Open problems about sumsets in finite abelian groups

Béla Bajnok

January 5, 2016

Three types of sumsets

G: finite abelian group written additively, $|G| = n$
$A = \{a_1, \ldots, a_m\} \subseteq G$, $|A| = m$
$h \in \mathbb{N}$

h-fold *sumset* of A:

$$hA = \{\Sigma_{i=1}^m \lambda_i a_i \ : \ (\lambda_1, \ldots, \lambda_m) \in \mathbb{N}_0^m, \ \Sigma_{i=1}^m \lambda_i = h\}$$

h-fold *restricted sumset* of A:

$$h\hat{}A = \{\Sigma_{i=1}^m \lambda_i a_i \ : \ (\lambda_1, \ldots, \lambda_m) \in \{0,1\}^m, \ \Sigma_{i=1}^m \lambda_i = h\}$$

h-fold *signed sumset* of A:

$$h_{\pm}A = \{\Sigma_{i=1}^m \lambda_i a_i \ : \ (\lambda_1, \ldots, \lambda_m) \in \mathbb{Z}^m, \ \Sigma_{i=1}^m |\lambda_i| = h\}$$

$h\hat{}A \subseteq hA \subseteq h_{\pm}A$ Rarely equal

Three functions

$$\rho(G, m, h) = \min\{|hA| \ : \ A \subseteq G, |A| = m\}$$

$$\rho\hat{}(G, m, h) = \min\{|h\hat{}A| \ : \ A \subseteq G, |A| = m\}$$

$$\rho_{\pm}(G, m, h) = \min\{|h_{\pm}A| \ : \ A \subseteq G, |A| = m\}$$

$\rho(G, m, h)$ known; $\rho\hat{}(G, m, h)$ and $\rho_{\pm}(G, m, h)$ not fully known

$$\rho\hat{}(G, m, 1) = \rho(G, m, 1) = \rho_{\pm}(G, m, 1) = m$$

$\rho\hat{}(G, m, h) \leq \rho(G, m, h) \leq \rho_{\pm}(G, m, h)$ Often equal

$$\rho\hat{}(\mathbb{Z}_3^2, 4, 2) = 5, \ \rho(\mathbb{Z}_3^2, 4, 2) = 7, \ \rho_{\pm}(\mathbb{Z}_3^2, 4, 2) = 8$$

$\rho(G, m, h)$

$$\rho(G, m, h) = \min\{|hA| \ : \ A \subseteq G, |A| = m\}$$

Cauchy, 1813; . . . ; Plagne, 2006

$\Downarrow$

$\rho(G, m, h)$ is known for all G, m, h

How to make hA small?

$G = \mathbb{Z}_n$

- Put A in a coset:

$$A \subseteq a + H \ \Rightarrow \ hA \subseteq h \cdot a + H$$

- Put A in an AP (arithmetic progression):

$$A \subseteq \cup_{i=0}^{k-1}\{a + i \cdot g\} \ \Rightarrow \ hA \subseteq \cup_{i=0}^{hk-h}\{a + i \cdot g\}$$

$\rho(G, m, h)$

Put A in an AP of cosets:

Choose $d \in D(n)$

$H \leq \mathbb{Z}_n$ with $|H| = d$ so $H = \cup_{j=0}^{d-1}\{j \cdot n/d\}$

Use $\lceil m/d \rceil$ cosets of H

$m = cd + k$ with $1 \leq k \leq d$

$A_d = A_d(n, m) = \cup_{i=0}^{c-1}(i + H) \bigcup \cup_{j=0}^{k-1}\{c + j \cdot n/d\}$

$$\Downarrow$$

$hA_d = \cup_{i=0}^{hc-1}(i + H) \bigcup \cup_{j=0}^{hk-h}\{hc + j \cdot n/d\}$

$$\Downarrow$$

$|hA_d| = \min\{n, hcd + \min\{d, hk - h + 1\}\}$

$\rho(G, m, h)$

$$f_d = f_d(m,h) = hcd + d = (h\lceil m/d \rceil - h + 1) \cdot d$$

$$\begin{aligned} |hA_d| &= \min\{n, hcd + \min\{d, hk - h + 1\}\} \\ &= \min\{n, f_d, hm - h + 1\} \\ &= \min\{f_n, f_d, f_1\} \end{aligned}$$

$$u(n,m,h) = \min\{f_d(m,h) \ : \ d \in D(n)\}$$

Theorem (Plagne)

For all G, m, and h $\qquad \rho(G,m,h) = u(n,m,h)$

Proof:

$\leq$: construction as above but in any G

$\geq$: generalized Kneser's Theorem

$u(n,m,h) \sim$ Hopf–Stiefel function

$\rho(G, m, h)$—Inverse Problems

$$|A| = m,\ |hA| = \rho(G, m, h) \ \Rightarrow \ A = ?$$

Examples:

- $\rho(\mathbb{Z}_{15}, 6, 2) = 9$
  $\Downarrow$
  $A = (a_1 + H) \cup (a_2 + H)$ with $|H| = 3$
- $\rho(\mathbb{Z}_{15}, 7, 2) = 13$
  $\Downarrow$
  $A = (a_1 + H) \cup (a_2 + H) \cup \{a_3\}$ with $|H| = 3$ or

  $A = (a_1 + H) \cup \{a_2, a_3\}$ with $|H| = 5$ or

  $A = \cup_{i=0}^{6} \{a + i \cdot g\}$

$\rho(G, m, h)$—Inverse Problems

Special Case

$p = \min\{p \text{ prime } : p|n\}$ and $m \leq p$

$$\Downarrow$$

$\rho(G, m, h) = \min\{p, hm - h + 1\}$

Theorem (Kemperman)

$hm - h + 1 < p$ and $|hA| = \rho(G, m, h) = hm - h + 1$

$$\Downarrow$$

- *$h = 1$ (and A arbitrary), or*
- *$A = AP$*

Conjecture

$m \leq p < hm - h + 1$ and $|hA| = \rho(G, m, h) = p$

$$\Downarrow$$

$A \subseteq a + H$ with $|H| = p$

$\rho\hat{}(\mathbb{Z}_n, m, h)$

$$\rho\hat{}(G, m, h) = \min\{|h\hat{}A| \ : \ A \subseteq G, |A| = m\}$$

How to make $h\hat{}A$ small? $G = \mathbb{Z}_n$

$H \leq G$ with $|H| = d$ so $H = \cup_{j=0}^{d-1}\{j \cdot n/d\}$
$m = cd + k$ with $1 \leq k \leq d$

$$A_d = A_d(n, m) = \cup_{i=0}^{c-1}(i + H) \bigcup \cup_{j=0}^{k-1}\{c + j \cdot n/d\}$$

$$|hA_d| = \min\{n, f_d, hm - h + 1\}$$

$$f_d = f_d(m, h) = hcd + d = (h\lceil m/d \rceil - h + 1) \cdot d$$

$$|h\hat{}A_d| = \begin{cases} \min\{n, f_d, hm - h^2 + 1\} & \text{if } h \leq \min\{k, d-1\} \\ \min\{n, hm - h^2 + 1 - \delta_d\} & \text{otherwise} \end{cases}$$

$\delta_d = \delta_d(m, h)$ is an explicitly computed "correction term"

$\rho\hat{}(\mathbb{Z}_n, m, h)$

$$u\hat{}(n, m, h) = \min\{|h\hat{}A_d| \ : \ d \in D(n)\}$$

$$\rho\hat{}(\mathbb{Z}_n, m, h) \le u\hat{}(n, m, h)$$

$$|h\hat{}A_1| = |h\hat{}A_n| = \min\{n, hm - h^2 + 1\}$$

$$\rho\hat{}(\mathbb{Z}_n, m, h) \le \min\{n, hm - h^2 + 1\}$$

Theorem (Dias da Silva, Hamidoune; Alon, Nathanson, Ruzsa)

p prime $\Rightarrow \rho\hat{}(\mathbb{Z}_p, m, h) = \min\{p, hm - h^2 + 1\}$

For $n \le 40, m, h$:

$$\rho\hat{}(\mathbb{Z}_n, m, h) = \begin{cases} u\hat{}(n, m, h) & \text{more than 99.9\% of time} \\ u\hat{}(n, m, h) - 1 & \text{otherwise} \end{cases}$$

$\rho\hat{}(\mathbb{Z}_n, m, h)$

$m = k_1 + (c-1)d + k_2$ with $1 \leq k_1, k_2 \leq d,\ k_1 + k_2 > d$

$B_d = \cup_{j=0}^{k_1-1}\{j \cdot n/d\} \bigcup \cup_{i=1}^{c-1}(i \cdot g + H) \bigcup \cup_{j=0}^{k_2-1}\{c \cdot g + (j_0 + j) \cdot n/d\}$

B_d is still in $\lceil m/d \rceil$ cosets of H but with ≤ 2 cosets not fully in B_d

$|h\hat{}B_d| < |h\hat{}A_d| \Leftrightarrow n, m, h$ are very special

$w\hat{}(n, m, h) = \min\{|h\hat{}B_d| \ : \ d \in D(n)\}$

$\rho\hat{}(\mathbb{Z}_n, m, h) \leq \min\{u\hat{}(n, m, h), w\hat{}(n, m, h)\}$

Problem

$\rho\hat{}(\mathbb{Z}_n, m, h) = \min\{u\hat{}(n, m, h), w\hat{}(n, m, h)\}$?

True for all n, m, h with $n \leq 40$

$\rho\hat{}(\mathbb{Z}_n, m, 2)$

For $h = 2$ this becomes:

Conjecture

$$\rho\hat{}(\mathbb{Z}_n, m, 2) = \begin{cases} \min\{\rho(\mathbb{Z}_n, m, 2), 2m-4\} & \text{if } 2|n \text{ and } 2|m, \text{ or} \\ & (2m-2)|n \text{ and } \log_2(m-1) \notin \mathbb{N}; \\ \min\{\rho(\mathbb{Z}_n, m, 2), 2m-3\} & \text{otherwise.} \end{cases}$$

Conjecture (Lev)

$\rho\hat{}(G, m, 2) \geq \min\{\rho(G, m, 2), 2m - 3 - |\mathrm{Ord}(G, 2)|\}$

Theorem (Eliahou, Kervaire)

p odd prime $\Rightarrow \rho\hat{}(\mathbb{Z}_p^r, m, 2) \geq \min\{\rho(\mathbb{Z}_p^r, m, 2), 2m - 3\}$

Theorem (Plagne)

$\rho\hat{}(G, m, 2) \leq \min\{\rho(G, m, 2), 2m - 2\}$

$\rho\hat{}(G, m, h)$

Recall:

Special Case

$p = \min\{p \text{ prime } : p|n\}$ and $m \leq p$

$\Downarrow$

$\rho(G, m, h) = \min\{p, hm - h + 1\}$

Conjecture

$p = \min\{p \textit{ prime } : p|n\}$ *and* $m \leq p$

$\Downarrow$

$\rho\hat{}(G, m, h) = \min\{p, hm - h^2 + 1\}$

Theorem (Károlyi)

Conjecture true for $h = 2$.

$\rho\hat{}(G, m, h)$—Inverse Problems

Theorem (Kemperman)

$hm - h + 1 < p$ *and* $|hA| = \rho(G, m, h) = hm - h + 1$

$\Downarrow$

- $h = 1$ *(and A arbitrary), or*
- $A = AP$

Conjecture

$hm - h^2 + 1 < p$ *and* $|hA| = \rho\hat{}(G, m, h) = hm - h^2 + 1$

$\Downarrow$

- $h \in \{1, m - 1\}$ *(and A arbitrary),*
- $h = 2$, $m = 4$, *and* $A = \{a, a + g_1, a + g_2, a + g_1 + g_2\}$, *or*
- $A = AP$

Theorem (Károlyi)

Conjecture true for $h = 2$.

$\hat{\rho}(G, m, h)$—Inverse Problems

Conjecture

$$m \leq p < hm - h + 1 \text{ and } |hA| = \rho(G, m, h) = p$$
$$\Downarrow$$
$$A \subseteq a + H \text{ with } |H| = p$$

Conjecture

$$m \leq p < hm - h^2 + 1 \text{ and } |h\hat{}A| = \rho\hat{}(G, m, h) = p$$
$$\Downarrow$$
$$A \subseteq a + H \text{ with } |H| = p$$

$\rho_{\pm}(G, m, h)$

$\rho_{\pm}(G, m, h) = \min\{|h_{\pm}A| \ : \ A \subseteq G, |A| = m\}$

All work with Matzke, 2014-2015

Surprises:

- $\rho_{\pm}(G, m, h)$ depends on structure of G not just $|G| = n$

  E.g. $\rho_{\pm}(\mathbb{Z}_3^2, 4, 2) = 8, \quad \rho_{\pm}(\mathbb{Z}_9, 4, 2) = 7$
- Usually $|h_{\pm}A| > |hA|$, but often $\rho_{\pm}(G, m, h) = \rho(G, m, h)$

  E.g. $n \leq 24 \Rightarrow \rho_{\pm}(G, m, h) = \rho(G, m, h)$ except $\rho_{\pm}(\mathbb{Z}_3^2, 4, 2)$
- Symmetric A (i.e. $A = -A$) is not always best

  Sometimes
  near-symmetric A (i.e. $A \setminus \{a\}$ is symmetric) or
  asymmetric A (i.e. $A \cap -A = \emptyset$)
  is best

  But one of these three types will always yield $\rho_{\pm}(G, m, h)$

$\rho_{\pm}(G, m, h)$

Theorem

For cyclic G,

$$\rho_{\pm}(G, m, h) = \rho(G, m, h).$$

Proof: For each $d \in D(n)$, find $R \subseteq G$ so that

- R is symmetric,
- $|R| \geq m$,
- $|h_{\pm}R| = |hR| \leq f_d(m, h)$.

(A symmetric set A with $|A| = m$ and $|hA| \leq f_d(m, h)$ may not exist.)

$\rho_{\pm}(G, m, h)$

Theorem

For G of type $(n_1, \ldots, n_r)$,

$$\rho_{\pm}(G, m, h) \leq u_{\pm}(G, m, h),$$

where

$$\begin{aligned} u_{\pm}(G, m, h) &= \min \{\Pi \rho_{\pm}(\mathbb{Z}_{n_i}, m_i, h) \ : \ m_i \leq n_i, \Pi m_i \geq m\} \\ &= \min \{\Pi u(n_i, m_i, h) \ : \ m_i \leq n_i, \Pi m_i \geq m\} \\ &= \min\{f_d(m, h) \ : \ d \in D(G, m)\} \end{aligned}$$

with

$$D(G, m) = \{d \in D(n) \ : \ d = \Pi d_i, d_i \in D(n_i), dn_r \geq d_r m\}$$

Note: for cyclic G, $D(G, m) = D(n)$.

$\rho_{\pm}(G, m, h)$

Corollary

$$u(n, m, h) \leq \rho_{\pm}(G, m, h) \leq u_{\pm}(G, m, h),$$

where

$$\begin{aligned} u(n, m, h) &= \min\{f_d(m, h) \ : \ d \in D(n)\} \\ u_{\pm}(G, m, h) &= \min\{f_d(m, h) \ : \ d \in D(G, m)\} \end{aligned}$$

Corollary

G is a 2-group $\Rightarrow \rho_{\pm}(G, m, h) = \rho(G, m, h)$

Corollary

G is such that $\nexists H \leq G, H \cong \mathbb{Z}_p^r, p > 2, r \geq 2$

$\Downarrow$

$\rho_{\pm}(G, m, h) = \rho(G, m, h)$

$\rho_{\pm}(G, m, h)$

Can we have $\rho_{\pm}(G, m, h) < u_{\pm}(G, m, h)$?

Proposition

$d \in D(n)$ odd, $d \geq 2m + 1 \Rightarrow \rho_{\pm}(G, m, 2) \leq d - 1$.

Proof:

- $\exists H \leq G, |H| = d$,
- $\exists A \subseteq H, |A| = m, A \cap (-A) = \emptyset$
- $0 \notin 2_{\pm} A$.

Conjecture

$D_o(n) = \{d \in D(n) \ : \ d \text{ odd}, \ d \geq 2m + 1\}$.

$\rho_{\pm}(G, m, h) = u_{\pm}(G, m, h)$ *for all* $h \geq 3$.

$$\rho_{\pm}(G, m, 2) = \begin{cases} u_{\pm}(G, m, 2) & \text{if } D_o(n) = \emptyset, \\ \min\{u_{\pm}(G, m, 2), d_m - 1\} & \text{if } d_m = \min D_0(n) \end{cases}$$

$\rho_{\pm}(\mathbb{Z}_p^r, m, h)$

Elementary abelian groups $\mathbb{Z}_p^r$ with p odd prime

Theorem

$p \leq h \;\Rightarrow\; \rho_{\pm}(\mathbb{Z}_p^r, m, h) = \rho(\mathbb{Z}_p^r, m, h)$

Theorem

$h \leq p - 1$
$\delta = 0$ *if* $h | p - 1$ *and* $\delta = 1$ *if* $h \not| p - 1$
k *max s.t.* $p^k + \delta \leq hm - h + 1$
c *max s.t.* $(hc + 1) \cdot p^k + \delta \leq hm - h + 1$

$m \leq (c + 1) \cdot p^k \;\Rightarrow\; \rho_{\pm}(\mathbb{Z}_p^r, m, h) = \rho(\mathbb{Z}_p^r, m, h)$

Conjecture

$m > (c + 1) \cdot p^k \;\Rightarrow\; \rho_{\pm}(\mathbb{Z}_p^r, m, h) > \rho(\mathbb{Z}_p^r, m, h)$

$\rho_{\pm}(\mathbb{Z}_p^2, m, 2)$

Conjecture holds for $r = 2$ and $h = 2$:

Theorem

$\rho_{\pm}(\mathbb{Z}_p^2, m, 2) = \rho(\mathbb{Z}_p^2, m, 2)$,

$\Updownarrow$

- $m \leq p$,
- $m \geq \frac{p^2+1}{2}$, *or*
- $\exists c \leq \frac{p-1}{2}$ *s.t.* $c \cdot p + \frac{p+1}{2} \leq m \leq (c+1) \cdot p$

Proof: Via results on critical pairs by Vosper, Kemperman, and Lev.

Note: $\left|m \ : \ \rho_{\pm}(\mathbb{Z}_p^2, m, 2) > \rho(\mathbb{Z}_p^2, m, 2)\right| = \frac{(p-1)^2}{4}$

Conjecture

$|m \ : \ \rho_{\pm}(G, m, h) > \rho(G, m, h)| < \frac{n}{4}$ *for every* G.

$\rho_{\pm}(\mathbb{Z}_p^2, m, 2)$

Theorem

$m = cp + v$ *with* $0 \leq c \leq p - 1$ *and* $1 \leq v \leq p$
$\Downarrow$

c	v	$\rho(\mathbb{Z}_p^2, m, 2)$		$\rho_{\pm}(\mathbb{Z}_p^2, m, 2)$		$u_{\pm}(\mathbb{Z}_p^2, m, 2)$
0	$v \leq \frac{p-1}{2}$	$2m-1$	$=$	$2m-1$	$=$	$2m-1$
	$v \geq \frac{p+1}{2}$	p	$=$	p	$=$	p
$1 \leq c \leq \frac{p-3}{2}$	$v \leq \frac{p-1}{2}$	$2m-1$	$<$	$\boxed{(2c+1)p}$	$=$	$(2c+1)p$
	$v \geq \frac{p+1}{2}$	$(2c+1)p$	$=$	$(2c+1)p$	$=$	$(2c+1)p$
$c = \frac{p-1}{2}$	$v \leq \frac{p-1}{2}$	$2m-1$	$<$	$\boxed{p^2-1}$	$<$	p^2
	$v \geq \frac{p+1}{2}$	p^2	$=$	p^2	$=$	p^2
$c \geq \frac{p+1}{2}$	*any* v	p^2	$=$	p^2	$=$	p^2

The two boxed entries were proven by Lee.

$\rho_{\pm}(G,m,h)$—Inverse Problems

$\mathcal{A}(G,m) = \mathrm{Sym}(G,m) \cup \mathrm{Nsym}(G,m) \cup \mathrm{Asym}(G,m)$ where

- $\mathrm{Sym}(G,m) = \{A \subseteq G \ : \ |A| = m, A = -A\}$
- $\mathrm{Nsym}(G,m) = \{A \subseteq G \ : \ |A| = m, A \setminus \{a\} = -(A \setminus \{a\})\}$
- $\mathrm{Asym}(G,m) = \{A \subseteq G \ : \ |A| = m, A \cap (-A) = \emptyset\}$

Theorem

$\rho_{\pm}(G,m,h) = \min\{|h_{\pm}A| \ : \ A \in \mathcal{A}(G,m)\}$

Note: each type is essential.

Problem

When is

- $\rho_{\pm}(G,m,h) = \min\{|h_{\pm}A| \ : \ A \in \mathrm{Sym}(G,m)\}$*?*
- $\rho_{\pm}(G,m,h) = \min\{|h_{\pm}A| \ : \ A \in \mathrm{Nsym}(G,m)\}$*?*
- $\rho_{\pm}(G,m,h) = \min\{|h_{\pm}A| \ : \ A \in \mathrm{Asym}(G,m)\}$*?*

The h-critical number

$$\chi(G,h) = \min\{m \ : \ A \subseteq G, |A| = m \Rightarrow hA = G\}$$

$$\chi_{\pm}(G,h) = \min\{m \ : \ A \subseteq G, |A| = m \Rightarrow h_{\pm}A = G\}$$

$$\chi\hat{}(G,h) = \min\{m \ : \ A \subseteq G, |A| = m \Rightarrow h\hat{}A = G\}$$

$\chi(G,h)$ exists $\forall G, h$

$\chi_{\pm}(G,h)$ exists $\forall G, h$

$\chi\hat{}(G,h)$ exists

$\Updownarrow$

- $h \in \{1, n-1\}$, $\forall G$
- $h \in \{2, n-2\}$, $G \not\cong \mathbb{Z}_2^r$
- $3 \leq h \leq n-3$, $\forall G$

$\chi(G, h)$

$$\chi(G, h) = \min\{m \ : \ A \subseteq G, |A| = m \Rightarrow hA = G\}$$

Theorem

$\chi(G, h) = v_1(n, h) + 1$

where $v_g(n, h) = \max\left\{\left(\left\lfloor \frac{d-1-\gcd(d,g)}{h} \right\rfloor + 1\right) \cdot \frac{n}{d} \ : \ d \in D(n)\right\}$.

Theorem (Diamanda, Yap)

$\max\{m \ : \ \exists A \subseteq \mathbb{Z}_n, |A| = m, A \cap 2A = \emptyset\} = v_1(n, 3)$

Theorem

$\max\{m \ : \ \exists A \subseteq \mathbb{Z}_n, |A| = m, A \cap 3A = \emptyset\} = v_2(n, 4)$

Theorem (Hamidoune, Plagne)

$k > l, \gcd(k - l, n) = 1 \Rightarrow$
$\max\{m \ : \ \exists A \subseteq \mathbb{Z}_n, |A| = m, kA \cap lA = \emptyset\} = v_{k-l}(n, k + l)$

$\chi\hat{}(G,h)$

$$\chi\hat{}(G,h) = \min\{m \ : \ A \subseteq G, |A| = m \Rightarrow h\hat{}A = G\}$$

$$\chi\hat{}(G,1) = \chi\hat{}(G,n-1) = n$$

Proposition

$$G \not\cong \mathbb{Z}_2^r \ \Rightarrow \ \chi\hat{}(G,2) = (n + |\mathrm{Ord}(G,2)| + 3)/2$$

Proposition

$$(n + |\mathrm{Ord}(G,2)| - 1)/2 \leq h \leq n-2 \ \Rightarrow \ \chi\hat{}(G,h) = h+2$$

Problem

$$3 \leq h \leq (n + |\mathrm{Ord}(G,2)| - 3)/2 \ \Rightarrow \ \chi\hat{}(G,h) = ?$$

Problem

$$3 \leq h \leq \lfloor n/2 \rfloor - 1 \ \Rightarrow \ \chi\hat{}(\mathbb{Z}_n,h) = ?$$

$\chi\hat{}(G, h)$

Theorem (Dias da Silva, Hamidoune; Alon, Nathanson, Ruzsa)

p *prime* $\Rightarrow \rho\hat{}(\mathbb{Z}_p, m, h) = \min\{p, hm - h^2 + 1\}$

Corollary

p *prime* $\Rightarrow \chi\hat{}(\mathbb{Z}_p, h) = \lfloor (p-2)/h \rfloor + h + 1$

Theorem (Gallardo, Grekos, Habsieger, Hennecart, Landreau, Plagne)

$n \geq 12$, *even* $\Rightarrow \chi\hat{}(\mathbb{Z}_n, 3) = n/2 + 1$

Theorem

$$n \geq 12, \textit{ even} \Rightarrow \chi\hat{}(\mathbb{Z}_n, h) = \begin{cases} n/2 + 1 & \textit{if } h = 3, 4, \ldots, n/2 - 2; \\ n/2 + 2 & \textit{if } h = n/2 - 1. \end{cases}$$

$\chi\hat{}(\mathbb{Z}_n, 3)$

Case 1: $\{d \in D(n) : d \equiv 2\ (3)\} \neq \emptyset$, p smallest
Recall:

Theorem

$$\chi(G,3) = v_1(n,3) + 1 = \left(1 + \frac{1}{p}\right)\frac{n}{3} + 1$$

Theorem

$n \geq 16 \Rightarrow$

$$\chi\hat{}(\mathbb{Z}_n, 3) \geq \begin{cases} \left(1 + \frac{1}{p}\right)\frac{n}{3} + 3 & \textit{if } n = p \\ \left(1 + \frac{1}{p}\right)\frac{n}{3} + 2 & \textit{if } n = 3p \\ \left(1 + \frac{1}{p}\right)\frac{n}{3} + 1 & \textit{otherwise} \end{cases}$$

Problem

$\chi\hat{}(\mathbb{Z}_n, 3) =$ *values above?*

True for n prime, n even, $n \leq 50$

$\chi\hat{}(\mathbb{Z}_n, 3)$

Case 2: $\{d \in D(n) : d \equiv 2\ (3)\} = \emptyset$
Recall:

Theorem

$\chi(G, 3) = v_1(n, 3) + 1 = \left\lfloor \frac{n}{3} \right\rfloor + 1$

Theorem

$n \geq 11 \Rightarrow$

$$\chi\hat{}(\mathbb{Z}_n, 3) \geq \begin{cases} \left\lfloor \frac{n}{3} \right\rfloor + 4 & \textit{if } 9|n \\ \left\lfloor \frac{n}{3} \right\rfloor + 3 & \textit{otherwise} \end{cases}$$

Problem

$\chi\hat{}(\mathbb{Z}_n, 3) =$ *values above?*

True for n prime, $n \leq 50$

The critical number

$$\chi(G,\mathbb{N}_0) = \min\{m \ : \ A \subseteq G, |A| = m \Rightarrow \cup_{h=0}^{\infty} hA = G\}$$

$$\chi_{\pm}(G,\mathbb{N}_0) = \min\{m \ : \ A \subseteq G, |A| = m \Rightarrow \cup_{h=0}^{\infty} h_{\pm}A = G\}$$

$$\chi\hat{}(G,\mathbb{N}_0) = \min\{m \ : \ A \subseteq G, |A| = m \Rightarrow \cup_{h=0}^{\infty} h\hat{}A = G\}$$

$$p = \min\{d \in D(n) \ : \ d > 1\}$$

$$\cup_{h=0}^{\infty} hA = \cup_{h=0}^{\infty} h_{\pm}A = \langle A \rangle$$

$$\Downarrow$$

$$\chi(G,\mathbb{N}_0) = \chi_{\pm}(G,\mathbb{N}_0) = n/p + 1$$

Theorem (Dias Da Silva, Diderrich, Freeze, Gao, Geroldinger, Griggs, Hamidoune, Mann, Wou)

$$n \geq 10 \Rightarrow \chi\hat{}(G,\mathbb{N}_0) = \begin{cases} \lfloor 2\sqrt{n-2} \rfloor + 1 & \text{if } G \text{ cyclic with } n = p \text{ or } n = pq \text{ where} \\ & q \text{ is prime, } 3 \leq p \leq q \leq p + \lfloor 2\sqrt{p-2} \rfloor + 1 \\ n/p + p - 1 & \text{otherwise} \end{cases}$$

$\chi\hat{}(G, \mathbb{N}_0)$—Inverse problems

$A \subseteq \mathbb{Z}_n \leftrightarrow A \subseteq (-n/2, n/2]$
$||A|| = \Sigma_{a \in A} |a|$

Proposition

$||A|| \leq n-2 \Rightarrow \forall b \in \mathbb{Z}_n, \Sigma(b \cdot A) \neq \mathbb{Z}_n$

Conjecture

p *prime*, $A \subseteq \mathbb{Z}_p$, $|A| = \chi\hat{}(\mathbb{Z}_p, \mathbb{N}_0) - 1 = \lfloor 2\sqrt{p-2} \rfloor$

$\Downarrow$

$\Sigma A \neq \mathbb{Z}_p \Leftrightarrow \exists b \in \mathbb{Z}_p \setminus \{0\}, \ ||b \cdot A|| \leq p-2$

Theorem (Nguyen, Szemerédi, Vu)

p *prime*, $A \subseteq \mathbb{Z}_p$, $|A| \geq 1.99\sqrt{p}$

$\Downarrow$

$\Sigma A \neq \mathbb{Z}_p \Rightarrow \exists b \in \mathbb{Z}_p \setminus \{0\}, \ ||b \cdot A|| \leq p + O(\sqrt{p})$

THANK YOU!

DANKE SCHÖN!