Divisibility properties of the number of $\mathbf{F}_p$-points of schemes defined over $\mathbf{Z}$

Lucile Devin

Université Paris-Sud – Université Paris-Saclay

AGC^{2}T, June 22, 2017

$N_X(p)$?

X set of solutions of the equation $f(x_1, \dots, x_n) = 0$ with $f \in \mathbf{Z}[X_1, \dots, X_n]$
more generally $X/\mathbf{Z}$: scheme of finite type.

For $p \in \mathcal{P}$, $N_X(p)$: number of solutions of $f(x_1, \dots, x_n) \equiv 0 \text{ [mod } p]$ in $\mathbf{F}_p^n$.
Precisely $N_X(p) := |(X \times_{\mathbf{Z}} \mathbf{F}_p)(\mathbf{F}_p)|$.

What do we know about $N_X(p)$?

$N_X(p)$?

X set of solutions of the equation $f(x_1, \ldots, x_n) = 0$ with $f \in \mathbf{Z}[X_1, \ldots, X_n]$
more generally $X/\mathbf{Z}$: scheme of finite type.

For $p \in \mathcal{P}$, $N_X(p)$: number of solutions of $f(x_1, \ldots, x_n) \equiv 0$ [mod p] in $\mathbf{F}_p^n$.
Precisely $N_X(p) := |(X \times_{\mathbf{Z}} \mathbf{F}_p)(\mathbf{F}_p)|$.

What do we know about $N_X(p)$?

$N_X(p)$?

X set of solutions of the equation $f(x_1, \dots, x_n) = 0$ with $f \in \mathbf{Z}[X_1, \dots, X_n]$ more generally $X/\mathbf{Z}$: scheme of finite type.

For $p \in \mathcal{P}$, $N_X(p)$: number of solutions of $f(x_1, \dots, x_n) \equiv 0 \; [\text{mod } p]$ in $\mathbf{F}_p^n$. Precisely $N_X(p) := |(X \times_{\mathbf{Z}} \mathbf{F}_p)(\mathbf{F}_p)|$.

What do we know about $N_X(p)$?

$N_X(p)$?

- Size (Lang–Weil): $N_X(p) \asymp p^d$.

- Grothendieck–Lefschetz trace formula: for $\ell \neq p$ two prime numbers, one has

$$N_X(p) = \sum_i (-1)^i \operatorname{tr}(\mathrm{Frob}_p \mid H_c^i(X \times_{\mathbf{Z}} \overline{\mathbf{F}}_p, \mathbf{Q}_\ell)).$$

- Case of projective irreducible curves: $N_C(p) = p - a_p(C) + 1$.

$N_X(p)$?

- Size (Lang–Weil): $N_X(p) \asymp p^d$.
- Grothendieck–Lefschetz trace formula: for $\ell \neq p$ two prime numbers, one has

$$N_X(p) = \sum_i (-1)^i \operatorname{tr}(\mathrm{Frob}_p \mid H^i_c(X \times_{\mathbf{Z}} \overline{\mathbf{F}}_p, \mathbf{Q}_\ell)).$$

- Case of projective irreducible curves: $N_C(p) = p - a_p(C) + 1$.

$N_X(p)$?

- Size (Lang–Weil): $N_X(p) \asymp p^d$.

- Grothendieck–Lefschetz trace formula: for $\ell \neq p$ two prime numbers, one has

$$N_X(p) = \sum_i (-1)^i \operatorname{tr}(\mathrm{Frob}_p \mid H^i_c(X \times_{\mathbf{Z}} \overline{\mathbf{F}}_p, \mathbf{Q}_\ell)).$$

- Case of projective irreducible curves: $N_C(p) = p - a_p(C) + 1$.

Case of elliptic curves

Theorem (Sato–Tate)

Let E be an elliptic curve over $\mathbf{Q}$ without CM, One can write

$$N_E(p) = p - 2\sqrt{p}\cos(\theta_p) + 1,$$

with $\theta_p \in [0, \pi]$. For all $0 \leq \alpha < \beta \leq \pi$, one has

$$\mathrm{dens}(\{p \in \mathcal{P} : \alpha \leq \theta_p \leq \beta\}) = \frac{2}{\pi}\int_{\alpha}^{\beta} \sin^2(t)dt.$$

Fité–Kedlaya–Roger–Sutherland : genus 2.

Case of elliptic curves

Theorem (Sato–Tate)

Let E be an elliptic curve over $\mathbf{Q}$ without CM, One can write

$$N_E(p) = p - 2\sqrt{p}\cos(\theta_p) + 1,$$

with $\theta_p \in [0, \pi]$. For all $0 \leq \alpha < \beta \leq \pi$, one has

$$\mathrm{dens}(\{p \in \mathcal{P} : \alpha \leq \theta_p \leq \beta\}) = \frac{2}{\pi}\int_\alpha^\beta \sin^2(t)dt.$$

Fité–Kedlaya–Roger–Sutherland : genus 2.

Notion of density

For $A \subset \mathcal{P}$.

Definition (Natural density)

Define

$$\overline{\text{dens}}(A) = \limsup_{N\to\infty} \frac{\sum_{a\in A\cap[1,N]} 1}{\sum_{p\in\mathcal{P}\cap[1,N]} 1} \quad \text{and} \quad \underline{\text{dens}}(A) = \liminf_{N\to\infty} \frac{\sum_{a\in A\cap[1,N]} 1}{\sum_{p\in\mathcal{P}\cap[1,N]} 1}.$$

If $\overline{\text{dens}}(A) = \underline{\text{dens}}(A)$, we denote $\text{dens}(A)$ their common value.

A motivation for studying $N_X(p)$ [mod p]

Theorem (Fouvry–Katz, 2001)

Let $d, n, D \in \mathbf{N}_{\geq 1}$, let X be a closed affine subscheme in $\mathbb{A}^n_{\mathbf{Z}[1/D]}$, such that $X/\mathbf{C}$ is irreducible and smooth of dimension d. Suppose that the set $\{p, p \nmid N_X(p)\}$ is infinite.
Then for every function $f : X \to \mathbb{A}^1$ there exists a constant C, a closed subscheme $X_2 \subset \mathbb{A}^n_{\mathbf{Z}[1/D]}$, of relative dimension $\leq n-2$, such that for every $h \in \mathbb{A}^n_{\mathbf{Z}[1/D]}(\mathbf{F}_p) - X_2(\mathbf{F}_p)$, for every prime $p \nmid D$, for every non-trivial additive character ψ on $\mathbf{F}_p$, one has

$$\left| \sum_{x \in X(\mathbf{F}_p)} \psi(f(x) + h_1 x_1 + \ldots + h_n x_n) \right| \leq C p^{\frac{d}{2}}.$$

Schemes with non-zero A-number

- Katz: For $S : f(x,y,z) = 0 \subset \mathbb{A}^3$ smooth, one has $A(S) = \deg(f)(\deg(f)-1)^2 \neq 0$ if $\deg(f) > 1$.
- Katz: For $X : F(x_1,\ldots,x_n) = \alpha \subset \mathbb{A}^n_{\mathbf{Z}}$ smooth with $\alpha \neq 0$ and F weighted homogeneous polynomial, one has $A(X) \geq 2$.
- Fouvry–Katz: for $n \geq 3$, $d \geq 1$ odd numbers, $a_1,\ldots,a_n$ integers satisfying $(a_1,\ldots,a_n) = 1$,

$$\begin{cases} \prod_{i=1}^n x_i & = 1 \\ \sum_{i=1}^n a_i x_i^d & = 0 \end{cases} \subset \mathbb{A}^n_{\mathbf{Z}}$$

has a non-zero A-number.

Properties of $N_X(p)$ [mod m]

Theorem (Serre, 2012)

Let X be a scheme of finite type over $\mathbf{Z}$. Let a and m be integers with $m \geq 1$. The set $\{p \notin \Sigma_X : p \nmid m, N_X(p) \equiv a \text{ [mod } m]\}$ has a natural density which is a positive rational number if it is not empty.

One prime is enough

Theorem

Let X be a scheme of finite type over $\mathbf{Z}$. Assume that

1. *either the variety $X \times_{\mathbf{Z}} \mathbf{Q}$ is projective and smooth, satisfying $h^{0,m}(X) = 0$, for every $m \geq 3$;*
2. *or the variety $X \times_{\mathbf{Z}} \mathbf{Q}$ has dimension ≤ 3 and is birational to a variety satisfying (1).*

Then for every $a_1, \ldots, a_n \in \mathbf{Z}$, the set $\{p \notin \Sigma_X, p \nmid \prod_{i=1}^{n}(N_X(p) - a_i)\}$ is either empty or has a positive lower density.

Idea of proof – Case of an irreducible curve

- Lang–Weil: $0 < N_X(p) < 2p$.
- Suppose $\exists p_0 \notin \Sigma_X$, $p_0 \nmid N_X(p_0)$, Serre:
  $\{p \notin \Sigma_X : p \nmid N_X(p_0), N_X(p) \equiv 0 \ [\text{mod } N_X(p_0)]\}$ has positive density.
- If $N_X(p_0) \geq 2$, one has

$$\{p \notin \Sigma_X : p \nmid N_X(p_0), N_X(p) \equiv 0 \ [\text{mod } N_X(p_0)]\} \subset \{p \notin \Sigma_X : p \nmid N_X(p)\}.$$

Idea of proof – Case of an irreducible curve

- Lang–Weil: $0 < N_X(p) < 2p$.
- Suppose $\exists p_0 \notin \Sigma_X,\ p_0 \nmid N_X(p_0)$, Serre:
  $\{p \notin \Sigma_X : p \nmid N_X(p_0), N_X(p) \equiv 0 \ [\text{mod } N_X(p_0)]\}$ has positive density.
- If $N_X(p_0) \geq 2$, one has

$$\{p \notin \Sigma_X : p \nmid N_X(p_0), N_X(p) \equiv 0 \ [\text{mod } N_X(p_0)]\} \subset \{p \notin \Sigma_X : p \nmid N_X(p)\}.$$

Idea of proof – Case of an irreducible curve

- Lang–Weil: $0 < N_X(p) < 2p$.

- Suppose $\exists p_0 \notin \Sigma_X$, $p_0 \nmid N_X(p_0)$, Serre:
  $\{p \notin \Sigma_X : p \nmid N_X(p_0), N_X(p) \equiv 0 \,[\mathrm{mod}\ N_X(p_0)]\}$ has positive density.

- If $N_X(p_0) \geq 2$, one has

$$\{p \notin \Sigma_X : p \nmid N_X(p_0), N_X(p) \equiv 0 \,[\mathrm{mod}\ N_X(p_0)]\} \subset \{p \notin \Sigma_X : p \nmid N_X(p)\}.$$

Idea of proof – Smooth projective case

$$\left.\begin{array}{r}\text{Poincaré Duality : for } i > d,\ p \mid \mathrm{tr}(\mathrm{Frob}_p \mid H^i_c(\overline{X}_p, \ell)) \\ \text{Mazur–Ogus : if } h^{0,i}(X) = 0 \text{ then } p \mid \mathrm{tr}(\mathrm{Frob}_p \mid H^i_c(\overline{X}_p, \ell))\end{array}\right\} \text{Choose}$$

$$M_X(p) = \sum_{i=0}^{2} (-1)^i \,\mathrm{tr}(\mathrm{Frob}_p \mid H^i_c(\overline{X}_p, \ell)).$$

$$M_X(p) \equiv N_X(p) \text{ [mod } p].$$

Theorem (Generalization of Serre's theorem)

The set $\{p \notin \Sigma : p \nmid m, M_X(p) \equiv a \text{ [mod } m]\}$ has a natural density which is a positive rational number if it is not empty.

Idea of proof – Smooth projective case

$$\left.\begin{array}{r} \text{Poincaré Duality : for } i > d,\ p \mid \operatorname{tr}(\mathrm{Frob}_p \mid H^i_c(\overline{X}_p, \ell)) \\ \text{Mazur–Ogus : if } h^{0,i}(X) = 0 \text{ then } p \mid \operatorname{tr}(\mathrm{Frob}_p \mid H^i_c(\overline{X}_p, \ell)) \end{array}\right\} \text{Choose}$$

$$M_X(p) = \sum_{i=0}^{2} (-1)^i \operatorname{tr}(\mathrm{Frob}_p \mid H^i_c(\overline{X}_p, \ell)).$$

$$M_X(p) \equiv N_X(p) \ [\mathrm{mod}\ p].$$

Theorem (Generalization of Serre's theorem)

The set $\{p \notin \Sigma : p \nmid m, M_X(p) \equiv a \ [\mathrm{mod}\ m]\}$ has a natural density which is a positive rational number if it is not empty.

Idea of proof – Smooth projective case

$$\left.\begin{array}{r}\text{Poincaré Duality}: \text{ for } i > d,\ p \mid \operatorname{tr}(\mathrm{Frob}_p \mid H^i_c(\overline{X}_p, \ell)) \\ \text{Mazur–Ogus}: \text{ if } h^{0,i}(X) = 0 \text{ then } p \mid \operatorname{tr}(\mathrm{Frob}_p \mid H^i_c(\overline{X}_p, \ell))\end{array}\right\} \text{Choose}$$

$$M_X(p) = \sum_{i=0}^{2} (-1)^i \operatorname{tr}(\mathrm{Frob}_p \mid H^i_c(\overline{X}_p, \ell)).$$

$$M_X(p) \equiv N_X(p) \ [\mathrm{mod}\ p].$$

Theorem (Generalization of Serre's theorem)

The set $\{p \notin \Sigma : p \nmid m, M_X(p) \equiv a \ [\mathrm{mod}\ m]\}$ *has a natural density which is a positive rational number if it is not empty.*

Fouvry–Katz revisited

Theorem

Let $d \leq 3, n, D \in \mathbf{N}_{\geq 1}$, let X be a closed affine subscheme in $\mathbb{A}^n_{\mathbf{Z}[1/D]}$, such that $X/\mathbf{C}$ is irreducible and smooth of dimension d. If $d = 3$ assume that X is birational to a smooth projective scheme Y with $h^{0,3}(Y) = 0$.
Suppose that the set $\{p \notin \Sigma_X : p \nmid N_X(p)\}$ is non-empty.
Then for every function $f : X \to \mathbb{A}^1$ there exists a constant C, a closed subscheme $X_2 \subset \mathbb{A}^n_{\mathbf{Z}[1/D]}$, of relative dimension $\leq n-2$, such that for every $h \in \mathbb{A}^n_{\mathbf{Z}[1/D]}(\mathbf{F}_p) - X_2(\mathbf{F}_p)$, for every prime $p \nmid D$, for every non-trivial additive character ψ on $\mathbf{F}_p$, one has

$$\left| \sum_{x \in X(\mathbf{F}_p)} \psi(f(x) + h_1 x_1 + \ldots + h_n x_n) \right| \leq C p^{\frac{d}{2}}.$$

How large is this prime?

Find one prime $p_0 \nmid \prod_{i=1}^{n}(N_X(p_0) - a_i)$.

- $C_q : y^2 = x^q + 1$, q prime, $p \mid N_{C_q}(p) \Rightarrow p \equiv 1$ [mod q].
- cubic surfaces: $\forall p, p \mid N_X(p)$.
- Question on average in families of hyperelliptic curves.

How large is this prime?

Find one prime $p_0 \nmid \prod_{i=1}^{n}(N_X(p_0) - a_i)$.

- $C_q : y^2 = x^q + 1$, q prime, $p \mid N_{C_q}(p) \Rightarrow p \equiv 1$ [mod q].
- cubic surfaces: $\forall p, p \mid N_X(p)$.
- Question on average in families of hyperelliptic curves.

A first answer in a one parameter family

Theorem

Let $g \geq 2$ be an integer and let $f \in \mathbf{Z}[T]$ be a separable polynomial of degree $2g$. For each $u \in \mathbf{Z}$ we consider the curve C_u with affine model

$$C_u : y^2 = f(t)(t-u).$$

Let $T \geq 1$. There exists a constant K_g depending only on g such that for every $\alpha_1, \ldots, \alpha_n \in \mathbf{Z}$, for most $u \in \mathbf{Z} \cap [-T, T]$, the least prime p of good reduction for C_u and satisfying $p \nmid \prod_{i=1}^{n}(N_{C_u}(p) - \alpha_i)$ is at most of size

$$(2K_g \log(T))^{\gamma/2} \left(\log(2K_g \log(T))\right)^{\frac{\gamma}{2}\left(1-\frac{2}{\gamma+2n-2}\right)},$$

where one can take $\gamma = 4g^2 + 2g + 4$.

Idea of proof – double sieve method

- Sieve for Frobenius (Kowalski):

$$\underbrace{\left|\bigcup_{i=1}^{n}\{u \in \mathbf{F}_p, p \mid \prod_{i=1}^{n}(N_{C_u}(p) - \alpha_i)\}\right|}_{\nu(p)} \ll_g p^{1-2/\gamma}(\log p)^{1-2/(\gamma+2n-2)}.$$

- Larger sieve (Zywina's version):

$$|\{u \in \mathbf{Z} : |u| \leq T, p \mid \prod_{i=1}^{n}(N_{C_u}(p) - \alpha_i), \forall p < Q(T)\}|$$

$$\leq \frac{\sum_{p \leq Q(T)} \log p}{\sum_{p \leq Q(T)} \frac{\log p}{\nu(p)} - \log(2T^2)}$$

Idea of proof – double sieve method

- Sieve for Frobenius (Kowalski):

$$\underbrace{\left|\bigcup_{i=1}^{n}\{u \in \mathbf{F}_p, p \mid \prod_{i=1}^{n}(N_{C_u}(p) - \alpha_i)\}\right|}_{\nu(p)} \ll_g p^{1-2/\gamma}(\log p)^{1-2/(\gamma+2n-2)}.$$

- Larger sieve (Zywina's version):

$$|\{u \in \mathbf{Z} : |u| \leq T, p \mid \prod_{i=1}^{n}(N_{C_u}(p) - \alpha_i), \forall p < Q(T)\}|$$

$$\leq \frac{\sum_{p \leq Q(T)} \log p}{\sum_{p \leq Q(T)} \frac{\log p}{\nu(p)} - \log(2T^2)}$$

Idea of proof – double sieve method

- Sieve for Frobenius (Kowalski):

$$\underbrace{\left|\bigcup_{i=1}^{n}\{u \in \mathbf{F}_p, p \mid \prod_{i=1}^{n}(N_{C_u}(p) - \alpha_i)\}\right|}_{\nu(p)} \ll_g p^{1-2/\gamma}(\log p)^{1-2/(\gamma+2n-2)}.$$

- Larger sieve (Zywina's version):

$$|\{u \in \mathbf{Z} : |u| \leq T, p \mid \prod_{i=1}^{n}(N_{C_u}(p) - \alpha_i), \forall p < Q(T)\}|$$

$$\leq \frac{\sum_{p \leq Q(T)} \log p}{\sum_{p \leq Q(T)} \frac{\log p}{\nu(p)} - \log(2T^2)} \asymp \frac{Q(T)}{\log T}.$$

Conclusion

- C an irreducible curve of genus $g \geq 1$:
  $\underline{\text{dens}}\{p : p \nmid \prod_{i=1}^{n}(N_C(p) - a_i)\} > 0$.
- In families of hyperelliptic curves, the least element of this set is generically of size polylogarithmic in the parameter.
- In general, under some geometric conditions on X, it suffices to find one prime in the set to ensure
  $\underline{\text{dens}}\{p \notin \Sigma_X, p \nmid \prod_{i=1}^{n}(N_X(p) - a_i)\} > 0$.
- We can find new example of scheme X with non-zero A-number, provided that we know the set of bad reduction primes.

Thank you !