Quadratic Residues and Difference Sets

Vsevolod F. Lev

The University of Haifa

Singapore, May 24, 2016

(Joint work with Jack Sonn, Quart. J. Math., 2016)

Sárközy's Conjecture

Notation: $\mathbb{F}_p = \mathcal{R}_p \cup \mathcal{N}_p \cup \{0\}$ – quadratic residues / non-residues.

Conjecture (Sárközy, 2012)

We have $\mathcal{R}_p \neq A + B$ *whenever* $A, B \subseteq \mathbb{F}_p$, $\min\{|A|, |B|\} > 1$.

Theorem (Shkredov, 2014: the case $A = B$)

We have $\mathcal{R}_p \neq A + A$ *whenever* $A \subseteq \mathbb{F}_p$ *(except if* $p = 3$ *and* $A = \{2\}$*).*
Also, $\mathcal{R}_p \neq \{a' + a'' \colon a', a'' \in A,\ a' \neq a''\}$.

The difference case ($B = -A$)

Is it true that $\mathcal{R}_p \neq \{a' - a'' \colon a', a'' \in A,\ a' \neq a''\}$ with $A \subseteq \mathbb{F}_p$?

The anticipated answer is NO: conjecturally, $A - A \subseteq \mathcal{R}_p \cup \{0\}$ implies $|A| \ll_\varepsilon p^\varepsilon$, and then $|A - A| \ll_\varepsilon p^{2\varepsilon} < |\mathcal{R}_p|$ for $\varepsilon < 0.25$ and p large.

Sárközy's Conjecture

Notation: $\mathbb{F}_p = \mathcal{R}_p \cup \mathcal{N}_p \cup \{0\}$ – quadratic residues / non-residues.

Conjecture (Sárközy, 2012)

We have $\mathcal{R}_p \neq A + B$ *whenever* $A, B \subseteq \mathbb{F}_p$, $\min\{|A|, |B|\} > 1$.

Theorem (Shkredov, 2014: the case $A = B$)

We have $\mathcal{R}_p \neq A + A$ *whenever* $A \subseteq \mathbb{F}_p$ *(except if* $p = 3$ *and* $A = \{2\}$*).*
Also, $\mathcal{R}_p \neq \{a' + a'' : a', a'' \in A,\ a' \neq a''\}$.

The difference case ($B = -A$)

Is it true that $\mathcal{R}_p \neq \{a' - a'' : a', a'' \in A,\ a' \neq a''\}$ with $A \subseteq \mathbb{F}_p$?

The anticipated answer is NO: conjecturally, $A - A \subseteq \mathcal{R}_p \cup \{0\}$ implies $|A| \ll_\varepsilon p^\varepsilon$, and then $|A - A| \ll_\varepsilon p^{2\varepsilon} < |\mathcal{R}_p|$ for $\varepsilon < 0.25$ and p large.

Sárközy's Conjecture

Notation: $\mathbb{F}_p = \mathcal{R}_p \cup \mathcal{N}_p \cup \{0\}$ – quadratic residues / non-residues.

Conjecture (Sárközy, 2012)

We have $\mathcal{R}_p \neq A + B$ whenever $A, B \subseteq \mathbb{F}_p$, $\min\{|A|, |B|\} > 1$.

Theorem (Shkredov, 2014: the case $A = B$)

We have $\mathcal{R}_p \neq A + A$ whenever $A \subseteq \mathbb{F}_p$ (except if $p = 3$ and $A = \{2\}$). Also, $\mathcal{R}_p \neq \{a' + a'' : a', a'' \in A,\ a' \neq a''\}$.

The difference case ($B = -A$)

Is it true that $\mathcal{R}_p \neq \{a' - a'' : a', a'' \in A,\ a' \neq a''\}$ with $A \subseteq \mathbb{F}_p$?

The anticipated answer is NO: conjecturally, $A - A \subseteq \mathcal{R}_p \cup \{0\}$ implies $|A| \ll_\varepsilon p^\varepsilon$, and then $|A - A| \ll_\varepsilon p^{2\varepsilon} < |\mathcal{R}_p|$ for $\varepsilon < 0.25$ and p large.

A Should-be-Easier Problem

Do there exist $A \subseteq \mathbb{F}_p$ such that $\mathcal{R}_p = \{a' - a'' : a', a'' \in A,\ a' \neq a''\}$ and indeed, the differences $a' - a''$ with $a', a'' \in A,\ a' \neq a''$ list all elements of $\mathcal{R}_p$ exactly once?

Notation: $A - A \stackrel{!}{=} \mathcal{R}_p$

Examples

- For $A_5 := \{2, 3\} \subseteq \mathbb{F}_5$, we have $A_5 - A_5 \stackrel{!}{=} \mathcal{R}_5$;
- For $A_{13} := \{2, 5, 6\} \subseteq \mathbb{F}_{13}$, we have $A_{13} - A_{13} \stackrel{!}{=} \mathcal{R}_{13}$.

Conjecture (Lev–Sonn, 2016)

For $p > 13$, there do not exist $A \subseteq \mathbb{F}_p$ with $A - A \stackrel{!}{=} \mathcal{R}_p$.

Theorem (Lev–Sonn, 2016)

For $13 < p < 10^{20}$, there do not exist $A \subseteq \mathbb{F}_p$ with $A - A \stackrel{!}{=} \mathcal{R}_p$.

A Should-be-Easier Problem

Do there exist $A \subseteq \mathbb{F}_p$ such that $\mathcal{R}_p = \{a' - a'' : a', a'' \in A,\ a' \neq a''\}$ and indeed, the differences $a' - a''$ with $a', a'' \in A,\ a' \neq a''$ list all elements of $\mathcal{R}_p$ exactly once?

Notation: $A - A \stackrel{!}{=} \mathcal{R}_p$

Examples

- For $A_5 := \{2, 3\} \subseteq \mathbb{F}_5$, we have $A_5 - A_5 \stackrel{!}{=} \mathcal{R}_5$;
- For $A_{13} := \{2, 5, 6\} \subseteq \mathbb{F}_{13}$, we have $A_{13} - A_{13} \stackrel{!}{=} \mathcal{R}_{13}$.

Conjecture (Lev–Sonn, 2016)

For $p > 13$, there do not exist $A \subseteq \mathbb{F}_p$ with $A - A \stackrel{!}{=} \mathcal{R}_p$.

Theorem (Lev–Sonn, 2016)

For $13 < p < 10^{20}$, there do not exist $A \subseteq \mathbb{F}_p$ with $A - A \stackrel{!}{=} \mathcal{R}_p$.

A Should-be-Easier Problem

Do there exist $A \subseteq \mathbb{F}_p$ such that $\mathcal{R}_p = \{a' - a'' : a', a'' \in A,\ a' \neq a''\}$ and indeed, the differences $a' - a''$ with $a', a'' \in A,\ a' \neq a''$ list all elements of $\mathcal{R}_p$ exactly once?

Notation: $A - A \stackrel{!}{=} \mathcal{R}_p$

Examples

- For $A_5 := \{2, 3\} \subseteq \mathbb{F}_5$, we have $A_5 - A_5 \stackrel{!}{=} \mathcal{R}_5$;
- For $A_{13} := \{2, 5, 6\} \subseteq \mathbb{F}_{13}$, we have $A_{13} - A_{13} \stackrel{!}{=} \mathcal{R}_{13}$.

Conjecture (Lev–Sonn, 2016)

For $p > 13$, there do not exist $A \subseteq \mathbb{F}_p$ with $A - A \stackrel{!}{=} \mathcal{R}_p$.

Theorem (Lev–Sonn, 2016)

For $13 < p < 10^{20}$, there do not exist $A \subseteq \mathbb{F}_p$ with $A - A \stackrel{!}{=} \mathcal{R}_p$.

A Should-be-Easier Problem

Do there exist $A \subseteq \mathbb{F}_p$ such that $\mathcal{R}_p = \{a' - a'' : a', a'' \in A,\ a' \neq a''\}$ and indeed, the differences $a' - a''$ with $a', a'' \in A,\ a' \neq a''$ list all elements of $\mathcal{R}_p$ exactly once?

Notation: $A - A \overset{!}{=} \mathcal{R}_p$

Examples

- For $A_5 := \{2, 3\} \subseteq \mathbb{F}_5$, we have $A_5 - A_5 \overset{!}{=} \mathcal{R}_5$;
- For $A_{13} := \{2, 5, 6\} \subseteq \mathbb{F}_{13}$, we have $A_{13} - A_{13} \overset{!}{=} \mathcal{R}_{13}$.

Conjecture (Lev–Sonn, 2016)

For $p > 13$, there do not exist $A \subseteq \mathbb{F}_p$ with $A - A \overset{!}{=} \mathcal{R}_p$.

Theorem (Lev–Sonn, 2016)

For $13 < p < 10^{20}$, there do not exist $A \subseteq \mathbb{F}_p$ with $A - A \overset{!}{=} \mathcal{R}_p$.

A Should-be-Easier Problem

Do there exist $A \subseteq \mathbb{F}_p$ such that $\mathcal{R}_p = \{a' - a'' : a', a'' \in A,\ a' \neq a''\}$ and indeed, the differences $a' - a''$ with $a', a'' \in A,\ a' \neq a''$ list all elements of $\mathcal{R}_p$ exactly once?

Notation: $A - A \stackrel{!}{=} \mathcal{R}_p$

Examples

- For $A_5 := \{2, 3\} \subseteq \mathbb{F}_5$, we have $A_5 - A_5 \stackrel{!}{=} \mathcal{R}_5$;
- For $A_{13} := \{2, 5, 6\} \subseteq \mathbb{F}_{13}$, we have $A_{13} - A_{13} \stackrel{!}{=} \mathcal{R}_{13}$.

Conjecture (Lev–Sonn, 2016)

For $p > 13$, there do not exist $A \subseteq \mathbb{F}_p$ with $A - A \stackrel{!}{=} \mathcal{R}_p$.

Theorem (Lev–Sonn, 2016)

For $13 < p < 10^{20}$, there do not exist $A \subseteq \mathbb{F}_p$ with $A - A \stackrel{!}{=} \mathcal{R}_p$.

A Should-be-Easier Problem

Do there exist $A \subseteq \mathbb{F}_p$ such that $\mathcal{R}_p = \{a' - a'' : a', a'' \in A,\ a' \neq a''\}$ and indeed, the differences $a' - a''$ with $a', a'' \in A,\ a' \neq a''$ list all elements of $\mathcal{R}_p$ exactly once?

Notation: $A - A \overset{!}{=} \mathcal{R}_p$

Examples

- For $A_5 := \{2, 3\} \subseteq \mathbb{F}_5$, we have $A_5 - A_5 \overset{!}{=} \mathcal{R}_5$;
- For $A_{13} := \{2, 5, 6\} \subseteq \mathbb{F}_{13}$, we have $A_{13} - A_{13} \overset{!}{=} \mathcal{R}_{13}$.

Conjecture (Lev–Sonn, 2016)

For $p > 13$, there do not exist $A \subseteq \mathbb{F}_p$ with $A - A \overset{!}{=} \mathcal{R}_p$.

Theorem (Lev–Sonn, 2016)

For $13 < p < 10^{20}$, there do not exist $A \subseteq \mathbb{F}_p$ with $A - A \overset{!}{=} \mathcal{R}_p$.

Basic Observations

- If $q = p^m$ with m even, then the subfield $A := \mathbb{F}_{\sqrt{q}} < \mathbb{F}_q$ satisfies $A - A \subseteq \mathcal{R}_q$. However, $A - A \stackrel{!}{=} \mathcal{R}_q$ does not hold!

Back to $\mathbb{F}_p$ with p prime:

- If $A - A \stackrel{!}{=} \mathcal{R}_p$, then $\mathcal{R}_p = -\mathcal{R}_p$, whence $p \equiv 1 \pmod 4$. This sieves out all primes $p \equiv 3 \pmod 4$.
- Writing $n := |A|$, for $A - A \stackrel{!}{=} \mathcal{R}_p$ to hold, one needs to have $n(n-1) = \frac{p-1}{2}$; that is,

$$p = 2n(n-1) + 1, \quad n = |A|.$$

(This also shows, in particular, that $p \equiv 1 \pmod 4$.)
- Affine equivalence: if $A - A \stackrel{!}{=} \mathcal{R}_p$, then, indeed, for each $\mu \in \mathcal{R}_p$ and $g \in \mathbb{F}_p$, letting $A' := \mu * A + g$, we will have $A' - A' \stackrel{!}{=} \mathcal{R}_p$.

Basic Observations

- If $q = p^m$ with m even, then the subfield $A := \mathbb{F}_{\sqrt{q}} < \mathbb{F}_q$ satisfies $A - A \subseteq \mathcal{R}_q$. However, $A - A \overset{!}{=} \mathcal{R}_q$ does not hold!

Back to $\mathbb{F}_p$ with p prime:

- If $A - A \overset{!}{=} \mathcal{R}_p$, then $\mathcal{R}_p = -\mathcal{R}_p$, whence $p \equiv 1 \pmod 4$. This sieves out all primes $p \equiv 3 \pmod 4$.
- Writing $n := |A|$, for $A - A \overset{!}{=} \mathcal{R}_p$ to hold, one needs to have $n(n-1) = \frac{p-1}{2}$; that is,

$$p = 2n(n-1) + 1, \quad n = |A|.$$

(This also shows, in particular, that $p \equiv 1 \pmod 4$.)

- Affine equivalence: if $A - A \overset{!}{=} \mathcal{R}_p$, then, indeed, for each $\mu \in \mathcal{R}_p$ and $g \in \mathbb{F}_p$, letting $A' := \mu * A + g$, we will have $A' - A' \overset{!}{=} \mathcal{R}_p$.

Basic Observations

- If $q = p^m$ with m even, then the subfield $A := \mathbb{F}_{\sqrt{q}} < \mathbb{F}_q$ satisfies $A - A \subseteq \mathcal{R}_q$. However, $A - A \stackrel{!}{=} \mathcal{R}_q$ does not hold!

Back to $\mathbb{F}_p$ with p prime:

- If $A - A \stackrel{!}{=} \mathcal{R}_p$, then $\mathcal{R}_p = -\mathcal{R}_p$, whence $p \equiv 1 \pmod 4$. This sieves out all primes $p \equiv 3 \pmod 4$.
- Writing $n := |A|$, for $A - A \stackrel{!}{=} \mathcal{R}_p$ to hold, one needs to have $n(n-1) = \frac{p-1}{2}$; that is,

$$p = 2n(n-1) + 1, \quad n = |A|.$$

  (This also shows, in particular, that $p \equiv 1 \pmod 4$.)
- Affine equivalence: if $A - A \stackrel{!}{=} \mathcal{R}_p$, then, indeed, for each $\mu \in \mathcal{R}_p$ and $g \in \mathbb{F}_p$, letting $A' := \mu * A + g$, we will have $A' - A' \stackrel{!}{=} \mathcal{R}_p$.

Basic Observations

- If $q = p^m$ with m even, then the subfield $A := \mathbb{F}_{\sqrt{q}} < \mathbb{F}_q$ satisfies $A - A \subseteq \mathcal{R}_q$. However, $A - A \stackrel{!}{=} \mathcal{R}_q$ does not hold!

Back to $\mathbb{F}_p$ with p prime:

- If $A - A \stackrel{!}{=} \mathcal{R}_p$, then $\mathcal{R}_p = -\mathcal{R}_p$, whence $p \equiv 1 \pmod 4$. This sieves out all primes $p \equiv 3 \pmod 4$.
- Writing $n := |A|$, for $A - A \stackrel{!}{=} \mathcal{R}_p$ to hold, one needs to have $n(n-1) = \frac{p-1}{2}$; that is,

$$p = 2n(n-1) + 1, \quad n = |A|.$$

  (This also shows, in particular, that $p \equiv 1 \pmod 4$.)
- Affine equivalence: if $A - A \stackrel{!}{=} \mathcal{R}_p$, then, indeed, for each $\mu \in \mathcal{R}_p$ and $g \in \mathbb{F}_p$, letting $A' := \mu * A + g$, we will have $A' - A' \stackrel{!}{=} \mathcal{R}_p$.

What is special about $A_5 = \{2, 3\}$ and $A_{13} = \{2, 5, 6\}$?

Both A_5 and A_{13} are cosets of a subgroup of the multiplicative group of the corresponding field: A_5 is a coset of $\{1, 4\} < \mathbb{F}_5^\times$, and A_{13} is a coset of $\{1, 3, 9\} < \mathbb{F}_{13}^\times$.

In addition, A_5 is affinely equivalent to the set $\{0, 1\}$, which is a union of 0 and a subgroup of $\mathbb{F}_5^\times$.

For $p > 13$, constructions of this sort do not work!

Theorem

For a prime $p > 13$, there is no coset $A = gH$, with $H < \mathbb{F}_p^\times$ and $g \in \mathbb{F}_p^\times$, such that $A - A \stackrel{!}{=} \mathcal{R}_p$.

Theorem

For a prime $p > 5$, there is no coset gH, with $H < \mathbb{F}_p^\times$ and $g \in \mathbb{F}_p^\times$, such that, letting $A := gH \cup \{0\}$, we have $A - A \stackrel{!}{=} \mathcal{R}_p$.

What is special about $A_5 = \{2, 3\}$ and $A_{13} = \{2, 5, 6\}$?

Both A_5 and A_{13} are cosets of a subgroup of the multiplicative group of the corresponding field: A_5 is a coset of $\{1, 4\} < \mathbb{F}_5^\times$, and A_{13} is a coset of $\{1, 3, 9\} < \mathbb{F}_{13}^\times$.

In addition, A_5 is affinely equivalent to the set $\{0, 1\}$, which is a union of 0 and a subgroup of $\mathbb{F}_5^\times$.

For $p > 13$, constructions of this sort do not work!

Theorem

For a prime $p > 13$, there is no coset $A = gH$, with $H < \mathbb{F}_p^\times$ and $g \in \mathbb{F}_p^\times$, such that $A - A \stackrel{!}{=} \mathcal{R}_p$.

Theorem

For a prime $p > 5$, there is no coset gH, with $H < \mathbb{F}_p^\times$ and $g \in \mathbb{F}_p^\times$, such that, letting $A := gH \cup \{0\}$, we have $A - A \stackrel{!}{=} \mathcal{R}_p$.

What is special about $A_5 = \{2, 3\}$ and $A_{13} = \{2, 5, 6\}$?

Both A_5 and A_{13} are cosets of a subgroup of the multiplicative group of the corresponding field: A_5 is a coset of $\{1, 4\} < \mathbb{F}_5^\times$, and A_{13} is a coset of $\{1, 3, 9\} < \mathbb{F}_{13}^\times$.

In addition, A_5 is affinely equivalent to the set $\{0, 1\}$, which is a union of 0 and a subgroup of $\mathbb{F}_5^\times$.

For $p > 13$, constructions of this sort do not work!

Theorem

For a prime $p > 13$, there is no coset $A = gH$, with $H < \mathbb{F}_p^\times$ and $g \in \mathbb{F}_p^\times$, such that $A - A \overset{!}{=} \mathcal{R}_p$.

Theorem

For a prime $p > 5$, there is no coset gH, with $H < \mathbb{F}_p^\times$ and $g \in \mathbb{F}_p^\times$, such that, letting $A := gH \cup \{0\}$, we have $A - A \overset{!}{=} \mathcal{R}_p$.

What is special about $A_5 = \{2, 3\}$ and $A_{13} = \{2, 5, 6\}$?

Both A_5 and A_{13} are cosets of a subgroup of the multiplicative group of the corresponding field: A_5 is a coset of $\{1, 4\} < \mathbb{F}_5^\times$, and A_{13} is a coset of $\{1, 3, 9\} < \mathbb{F}_{13}^\times$.

In addition, A_5 is affinely equivalent to the set $\{0, 1\}$, which is a union of 0 and a subgroup of $\mathbb{F}_5^\times$.

For $p > 13$, constructions of this sort do not work!

Theorem

For a prime $p > 13$, there is no coset $A = gH$, with $H < \mathbb{F}_p^\times$ and $g \in \mathbb{F}_p^\times$, such that $A - A \overset{!}{=} \mathcal{R}_p$.

Theorem

For a prime $p > 5$, there is no coset gH, with $H < \mathbb{F}_p^\times$ and $g \in \mathbb{F}_p^\times$, such that, letting $A := gH \cup \{0\}$, we have $A - A \overset{!}{=} \mathcal{R}_p$.

Sketch of the Proof

Suppose, for instance, that $H - H \overset{!}{=} \mathcal{R}_p$ with some $H < \mathbb{F}_p^\times$.

For all $h_1, h_2 \in H$ with $h_1 \neq \pm h_2$ we have then $h_1 - h_2 \in \mathcal{R}_p$, but also $h_1 + h_2 = (h_1^2 - h_2^2)/(h_1 - h_2) \in \mathcal{R}_p$. It follows that the sums

$$\sigma(x) := \sum_{h \in H} \big(\chi_p(x+h) + \chi_p(x-h)\big), \quad x \in \mathbb{F}_p$$

where χ_p is the quadratic character mod p, are very large for $x \in H$ and also for $x \in -H$.
(One needs to show that $-1 \notin H$, so that $-H$ is disjoint from H.)

As a result, the sum

$$\sum_{x \in H \cup (-H)} \sigma^2(x)$$

is very large – in fact, larger than the complete sum

$$\sum_{x \in \mathbb{F}_p} \sigma^2(x) = 2n(2n^2 - 4n + 1), \quad n = |H|.$$

Sketch of the Proof

Suppose, for instance, that $H - H \overset{!}{=} \mathcal{R}_p$ with some $H < \mathbb{F}_p^\times$.

For all $h_1, h_2 \in H$ with $h_1 \neq \pm h_2$ we have then $h_1 - h_2 \in \mathcal{R}_p$, but also $h_1 + h_2 = (h_1^2 - h_2^2)/(h_1 - h_2) \in \mathcal{R}_p$. It follows that the sums

$$\sigma(x) := \sum_{h \in H} \big(\chi_p(x+h) + \chi_p(x-h)\big), \quad x \in \mathbb{F}_p$$

where χ_p is the quadratic character mod p, are very large for $x \in H$ and also for $x \in -H$.
(One needs to show that $-1 \notin H$, so that $-H$ is disjoint from H.)

As a result, the sum

$$\sum_{x \in H \cup (-H)} \sigma^2(x)$$

is very large – in fact, larger than the complete sum

$$\sum_{x \in \mathbb{F}_p} \sigma^2(x) = 2n(2n^2 - 4n + 1), \quad n = |H|.$$

Multipliers

Definition

An element $\mu \in \mathbb{F}_p^\times$ is a *multiplier* of the set $A \subseteq \mathbb{F}_p$ if $\mu * A = A + g$ for some $g \in \mathbb{F}_p$, where $\mu * A := \{\mu a \colon a \in A\}$.

Let $M_A \subseteq \mathbb{F}_p^\times$ denote the set of all multipliers of A (notice that $1 \in M_A$).

- If $\mu_1, \mu_2 \in M_A$, then also $\mu_1\mu_2 \in M_A$; hence, $M_A < \mathbb{F}_p^\times$;
- If $A' = \mu A + g$ for some $\mu \in \mathbb{F}_p^\times$ and $g \in \mathbb{F}_p$, then $M_{A'} = M_A$;
- every $A \subseteq \mathbb{F}_p$ has a translate which is fixed by all multipliers of A: namely, if $g \in \mathbb{F}_p$ is so chosen that the elements of $A' := A + g$ add up to 0, then $\mu * A' = A'$ for each $\mu \in M_{A'} = M_A$.

If $H < \mathbb{F}_p^\times$ and $A = g_1H \cup \dots \cup g_kH$, or $A = \{0\} \cup g_1H \cup \dots \cup g_kH$, then $H \le M_A$.

Conversely, writing $H := M_A$, we have $(A + g) \setminus \{0\} = g_1H \cup \dots \cup g_kH$.

Multipliers

Definition

An element $\mu \in \mathbb{F}_p^\times$ is a *multiplier* of the set $A \subseteq \mathbb{F}_p$ if $\mu * A = A + g$ for some $g \in \mathbb{F}_p$, where $\mu * A := \{\mu a\colon a \in A\}$.

Let $M_A \subseteq \mathbb{F}_p^\times$ denote the set of all multipliers of A (notice that $1 \in M_A$).

- If $\mu_1, \mu_2 \in M_A$, then also $\mu_1\mu_2 \in M_A$; hence, $M_A < \mathbb{F}_p^\times$;
- If $A' = \mu A + g$ for some $\mu \in \mathbb{F}_p^\times$ and $g \in \mathbb{F}_p$, then $M_{A'} = M_A$;
- every $A \subseteq \mathbb{F}_p$ has a translate which is fixed by all multipliers of A: namely, if $g \in \mathbb{F}_p$ is so chosen that the elements of $A' := A + g$ add up to 0, then $\mu * A' = A'$ for each $\mu \in M_{A'} = M_A$.

If $H < \mathbb{F}_p^\times$ and $A = g_1H \cup \dots \cup g_kH$, or $A = \{0\} \cup g_1H \cup \dots \cup g_kH$, then $H \le M_A$.

Conversely, writing $H := M_A$, we have $(A + g) \setminus \{0\} = g_1H \cup \dots \cup g_kH$.

Multipliers

Definition

An element $\mu \in \mathbb{F}_p^\times$ is a *multiplier* of the set $A \subseteq \mathbb{F}_p$ if $\mu * A = A + g$ for some $g \in \mathbb{F}_p$, where $\mu * A := \{\mu a \colon a \in A\}$.

Let $M_A \subseteq \mathbb{F}_p^\times$ denote the set of all multipliers of A (notice that $1 \in M_A$).

- If $\mu_1, \mu_2 \in M_A$, then also $\mu_1 \mu_2 \in M_A$; hence, $M_A < \mathbb{F}_p^\times$;
- If $A' = \mu A + g$ for some $\mu \in \mathbb{F}_p^\times$ and $g \in \mathbb{F}_p$, then $M_{A'} = M_A$;
- every $A \subseteq \mathbb{F}_p$ has a translate which is fixed by all multipliers of A: namely, if $g \in \mathbb{F}_p$ is so chosen that the elements of $A' := A + g$ add up to 0, then $\mu * A' = A'$ for each $\mu \in M_{A'} = M_A$.

If $H < \mathbb{F}_p^\times$ and $A = g_1 H \cup \dots \cup g_k H$, or $A = \{0\} \cup g_1 H \cup \dots \cup g_k H$, then $H \leq M_A$.

Conversely, writing $H := M_A$, we have $(A + g) \setminus \{0\} = g_1 H \cup \dots \cup g_k H$.

Multipliers

Definition

An element $\mu \in \mathbb{F}_p^\times$ is a *multiplier* of the set $A \subseteq \mathbb{F}_p$ if $\mu * A = A + g$ for some $g \in \mathbb{F}_p$, where $\mu * A := \{\mu a\colon a \in A\}$.

Let $M_A \subseteq \mathbb{F}_p^\times$ denote the set of all multipliers of A (notice that $1 \in M_A$).

- If $\mu_1, \mu_2 \in M_A$, then also $\mu_1\mu_2 \in M_A$; hence, $M_A < \mathbb{F}_p^\times$;
- If $A' = \mu A + g$ for some $\mu \in \mathbb{F}_p^\times$ and $g \in \mathbb{F}_p$, then $M_{A'} = M_A$;
- every $A \subseteq \mathbb{F}_p$ has a translate which is fixed by all multipliers of A: namely, if $g \in \mathbb{F}_p$ is so chosen that the elements of $A' := A + g$ add up to 0, then $\mu * A' = A'$ for each $\mu \in M_{A'} = M_A$.

If $H < \mathbb{F}_p^\times$ and $A = g_1H \cup \cdots \cup g_kH$, or $A = \{0\} \cup g_1H \cup \cdots \cup g_kH$, then $H \le M_A$.

Conversely, writing $H := M_A$, we have $(A + g) \setminus \{0\} = g_1H \cup \cdots \cup g_kH$.

Multipliers

Definition

An element $\mu \in \mathbb{F}_p^\times$ is a *multiplier* of the set $A \subseteq \mathbb{F}_p$ if $\mu * A = A + g$ for some $g \in \mathbb{F}_p$, where $\mu * A := \{\mu a \colon a \in A\}$.

Let $M_A \subseteq \mathbb{F}_p^\times$ denote the set of all multipliers of A (notice that $1 \in M_A$).

- If $\mu_1, \mu_2 \in M_A$, then also $\mu_1 \mu_2 \in M_A$; hence, $M_A < \mathbb{F}_p^\times$;
- If $A' = \mu A + g$ for some $\mu \in \mathbb{F}_p^\times$ and $g \in \mathbb{F}_p$, then $M_{A'} = M_A$;
- every $A \subseteq \mathbb{F}_p$ has a translate which is fixed by all multipliers of A: namely, if $g \in \mathbb{F}_p$ is so chosen that the elements of $A' := A + g$ add up to 0, then $\mu * A' = A'$ for each $\mu \in M_{A'} = M_A$.

If $H < \mathbb{F}_p^\times$ and $A = g_1 H \cup \dots \cup g_k H$, or $A = \{0\} \cup g_1 H \cup \dots \cup g_k H$, then $H \leq M_A$.

Conversely, writing $H := M_A$, we have $(A + g) \setminus \{0\} = g_1 H \cup \dots \cup g_k H$.

Sets $A \subseteq \mathbb{F}_p$ with $A - A \stackrel{!}{=} \mathcal{R}_p$ Have M_A Large

For a prime $p \equiv 1 \pmod 4$, let

$$G_p := \gcd \left\{ \operatorname{ord}_p(q) \colon q \mid \tfrac{p-1}{4},\ q \text{ is prime} \right\}.$$

One can expect G_p to be quite large for most p. Computationally, among all primes $p = 2n(n-1) + 1 < 10^{12}$, there are less than 1.4% those with $G_p < \sqrt{p}$.

Theorem

If $A - A \stackrel{!}{=} \mathcal{R}_p$, then M_A lies above the order-G_p subgroup of $\mathbb{F}_p^\times$; equivalently, $|M_A|$ is divisible by G_p.

The proof uses basic algebraic number theory: let $\zeta := \exp(2\pi i/p)$ and $\alpha := \sum_{a \in A} \zeta^a$; then $A - A \stackrel{!}{=} \mathcal{R}_p$ translates as $|\alpha|^2 = n + \rho$ with $\rho = \sum_{r \in \mathcal{R}_p} \zeta^r = \frac{1}{2}(\sqrt{p} - 1)$, and we factor α into a product of prime ideals and consider the action of $\operatorname{Gal}(\mathbb{Q}[\zeta]/\mathbb{Q})$ on these ideals etc.

Sets $A \subseteq \mathbb{F}_p$ with $A - A \stackrel{!}{=} \mathcal{R}_p$ Have M_A Large

For a prime $p \equiv 1 \pmod 4$, let

$$G_p := \gcd \left\{ \mathrm{ord}_p(q) \colon q \mid \tfrac{p-1}{4},\ q \text{ is prime} \right\}.$$

One can expect G_p to be quite large for most p. Computationally, among all primes $p = 2n(n-1) + 1 < 10^{12}$, there are less than 1.4% those with $G_p < \sqrt{p}$.

Theorem

If $A - A \stackrel{!}{=} \mathcal{R}_p$, then M_A lies above the order-G_p subgroup of $\mathbb{F}_p^\times$; equivalently, $|M_A|$ is divisible by G_p.

The proof uses basic algebraic number theory: let $\zeta := \exp(2\pi i/p)$ and $\alpha := \sum_{a \in A} \zeta^a$; then $A - A \stackrel{!}{=} \mathcal{R}_p$ translates as $|\alpha|^2 = n + \rho$ with $\rho = \sum_{r \in \mathcal{R}_p} \zeta^r = \frac{1}{2}(\sqrt{p} - 1)$, and we factor α into a product of prime ideals and consider the action of $\mathrm{Gal}(\mathbb{Q}[\zeta]/\mathbb{Q})$ on these ideals etc.

Sets $A \subseteq \mathbb{F}_p$ with $A - A \stackrel{!}{=} \mathcal{R}_p$ Have M_A Large

For a prime $p \equiv 1 \pmod 4$, let

$$G_p := \gcd \left\{ \operatorname{ord}_p(q) \colon \, q \mid \tfrac{p-1}{4}, \; q \text{ is prime} \right\}.$$

One can expect G_p to be quite large for most p. Computationally, among all primes $p = 2n(n-1) + 1 < 10^{12}$, there are less than 1.4% those with $G_p < \sqrt{p}$.

Theorem

If $A - A \stackrel{!}{=} \mathcal{R}_p$, then M_A lies above the order-G_p subgroup of $\mathbb{F}_p^\times$; equivalently, $|M_A|$ is divisible by G_p.

The proof uses basic algebraic number theory: let $\zeta := \exp(2\pi i/p)$ and $\alpha := \sum_{a \in A} \zeta^a$; then $A - A \stackrel{!}{=} \mathcal{R}_p$ translates as $|\alpha|^2 = n + \rho$ with $\rho = \sum_{r \in \mathcal{R}_p} \zeta^r = \frac{1}{2}(\sqrt{p} - 1)$, and we factor α into a product of prime ideals and consider the action of $\mathrm{Gal}(\mathbb{Q}[\zeta]/\mathbb{Q})$ on these ideals etc.

Sets $A \subseteq \mathbb{F}_p$ with $A - A \stackrel{!}{=} \mathcal{R}_p$ Have M_A Large

For a prime $p \equiv 1 \pmod 4$, let

$$G_p := \gcd \left\{ \operatorname{ord}_p(q) \colon q \mid \tfrac{p-1}{4},\ q \text{ is prime} \right\}.$$

One can expect G_p to be quite large for most p. Computationally, among all primes $p = 2n(n-1) + 1 < 10^{12}$, there are less than 1.4% those with $G_p < \sqrt{p}$.

Theorem

If $A - A \stackrel{!}{=} \mathcal{R}_p$, then M_A lies above the order-G_p subgroup of $\mathbb{F}_p^\times$; equivalently, $|M_A|$ is divisible by G_p.

The proof uses basic algebraic number theory: let $\zeta := \exp(2\pi i/p)$ and $\alpha := \sum_{a \in A} \zeta^a$; then $A - A \stackrel{!}{=} \mathcal{R}_p$ translates as $|\alpha|^2 = n + \rho$ with $\rho = \sum_{r \in \mathcal{R}_p} \zeta^r = \frac{1}{2}(\sqrt{p} - 1)$, and we factor α into a product of prime ideals and consider the action of $\mathrm{Gal}(\mathbb{Q}[\zeta]/\mathbb{Q})$ on these ideals etc.

Some Consequences

Theorem (R)

If $A - A \stackrel{!}{=} \mathcal{R}_p$, then M_A lies above the order-G_p subgroup of $\mathbb{F}_p^\times$; equivalently, $|M_A|$ is divisible by G_p.

Corollary

If $p = 2n(n-1) + 1$ is "exceptional", then either G_p is a proper divisor of n, or G_p is a proper divisor of $n - 1$.

This sieves out over 99.7% of all primes $p = 2n(n-1) + 1 < 10^{12}$!

For integer $k \geq 1$, let Φ_k denote the k-th cyclotomic polynomial.

Corollary

Suppose that p is "exceptional". If $\operatorname{ord}_p(z) \mid G_p$ and $\operatorname{ord}_p(z) \nmid k$ for some $z \in \mathbb{F}_p$ and $k \geq 1$, then $\Phi_k(z) \in \mathcal{R}_p$.

Thus, if $z^{G_p} = 1$, $z^k \neq 1$, and $\Phi_k(z) \in \mathcal{N}_p$, then p is *not* exceptional.

Some Consequences

Theorem (R)

If $A - A \stackrel{!}{=} \mathcal{R}_p$, then M_A lies above the order-G_p subgroup of $\mathbb{F}_p^\times$; equivalently, $|M_A|$ is divisible by G_p.

Corollary

If $p = 2n(n-1)+1$ is "exceptional", then either G_p is a proper divisor of n, or G_p is a proper divisor of $n-1$.

This sieves out over 99.7% of all primes $p = 2n(n-1)+1 < 10^{12}$!

For integer $k \geq 1$, let Φ_k denote the k-th cyclotomic polynomial.

Corollary

Suppose that p is "exceptional". If $\operatorname{ord}_p(z) \mid G_p$ and $\operatorname{ord}_p(z) \nmid k$ for some $z \in \mathbb{F}_p$ and $k \geq 1$, then $\Phi_k(z) \in \mathcal{R}_p$.

Thus, if $z^{G_p} = 1$, $z^k \neq 1$, and $\Phi_k(z) \in \mathcal{N}_p$, then p is *not* exceptional.

Some Consequences

Theorem (R)

If $A - A \stackrel{!}{=} \mathcal{R}_p$, then M_A lies above the order-G_p subgroup of $\mathbb{F}_p^\times$; equivalently, $|M_A|$ is divisible by G_p.

Corollary

If $p = 2n(n-1)+1$ is "exceptional", then either G_p is a proper divisor of n, or G_p is a proper divisor of $n-1$.

This sieves out over 99.7% of all primes $p = 2n(n-1)+1 < 10^{12}$!

For integer $k \geq 1$, let Φ_k denote the k-th cyclotomic polynomial.

Corollary

Suppose that p is "exceptional". If $\operatorname{ord}_p(z) \mid G_p$ and $\operatorname{ord}_p(z) \nmid k$ for some $z \in \mathbb{F}_p$ and $k \geq 1$, then $\Phi_k(z) \in \mathcal{R}_p$.

Thus, if $z^{G_p} = 1$, $z^k \neq 1$, and $\Phi_k(z) \in \mathcal{N}_p$, then p is *not* exceptional.

The Odd Orders

Theorem

If p is "exceptional", then $\operatorname{ord}_p(q)$ is odd for every prime $q \mid \frac{p-1}{4}$.

Corollary

If $p = 2n(n-1)+1$ is "exceptional", then either $n \equiv 2 \pmod 4$, or $n \equiv 3 \pmod 4$; hence, $p \equiv 5 \pmod 8$.

(If we had $n \in \{0, 1\} \pmod 4$, then $\frac{p-1}{4}$ were even; consequently, $\frac{p-1}{4}$ and $p-1$ would have same prime divisors. Hence, all prime divisors of $p-1$ would be of odd order, while $p-1$ itself has even order.)

Theorem (The previous theorem + biquadratic reciprocity)

If $p = 2n(n-1)+1$ is "exceptional", then neither n not $n-1$ have prime divisors congruent to 7 modulo 8. Moreover, of the numbers n and $n-1$, the odd one has no prime divisors congruent to 5 modulo 8, and the even one has no prime divisors congruent to 3 modulo 8.

The Odd Orders

Theorem

If p is "exceptional", then $\operatorname{ord}_p(q)$ is odd for every prime $q \mid \frac{p-1}{4}$.

Corollary

If $p = 2n(n-1)+1$ is "exceptional", then either $n \equiv 2 \pmod 4$, or $n \equiv 3 \pmod 4$; hence, $p \equiv 5 \pmod 8$.

(If we had $n \in \{0,1\} \pmod 4$, then $\frac{p-1}{4}$ were even; consequently, $\frac{p-1}{4}$ and $p-1$ would have same prime divisors. Hence, all prime divisors of $p-1$ would be of odd order, while $p-1$ itself has even order.)

Theorem (The previous theorem + biquadratic reciprocity)

If $p = 2n(n-1)+1$ is "exceptional", then neither n not $n-1$ have prime divisors congruent to 7 modulo 8. Moreover, of the numbers n and $n-1$, the odd one has no prime divisors congruent to 5 modulo 8, and the even one has no prime divisors congruent to 3 modulo 8.

The Odd Orders

Theorem

If p is "exceptional", then $\mathrm{ord}_p(q)$ is odd for every prime $q \mid \frac{p-1}{4}$.

Corollary

If $p = 2n(n-1)+1$ is "exceptional", then either $n \equiv 2 \pmod 4$, or $n \equiv 3 \pmod 4$; hence, $p \equiv 5 \pmod 8$.

(If we had $n \in \{0,1\} \pmod 4$, then $\frac{p-1}{4}$ were even; consequently, $\frac{p-1}{4}$ and $p-1$ would have same prime divisors. Hence, all prime divisors of $p-1$ would be of odd order, while $p-1$ itself has even order.)

Theorem (The previous theorem + biquadratic reciprocity)

If $p = 2n(n-1)+1$ is "exceptional", then neither n not $n-1$ have prime divisors congruent to 7 modulo 8. Moreover, of the numbers n and $n-1$, the odd one has no prime divisors congruent to 5 modulo 8, and the even one has no prime divisors congruent to 3 modulo 8.

Computational Evidence

In the range $13 < p < 10^{20}$, there are only five (!) primes $p = 2n(n-1)+1$ such that $G_p \mid n-\delta$ with $\delta \in \{0,1\}$, and the prime divisors of n and $n-1$ satisfy the congruence conditions just stated:

n	δ	$(n-\delta)/G_p$	$n-1,\ n$
51	1	2	$2 \cdot 5^2,\ 3 \cdot 17$
650	0	2	$11 \cdot 59,\ 2 \cdot 5^2 \cdot 13$
32283	1	2	$2 \cdot 16141,\ 3^2 \cdot 17 \cdot 211$
57303490	1	3	$3 \cdot 1579 \cdot 12097,\ 2 \cdot 5 \cdot 5730349$
377687811	0	3	$2 \cdot 5 \cdot 17 \cdot 113 \cdot 19661,\ 3 \cdot 1787 \cdot 70451$

These five primes are easily handled using the cyclotomic polynomial test. Thus, there are no exceptional primes in the specified range $13 < p < 10^{20}$.

Difference Sets

Theorem (R)

If p is "exceptional", then $\mathrm{ord}_p(q)$ is odd for every prime $q \mid \frac{p-1}{4}$.

The proof uses the Semi-primitivity Theorem from the theory of *difference sets* (in the design-theory meaning of this term).

Definition

For integer $v, k, \lambda > 0$, a (v, k, λ)-difference set is a k-element subset of a v-element group, such that every non-zero group element has exactly λ representations as a difference of two elements of the set.

Difference sets come into the play via the following observation.

Claim

Suppose that $A - A \stackrel{!}{=} \mathcal{R}_p$, and write $n := |A|$. The for any fixed $\nu \in \mathcal{N}_p$, the n^2 sums $a' + \nu a''$ with $a', a'' \in A$ are pairwise distinct, and the set D of all these sums is a $(p, n^2, n(n+1)/2)$-difference set in $\mathbb{F}_p$.

Difference Sets

Theorem (R)

If p is "exceptional", then $\mathrm{ord}_p(q)$ is odd for every prime $q \mid \frac{p-1}{4}$.

The proof uses the Semi-primitivity Theorem from the theory of *difference sets* (in the design-theory meaning of this term).

Definition

For integer $v, k, \lambda > 0$, a (v, k, λ)-difference set is a k-element subset of a v-element group, such that every non-zero group element has exactly λ representations as a difference of two elements of the set.

Difference sets come into the play via the following observation.

Claim

Suppose that $A - A \stackrel{!}{=} \mathcal{R}_p$, and write $n := |A|$. The for any fixed $\nu \in \mathcal{N}_p$, the n^2 sums $a' + \nu a''$ with $a', a'' \in A$ are pairwise distinct, and the set D of all these sums is a $(p, n^2, n(n+1)/2)$-difference set in $\mathbb{F}_p$.

Difference Sets

Theorem (R)

If p is "exceptional", then $\mathrm{ord}_p(q)$ is odd for every prime $q \mid \frac{p-1}{4}$.

The proof uses the Semi-primitivity Theorem from the theory of *difference sets* (in the design-theory meaning of this term).

Definition

For integer $v, k, \lambda > 0$, a (v, k, λ)-difference set is a k-element subset of a v-element group, such that every non-zero group element has exactly λ representations as a difference of two elements of the set.

Difference sets come into the play via the following observation.

Claim

Suppose that $A - A \stackrel{!}{=} \mathcal{R}_p$, and write $n := |A|$. The for any fixed $\nu \in \mathcal{N}_p$, the n^2 sums $a' + \nu a''$ with $a', a'' \in A$ are pairwise distinct, and the set D of all these sums is a $(p, n^2, n(n+1)/2)$-difference set in $\mathbb{F}_p$.

Proof of the Claim

Claim (R)

Suppose that $A - A \stackrel{!}{=} \mathcal{R}_p$, and write $n := |A|$. The for any fixed $\nu \in \mathcal{N}_p$, the n^2 sums $a' + \nu a''$ with $a', a'' \in A$ are pairwise distinct, and the set D of all these sums is a $(p, n^2, n(n+1)/2)$-difference set in $\mathbb{F}_p$.

The group-ring proof

In the group ring $\mathbb{Z}\mathbb{F}_p$, we have

$$D = AA^{(\nu)},\ AA^{(-1)} = n + \mathcal{R}_p,\ \mathcal{R}_p^{(\nu)} = \mathcal{N}_p,\ \text{and } \mathcal{R}_p\mathcal{N}_p = \frac{n(n-1)}{2}\,\mathbb{F}_p^\times$$

(the last equality reflecting the fact that for $p \equiv 1 \pmod 4$, every element of $\mathbb{F}_p^\times$ has exactly $\frac{p-1}{4}$ representations as a sum of a quadratic residue and a quadratic non-residue). Hence,

$$DD^{(-1)} = AA^{(\nu)}A^{(-1)}A^{(-\nu)} = (n + \mathcal{R}_p)(n + \mathcal{R}_p)^{(\nu)}$$

$$= (n + \mathcal{R}_p)(n + \mathcal{N}_p) = n^2 + n\mathbb{F}_p^\times + \frac{n(n-1)}{2}\,\mathbb{F}_p^\times = n^2 + \frac{n(n+1)}{2}\,\mathbb{F}_p^\times.$$

From Semi-primitivity to "$\mathrm{ord}_p(q)$ *is odd for* $q \mid \frac{p-1}{4}$"

Theorem (Semi-primitivity Theorem)

Suppose that G is a finite abelian group of exponent e. If G possesses a (v, k, λ)-difference set (so that $v = |G|$), then for any prime q with $q \mid k - \lambda$ and $q \nmid v$, the order of q in $(\mathbb{Z}/e\mathbb{Z})^\times$ is odd.

If $A - A \overset{!}{=} \mathcal{R}_p$, then $D := \{a' + \nu a'' : a', a'' \in A\}$ is a (v, k, λ)-difference set in $\mathbb{F}_p$ with $v = p$, $k = n^2$, and $\lambda = n(n+1)/2$. Thus, for any prime q dividing $k - \lambda = \frac{n(n-1)}{2} = \frac{p-1}{4}$, the order of q in $(\mathbb{Z}/p\mathbb{Z})^\times$ is odd.

The Big Difference Set Conjecture

If D is a (v, k, λ)-difference set, then every prime q dividing $k - \lambda$ but not dividing v is a multiplier of D; that is, $q * D = D + g$.

Conditionally to this conjecture, if $p = 2n(n-1) + 1$ is "exceptional", then either n, or $n - 1$ is divisible by $\mathrm{lcm}\,\{\mathrm{ord}_p(q) : q \mid \frac{p-1}{4} \text{ is prime}\}$ (instead of the unconditional gcd).

From Semi-primitivity to "$\mathrm{ord}_p(q)$ *is odd for* $q \mid \frac{p-1}{4}$"

Theorem (Semi-primitivity Theorem)

Suppose that G is a finite abelian group of exponent e. If G possesses a (v, k, λ)-difference set (so that $v = |G|$), then for any prime q with $q \mid k - \lambda$ and $q \nmid v$, the order of q in $(\mathbb{Z}/e\mathbb{Z})^\times$ is odd.

If $A - A \overset{!}{=} \mathcal{R}_p$, then $D := \{a' + \nu a'' \colon a', a'' \in A\}$ is a (v, k, λ)-difference set in $\mathbb{F}_p$ with $v = p$, $k = n^2$, and $\lambda = n(n+1)/2$. Thus, for any prime q dividing $k - \lambda = \frac{n(n-1)}{2} = \frac{p-1}{4}$, the order of q in $(\mathbb{Z}/p\mathbb{Z})^\times$ is odd.

The Big Difference Set Conjecture

If D is a (v, k, λ)-difference set, then every prime q dividing $k - \lambda$ but not dividing v is a multiplier of D; that is, $q * D = D + g$.

Conditionally to this conjecture, if $p = 2n(n-1) + 1$ is "exceptional", then either n, or $n - 1$ is divisible by $\mathrm{lcm}\,\{\mathrm{ord}_p(q) \colon q \mid \frac{p-1}{4} \text{ is prime}\}$ (instead of the unconditional gcd).

From Semi-primitivity to "$\mathrm{ord}_p(q)$ *is odd for* $q \mid \frac{p-1}{4}$"

Theorem (Semi-primitivity Theorem)

Suppose that G is a finite abelian group of exponent e. If G possesses a (v, k, λ)-difference set (so that $v = |G|$), then for any prime q with $q \mid k - \lambda$ and $q \nmid v$, the order of q in $(\mathbb{Z}/e\mathbb{Z})^\times$ is odd.

If $A - A \overset{!}{=} \mathcal{R}_p$, then $D := \{a' + \nu a'' : a', a'' \in A\}$ is a (v, k, λ)-difference set in $\mathbb{F}_p$ with $v = p$, $k = n^2$, and $\lambda = n(n+1)/2$. Thus, for any prime q dividing $k - \lambda = \frac{n(n-1)}{2} = \frac{p-1}{4}$, the order of q in $(\mathbb{Z}/p\mathbb{Z})^\times$ is odd.

The Big Difference Set Conjecture

If D is a (v, k, λ)-difference set, then every prime q dividing $k - \lambda$ but not dividing v is a multiplier of D; that is, $q * D = D + g$.

Conditionally to this conjecture, if $p = 2n(n-1) + 1$ is "exceptional", then either n, or $n - 1$ is divisible by $\mathrm{lcm}\,\{\mathrm{ord}_p(q) \colon q \mid \frac{p-1}{4} \text{ is prime}\}$ (instead of the unconditional gcd).

Summary

- For $A \subseteq \mathbb{F}_p$, we write $A - A \stackrel{!}{=} \mathcal{R}_p$ to indicate that the differences $a'' - a'$ $(a', a'' \in A)$ list all quadratic residues modulo p, every residue being listed exactly once.
- Conjecturally, this never happens, with just two exceptions: $p = 5$ $(A_5 = \{2, 3\})$ and $p = 13$ $(A_{13} = \{2, 5, 6\})$. We prove this for $13 < p < 10^{20} = 100,000,000,000,000,000,000$.
- Our methods involve elementary number theory / combinatorics, algebraic number theory, biquadratic reciprocity, and the theory of difference sets...
- ... which becomes relevant through the following observation: If $A - A \stackrel{!}{=} \mathcal{R}_p$, then for any fixed quadratic non-residue ν, the set $D := \{a' + \nu a'' : a', a'' \in A\}$ is a $(p, n^2, n(n+1)/2)$-difference set.

Summary

- For $A \subseteq \mathbb{F}_p$, we write $A - A \stackrel{!}{=} \mathcal{R}_p$ to indicate that the differences $a'' - a'$ ($a', a'' \in A$) list all quadratic residues modulo p, every residue being listed exactly once.
- Conjecturally, this never happens, with just two exceptions: $p = 5$ ($A_5 = \{2, 3\}$) and $p = 13$ ($A_{13} = \{2, 5, 6\}$). We prove this for $13 < p < 10^{20} = 100,000,000,000,000,000,000$.
- Our methods involve elementary number theory / combinatorics, algebraic number theory, biquadratic reciprocity, and the theory of difference sets...
- ... which becomes relevant through the following observation: If $A - A \stackrel{!}{=} \mathcal{R}_p$, then for any fixed quadratic non-residue ν, the set $D := \{a' + \nu a'' : a', a'' \in A\}$ is a $(p, n^2, n(n+1)/2)$-difference set.

Summary

- For $A \subseteq \mathbb{F}_p$, we write $A - A \stackrel{!}{=} \mathcal{R}_p$ to indicate that the differences $a'' - a'$ ($a', a'' \in A$) list all quadratic residues modulo p, every residue being listed exactly once.
- Conjecturally, this never happens, with just two exceptions: $p = 5$ ($A_5 = \{2, 3\}$) and $p = 13$ ($A_{13} = \{2, 5, 6\}$). We prove this for $13 < p < 10^{20} = 100,000,000,000,000,000,000$.
- Our methods involve elementary number theory / combinatorics, algebraic number theory, biquadratic reciprocity, and the theory of difference sets...
- ... which becomes relevant through the following observation: If $A - A \stackrel{!}{=} \mathcal{R}_p$, then for any fixed quadratic non-residue ν, the set $D := \{a' + \nu a'' : a', a'' \in A\}$ is a $(p, n^2, n(n+1)/2)$-difference set.

Summary

- For $A \subseteq \mathbb{F}_p$, we write $A - A \stackrel{!}{=} \mathcal{R}_p$ to indicate that the differences $a'' - a'$ ($a', a'' \in A$) list all quadratic residues modulo p, every residue being listed exactly once.
- Conjecturally, this never happens, with just two exceptions: $p = 5$ ($A_5 = \{2, 3\}$) and $p = 13$ ($A_{13} = \{2, 5, 6\}$). We prove this for $13 < p < 10^{20} = 100,000,000,000,000,000,000$.
- Our methods involve elementary number theory / combinatorics, algebraic number theory, biquadratic reciprocity, and the theory of difference sets...
- ... which becomes relevant through the following observation: If $A - A \stackrel{!}{=} \mathcal{R}_p$, then for any fixed quadratic non-residue ν, the set $D := \{a' + \nu a'' : a', a'' \in A\}$ is a $(p, n^2, n(n+1)/2)$-difference set.

Thank you!