k. \tag{3}$$

Central in our considerations are *even trigonometric polynomials*, that is, functions of the form

$$f(\vartheta) = \sum_{n \in \mathbf{Z}} c_n e^{in\vartheta},$$

where $c_0 = 1, c_n = c_{-n}$ and only a finite number of c_n are non-zero. Alternatively,

$$f(\vartheta) = 1 + \sum_{n \in \mathbf{Z}_{\geq 1}} 2c_n \cos n\vartheta.$$

Given such a function f, one can consider the polynomials

$$\psi_d(t) = \sum_{\substack{n \in \mathbf{Z}_{\geq 1} \\ n \equiv 0 \bmod d}} c_n t^n$$

as d ranges over $\mathbf{N}$. Note that one could also consider power series of this form, but this is not necessary for our result.

Substituting the angles φ_k associated to our α_k, we obtain

Proposition 1.2. *Let C, O_d^C and φ_k be as above. Let f be an even trigonometric polynomial, with associated polynomials ψ_d. Then*

$$\sum_{k=1}^{g} f(\varphi_k) + \sum_{d \in \mathbf{Z}_{\geq 1}} dO_d^C \psi_d(q^{1/2}) = g(C) + \psi_1(q^{-1/2}) + \psi_1(q^{1/2}).$$

Proof. Using equations (3) and (2), we obtain

$$\begin{aligned}
\sum_{k=1}^{g} f(\varphi_k) &= g(C) + \sum_{n,k} 2c_n \cos n\varphi_k \\
&= g(C) + \sum_{n} c_n \sum_{k} 2\cos n\varphi_k \\
&= g(C) + \sum_{n} c_n (q^{n/2} + q^{-n/2} - q^{-n/2}\#C(\mathbf{F}_{q^n})) \\
&= g(C) + \sum_{n} c_n q^{n/2} + \sum_{n} c_n q^{-n/2} - \sum_{n} c_n q^{-n/2} \sum_{d|n} dO_d^C \\
&= g(C) + \psi_1(q^{1/2}) + \psi_1(q^{-1/2}) - \sum_{d} dO_d^C \psi_d(q^{1/2}).
\end{aligned}$$

□

Let us call an even trigonometric polynomial *neat* if $f \geq 0$ and $\forall n : c_n \geq 0$. One easily checks (by only considering the term with $d = 1$) that for neat f with associated ψ_1, the inequalities

$$\#C(\mathbf{F}_q) - 1 \leq \frac{g + \psi_1(q^{1/2})}{\psi_1(q^{-1/2})}$$

and

$$g \geq (\#C(\mathbf{F}_q) - 1)\psi_1(q^{-1/2}) - \psi(q^{1/2})$$

hold. Finding f such that these inequalities give sharp bounds is a special branch of sports. We will merely derive an asymptotic result:

Theorem 1.3. *Let N be an integer. Then*

$$\limsup_{C|\mathbf{F}_q} \frac{1}{g(C)} \sum_{d=1}^{N} \frac{dO_d^C}{q^{d/2} - 1} \leq 1.$$

Proof. Given a neat trigonometric polynomial f with associated ψ_d, one certainly has

$$\sum_{d=1}^{N} dO_d^C \psi_d(q^{-1/2}) \leq g(C) + \psi_1(q^{1/2}) + \psi_1(q^{-1/2}),$$

so because g tends to infinity as we take the lim sup,

$$\limsup_{C|\mathbf{F}_q} \frac{1}{g(C)} \sum_{d=1}^{N} dO_d^C \psi_d(q^{-1/2}) \leq 1.$$

So if there exists a sequence of neat even trigonometric polynomials for which the ψ_d converge to $1/(t^{-d} - 1) = t^d + t^{2d} + \ldots$, then the theorem will be proved.

This will follow from the next two claims:

(1) The coefficients of a neat even trigonometric polynomial f are bounded by 1.

Proof. Indeed, since c_n and f are both positive,

$$\begin{aligned} c_n &= |\frac{1}{2\pi} \int_0^{2\pi} f(\vartheta) \cos n\vartheta d\vartheta| \leq \frac{1}{2\pi} \int_0^{2\pi} |f(\vartheta) \cos n\vartheta| d\vartheta \\ &= \frac{1}{2\pi} \int_0^{2\pi} f(\vartheta) |\cos n\vartheta| d\vartheta \leq \frac{1}{2\pi} \int_0^{2\pi} f(\vartheta) d\vartheta = 1. \end{aligned}$$

□

(2) For fixed B and ϵ, there exists an f with $c_n \geq 1 - \epsilon$ for all $n \leq B$.

Proof. One checks that for m big enough,

$$\begin{aligned} f_m(\vartheta) &= \frac{1}{2m+1}(1 + 2\cos\vartheta + \ldots + 2\cos m\vartheta)^2 \\ &= \frac{1}{2m+1}((2m+1) + 2m\cos\vartheta + \ldots + \cos 2m\vartheta) \end{aligned}$$

does the job. □

Taking the limit over the inequalities furnished by our special fs, our theorem is proved. □

For $N = 1$, one obtains

Corollary 1.4 (Drinfel'd-Vlăduţ). *Let q be a prime power, and consider the curves C defined over $\mathbf{F}_q$. Then*

$$A(q) = \limsup_{C|\mathbf{F}_q} \frac{\operatorname{dev}(C)}{g(C)} = \limsup_{C|\mathbf{F}_q} \frac{\#C(\mathbf{F}_q)}{g(C)} \leq q^{1/2} - 1.$$

One might attempt to generalize this to arbitrary varieties, but for those, the formula analogous to (1) is harder: one needs trace maps on more cohomology groups than H^1.

2. Ihara-Vlăduţ

Our next goal is to show that for certain q, the upper bound in [VD83] is also a lower bound, implying the inequality

$$A(q) = q^{1/2} - 1.$$

For q a square p^{2n}, this has been proved in complete generality, but the technical demands increase drastically with n. Our case $n = 1$ requires the theory of modular curves, whereas $n = 2$ (proved by Ihara and Zink) uses Shimura curves. The proof for general n, due to Ihara alone, uses both Shimura curves and class field theory. We will stick with $n = 1$, which is complicated enough already. Incidentally, for q that are not even powers of a prime, there is still little known about lower bounds on $A(q)$.

We need a few technical notions for this, using some categorical terminology. For an object M of a category C, denote by h_M the contravariant functor $\operatorname{Hom}_C(-, M)$.

Definition 2.1. *Let C be a category, and let $\mathscr{F}$ be a functor from C to $\mathfrak{Set}$. A* moduli object *for $\mathscr{F}$ is an object M of C such that we have a natural transformation $\mathscr{F} \to h_M$ that is universal in the following sense: For any natural transformation $\mathscr{F} \to h_N$, there is a morphism $M \to N$ inducing a natural transformation $h_M \to h_N$ making the following diagram commute:*

$$\begin{tikzcd} \mathscr{F} \arrow[rr] \arrow[dr] & & h_N \\ & h_M \arrow[ur] & \end{tikzcd}$$

Clearly (by the Yoneda lemma), moduli objects are unique up to (canonical) isomorphism.

Definition 2.2. *Let $\mathfrak{Sch}_S$ be the category of schemes over a fixed base scheme S, and let $\mathscr{F}$ be a functor from $\mathfrak{Sch}_S$ to $\mathfrak{Set}$. A* coarse moduli variety *for $\mathscr{F}$ is a scheme M over S that is a moduli object for $\mathscr{F}$ having the property that for algebraically closed fields k over S, the map $\mathscr{F}(\operatorname{Spec}(k)) =: \mathscr{F}(k) \to M(k) := \operatorname{Hom}(\operatorname{Spec}(k), M)$ is an isomorphism.*

Since isomorphic objects have the same functors of points, the second condition of should really be seen as a demand on $\mathscr{F}$ instead of on M. It is automatically fulfilled if the natural transformation $\mathscr{F} \to h_M$ is an isomorphism, in which case M is called a *fine moduli variety*. Again, this is really a demand on $\mathscr{F}$.

Definition 2.3. *Let T be a scheme. Then an* elliptic curve *over T is a proper smooth curve with geometrically connected fibers of genus one, together with a point 0 of $E(T)$.*

Let $E|T$ be an elliptic curve over T. A $\Gamma_0(N)$-structure *is a subgroup scheme G of E that becomes the constant group scheme $\mathbf{Z}/N\mathbf{Z}$ after some surjective finite étale base change.*

Let S be a base scheme, and T a scheme over S. We define $\mathscr{E}_S(T)$ to be the set of S-isomorphism classes of pairs $(E|T, G)$, with $E|T$ an elliptic curve over T and G a $\Gamma_0(N)$-structure on $E|T$. Using pullbacks, this is a contravariant functor.

The functor we are interested in (although this is not immediately obvious) is $\mathscr{E}_S$. It is not necessary to completely understand this definition, as long as one is willing to accept the upcoming Theorem 2.4 and the fact that it corresponds to the usual notions over fields.

The following fundamental theorem is attributed to Igusa.

Theorem 2.4. *The functor $\mathscr{E}_{\mathbf{Z}[1/N]}$ has a coarse moduli variety $Y_0(N)$, which is an affine curve over $\mathbf{Z}[1/N]$.*

The proof is given in [Edi97]. It is not proved there that over algebraically closed fields k, the association $\mathscr{F}(k) \to M(k) = \mathrm{Hom}(\mathrm{Spec}(k), M)$ is an isomorphism: however, surjectivity is clear from the proof, and injective corresponds more or less to the fact that all twists of an elliptic curve over a field k become isomorphic over some finite extension, hence over k itself if k is algebraically closed.

This abstract result has the following concrete interpretation: the curve $Y_0(N)_{\mathbf{C}}$ over $\mathbf{C}$, known from the theory of modular forms, can be defined by equations with coefficients in $\mathbf{Q}$, and for $p \nmid N$, it allows a model over $\mathbf{Z}_p$ that reduces well. This is what Igusa himself actually proved. Another way to explicitly construct this moduli variety over $\mathbf{F}_q$ is by considering the universal elliptic curve over $\mathbf{F}_q(j)$, adjoining the coordinates of the N-torsion point to $\mathbf{F}_q(j)$, then finally to construct the non-singular curve over $\mathbf{F}_q$ corresponding to this function field.

Using this strong result, we will see that for coprime N and p, the moduli variety $Y_0(N)$ has many points over $\mathbf{F}_{p^2}$. We need some lemmas before we start the proof.

Lemma 2.5. *Let $\mathscr{F}$ be a functor with coarse moduli space M, and let K be a field contained in an algebraically closed field k. Then two elements of $\mathscr{F}(K)$ give rise to the same elements of $M(K)$ if and only if they give rise to the same elements of $\mathscr{F}(k)$.*

Proof. Clear from the diagram

$$\begin{tikzcd}
\mathscr{F}(K) \arrow[r] \arrow[d] & M(K) \arrow[d] \\
\mathscr{F}(k) \arrow[r] & M(k)
\end{tikzcd}$$

where the arrow on the right is an injection and the bottom arrow is an isomorphism. □

Corollary 2.6. *Let N and p be coprime. Let (E, φ) and (E', φ') be two elliptic curves over $\mathbf{F}_{p^2}$ provided with an N-isogeny. Then these couples give rise to the same $\mathbf{F}_{p^2}$-point of $Y_0(N)$ if and only if they become isomorphic over $\overline{\mathbf{F}}_{p^2}$.*

Lemma 2.7 (Eichler-Deuring).

$$\sum_{\substack{E|\overline{\mathbf{F}}_{p^2} \\ \text{supersingular}}} \frac{1}{|\mathrm{Aut}(E)|} = \frac{p-1}{24}.$$

Proof. See [Sil92]. □

Lemma 2.8. *Let l and p be two distinct primes, and let E be an elliptic curve over $\mathbf{F}_{p^2}$. Then E admits at least $\frac{2}{\mathrm{Aut}(E)}(l+1)$ isogenies up to $\overline{\mathbf{F}}_{p^2}$-isomorphism.*

Proof. The $l+1$ l-isogenies (E, φ_G) that we get from subgroups G of order l of $E[l]$ are by definition isomorphic if and only if the corresponding groups can be transformed into each other by an automorphism; $[-1]$ fixes these subgroups. □

Note that the quotients associated to these isogenies can be isomorphic without the isogenies themselves being isomorphic (consider supersingular curves and take l large enough).

Given an curve C over $\mathbf{F}_q$, we denote by Frob_q^C its Frobenius endomorphism.

Lemma 2.9. *Let $E_0|\mathbf{F}_q$ be an elliptic curve, and let α be an automorphism of E_0 defined over $\mathbf{F}_q$. Then there exists an elliptic curve E_ξ over $\mathbf{F}_q$ and an $\overline{\mathbf{F}}_q$-isomorphism f from E_ξ to E_0 that transforms* $\mathrm{Frob}_q^{E_0}\,\alpha$ *into* $\mathrm{Frob}_q^{E_1}$.

Proof. We know (see [Sil92]) that the elliptic twists of E_0 correspond to the elements of the cohomology group $H^1(G_{\mathbf{F}_{p^2}}, \mathrm{Aut}(E_0))$. We can construct a cocycle ξ sending the inverse of the Frobenius σ of $\mathbf{F}_{p^2}$ to α. Indeed, this follows from the fact that α is defined over $\mathbf{F}_{p^2}$: denoting by n the order of α, the element $\sigma^{-i} \mapsto \alpha^i$ of $H^1(\mathrm{Gal}(\mathbf{F}_{p^{2n}}|\mathbf{F}_{p^2}), \mathrm{Aut}(E_0))$ is well-defined, and we just inflate this. (Note that since $G_{\mathbf{F}_{p^2}}$ is procyclic, this cocycle is also uniquely determined.) So there will exist a twist E_ξ with an isomorphism f to E_0 for which $f^{\sigma^{-1}} f^{-1} = \alpha$. But this certainly implies that under the isomorphism f, the composition $\mathrm{Frob}_{p^2}^{E_0}\,\alpha$ on E_0 is transformed into the Frobenius on E_ξ: $\mathrm{Frob}_{p^2}^{E_0}\,\alpha f = \mathrm{Frob}_{p^2}^{E_0} f^{\sigma^{-1}} = f\,\mathrm{Frob}_{p^2}^{E_\xi}$! □

Now we can finally prove the following

Theorem 2.10 (Ihara-Vlăduţ). *Let $(l, p) = 1$. Then*

$$X_0(l)(\mathbf{F}_{p^2}) \geq \frac{(p-1)(l+1)}{12}.$$

Sketch of Proof. Consider the pairs $(E|\varphi)$ over $\overline{\mathbf{F}}_{p^2}$, with E be supersingular and $\varphi : E \to E'$ an l-isogeny. Note that E' is again supersingular. Using 2.8 and 2.7, we see that there are at least $(p-1)(l+1)/12$ of these pairs are distinct over $\overline{\mathbf{F}}_{p^2}$, hence by 2.6 they give rise to $(p-1)(l+1)/12$ distinct $\overline{\mathbf{F}}_{p^2}$-points.

If we can show that these pairs (E, φ) are actually defined over $\mathbf{F}_{p^2}$, then we are done: by coarse representability, the points constructed above then already show up over $\mathbf{F}_{p^2}$. Now E and E' are certainly defined over $\mathbf{F}_{p^2}$: this is a standard result on supersingularity (see [Sil92]). Choose forms E_0 and E_0' of E and E', and let σ be the Frobenius of $\mathbf{F}_{p^2}$. We want $\varphi^\sigma = \varphi$, for which it suffices to show

$$\varphi\,\mathrm{Frob}_{p^2}^{E_0} = \mathrm{Frob}_{p^2}^{E_0'}\,\varphi. \tag{4}$$

It is again a standard result that for any supersingular E, $\mathrm{Frob}_{p^2}^{E} = \alpha[p] = [p]\alpha$ for some $\mathbf{F}_{p^2}$-automorphism α of E. Therefore, by twisting as in 2.9, we may assume that both Frobenii are $[p]$, and then (4) obviously holds. □

In fact, we have shown that for a supersingular curve E over $\mathbf{F}_q$, every subgroup of E of order l is rational over $\mathbf{F}_q$ on some twist of E.

We now have our reverse inequality:

Corollary 2.11. *Let $q = p^2$ be a square of a prime, and consider the curves C defined over $\mathbf{F}_q$. Then*

$$A(q) = \limsup_{C|\mathbf{F}_q} \frac{\mathrm{dev}(C)}{g(C)} = \limsup_{C|\mathbf{F}_q} \frac{\#C(\mathbf{F}_q)}{g(C)} = q^{1/2} - 1.$$

Proof. Follows by considering the $X_0(l)$ for l a prime unequal to p, and combining the previous result with the fact that these curves have genus asymptotic to $\lfloor l/12 \rfloor$. This asymptotic is well-known in the complex case, and also follows in our case because of good reduction. Indeed, in complete generality, the Euler-Poincaré characteristic does not change under reduction, and in the case of good reduction, first of all the h^0 do not change, hence nor do the h^1, which, again by good reduction, measure the genus.

Incidentally, [TVZ82] claim equality instead of this asymptotic, but this is incorrect. □

As mentioned in an earlier talk, this also means that modular curves, with their abundance of rational points, lead to Goppa codes that are "good" in some technical sense. Note, though, that explicitly constructing an infinite family of modular curves is a rather daunting task.

References

[Edi97] S.J. Edixhoven, *The modular curves $X_0(N)$*, Lecture notes, available at `http://www.math.leidenuniv.nl/~edix/public_html_rennes/cours/trieste.html`, 1997.

[Ser85] J.-P. Serre, *Rational Points on Curves over Finite Fields*, Lectures at Harvard University, notes by Fernando Q. Gouvéa, 1985.

[Sil92] J.H. Silverman, *The Arithmetic of Elliptic Curves*, Springer Verlag, 1992.

[TVZ82] M.A. Tsfasman, S.G. Vlăduţ, and Th. Zink, *Modular curves, Shimura curves, and Goppa codes, better than Varshamov-Gilbert bound*, Mathematische Nachrichten **109** (1982), 21–28.

[VD83] S.G. Vlăduţ and V.G. Drinfel'd, *The number of points of an algebraic curve*, Functional Analysis and Applications **17** (1983), no. 1, 53–54.