Lattice Pints in Small Boxes over Finite Fields

Mei-Chu Chang

University of California, Riverside

joint work with

J. Cilleruelo, M. Z. Garaev, J. Hernandez,

I. E. Shparlinski, A. Zumalacárregui

Bounding the number of solutions

$$(x_1, \ldots, x_n) \in \prod_{i=1}^{n} [R_i + 1, R_i + M]$$

$$\begin{cases} F_1(x_1, \ldots, x_n) = 0 \\ \\ \qquad \ldots \\ \\ F_m(x_1, \ldots, x_n) = 0 \end{cases}$$

Bombieri-Pila

$F(x,y) \in \mathbb{Z}[x,y], \ \deg F = d,$ **irreducible curve**

$$B = [R+1, R+M] \times [S+1, S+M]$$

$$|\{(x,y) \in B : F(x,y) = 0\}| < C_{d,\varepsilon} M^{1/d}$$

sharp: $y = x^d,$ **Marmo, Salberger-Wooley**

over $\mathbb{Z}$

Wooley

$$(\star)\begin{cases} x_1+\ldots+x_s=y_1+\ldots+y_s \\ x_1^2+\ldots+x_s^2=y_1^2+\ldots+y_s^2 \\ \qquad\qquad \ldots \qquad\qquad\qquad 1\le x_i,y_i\le M \\ x_1^d+\ldots+x_s^d=y_1^d+\ldots+y_s^d \end{cases}$$

If $d\ge 3, s\ge \kappa=d^2-1$**, then**

number of solutions $\ll M^{2s-d(d+1)/2+\varepsilon}$

Problem:

$F(x,y) \in \mathbb{F}_p[x,y]$ **irreducible,** $d = \deg F \geq 2$

$$B = [R+1, R+M] \times [S+1, S+M]$$

want to estimate numbers of zeros in B

two special cases we consider:

$$y \equiv f(x),$$

$$y^2 \equiv f(x)$$

Polynomial Map

$$f(x) \in \mathbb{F}_p[x], \quad d = \deg f \geq 2$$

$$B = [R+1, R+M] \times [S+1, S+M]$$

Want upper bound on

$$J = J_f(M; R, S) = |\{(x, y) \in B : y \equiv f(x)\}|$$

Cilleruelo-Garaev-Ostafe-Shparlinski

- $J \ll M \left(\frac{M}{p}\right)^{1/\,2(d^2-1)\,+\varepsilon} + M^{1-1/2(d+1)\,+\varepsilon}$
- **If** $M \leq p^{2/(d^2+3)}$**, then** $J \ll M^{1/d+\varepsilon}$

our result (uniform in f)

$y \equiv f(x), \quad B = [R+1, R+M] \times [S+1, S+M]$

Theorem 1. $d = deg f \geq 2$

$$J \ll \frac{M^2}{p} + M^{1-1/2^{d-1}} p^{\varepsilon}$$

over $\mathbb{F}_p$

$$f(x) \in \mathbb{F}_p[x], \quad d = \deg f \geq 2$$

$$B = [R+1, R+M] \times [S+1, S+M]$$

Want upper bound on

$$I = I_f(M; R, S) = |\{(x, y) \in B : y^2 \equiv f(x)\}|$$

trivial bound: $2M$
use Bombieri-Weil $I = \frac{M^2}{p} + O(p^{1/2}(\log p)^2)$

over $\mathbb{F}_p$; Bombieri-Weil

$$y^2 \equiv f(x), \quad B = [R+1, R+M] \times [S+1, S+M]$$

$$I < \begin{cases} 2M & \text{if } M < p^{1/2}(\log p)^2 \\ p^{1/2}(\log p)^2 & \text{if } p^{1/2}(\log p)^2 \le M < p^{3/4}\log p \\ \frac{M^2}{p} & \text{if } p^{3/4}\log p \le M \end{cases}$$

Cilleruelo-Garaev-Ostafe-Shparlinski
Cilleruelo-Shparlinski-Zumalacárregui

our result (uniform in f); more combinatorial (uses geometry of numbers)

$$y^2 \equiv f(x), \quad B = [R+1, R+M] \times [S+1, S+M]$$

Theorem 2. $deg f = 3$;

$$I < M^{1+\varepsilon} \begin{cases} M^{-2/3} & \text{if } M < p^{1/8} \\ \left(\frac{M^4}{p}\right)^{1/6} & \text{if } p^{1/8} \le M < p^{5/23} \\ \left(\frac{M^3}{p}\right)^{1/16} & \text{if } p^{5/23} \le M < p^{1/3} \end{cases}$$

our result (uniform in f)

$$y^2 \equiv f(x), \quad B = [R+1, R+M] \times [S+1, S+M]$$

Theorem 3. $d = deg f \geq 4$

$$I \leq M \left(\frac{M^3}{p} \right)^{1/2\kappa+\varepsilon} + M^{1-(d-3)/2\kappa+\varepsilon}$$

- **non-trivial, if** $M < p^{1/3-\varepsilon}$
- **no nontrivial result yet for** $p^{1/3} < M < p^{1/2}$

diameter of polynomial dynamical systems: application of Theorem 1

$$f \in \mathbb{F}_p[X],\ u_0 \in \mathbb{F}_p,\ u_n = f(u_{n-1}),\ n = 0, 1, \ldots$$

diameter $$D_{f,u_0}(N) = \max_{0 \le k,m \le N-1} |u_k - u_m|$$

our result (uniform in f)

$y \equiv f(x), \quad B = [R+1, R+M] \times [S+1, S+M]$

Theorem 1. $d = deg f \geq 2$

$$J \ll \frac{M^2}{p} + M^{1-1/2^{d-1}} p^{\varepsilon}$$

diameter of polynomial dynamical systems: application of Theorem 1

$$f \in \mathbb{F}_p[X],\ u_0 \in \mathbb{F}_p,\ u_n = f(u_{n-1}),\ n = 0, 1, \ldots$$

diameter $$D_{f,u_0}(N) = \max_{0 \le k,m \le N-1} |u_k - u_m|$$

Corollary 4. $d = deg f \ge 2,\ \ N \le T =$ period

$$D_{f,u_0}(N) \gg \min\{N^{1/2}p^{1/2}, N^{1+1/(2^{d-1}-1)}p^{-\varepsilon}\}$$

Gutierrez-Shparlinski $T_{f,u_0} \geq N \geq p^{1/2+\varepsilon}$

$$D_{f,u_0}(N) = p^{1-\varepsilon}$$

(C-) $\deg f = 2$

$$D_{f,u_0}(N) \gtrsim \min\left\{Np^{\,c_1}, \frac{1}{\log p} N^{\frac{4}{5}} p^{\frac{1}{5}}, N^{\,\frac{1}{13}} \log\log N\right\}$$

$$D_{f,u_0}(T) \gtrsim \min\left\{p^{\,5c_1}, e^{\,T/4}\right\}$$

- $H_{\mathbf{a}}: \; Y^2 = X^{2g+1} + a_{2g-1}X^{2g-1} + \ldots + a_1 X + a_0$

  where $\mathbf{a} = (a_0, \ldots, a_{2g-1}) \in \mathbb{F}_p^{2g}$

- $H_{\mathbf{a}}: \; Y^2 = X^{2g+1} + a_{2g-1}X^{2g-1} + \ldots + a_1 X + a_0$

  where $\mathbf{a} = (a_0, \ldots, a_{2g-1}) \in \mathbb{F}_p^{2g}$
- $H_{\mathbf{a}} \cong H_{\mathbf{b}} \iff \exists\, \alpha \in \mathbb{F}_p^*$ s.t.

  $a_i \equiv \alpha^{4g+2-2i} b_i \pmod{p}, \quad i = 0, \ldots, 2g-1$

hyperelliptic curve

- $H_{\mathbf{a}}: \; Y^2 = X^{2g+1} + a_{2g-1}X^{2g-1} + \ldots + a_1 X + a_0$

  where $\mathbf{a} = (a_0, \ldots, a_{2g-1}) \in \mathbb{F}_p^{2g}$

- $H_{\mathbf{a}} \cong H_{\mathbf{b}} \iff \exists\, \alpha \in \mathbb{F}_p^*$ s.t.

  $a_i \equiv \alpha^{4g+2-2i} b_i \pmod{p}, \quad i = 0, \ldots, 2g-1$

- $\mathfrak{B} = \prod_{i=0}^{2g-1} [R_i + 1, R_i + M]$

$$N(H; \mathfrak{B}) = |\{\mathbf{a} = (a_0, \ldots, a_{2g-1}) \in \mathfrak{B} : \; H_{\mathbf{a}} \cong H\}|$$

our result (uniform in f)

$y \equiv f(x), \quad B = [R+1, R+M] \times [S+1, S+M]$

Theorem 1. $d = deg f \geq 2$

$$J \ll \frac{M^2}{p} + M^{1-1/2^{d-1}} p^{\varepsilon}$$

application, any range

$y \equiv f(x), \quad B = [R+1, R+M] \times [S+1, S+M]$

Theorem 1. $d = deg f \geq 2$

$$J \ll \frac{M^2}{p} + M^{1-1/2^{d-1}} p^{\varepsilon}$$

Corollary 5.

$H =$ **hyperelliptic curve,** $g \geq 2$ **over** $\mathbb{F}_p$

$$N(H; \mathfrak{B}) = |\{\mathbf{a} = (a_0, \ldots, a_{2g-1}) \in \mathfrak{B} : \ H_{\mathbf{a}} \cong H\}|$$

$$N(H; \mathfrak{B}) \ll \frac{M^2}{p} + M^{1/2+\varepsilon}$$

Optimal, certain range

Theorem 6. $g \geq 1, \quad h \in [3, 2g+1]$

$$N(H;\mathfrak{B}) < \left(M^{1/h} + M \left(\frac{M^4}{p} \right)^{2/h(h+1)} \right) M^{\varepsilon}$$

- **If** $M < p^{1/(2g^2+2g+4)}$**, take** $h = 2g+1$**, then** $N(H;\mathfrak{B}) \leq M^{1/(2g+1)+\varepsilon}$

lower bound on isom classes

$$\mathfrak{B} = \prod_{i=0}^{2g-1} [R_i + 1, R_i + M]$$

$$H_{\mathbf{a}}: \; Y^2 = X^{2g+1} + a_{2g-1}X^{2g-1} + \ldots + a_1 X + a_0, \;\; \mathbf{a} \in \mathfrak{B}$$

Theorem 7. $g \geq 1$

$$|\{\textbf{isom classes } H_{\mathbf{a}} : \mathbf{a} \in \mathfrak{B}\}| \gg \min\{p^{2g-1}, M^{2g+\varepsilon}\}$$

- **If $g \geq 2$ the ε term can be removed when $M > p^{1/(2g)}$**

outline of proof $y^2 \equiv f(x), \quad B = [R+1, R+M] \times [S+1, S+M]$

Theorem 2. $\quad deg f = 3$

$$I < M^{1+\varepsilon} \begin{cases} M^{-2/3} & \text{if } M < p^{1/8} \\ \left(\frac{M^4}{p}\right)^{1/6} & \text{if } p^{1/8} \le M < p^{5/23} \\ \left(\frac{M^3}{p}\right)^{1/16} & \text{if } p^{5/23} \le M < p^{1/3} \end{cases}$$

Proof. Assume $p^{1/3-\varepsilon} > M > p^{5/23}$

$$(x, y) \mapsto (x - x_0, y - y_0)$$

$$(\star) \quad y^2 - c_0 y \equiv c_3 x^3 + c_2 x^2 + c_1 x, \quad |x|, |y| \le M$$

$(\star)\ \ y^2 - c_0 y \equiv c_3 x^3 + c_2 x^2 + c_1 x, \ \ |x|, |y| \le M$

$$\mathcal{E} = \{(x, y) \in [-M, M]^2 : (x, y) \text{ satisfies } (\star)\}$$

$$|\mathcal{E}| \sim |\pi_1(\mathcal{E})| := \rho M$$

$$\bar{S} = \left\{(x, x^2, x^3) : x \in \pi_1(\mathcal{E})\right\}, \ \ I_i = [-8M^i, 8M^i]$$

$$\mathcal{S} = 8\bar{S}$$

$$= \left\{\left(\sum_1^8 x_i, \sum_1^8 x_i^2, \sum_1^8 x_i^3\right) \in I_1 \times I_2 \times I_3 : x_i \in \pi_1(\mathcal{E})\right\}$$

$$N(s) = \sharp\left\{(x_1, \ldots, x_8) : x_i \in \pi_1(\mathcal{E}), s = \left(\sum_1^8 x_i, \sum_1^8 x_i^2, \sum_1^8 x_i^3\right)\right\}$$

$$\begin{aligned}|\pi_1(\mathcal{E})|^8 = \sum_{s\in\mathcal{S}} N(s) \leq & (|\mathcal{S}| \sum_{s\in\mathcal{S}} N(s)^2)^{1/2} \\ \leq & (|\mathcal{S}| \sum_{s\in\mathcal{S}} M^{10+\varepsilon})^{1/2}\end{aligned}$$

$$|\mathcal{S}| \geq \rho^{16} M^{6+\varepsilon}$$

$(\star)$ $y^2 - c_0 y \equiv c_3 x^3 + c_2 x^2 + c_1 x, \ \ |x|, |y| \le M; \quad I_i = [-8M^i, 8M^i]$

- at least $\rho^{16} M^{6+\varepsilon}$ triples $(z_1, z_2, z_3) \in I_1 \times I_2 \times I_3$ s.t.

$$c_3 z_3 + c_2 z_2 + c_1 z_1 \equiv \tilde{z}_2 - c_0 \tilde{z}_1 \pmod{p}, \quad \text{for some } \tilde{z}_i \in I_i$$

- lattice $\Gamma = \{(z_2, z_3, \tilde{z}_2, z_1, \tilde{z}_1) \in \mathbb{Z}^5 :$

$$c_3 z_3 + c_2 z_2 + c_1 z_1 + \tilde{z}_2 + c_0 \tilde{z}_1 \equiv 0 \pmod{p}\}$$

- body $D = \{(x_2, x_3, \tilde{x}_2, x_1, \tilde{x}_1) \in \mathbb{R}^5 :$

$$|x_1|, |\tilde{x}_1| \le 8M, |x_2|, |\tilde{x}_2| \le 8M^2, |x_3| \le 8M^3\}$$

$$\sharp(D \cap \Gamma) \geq \rho^{16} M^{6+\varepsilon}$$

by Mikowski, successive minima $\lambda_i = \lambda_i(D, \Gamma)$, $i = 1, \ldots, 5$, satisfy the inequality

$$\prod_{i=1}^{5} \min\{1, \lambda_i\} \ll \rho^{-16} M^{-6+\varepsilon}$$