Waring's Problem over finite fields

Todd Cochrane

Department of Mathematics
Kansas State University
Visitor, Georgia Institute of Technology

Waring's number $\pmod{p}$ defined

Let p be a prime, $\mathbb{F}_p = \mathbb{Z}/(p)$, and k a positive integer.

Definition. Waring's number $\gamma(k,p)$ is the smallest s such that for any integer a the congruence

$$x_1^k + x_2^k + \cdots + x_s^k \equiv a \pmod{p}$$

is solvable in integers x_i. (Note: $x_i = 0$ is allowed.)

- Plainly, $\gamma(k,p)$ exists and $\gamma(k,p) \leq p-1$, since 1 is a k-th power.

- We may assume $k|(p-1)$ since if $d = (k, p-1)$ then clearly $\gamma(d,p) = \gamma(k,p)$.

For any subsets S, T of $\mathbb{F}_p$ and $n \in \mathbb{N}$,

$$S + T := \{s + t : s \in S, t \in T\},$$
$$nS := S + S + \cdots + S, \quad \text{(n-times)}$$
$$\gamma(S, p) := \text{minimal } n \text{ such that } nS = \mathbb{F}_p.$$

For Waring's Number we have, $\gamma(k, p) = \gamma(A_0, p)$, where

$$A_0 = \{x^k : x \in \mathbb{F}_p\}.$$

Throughout, we let A denote the multiplicative group of nonzero k-th powers and $A_0 = A \cup \{0\}$.

Waring's Problem: Estimate $\gamma(k, p)$ and, when possible, evaluate it.

Methods:

I. Additive Combinatorics.

II. Finite Circle Method: Exponential Sums

III. Geometric Lattice Method.

$A = \{x^k : x \in \mathbb{F}_p^*\}, \quad A_0 = A \cup \{0\}.$

$$nA_0 = A\omega_1 \cup A\omega_2 \cdots \cup A\omega_\ell \cup \{0\}$$

If $nA_0 \neq \mathbb{F}_p$ then $|(n+1)A_0| \geq |nA_0| + |A|$, so

$$|nA_0| \geq \min\{p, n|A| + 1\} = \min\{p, n\tfrac{p-1}{k} + 1\}.$$

Theorem 1 (Cauchy's Bound (1813))

For any prime p and positive integer k,

$$\gamma(k, p) \leq k.$$

This bound is sharp if $|A| = 1$ or 2, that is, $k = p - 1$ or $(p-1)/2$. In these cases A_0 is an arithmetic progression, $\{0, 1\}$, $\{-1, 0, 1\}$, so nA_0 grows very slowly.

Lemma 2 (Cauchy-Davenport Inequality (1813), (1935))

For any subsets S, T of $\mathbb{F}_p$, we have

$$|S+T| \geq \min\{|S|+|T|-1, p\}.$$

Thus, for any subset S of $\mathbb{F}_p$,

$$|nS| \geq \min\{n(|S|-1)+1, p).$$

Theorem 3 (Generalized Cauchy Bound)

For any subset S of $\mathbb{F}_p$ with $|S|>1$,

$$\gamma(S,p) \leq \left\lceil \frac{p-1}{|S|-1} \right\rceil.$$

Such a bound is best possible if S is an arithmetic progression.

Note: For the case of the k-th powers, $|A_0| = \frac{p-1}{k}+1$, so we recover $\gamma(k,p) \leq k$.

Theorem 4 (S. Chowla, Mann and Strauss (1959))

If A is the group of nonzero k-th powers and $|A| > 2$, then

$$\gamma(k, p) \leq \lfloor k/2 \rfloor + 1$$

Proof. For a multiplicative subgroup A we have in fact

$$|nA| \geq \min\{(2n-1)(|A|-1)+1, p\},$$

as a consequence of Vosper's Theorem and fact that A is not an arithmetic progression, in fact, it's a geometric progression.

Example 5

(i) For $k = 2$, $\gamma(2, p) = 2$ for all odd p.

(ii) For $k = 3$, $3|(p-1)$

$$\gamma(3,p) = \begin{cases} 2 & \text{for } |A| > 2, \quad \text{i.e. } p > 7 \quad (CMS) \\ 3 & \text{for } |A| = 1, 2, \quad \text{i.e. } p = 7 \end{cases}$$

(iii) For $k = 4$, $4|(p-1)$,

$$\gamma(4,p) \leq 3 \quad \text{for } |A| > 2, \quad \text{i.e. } p > 5 \quad (CMS)$$
$$\gamma(4,p) = 4 \quad \text{for } |A| = 1, 2, \quad \text{i.e. } p = 5$$

$G(k)$ = minimal s such that every sufficiently large positive integer is a sum of at most s positive k-th powers.

Lower Bounds: Maillet, Hurwitz, Hardy and Littlewood

$G(k) \geq k+1$ for any $k > 1$. (density argument)
$G(k) \geq 4k$ for $k = 2^n$, $n \geq 2$. (congruence constraint)

Upper Bounds:
Hardy and Littlewood (1922): $G(k) \leq (k-2)2^{k-1} + 5$ (circle-method)

Improvements: Hardy & Littlewood (1925), Vinogradov (1934-1959), K-C Tong (1957), J-R Chen (1958), Vaughan (1989)

Wooley (1992): $G(k) \leq k\,(\log k + \log\log k + O(1))$

In the classical problem the only known values of $G(k)$ are

$$G(2) = 4, \quad \text{Lagrange's Theorem (1770)}$$
$$G(4) = 16, \quad \text{Davenport (1939).}$$

$3 \leq G(3) \leq 7, \qquad 6 \leq G(5) \leq 17, \qquad$ etc.

For Waring's problem over $\mathbb{F}_p$, we'll see that

$$\gamma(k,p) = \begin{cases} 1 \text{ or } 2 & \text{for } p > k^4 \\ 1, 2 \text{ or } 3 & \text{for } p > k^3 \\ etc. \end{cases}$$

thus, if we fix a small value for k, eg. $k = 4, 5, ..,$ $\gamma(k,p)$ can be explicitly evaluated by testing small primes; see C. Small (1977), Moreno (2005) for tables of such values.

We've seen that for $|A| = 1, 2$, $\gamma(k,p) = k$, and that for $|A| > 2$, $\gamma(k,p) < \frac{k}{2} + 1$. Can we do better?

Example 6

Suppose that $S = \{0, 1, a\}$ with $a \approx \sqrt{p}$. Then for $n < \min\{a, p/a\}$, $|nS| = \binom{n+2}{2}$. Letting $n \approx \sqrt{p}$ we get $|[\sqrt{p}]S| > p/2$, and so $2[\sqrt{p}]S = \mathbb{F}_p$, that is,

$$\sqrt{2p} < \gamma(S,p) < 2\sqrt{p}, \quad \text{(roughly)}$$

Heilbronn Conjectures (1964):

I: For $|A| > 2$, $\gamma(k,p) \ll k^{1/2}$.

II: For any $\varepsilon > 0$, $\gamma(k,p) \ll_\epsilon k^\varepsilon$ for $|A| > c_\varepsilon$.

Let $A = \{x^k : x \in \mathbb{F}_p^*\}$.

Example 7

Suppose $|A| = 4$, say $A = \{\pm 1, \pm\alpha\}$ where $\alpha^2 \equiv -1 \pmod p$. To represent c as a minimal sum of k-th powers we need to solve

$$x + y\alpha \equiv c \pmod p \qquad (1)$$

with $|x| + |y|$ minimal. Let $\mathcal{L}$ be the lattice of integer points satisfying $x + y\alpha \equiv 0 \pmod p$. Inside any fundamental parallelogram for the lattice, (2) has a unique solution.

Note: Since $|A| = 4$, $4|(p-1)$ so $p = a^2 + b^2$ for some a, b, and $\{(a, b), (-b, a)\}$ is a basis for $\mathcal{L}$.

$|A| =$3,4 or 6, the cases where $\phi(|A|) = 2$

Let A be a multiplicative subgroup of $\mathbb{F}_p$.

Theorem 8 (Cipra, Pinner, C (2007))

a) Suppose $|A| = 4$ and a, b are the unique positive integers with $a > b$ and $a^2 + b^2 = p$. Then $\gamma(k,p) = a - 1$.

b) Suppose $|A| = 3$ or 6, and a, b are the unique positive integers with $a > b$ and $a^2 + b^2 + ab = p$. If $|A| = 3$, $\gamma(k,p) = a + b - 1$. If $|A| = 6$, $\gamma(k,p) = \left\lfloor \frac{2}{3}a + \frac{1}{3}b \right\rfloor$.

In particular, for $|A| = 3, 4, 6$, that is, $k = \frac{p-1}{3}, \frac{p-1}{4}, \frac{p-1}{6}$,

$$\sqrt{2k} - 1 \leq \gamma(k,p) \leq 2\sqrt{k},$$

More generally if $A = \{1, \alpha, \alpha^2, \dots, \alpha^{t-1}\}$, then we need to obtain a minimal solution of

$$\sum_{i=0}^{t-1} x_i \alpha^i \equiv a \pmod{p}.$$

Since α is a zero of the cyclotomic polynomial of degree $r := \phi(t)$ we work instead with a lattice in r-dim space defined by

$$x_0 + x_1\alpha + \cdots + x_{r-1}\alpha^{r-1} \equiv 0 \pmod{p}.$$

and make use of the cyclotomic polynomial to construct a basis of “small" solutions.

The lattice method leads to a small solution, but with the x_i positive or negative.

Plus-Minus Waring's Number: Let $\delta(k,p)$ be the smallest s such that

$$\pm x_1^k \pm x_2^k + \cdots \pm x_s^k \equiv a \pmod{p},$$

is solvable for all a.

The lattice method leads to a bound on $\delta(k,p)$. To estimate $\gamma(k,p)$ we use

Lemma 9 (Cipra, Pinner, C (2009))

For any group of k-th powers A in $\mathbb{F}_p^*$,
$\gamma(k,p) \leq \min\{|A|,\ 2\log(\log p)\}\delta(k,p)$.

Open Problem 1: Is there an absolute constant C such that $\gamma(k,p) < C\delta(k,p)$?

The geometric lattice method yields,

Theorem 10 (Heilbronn (1964), Bovey (1977))

Let A be a multiplicative subgroup of $\mathbb{F}_p$ with $|A| = t$. Then

$$\gamma(k, p) \le c(t) k^{1/\phi(t)}.$$

- The estimate is useful for $|A| < \log p$
- Bovey: $c(t) = t^2 (H_t + 1)^{\phi(t)} \log p$, where
  $H_t =$ Height of the t-th order cyclotomic polynomial.

What further is known about $c(t)$ in Heilbronn, Bovey Theorem?

$$\gamma(k,p) \le c(t)k^{1/\phi(t)}, \quad t := |A|$$

Theorem 11 (Pinner, C (2008))

For prime power t,

$$c(t) < 2\, t^3.$$

Proof. Geometric Lattice Method

Theorem 12 (Croot, C (2011))

For odd t, with $\phi(t) < (\log_3 t)^{1/3}$,

$$c(t) < t^4$$

Proof. Additive combinatorics.

Theorem 13 (Konyagin (1994), Cipra, Pinner, C (2007))

$c(t) \ll t^{2+\epsilon}$ *for* $t > \log p$.

Proof. Exponential sums

$$\gamma(k,p) \le c(t)k^{1/\phi(t)}, \quad t := |A|$$

Theorem 14 (Cipra, Pinner, C (2007))

For any t, $c(t) \gg \frac{1}{\sqrt{\log t}}$

Theorem 15 (Cipra (2008))

For prime t, $c(t) > t/3$.

Open Problem 2: What is the correct size for $c(t)$ for a general group of order $t < \log p$?

Heilbronn Conjectures (1964): $A =$ nonzero k-th powers
I: For $|A| > 2$, $\gamma(k,p) \ll k^{1/2}$.

II: For any $\varepsilon > 0$, $\gamma(k,p) \ll_\epsilon k^\varepsilon$ for $|A| > c_\varepsilon$.

In view of the cases $|A| = 3, 4, 6$ the exponent $1/2$ in the first conjecture is optimal.

- Conjecture II was proven by Konyagin (1992).

- Conjecture I was proven by Cipra, Pinner, C (2007).

Both proofs use a Heilbronn-Bovey type bound for small $|A|$ and exponential sums for large $|A|$.

Earlier progress: For $|A| > 2$,
I. Chowla (1943): $\gamma(k,p) \ll k^{.88}$
Dodson (1971): $\gamma(k,p) \ll k^{7/8}$
Dodson and Tietaväinen (1976): $\gamma(k,p) \leq 68(\log k)^2 k^{1/2}$

Let $e_p(x) = e^{2\pi i x/p}$. Gauss Sum: $\sum_{x=0}^{p-1} e_p(\lambda x^k)$. Define

$$\Phi_k := \max_{\lambda, p \nmid \lambda} \left| \sum_{x=0}^{p-1} e_p(\lambda x^k) \right| .$$

$$N := \#\{\mathbf{x} \in \mathbb{F}_p^s : x_1^k + \cdots + x_s^k = a\}.$$

$$N = \frac{1}{p} \sum_{\mathbf{x} \in \mathbb{F}_p^s} \sum_{\lambda=0}^{p-1} e_p(\lambda(x_1^k + \cdots + x_s^k - a))$$

$$= p^{s-1} + \frac{1}{p} \sum_{\lambda=1}^{p-1} e_p(-\lambda a) \left(\sum_{x=1}^{p} e_p(\lambda x^k) \right)^s .$$

$$\Rightarrow |N - p^{s-1}| < \Phi_k^s$$

We just want $N > 0$ for Waring's problem, that is, $p^{s-1} \geq \Phi_k^s$, $(s-1)\log p \geq s \log \Phi_k$, $s \geq \log p / \log(p/\Phi_k)$.

$$\Phi_k = \max_{\lambda, p\nmid\lambda} \left| \sum_{x=1}^{p} e_p(\lambda x^k) \right|.$$

Proposition 0.1 (Unknown origin)

$$\gamma(k,p) \leq \left\lceil \frac{\log p}{\log\left(p/\Phi_k\right)} \right\rceil.$$

In particular,

- If $\Phi_k \leq (1-\epsilon)p$ then $\gamma(k,p) \ll_\epsilon \log p$
- If $\Phi_k \leq p^{1-\epsilon}$ then $\gamma(k,p) \leq \lceil \frac{1}{\epsilon} \rceil$

Gauss Bound on Gauss Sum

Gauss bound: $\Phi_k \le (k-1)\sqrt{p}$,

$$|A| > p^{\lambda} > p^{1/2} \Rightarrow \gamma(k,p) \le \frac{1}{\lambda - \frac{1}{2}}$$

Example 16

Applying the Gauss bound we see that if $|A| > p^{3/4}$, then $\gamma(k,p) \le 4$. Equivalently, using $|A| = (p-1)/k$,

$$\gamma(k,p) \le 4 \quad \text{for } p > k^4.$$

This falls a little short of the estimate we stated earlier $\gamma(k,p) \le 2$ for $p > k^4$.

Konyagin's bound on Φ_k, useful for $\log p < |A| < p^\epsilon$

Theorem 17 (Konyagin (1994))

For $|A| > \log p/(\log\log p)^{1-\epsilon}$,

$$\Phi_k \leq p\left(1 - \frac{c_\epsilon}{(\log p)^{1+\epsilon}}\right),$$
$$\gamma(k,p) \leq c_\epsilon(\log p)^{2+\epsilon}$$

where $t = |A|$, $\phi(t)$ *is the Euler phi-function.*

Proof. Harmonic analysis, cyclotomic extensions, Dobrowolski's bound on Mahler Measure. Basically, show that the elements of A cannot be too clustered, so we get some cancellation in sum.

• Konyagin (1994): For any $C > 0$ there exist infinitely many A with $|A| > C\frac{\log p}{\log\log p}$ and $\gamma(k,p) \geq (\log p)^C$. Thus the theorem above is nearly best possible.

Conjecture: Konyagin (1994): For $|A| > \log p$, $\gamma(k,p) \ll \log p$.

EXAMPLE 18

Let $p = 2^t - 1$ be a Mersenne prime,
$A =< 2 >$, so that $|A| = t$.
For Waring's problem we wish to solve, for a given c,

$$x_0 + x_1 2 + x_2 2^2 + x_3 2^3 + \cdots + x_{t-1} 2^{t-1} \equiv c \pmod{p}$$

in nonnegative integers x_i. Any minimal representation of c must have all $x_i = 0$ or 1 and so

$$\gamma(k, p) = t - 1 \approx \log_2 p.$$

Thus we have a group A with $|A| \approx \log_2 p$ and $\gamma(k, p) \approx \log_2 p$.

Theorem 19 (Bourgain, Konyagin (2003))

If $|A| > p^\epsilon$ then

$$\Phi_k \ll p^{1-\delta}, \quad \text{for some } \delta = \delta(\epsilon),$$

Proof. Additive combinatorics/Harmonic Analysis including the the Balog, Szemeredi, Gower's Theorem (1994),(1998).

Theorem 20 (Bourgain (2009))

If $|A| > p^\epsilon$ then

$$\Phi_k \le p^{1-e^{-c/\epsilon}}$$

for some absolute constant c.

Corollary 21

There is an absolute constant C such that for $|A| > p^\epsilon$,

$$\gamma(k,p) \le C^{1/\epsilon},$$

Conjecture: Montgomery, Vaughan, Wooley (1995)

$$\Phi_k \ll \sqrt{kp\log(kp)}$$

Companion Conjecture: If A is the group of k-th powers with $|A| > \log p$, then

$$\gamma(k,p) \ll \frac{\log p}{\log(\frac{|A|}{\log p})}.$$

In particular, this would imply the Konyagin conjecture,

$$\gamma(k,p) \ll \log p \quad \text{for} \quad |A| \gg \log p,$$

and imply that

$$\gamma(k,p) \ll \frac{1}{\epsilon}, \quad \text{for } |A| > p^{\epsilon},$$

Note, the preceding example with the Mersenne prime and $A =< 2 >$, shows that the conjectured bound of MVW cannot be sharpened.

For $S \subset \mathbb{F}_p$ let

$$S \cdot S = \{xy : x, y \in S\}, \quad S + S = \{x + y : x, y \in S\}.$$

Theorem 22 (Bourgain and Konyagin (2003), Bourgain, Katz, Tao (2004))

For $\epsilon > 0$ there is a $\delta = \delta(\epsilon) > 0$ such that if $|S| < p^{1-\epsilon}$,

$$\max\{|S \cdot S|, |S + S|\} \geq |S|^{1+\delta}.$$

Improvements by Garaev (2008), Katz and Shen (2008), Shen (2008), Bourgain and Garaev (2009)

Theorem 23 (L. Li (2009))

For any subset S of $\mathbb{F}_p$,

$$\max\{|S \cdot S|, |S + S|\} \gg \begin{cases} |S|^{13/12}\left(1 + \frac{|S|}{\sqrt{p}}\right), & |S| < p^{35/68} \\ |S|\left(\frac{p}{|S|}\right)^{1/11}, & |S| > p^{35/68}. \end{cases}$$

Growth of $A + A$ for multiplicative group

For A, a multiplicative subgroup, $A \cdot A = A$, so we must have good growth in $A + A$.

Theorem 24 (Heath-Brown and Konyagin (2000), Bourgain and Konyagin (2003), Pinner,C (2009))

$$|A + A| > \min\{\frac{1}{4}|A|^{3/2}, p/2\}.$$

Proof. Stepanov method.

Theorem 25 (Shkredov (2010), Schoen and Shkredov (2010), Shkredov and Vyugin (2011))

$$|A + A| \gg |A|^{5/3}(\log |A|)^{-1/2}, \quad \textit{for} \quad |A| \ll \sqrt{p}.$$

Proof: Stepanov, Additive combinatorics, Harmonic Analysis

Definition: For any subset S let $S^2 = SS$

$$nS^2 = SS + SS + \cdots + SS. \quad (n - \mathit{times})$$

Theorem 26 (Bourgain (2005))

If $S \subset \mathbb{F}_p$ with $|S| > p^{3/4}$ then $3S^2 = \mathbb{F}_p$.

Theorem 27 (Pinner, C (2009))

For any subsets S, T of $\mathbb{F}_p$ and positive integer n,

$$|S||T|^{1-\frac{2}{n}} > p \quad \Rightarrow \quad nST = \mathbb{F}_p.$$

Proof. Use exponential sums to count the number N of solutions of the equation

$$x_1 y_1 + x_2 y_2 + \cdots + x_n y_n = a.$$

with $x_i \in S$, $y_i \in T$, $1 \leq i \leq n$, obtaining

$$\left| N - \frac{|S|^n |T|^n}{p} \right| < |S|^{\frac{n}{2}+1} |T|^{\frac{n}{2}} p^{\frac{n}{2}-1}.$$

The previous theorem requires $|S||T| > p^{1+\epsilon}$ to be effective.

Theorem 28 (Glibichuk (2006), Glibichuk and Konyagin (2007))

For any subsets S, T of $\mathbb{F}_p$ with $|S||T| \geq 2p$ we have $8ST = \mathbb{F}_p$.

Proof. Additive Combinatorics. If $|S||T| \geq p$ then there exists an $x \in \mathbb{F}_p$ with

$$|S + xT| > p/2 \quad \textit{and} \quad |S - xT| > p/2.$$

For any symmetric ($S = -S$) or antisymmetric ($S \cap -S = \emptyset$) set S, and arbitrary T it suffices to have $|S||T| \geq p$.

A is group of k-th powers and $|A| > \sqrt{p}$ we see that $8A^2 = \mathbb{F}_p$, that is, $\gamma(k, p) \leq 8$.

The Two Step Process for estimating $|nA|$

Estimation of $|nA|$:

1. Obtain good growth for $nA - nA$. (This leads to an upper bound for $\delta(k, p)$.)

2. Use Rusza's triangle inequality to get good growth for nA.

Rusza's triangle inequality: For any $S, T \subseteq \mathbb{F}_p$

$$|S + T| \geq |S|^{1/2}|T - T|^{1/2},$$

Iterate:

$$\begin{aligned}
|2A| &\geq |A|^{1/2}|A - A|^{1/2} \\
|4A| &\geq |A|^{1/4}|A - A|^{1/4}|2A - 2A|^{1/2} \\
&\vdots
\end{aligned}$$

Lemma 29 (Glibichuk, Konyagin (2007))

For $X, Y \subset \mathbb{F}_p$ with $|Y| > 1$ and $\frac{X-X}{Y-Y} \neq \mathbb{F}_p$ we have

$$|2XY - 2XY + Y^2 - Y^2| \geq |X||Y|.$$

Proof.

If $\frac{X-X}{Y-Y} \neq \mathbb{F}_p$ then there exist $x_1, x_2 \in X$, $y_1, y_2 \in Y$ such that $\frac{x_1-x_2}{y_1-y_2} + 1 \notin \frac{X-X}{Y-Y}$. But then the mapping from $X \times Y$ into $2XY - 2XY + Y^2 - Y^2$ given by

$$(x, y) \to (y_1 - y_2)x + (x_1 - x_2 + y_1 - y_2)y,$$

is one-to-one and the lemma follows. □

Let $a_k = \frac{4^k+8}{6}$.

THEOREM 30 (GLIBICHUK AND KONYAGIN (2007), CIPRA, PINNER, C (2009))

For $k \geq 3$

$$|a_kA - a_kA| \geq \min\{\lambda^2|A|^k, 3^{3/7}p^{4/7}\}.$$

$$|A - A| \geq \min\{\frac{1}{4}|A|^{3/2}, p/2\}$$

$$|3A - 3A| \geq \min\{|A|^2, 2p^{2/3}\}$$

$$|12A - 12A| \geq \min\{\frac{1}{16}|A|^3, 3^{3/7}p^{4/7}\}$$

$$|44A - 44A| \geq \min\{\frac{1}{16}|A|^4, 3^{3/7}p^{4/7}\}$$

$$n_k = \frac{2}{3}4^{k+1} + k - \frac{14}{3}.$$

Theorem 31 (Cipra, Pinner, C (2009))

$$|n_k A| \geq \min\{\beta_k |A|^{k+1}, \sqrt{2p}, \},$$

where $\beta_k = (1/4)^{\frac{4}{3} - \frac{4}{3 \cdot 4^k}}$.

$$|2A| \geq \min\{.25|A|^{3/2}, p/2\}$$
$$|7A| \geq \min\{.25|A|^2, \sqrt{2p}\}$$
$$|40A| \geq \min\{.177|A|^3, \sqrt{2p}\}$$
$$|169A| \geq \min\{.163|A|^4, \sqrt{2p}\}.$$

For any multiplicative subgroup A,

$$\begin{aligned} 8A &= \mathbb{F}_p \quad \text{for } |A| > p^{1/2} \\ 32A &= \mathbb{F}_p \quad \text{for } |A| > 3.18p^{1/3} \\ 392A &= \mathbb{F}_p \quad \text{for } |A| > 2.38p^{1/4} \\ &\textit{etc.} \end{aligned}$$

Theorem 32 (Glibichuk and Konyagin (2007), Cipra, Pinner, C (2009))

For $|A| > p^\epsilon$, $\gamma(k,p) \ll 4^{1/\epsilon}$.

This is the same strength as the Bourgain bound obtained via exp. sums but with an explicit constant 4.

Open Problem 3. Reduce the constant 4, or better yet show that $\gamma(k,p)$ is less than polynomial growth in $1/\epsilon$.

Conjecture: $\gamma(k,p) \ll \frac{1}{\epsilon}$ for $|A| \gg p^\epsilon$.

Theorem 33 (Pinner, C (2009))

If A is the group of k-th powers with $|A| > 2$ then we have

$$\gamma(k,p) \leq 83\, k^{1/2},$$

$$\delta(k,p) \leq 20\, k^{1/2}.$$

Proof. Use Glibichuk-Konyagin method for “large" A ($|A| > 34$) and geometric lattice method for small A.

Let A be the multiplicative group of k-th powers.

Open Problem 4: When does $\gamma(k, p) = 2$, that is, how large must $|A|$ be so that $A + A = \mathbb{F}_p$? Same problem for $\gamma(k, p) = 3$, etc.

What's known:
Hua and Vandiver (1949), Weil (1949): For $a \neq 0$,

$$|N(a) - p^{s-1}| \leq (k-1)^s p^{\frac{s-1}{2}},$$

where $N(a)$ is the number of solutions in $\mathbb{F}_p$ of the Waring equation

$$x_1^k + \cdots + x_s^k = a.$$

For $|A| > p^{3/4}$ $\quad \gamma(k, p) = 2.$
For $|A| > p^{2/3}$, $\quad \gamma(k, p) \leq 3.$

This is still the best known estimate for when $\gamma(k, p) = 2$ or 3.

Pinner, C (2010):
For $|A| \gg p^{10/17}, \quad \gamma(k,p) \leq 4$.
For $|A| \gg p^{6/11}, \quad \gamma(k,p) \leq 5$.
Proof. Use Heath-Brown, Konyagin estimate $N_2(A) \ll |A|^{5/2}$, for number of solutions of the equation

$$x_1 + x_2 = x_3 + x_4,$$

with $x_i \in A$, together with

$$|N(a) - p^{s-1}| \leq k^s \Phi_k^{s-3} N_2(A)/|A|.$$

Shkredov and Vyugin (2011): Using improvements of $|2A|$,
For $|A| \gg p^{33/67}, \quad \gamma(k,p) \leq 6$.

Open Problem 5. Obtain improvements in size of $|A|$ so that $\gamma(k,p) \leq 2, 3, 4, 5, \textit{etc}$.

Summary of Waring's number over $\mathbb{F}_p$

Let $t = |A|$, $\gamma(k,p) =$ Waring's number

$t = 1, 2$	$\gamma(k,p) = k$
$t = 3, 4, 6$	$\gamma(k,p) \approx \sqrt{k}$
$t < \log p$	$\gamma(k,p) \leq c(t)k^{1/\phi(t)}$
$t \geq \log p$	$\gamma(k,p) \ll (\log p)^{2+\epsilon}$
$t \geq p^{\epsilon}$	$\gamma(k,p) \ll 4^{1/\epsilon}$
$t \gg p^{1/2}$	$\gamma(k,p) \leq 6$
$t \geq p^{3/4}$	$\gamma(k,p) \leq 2$

Waring's number for a general finite field $\mathbb{F}_q$

$q = p^n$

$A =$ the group of nonzero k-th powers in $\mathbb{F}_q$

$\gamma(k, q) = \gamma(A, q)$= Waring's number.

First note that $\gamma(k, q)$ exists iff A contains a set of n linearly independent points over $\mathbb{F}_p$.

We assume $\gamma(k, q)$ exists in what follows.

Cauchy Bound: $\gamma(k, q) \leq k$,   for any k and q.

THEOREM 34 (HEILBRONN I: (CIPRA (2009))

If $\gamma(k, q)$ exists then

$$\gamma(k, q) \leq \begin{cases} 16\sqrt{k+1}, & \text{for } q = p^2. \\ 10\sqrt{k+1}, & \text{for } q = p^n,\ n \geq 3, \end{cases}$$

Theorem 35 (Cipra, C (2011))

If $\gamma(k,q)$ exists and $|A| > 1$ then

$$\gamma(k,q) \leq 633(2k)^{\frac{\log 4}{\log |A|}}.$$

Thus for $|A| > p^{\epsilon}$ we have

$$\gamma(k,p) \ll 4^{1/\epsilon}.$$

Let $q = p^n$, A be the group of k-th powers in $\mathbb{F}_q$ and

$$A' = A \cap \mathbb{F}_p.$$

Theorem 36 (Cipra (2009))

If $\gamma(k, q)$ exists, then

$$\gamma(k, q) \leq 8n \left\lceil \frac{(k+1)^{1/n} - 1}{|A'|} \right\rceil,$$

This sharpens work of Winterhof (2001).

The End.