On the number of points of some varieties over finite fields

Marc PERRET

Abstract

We prove that the number of $\mathbf{F}_q$-rational points of an irreducible projective smooth 3-dimentional geometrically unirational variety defined over the finite field $\mathbf{F}_q$ with q elements is congruent to 1 modulo q. Some Fermat 3-folds, some classes of rationally connected 3-folds and some weighted projective d-folds having also this property are given.

Mathematics Subject Classification 14G15, 14J30, 14G05.

Introduction

Let $\mathbf{F}_q$ be the finite field with q elements. We study the effect of the geometry of certain algebraic varieties defined over $\mathbf{F}_q$ on their number of rational points. As proved by Lachaud and the author, this number of points, taken modulo q, depends only on the birational class of the variety if it is smooth, irreductible and projective of dimension 3 :

Theorem (Lachaud, Perret, [12]). *Let X and Y be projective smooth irreducible 3-dimensional varieties, birationally equivalent over $\mathbf{F}_q$. Then*

$$\sharp X(\mathbf{F}_q) \equiv \sharp Y(\mathbf{F}_q) \ (mod\ q).$$

In particular, a rational smooth projective variety of dimension 3 have only one rational point over $\mathbf{F}_q$ modulo q, hence also over $\mathbf{F}_{q^n}$ modulo q^n for any n. It is natural to ask whether this condition characterize rational varieties. It turns out that this is not the case, as showed by the following theorem.

Definition. A variety X defined over $\mathbf{F}_q$ satisfies the *congruence property over* $\mathbf{F}_q$ if

$$\sharp X(\mathbf{F}_{q^n}) \equiv\ 1\ mod\ q^n, \forall n \in \mathbf{N}^*.$$

Theorem 1. *Let X be a projective smooth irreducible 3-dimensional and geometrically unirationnal variety defined over $\mathbf{F}_q$. Suppose that the characteristic p of X is greater than 5. Then X satisfies the congruence property over $\mathbf{F}_q$.*

This is a refinement of a result of N. Katz, who proved in [6] (exposé XXI, page 5) the same congruence, but only modulo the prime divisor p of q^n. His congruence, however, holds for a broader class of varieties, which he called *special.* They are proper varieties X of dimension n, for which the Frobenius is a nilpotent operator on the last coherent cohomology space $H^n(X, \mathcal{O}_X)$. Unirational varieties are of course special, but also supersingular elliptic curves for instance. Note that Katz' congruence cannot hold modulo q, since this is false for supersingular curves for $q = p^2$.

The second theorem is a generalisation of Chevalley-Warning (see [5] and [19]) and Ax-Katz (see [3] and [9]) theorems in the weighted setting. We will deduce from it in the fourth section many irrational (not necessary smooth) varieties, of any dimension, satisfying the congruence property. We denote by $\lceil x \rceil$ the least integer greater than x.

Theorem 2. *Let $\mathbf{F}_q[X_1, \ldots, X_n]$ be the polynomial ring graded by $\deg X_i = a_i \geq 1$. Let $F_1, \ldots, F_r$ be polynomials of weighted degrees $d_1, \ldots, d_r$. Suppose that each indeterminate appears in at least one of the F_i's. Then the number $N(F_1 = 0, \ldots, F_r = 0)$ of zeroes in $\mathbf{F}_q^n$ of the system of equations $F_1 = 0, \ldots, F_r = 0$ is congruent to 0 modulo q^μ, where*

$$\mu = \left\lceil \frac{\sum_{j=1}^n a_j - \sum_{i=1}^r d_i}{max_{1 \leq i \leq r} d_i} \right\rceil.$$

As a first corollary, we will obtain in section 3 :

Corollary 1. *Let $a_0, \ldots, a_n$ be positive integers, $\mathbf{P}^n_{\mathbf{F}_q}(a_0, \ldots, a_n)$ the associated weighted projective space, and X be the subvariety defined by r homogeneous polynomials $F_1, \ldots, F_r$ of weighted degrees $d_1, \ldots, d_r$. Suppose that X doesn't lie in a coordinates hyperplane $\mathbf{P}^{n-1}_{\mathbf{F}_q}(a_0, \ldots \hat{a}_i, \ldots, a_n)$. Let*

$$\mu = \left\lceil \frac{\sum_{j=0}^n a_j - \sum_{i=1}^r d_i}{max_{1 \leq i \leq r} d_i} \right\rceil.$$

If $\mu \geq 1$, then

$$\sharp X(\mathbf{F}_q) \equiv \ 1 + q + \ldots + q^{\mu - 1} \ (mod \ q^\mu).$$

Moreover, it follows immediatelly from theorem 2, together with a lemma of Moreno and Moreno in [13], that

Corollary 2. *Let $\mathbf{F}_q[X_1, \ldots, X_n]$ be the polynomial ring with n indeterminates graded by $\deg X_i = a_i \geq 1$. Let $F_1, \ldots, F_r$ be polynomials of weighted degrees $d_1, \ldots, d_r$, and suppose that each indeterminate appears in at least one of the F_i's. If $q = p^f$, then the number $N(F_1 = 0, \ldots, F_r = 0)$ of zeroes in $\mathbf{F}_q^n$ of the system $F_1 = 0, \ldots, F_r = 0$ is congruent to zero modulo p^μ, where*

$$\mu = \left\lceil f \frac{\sum_{j=1}^n a_j - \sum_{i=1}^r \sigma_p(d_i)}{max_{1 \leq i \leq r} \sigma_p(d_i)} \right\rceil,$$

and where $\sigma_p(d)$ denotes the p-weight of the integer d.

The present paper is organized has follow. We prove theorem 1 in the first section, and theorem 2 in the second one. The third section is devoted to some properties of subvarieties of weighted projective spaces over finite fields. We deduce corollary 1 from these in this section, and some examples of varieties having the congruence property in the fourth one. We end by a question in section 5.

The author is gratefull to François Gramain for his help for lemma 1, and to Jean-Pierre Serre for an enlightening letter.

1. Proof of theorem 1

Since the projective space $\mathbf{P}^3_{\mathbf{F}_q}$ has the congruence property over $\mathbf{F}_q$, theorem 1 follows from lemma 2 bellow. Recall that a *Weil number* of modulus q^α, for an half-natural number α, is an algebraic integer of modulus q^α, as well as all its conjugates. Denote by φ_q the *q-th* Frobenius automorphism of $\overline{\mathbf{F}}_q$. The extension of a variety V from $\mathbf{F}_q$ to $\overline{\mathbf{F}}_q$ is denoted by $\overline{V}$.

Lemma 1. *Let V be an irreducible smooth projective d-dimensional variety defined over $\mathbf{F}_q$. Then the following conditions are equivalent :*

($\imath$) $V \times_{\mathbf{F}_q} \mathbf{F}_{q^{n_0}}$ satisfies the congruence property over $\mathbf{F}_{q^{n_0}}$ for some integer $n_0 \geq 1$.

($\imath\imath$) V satisfies the congruence property over $\mathbf{F}_q$.

($\imath\imath\imath$) The first betti number of V vanishes, and for $2 \leq i \leq 2d$, the eigenvalues of the Frobenius on $H^i_{\acute{e}t}(\overline{V}, \mathbf{Q}_\ell)$ are of the form q-times a Weil number of modulus $q^{\frac{i}{2}-1}$.

Proof of lemma 1. ($\imath\imath\imath$) implies ($\imath\imath$) thanks to Grothendieck formula giving the number of rational points of V over $\mathbf{F}_q$. Suppose that ($\imath$) holds. By Grothendieck formula and Poincaré duality,

$$\begin{aligned}\sharp V(\mathbf{F}_{q^{n_0 n}}) = 1 &+ q^{dn_0 n} \\ &- (1+q^{(d-1)n_0 n}) \sum_{k=1}^{b_1(V)} \alpha_{1,k}^{n_0 n} \\ &+ (1+q^{(d-2)n_0 n}) \sum_{k=1}^{b_2(V)} \alpha_{2,k}^{n_0 n} \\ &+ \dots \\ &+ (-1)^d \sum_{k=1}^{b_d(V)} \alpha_{d,k}^{n_0 n}\end{aligned}$$

for some Weil numbers of modulus $\mid \alpha_{i,k} \mid = q^{\frac{i}{2}}$ thanks to Deligne. Define

$$u_n = -\sum_{k=1}^{b_1(V)} \left(\frac{\alpha_{1,k}}{q}\right)^{n_0 n} + \sum_{k=1}^{b_2(V)} \left(\frac{\alpha_{2,k}}{q}\right)^{n_0 n} + \dots + (-1)^d \sum_{k=1}^{b_d(V)} \left(\frac{\alpha_{d,k}}{q}\right)^{n_0 n}.$$

This is by hypothesis a rational integer. Since each $\frac{\alpha_{i,k}}{q}$ is an algebraic number, there exists a linear induction relation

$$u_{n+s} = r_1 u_{n+s-1} + \cdots + r_s u_n$$

satisfied by $u_n \in \mathbf{Z}$ with rational coefficients, with minimal length s. But $\mathbf{Z}$ is Fatou, which means that each coefficient r_i lies in fact in $\mathbf{Z}$. Indeed, let $P(X) = u_0 + u_1 X + \ldots + u_{s-1}X^{s-1} \in \mathbf{Z}[X]$ and $Q(X) = 1 - r_1 X - \ldots - r_s X^s \in \mathbf{Q}[X]$. One can suppose that the $u_n, n \in \mathbf{N}$, are coprimes. The induction relation writes $\frac{P(X)}{Q(X)} = \sum_{n=0}^{\infty} u_n X^n \in \mathbf{Z}[[X]]$. Let $F(X)$ be this formal serie. By minimality, P and Q are coprime in $\mathbf{Q}[X]$. Denote by $c(R)$ the content of a formal serie R in $\mathbf{Z}[[X]]$ if it exists. Let $Q(X) = \frac{\widetilde{Q}(X)}{d}$ for a certain $d \in \mathbf{N}^*$ and a certain primitive polynomial $\widetilde{Q}(X) \in \mathbf{Z}[X]$. We have $\widetilde{Q}(X)F = dP$, hence by Gauss lemma d divides $c(F) = 1$, that is $Q = \widetilde{Q}(X) \in \mathbf{Z}[X]$, so that $r_1, \ldots, r_s \in \mathbf{Z}$.

Hence, $\frac{\alpha_{i,k}^{n_0}}{q^{n_0}}$ is an algebraic integer, so that $\frac{\alpha_{i,k}}{q}$ is also an algebraic integer. In particular, $b_1 = 0$, and each eigenvalue of the Frobenius of V on $H^i_{\acute{e}t}(\overline{V}, \mathbf{Q}_\ell)$ is of the form $q\zeta$, for an algebraic integer ζ of modulus $q^{\frac{i}{2}-1}$ for $i \geq 2$, and lemma 1 is proved.

Note that the above proof of the Fatou property of $\mathbf{Z}$ may be well known, and is given only for completness.

Lemma 2 (Heredity lemma). *Let X and Y be two irreducible projective smooth 3-dimensional variety defined over $\mathbf{F}_q$. Suppose that the characteristic p isn't equal to $2, 3$ and 5, that there exists a dominant rational map*

$$\psi : \overline{Y} - \cdots \to \overline{X}$$

defined over $\overline{\mathbf{F}}_q$, and that Y satisfies the congruence property over $\mathbf{F}_q$. Then X satisfies also the congruence property over $\mathbf{F}_q$.

Proof of lemma 2. Let Γ_ψ be the closure of the graph of ψ in $\overline{Y} \times \overline{X}$. This is a projective variety, which can be desingularized over $\overline{\mathbf{F}}_q$ as a *smooth projective* variety $\overline{Z}$ by Abhyankar theorem thanks to the restriction on the characteristic. We obtain a *regular* lifting of ψ from a *smooth projective* variety $\overline{Z}$ geometrically birational to $\overline{Y}$

$$\begin{tikzcd}
\overline{Z} \arrow[d] \arrow[dr] & \\
\overline{Y} \arrow[r, dashed] & \overline{X}.
\end{tikzcd}$$

These varieties and map are defined over a common finite extension $\mathbf{F}_{q^{n_0}}$ of $\mathbf{F}_q$. By Lachaud and the author's theorem stated in the introduction, we deduce that

$$\sharp Z(\mathbf{F}_{q^{n_0 n}}) \equiv \sharp Y(\mathbf{F}_{q^{n_0 n}}) \equiv \ 1 \ mod \ q^{n_0 n}$$

for any n. From lemma 1, we have $b_1(Z) = 0$, and the eigenvalues of the Frobenius of Z on $H^i_{\acute{e}t}(\overline{Z}, \mathbf{Q}_\ell)$ are of the form $q^{n_0}\zeta$ for some Weil numbers ζ of modulus $q^{n_0(\frac{i}{2}-1)}$. But the regular surjective morphism from Z to $X \times_{\mathbf{F}_q} \mathbf{F}_{q^{n_0}}$ induces some injective linear maps from $H^i_{ét}(\overline{X}, \mathbf{Q}_\ell)$ to $H^i_{ét}(\overline{Z}, \mathbf{Q}_\ell)$ for all $i \geq 0$ by [11], proposition 1.2.4. Hence, the eigenvalues of the Frobenius on $X \times_{\mathbf{F}_q} \mathbf{F}_{q^{n_0}}$ have the same shape than Z ones, so that those of X writes also q-times a Weil number of modulus $q^{\frac{i}{2}-1}$. Lemma 2 follows from Grothendieck formula giving the number of $\mathbf{F}_q$-rational points of X.

2. Proof of theorem 2

We will adapt D. Wan's proof of Katz theorem given in [18]. It is also possible to adapt Adolphson and Sperber proof of Katz theorem, using Newton polyedrons (see [1]).
First of all, we recall (and modify slightly) Wan's notations. If

$$W(i) = \Big\{ w(i) = (w_1(i), \ldots, w_n(i)) \in \mathbf{N}^n \mid weight(w(i)) := a_1 w_1(i) + \ldots a_n w_n(i) \leq d_i \Big\},$$

then one can write $F_i(X) = \sum_{w(i) \in W(i)} a(w(i)) X^{w(i)}$ for some $a(w(i)) \in \mathbf{F}_q$. Let T be the Teichmüller set of representatives of $\mathbf{F}_q$ in the unramified extension K of $\mathbf{Q}_p$ whose residue field is $\mathbf{F}_q$. Let ζ be a primitive p-th root of unity in $\overline{\mathbf{Q}}_p$. By Lagrange interpolation theorem, there is an unique polynomial

$$C(U) = \sum_{m=0}^{q-1} c(m) U^m \in K(\zeta)[U],$$

such that $C(t) = \zeta^{Tr_{\mathbf{F}_q/\mathbf{F}_p}(t)}$ for any $t \in T$.

Lemma 3 (Ax). *We have*

$$c(m) \equiv \ 0 \ mod \ (1-\zeta)^{\sigma(m)}$$

for any $0 \leq m \leq q-1$, where $\sigma(m)$ is the p-weight of m.

Proof of lemma 3. This is relation (4) in [3]. It follows from Stickelberger theorem.

Let M be the set of functions $m = (m_1, \ldots, m_r)$ from $W(1) \times \ldots \times W(r)$ to $\{0, \ldots, q-1\}^r$. For $m \in M$, let

$$e(m) = \sum_{i=1}^{r} \sum_{w(i) \in W(i)} m_i(w(i)) \ w(i) \in \mathbf{N}^n,$$

and

$$e(m)' = (e'_1, \ldots, e'_r) \in \mathbf{N}^r, \qquad e'_i = \sum_{w(i) \in W(i)} m_i(w(i)).$$

Lemma 4 (Ax-Wan).

$$q^r N(F_1 = 0, \dots, F_r = 0) = \sum_{m \in M} \left\{ \prod_{i=1}^{r} \prod_{w(i) \in W(i)} A(w(i))^{m_i(w(i))} \right\} \times \left\{ \prod_{i=1}^{r} \prod_{w(i) \in W(i)} C(m_i(w(i))) \right\} \times \left\{ \Big(\sum_{t \in T^n} t^{e(m)} \Big) . \Big(\sum_{t' \in T^r} (t')^{e'(m)} \Big) \right\},$$

where $A(w)$ is the Teichmüller representative of $a(w)$ in T.

Proof of lemma 4. This is relation (4) in [18]. The proof involves the existence of an additive character η from $\mathbf{F}_q$ with values in K.

Finally, consider for $m \in M$ the polynomial

$$P_m(U_1, \dots, U_n) = U^{e(m)} \in K[U_1, \dots, U_n],$$

weighted by $deg(U_i) = a_i$.

Lemma 5 (Ax-Wan). *Let $m \in M$.*

($\imath$) If $e(m)$ and $e(m)'$ are not both multiples of $q - 1$ in $\mathbf{N}^n$ and $\mathbf{N}^r$ respectively, then

$$\sum_{t \in T^n} t^{e(m)} . \sum_{t' \in T^r} (t')^{e'(m)} = 0.$$

($\imath\imath$) Suppose that $e(m)$ et $e'(m)$ are multiples of $q - 1$. Denote by $s_1 \in \{1, \dots, n\}$ the number of non-zero entries of $e(m)$, and by $s_2 \in \{1, \dots, r\}$ those of $e'(m)$. Then

$$\sum_{t \in T^n} t^{e(m)} . \sum_{t' \in T^r} (t')^{e'(m)} = (q-1)^{s_1 + s_2} q^{n + r - s_1 - s_2}.$$

For a proof of lemma 5, see [18], page 5.

We are now ready to prove theorem 2. From lemmas 4 and 5, the functions m whose contribution in the number $N(F_1 = 0, \dots, F_r = 0)$ are non-trivial are those for which $e(m)$ and $e'(m)$ are both multiples of $q - 1$ by integer-valued vectors. Let m be such a function. Let $j_1, \dots, j_{s_1}$ be the indexes for which $e_j \neq 0$, and $i_1, \dots, i_{s_2}$ those for which $e'_i \neq 0$. A look at the degree in $U = (U_1, \dots, U_n)$ of P_m gives, thanks to the graduation :

$$\begin{aligned}
a_{j_1}(q-1)+\ldots+a_{j_s}(q-1) &\leq weight(e(m))\\
&= \sum_{i=1}^{r} \sum_{w(i)\in W(i)} m_i(w(i)).poids(w(i))\\
&\leq \sum_{i=1}^{r} d_i \sum_{w(i)\in W(i)} m_i(w(i))\\
&\leq \sum_{i=1}^{r} d_i e'_i.
\end{aligned}$$

If $D(i_1,\ldots,i_{s_2})$ is the *maximum* of $d_{i_1},\ldots,d_{i_{s_2}}$, we have, since each e'_{i_k} is a non-zero multiple of $q-1$:

$$\begin{aligned}
a_{j_1}(q-1)+\ldots+a_{j_{s_1}}(q-1) &\leq \sum_{k=1}^{s_2} d_{i_k} e'_{i_k}\\
&= D(i_1,\ldots,i_{s_2})\sum_{k=1}^{s_2} e'_{i_k} - \sum_{k=1}^{s_2}(D(i_1,\ldots,i_{s_2})-d_{i_k})e'_{i_k}\\
&\leq D(i_1,\ldots,i_{s_2})\sum_{k=1}^{s_2} e'_{i_k} - (q-1)\sum_{k=1}^{s_2}(D(i_1,\ldots,i_{s_2})-d_{i_k}).
\end{aligned}$$

Hence

$$\begin{aligned}
(q-1)\left\lceil \frac{\sum_{k=1}^{s_1} a_{j_k} + s_2 D(i_1,\ldots,i_{s_2}) - \sum_{k=1}^{s_2} d_{i_k}}{D(i_1,\ldots,i_{s_2})}\right\rceil &\leq \sum_{k=1}^{s_2} e'_{i_k}\\
&= \sum_{k=1}^{s_2} \sum_{w(i_k)\in W(i_k)} m_{i_k}(w(i_k)).
\end{aligned}$$

We can deduce from this, exactly in the same way than in [3] (or than in [18]) that if $q=p^f$, then

$$f(q-1)\left\lceil \frac{\sum_{k=1}^{s_1} a_{j_k} + s_2 D(i_1,\ldots,i_{s_2}) - \sum_{k=1}^{s_2} d_{i_k}}{D(i_1,\ldots,i_{s_2})}\right\rceil \leq \sum_{i=1}^{r} \sum_{w(i)\in W(i)} \sigma(m_i(w(i))).$$

Together with lemmas 3, 4 and 5, we deduce that q^h divides $q^r N(F_1=0,\ldots,F_r=0)$ when h is the minimum, for all $1\leq s_1\leq n$ and $1\leq s_2\leq r$, and also for all $1\leq j_1<\ldots<j_{s_1}\leq n$ and all $1\leq i_1<\ldots<i_{s_2}\leq r$, of the quantities

$$\left\lceil \frac{\sum_{k=1}^{s_1} a_{j_k} + s_2 D(i_1,\ldots,i_{s_2}) - \sum_{k=1}^{s_2} d_{i_k}}{D(i_1,\ldots,i_{s_2})}\right\rceil + n + r - s_1.$$

Now, if $d(i_1,\ldots,i_{s_2})$ is the *minimum* of $d_{i_1},\ldots,d_{i_{s_2}}$, we have

$$\frac{\sum_{k=1}^{s_1} a_{j_k} + a_{j_{s_1+1}} - \sum_{k=1}^{s_2} d_{i_k}}{D(i_1,\ldots,i_{s_2})} \leq \frac{\sum_{k=1}^{s_1} a_{j_k} - \sum_{k=1}^{s_2} d_{i_k}}{D(i_1,\ldots,i_{s_2})} + \frac{a_{j_{s_1+1}}}{d(i_1,\ldots,i_{s_2})},$$

so that on the first hand,

$$\left\lceil \frac{\sum_{k=1}^{s_1} a_{j_k} - \sum_{k=1}^{s_2} d_{i_k}}{D(i_1,\ldots,i_{s_2})} \right\rceil - s_1 \geq \left\lceil \frac{\sum_{k=1}^{s_1} a_{j_k} + a_{j_{s_1+1}} - \sum_{k=1}^{s_2} d_{i_k}}{D(i_1,\ldots,i_{s_2})} \right\rceil - (s_1+1) - \left(\left\lceil \frac{a_{j_{s_1+1}}}{d(i_1,\ldots,i_{s_2})} \right\rceil - 1 \right).$$

On the other hand,

$$\left\lceil \frac{\sum_{j=1}^{n} a_j - \sum_{k=1}^{s_2} d_{i_k}}{D(i_1,\ldots,i_{s_2})} \right\rceil \geq \left\lceil \frac{\sum_{j=1}^{n} a_j - \sum_{k=1}^{s_2} d_{i_k} - d_{i_{s_2+1}}}{D(i_1,\ldots,i_{s_2},i_{s_2+1})} \right\rceil.$$

From both inequalities above, we deduce

$$h = \left\lceil \frac{\sum_{j=1}^{n} a_j - \sum_{i=1}^{r} d_i}{max_{1\leq i\leq r} d_i} \right\rceil - \sum_{j=1}^{n} \left(\left\lceil \frac{a_j}{min_{1\leq i\leq r} d_i} \right\rceil - 1 \right) + r.$$

Since each X_j appears in at least one of the F_i's by hypothesis, one has $a_j \leq min_{1\leq i\leq r} d_i$, so that the last sum vanishes. This completes the proof of theorem 3.

3. Weighted projective varieties over finite fields

Let $a_0,\ldots,a_n$ be non-negative integers. The *weighted projective space* $\mathbf{P}_k(a_0,\ldots,a_n)$ over a field k is the scheme *Proj* $k[X_0,\ldots,X_n]$ where the polynomial ring is graded by $\deg X_i = a_i$. This is the quotient of the standard $(n+1)$-dimensional affine space over k without its origin $\mathbf{A}_k^{n+1} - \{0,\ldots,0\}$ by the action of the multiplicative group $GL_k(1)$ given by

$$t.(x_0,\ldots,x_n) = (t^{a_0}x_0,\ldots,t^{a_n}x_n).$$

The orbit of the non-zero point $x = (x_0,\ldots,x_n) \in \mathbf{A}_k^{n+1}(\overline{k})$ is the rational curve $[x] = \{(t^{a_0}x_0,\ldots,t^{a_n}x_n) \mid t \in \overline{k}^*\} \subset \mathbf{A}_k^{n+1}$. See [7] or [8] for more details on weighted projective spaces.

Lemma 6. *Let* $[x] = [x_0 : \ldots : x_n] \in \mathbf{P} = \mathbf{P}_k(a_0,\ldots,a_n)$. *Then* $[x] \in \mathbf{P}(k)$ *if and only if* $[x_0 : \ldots : x_n] \cap k^{n+1} \neq \emptyset$.

Proof of lemma 6. This follows from Hilbert 90-theorem as in the standard case.

Now, we come to weighted projective spaces over finite fields.

Lemma 7. *Let $[x]$ be a rational class over $\mathbf{F}_q$. There are exactely $q-1$ distinct representatives of $[x]$ in $\mathbf{F}_q^{n+1} - \{0,\dots,0\}$.*

Proof of lemma 7. We can suppose that $x = (x_0,\dots,x_n) \in \mathbf{F}_q^{n+1}$ is a rational representative of $[x]$. We can also suppose that $x_0, x_1, \dots$ and x_r do not vanish, and that $x_{r+1} = \dots = x_n = 0$. It suffice to prove that

$$\{t \in \overline{\mathbf{F}}_q^* \mid (t^{a_0}x_0,\dots,t^{a_r}x_r) \in \mathbf{F}_q^{r+1}\} = \mathbf{F}_q^*.$$

Suppose first that $a_0,\dots,a_r$ are coprimes. Let $u_0,\dots,u_r$ be some Bezout coefficients : $u_0a_0 + \dots + u_ra_r = 1$. If $t.(x_0,\dots,x_r) \in \mathbf{F}_q^{r+1}$, that is if $t^{a_i} \in \mathbf{F}_q^*$ for all $0 \le i \le r$, then $t = (t^{a_0})^{u_0}\dots(t^{a_r})^{u_r} \in \mathbf{F}_q^*$. Conversely, the left hand set possess no less than $q-1$ distincts elements, since the relation $t_1.(x_0,\dots,x_r) = t_2.(x_0,\dots,x_r)$ implies

$$t_1 = (t_1^{a_0})^{u_0}\dots(t_1^{a_r})^{u_r} = (t_2^{a_0})^{u_0}\dots(t_2^{a_r})^{u_r} = t_2.$$

Now, if $gcd(a_0,\dots,a_r) = d \ge 2$, define $b_i = a_i/d \in \mathbf{N}^*$. the change of variable $u = t^d$ implies

$$\{(t^{a_0}x_0,\dots,t^{a_r}x_r); t \in \overline{\mathbf{F}}_q^*\} = \{(u^{b_0}x_0,\dots,u^{b_r}x_r); u \in \overline{\mathbf{F}}_q^*\},$$

and lemma 7 is proved.

Proof of corollary 1. Denote by X_{aff} the locus of zeroes of $F_1,\dots,F_r$ in the standard affine space $\mathbf{A}^{n+1}_{\mathbf{F}_q}$. From theorem 3, we have $\sharp X_{aff}(\mathbf{F}_q) \equiv 0$ $(mod\ q^\mu)$, and by lemma 7

$$\begin{aligned}\sharp X(\mathbf{F}_q) &= \frac{\sharp X_{aff}(\mathbf{F}_q) - 1}{q-1} \\ &\equiv (0-1)(-1-q-\dots-q^{\mu-1}) \quad (mod\ q^\mu) \\ &\equiv 1+q+\dots+q^{\mu-1} \quad (mod\ q^\mu).\end{aligned}$$

Note that a similar argument than in lemma 1 would prove the following :

Corollary 3. *In the situation of corollary 1, if X is quasismooth, we have :*

($\imath$) $b_{2i+1}(X) = 0$ if $2i+1 \le \mu - 1$.
($\imath\imath$) $b_{2i}(X) = 1$ if $2i \le \mu - 1$.
($\imath\imath\imath$) The eigenvalues of the Frobenius on $H^i_{\acute{e}t}(\overline{X}, \mathbf{Q}_\ell)$ are of the form q^μ-times a Weil number of modulus $q^{\frac{i}{2}-\mu}$ if $i \ge \mu$.

4. Some varieties having the congruence property

1) Conic bundles. A *conic bundle with base S over k* is a complete smooth irreducible variety X over a field k of characteristic $\ne 2$, together with a rational fibering $\pi : X \to S$ over a smooth base S defined over k, and whose fibres are isomorphic to rational curves. A conic bundle is *standard* if π is a flat regular map, and if $PicX = \pi^*(PicS) \oplus \mathbf{Z}K_X$

where K_X is the canonical class of X. Two conic bundles $\pi : X \to S$ and $\pi' : X' \to S'$ are *equivalents* if there exist birational maps $f : X \cdots \to X'$ and $g : S \cdots \to S'$ such that an obvious diagram is commutative. The reader will find more details on conic bundles in [4] or [14].

Proposition 1 *Let X be a $\mathbf{F}_q - 3$-dimensional geometric conic bundle with unirational base. Then X satisfies the congruence property over $\mathbf{F}_q$.*

Proof. By hypothesis, $\overline{X}$ is a conic bundle with unirational base $\overline{S}$ over $\overline{\mathbf{F}}_q$. By a theorem of Zagorskii (see [22]), it is birational to a standard conic bundle over a finite extension $\mathbf{F}_{q^{n_0}}$ of $\mathbf{F}_q$. Thank's to Lachaud and the author's theorem, we may assume that X is itself standard. Now, let $C \subset S$ be the *degenerate curve* (see [14]). This is the reduced curve such that the fiber X_x of a point $x \in S$ is a non-degenerate conic if $x \notin C$, a reduced degenerate conic if x is in the regular locus of C, and a double line if x is a singular point of C. If V is any subvariety of S, define for any n the sets

$$V(\mathbf{F}_{q^{n_0 n}})_1 = \{x \in V(\mathbf{F}_{q^{n_0 n}}) \mid X_x(\mathbf{F}_{q^{n_0 n}}) \neq \emptyset\},$$

$$V(\mathbf{F}_{q^{n_0 n}})_0 = \{x \in V(\mathbf{F}_{q^{n_0 n}}) \mid X_x(\mathbf{F}_{q^{n_0 n}}) = \emptyset\}.$$

As is well known (this is the simplest version of Chevalley-Warning theorem), a quadratic form in 3 variables over a finite field have always at least one non-trivial zero, so that $(S - C)(\mathbf{F}_{q^{n_0 n}})_0$ is empty. $C_{sing}(\mathbf{F}_{q^{n_0 n}})_0$ is also empty since $ax^2 = 0$ has always $q^{n_0 n} + 1$ zeroes over $\mathbf{F}_{q^{n_0 n}}$. Hence,

$$\begin{aligned}
\sharp X(\mathbf{F}_{q^{n_0 n}}) &= (q^{n_0 n} + 1)(\sharp S(\mathbf{F}_{q^{n_0 n}}) - \sharp C(\mathbf{F}_{q^{n_0 n}})) \\
&\quad + (2q^{n_0 n} + 1)\sharp C_{reg}(\mathbf{F}_{q^{n_0 n}})_1 + 1 \times \sharp C_{reg}(\mathbf{F}_{q^{n_0 n}})_0 \\
&\quad + (q^{n_0 n} + 1)\sharp C_{sing}(\mathbf{F}_{q^{n_0 n}}) \\
&\equiv \sharp S(\mathbf{F}_{q^{n_0 n}}) - \sharp C(\mathbf{F}_{q^{n_0 n}}) + \sharp C_{reg}(\mathbf{F}_{q^{n_0 n}})_1 + \sharp C_{reg}(\mathbf{F}_{q^{n_0 n}})_0 + \sharp C_{sing}(\mathbf{F}_{q^{n_0 n}}) \\
&= \sharp S(\mathbf{F}_{q^{n_0 n}}) \ (mod\ q^{n_0 n}).
\end{aligned}$$

But S is an unirational smooth proper surface, hence by the analogue of theorem 1 for surfaces (whose proof is similar), its number of points satisfies $\sharp S(\mathbf{F}_q^{n_0 n}) \equiv 1$ modulo $q^{n_0 n}$ (see the introduction of [12] for details). Theorem 1 in case ($\imath\imath$) follows from lemma 1.

2) Fano varietes

Proposition 2. *A smooth projective* 3*-dimensional variety defined over* $\mathbf{F}_q$*, geometrically birational to a smooth Fano variety with Picard number* 1*, satisfies the congruence property over* $\mathbf{F}_q$*.*

Proof. A look at Shepherd-Barron classification of such Fano 3-folds in positive characteristic (see [15]) shows that these varieties are unirational, except perhaps the quartic hypersurfaces in $\mathbf{P}^4$ and the double covers of the projective space $\mathbf{P}^3_{\overline{\mathbf{F}}_p}$, branched along a smooth sextic. If $S(x,y,z,t)=0$ is the equation of this sextic, then an equation of the double cover is given by

$$S(x,y,z,t)=u^2$$

in the weighted projective space $\mathbf{P}(1,1,1,1,3)$. Proposition 2 follows from corollary 1 since $6=\deg(S-u^2)<1+1+1+1+3=7$. The quartic case follows immediatelly from the classical Ax theorem ([3]), which is neither than theorem 2 for the standard graduation.

3) Fermat 3-folds

Proposition 3. *Let $F_m : x^m+y^m+z^m+t^m+u^m=0$ be the Fermat 3-fold of degree $m\geq 5$ over $\mathbf{Z}$. If p is a prime number, prime to m, let $F_m(p)$ be the Fermat variety over $\mathbf{F}_p$. Each condition implies the following one :*

($\imath$) $p^\alpha\equiv -1$ mod m for some $\alpha\in\mathbf{N}$.
($\imath\imath$) $F_m(p)$ is geometrically unirational.
($\imath\imath\imath$) $F_m(p)$ satisfies the congruence property over $\mathbf{F}_p$.

Suppose moreover that $m\leq 12$, or that m is a Fermat prime number. Then ($\imath\imath\imath$) implies ($\imath$).

Of course, it is expected that ($\imath\imath\imath$) implies ($\imath$) for all m.

Proof. ($\imath\imath$) implies ($\imath\imath\imath$) is nothing but theorem 1. We prove that ($\imath$) implies ($\imath\imath$) : if $q=p^\alpha$, it suffices to prove that $F_{q+1}(p)$ is unirational. The following is a slight modification of Shioda's proof that Fermat surfaces are unirational under the same condition given in [16]. Changing y, t and u respectivelly by $\zeta_{q+1}y$, $\zeta_{q+1}t$ and $\zeta_{q+1}u$, where ζ_{q+1} is a primitive $q+1$-th root of -1 in $\overline{\mathbf{F}}_p$, enables us to write the equation over $\overline{\mathbf{F}}_p$ of $F_{q+1}(p)$ as

$$x^{q+1}-y^{q+1}+z^{q+1}-t^{q+1}=u^{q+1}.$$

Let $X=x+y, Y=x-y, Z=z+t$ and $T=z-t$. Then, in affine coordinates with $T=1$, and with $a^q=Y$:

$$(Xa+Z)q=u^{q+1}-Z-Xa^{q^2}.$$

Let $b=Xa+Z$ and $c=-Xa^{q^2}-Z+u^{q+1}$, we obtain

$$b^q=c.$$

Now, if $k=\overline{\mathbf{F}}_p$, we have

$$k(F_{q+1}(p))=k(X,Y,Z,u)\subset k(X,a,Z,u)=k(a,b,c,u)=k(a,b,u),$$

which proves that $F_{q+1}(p)$ is geometricaly unirational.

Finally, we prove that ($\imath\imath\imath$) implies ($\imath$) at least for small values of m.

Lemma 8. *let $m \geq 5$ be an integer, and p a prime number, $p \equiv 1$ mod m. Then $F_m(p)$ doesn't satisfy the congruence property.*

Proof of lemma 8. The eigenvalues of the Frobenius endomorphism on $H^3_{\acute{e}t}(\overline{F_m(p)}, \mathbf{Q}_\ell)$ are the Jacobi sums $j(a_0, a_1, a_2, a_3, a_4)$ for $0 \neq a_i \in \mathbf{Z}/m\mathbf{Z}$ and $a_0 + \cdots + a_4 = 0$ (see [20]). But the prime decomposition of the principal ideal generated by these sums in the integer ring $\mathcal{O}$ of the m-th cyclotomic field is given by Stickelberger theorem (see [21]). Now, if $p \equiv 1 \bmod m$, then p splits completely in $\mathcal{O}$. Let $\mathcal{P}$ be a prime of $\mathcal{O}$ lying above p. A direct application of Stickelberger theorem for tha particular 5-tuple $(1, 1, 1, 1, m-4)$ shows that $v_{\mathcal{P}}(j(1, 1, 1, 1, m-4)) = 0$. Hence, $\frac{j(1,1,1,1,m-4)}{p}$ is not an algebraic integer, and by lemma 1 the Fermat variety $F_m(p)$ cannot satisfies the congruence property.

Suppose now for instance that m is a Fermat prime number. Let p be a prime, prime to m, and suppose that -1 is not a power of p modulo m. Then $p \equiv 1 \bmod m$, and by lemma 8 $(\imath\imath\imath)$ cannot hold.

5. A question

It is a remarkable fact for a variety over a finite field to satisfy the congruence property. This property is certainly the reflect of some geometrical property of the variety. It may be natural to ask :

Question 1. *Let X projective smooth irreducible simply connected variety defined over $\mathbf{F}_q$ satisfying the congruence property. Is it true that X is geometrically unirational ?*

Of course, if the answer turns to be negative, then the question would become : is there any geometrical property of a variety, from which the congruence property for the number of rational points is the reflect ? For instance, is it true that X is rationally connected ? Note that by theorem 1 the converse of question 1 is true in dimension (less than) 3. This converse is also true in any dimension by the same proof under the embeded resolution property of varieties over algebraically closed fields of positive characteristic (see [12]). Note also that the congruence property for the number of rational points over any finite extensions possess in common with unirationality the heredity property (see lemma 2). Moreover, from lemma 9 bellow, this question in the case of surfaces is equivalent, under a conjecture of Tate, to a conjecture of Shioda. Finally, the answer is positive for some Fermat 3-folds by proposition 3.

Before stating Shioda's conjecture, recall that a smooth projective irreducible surface in finite characteristic is *supersingular* if its Neron-Severi group generates ℓ-adically its second étale cohomology group $H^2_{\acute{e}t}(\overline{X}, \mathbf{Q}_\ell)$.

Conjecture (Shioda [17]). *Let X be a simply connected projective smooth irreducible surface defined over $\overline{\mathbf{F}}_q$. Suppose that X is supersingular. Then X is unirational.*

This was also conjectured by M. Artin for $K3$ surfaces in [2]. This conjecture is proved by Shioda himself for Kummer surfaces, and for Fermat surfaces by Katzura and Shioda in [10]. The equivalence of this conjecture and question 1 for surfaces follows from the following lemma, which says that (under Tate's conjecture) the congruence property is a generalization in highter dimension of the supersingular property for surfaces.

Lemma 9. *Let X be a smooth projective irreducible simply connected surface defined over $\mathbf{F}_q$. Suppose that Tate's conjecture of algebraicity of invariant cohomology classes is true. Then X is supersingular if, and only if, $\sharp X(\mathbf{F}_{q^n}) \equiv 1$ (mod q^n) for any $n \geq 1$.*

Proof. Since the Neron-Severi group is finitely generated, a generating familly is defined over a finite extension $\mathbf{F}_{q^{n_0}}$ of $\mathbf{F}_q$. Hence, the direct side of the lemma follows from Grothendieck formula and lemma 1. Conversely, if X satisfies the congruence relation, then the Frobenius linear map on $H^2_{\acute{e}t}(\overline{X}, \mathbf{Q}_\ell)$ equals q times the identity by lemma 1, hence X is supersingular by Tate's conjecture.

Thanks to theorem 1, an affirmative answer to question 1 would imply an affirmative one to the following questions :

Question 2. *Is it true that any 3-dimensional smooth conic bundle with smooth unirational base is unirational in finite characteristic ?*

Question 3. *Is it true that any 3-dimensional smooth Fano variety with Picard number 1 is unirational in finite characteristic ?*

Bibliography.

[1] A. Adolphson and S. Sperber, p-adic estimates for exponential sums and the theorem of Chevalley-Warning, *Ann. Sci. Ec. Norm. Sup.* **20** (1987), 545-556.

[2] M. Artin, Supersingular $K3$ surfaces, *Ann. Sci. Ec. Norm. Sup.* **7** (1974), 543-568.

[3] J. Ax, Zeroes of polynomials over finite fields, *Amer. Journ. Math.* **86** (1964), 255-261.

[4] A. Beauville, Variétés de Prym et Jacobiennes intermédiaires, *Ann. Sci. Ec. Norm. Sup.* **10** (1977), 309-391.

[5] C. Chevalley, Démonstration d'une hypothèse de E. Artin, *Abh. Math. Sem. Univ. Hamburg* **11** (1936), 73-75.

[6] P. Deligne and N. M. Katz, Groupe de monodromie en géométrie algébrique II, SGA 7, *Lecture Notes in Maths* **340** (1973), Springer-Verlag, Heidelberg.

[7] I. Dolgachev, Weighted projective spaces, in the proceedings "Group actions and vectorfields", *Lecture Notes in Maths* **956**, Springer-Verlag, 34-71.

[8] A. R. Iano-Fletcher, Working with weighted complete intersections, in *Explicit birational geometry of 3-folds*, (Corti and Reid editors), London Math. Soc. Lecture Notes Series **281** (2000), 101-173.

[9] N. M. Katz, On a theorem of Ax, *Amer. Journ. Math.* **93** (1971), 485-499.

[10] T. Katzura and T. Shioda, On Fermat varieties *Tôhoku Journ. of Maths.* **31** (1979), 97-115.

[11] S. L. Kleiman, Algebraic cycles and the Weil conjectures, in *10 exposés sur la cohomologie des Shémas*, North Holland, Amsterdam (1968).

[12] G. Lachaud et M. Perret, Un invariant birationnel des variétés de dimension 3 sur les corps finis, *Journ. of Alg. Geom.* **9** (2000), 451-458.

[13] O. Moreno et C. J. Moreno, Improvement of the Chevalley-Warning and the Ax-Katz theorems, *Amer. Journ. Math.* **117** (1995), 241-244.

[14] V. G. Sarkisov, Birational automorphisms of conic bundles, *Izv. Acad. Nauk. USSR* **44** (1980), 177-202.

[15] N. I. Shepherd-Barron, Fano threefolds in positive characteristic, *Compositio Math.* **105** (1997), 237-265.

[16] T. Shioda, Example of unirational surfaces in characteristic p, *Math. Ann.* **211** (1974), 233-236.

[17] T. Shioda, Some results on unirationality of algebraic surfaces, *Math. Ann.* **230** (1977), 153-168.

[18] Daquing Wan, An elementary proof of a theorem of Katz, *Amer. Journ. Math.* **111** (1989), 1-8.

[19] E. Warning, Bermerkung zur vorstehenden Arbeit von Herrn Chevalley, *Abh. Math. Sem. Univ. Hamburg* **11** (1936), 76-83.

[20] A. Weil, Number of solutions of equations in finite fields, *Bull. Amer. Math. Soc.* **55** (1949), 497-508.

[21] A. Weil, Jacobi sums as “Grossencharactere”, *Trans. Amer. Math. Soc.* **73** (1952), 487-495.

[22] A. A. Zagorskii, Three-dimensional conic bundles, *Math. Zametki* **21** (1977), 745-758; English translation in Math. Notes **21** (1977).

Marc PERRET
Unité de Mathématiques Pures et Appliquées
UMR 5669
École Normale Supérieure de Lyon
46 Allée d'Italie
69 363 Lyon Cedex 7
FRANCE
perret@umpa.ens-lyon.fr