ON ADDITIVE AND MULTIPLICATIVE DECOMPOSITIONS OF SUBSETS OF $\mathbb{F}_p$

András Sárközy

Eötvös Loránd University, Faculty of Siences
Department of Algebra and Number Theory
Budapest, Hungary

sarkozy@cs.elte.hu

1. Introduction

We will need

Definition 1

Let $\mathcal{G}$ be an additive semigroup and $\mathcal{A}, \mathcal{B}_1, \dots, \mathcal{B}_k$ subsets of $\mathcal{G}$ with

$$|\mathcal{B}_i| \geq 2 \quad \text{for} \quad i = 1, 2, \dots, k. \tag{1}$$

If

$$\mathcal{A} = \mathcal{B}_1 + \mathcal{B}_2 + \cdots + \mathcal{B}_k \,,$$

then this is called an (additive) *k-decomposition* of $\mathcal{A}$, while if

$$\mathcal{A} = \mathcal{B}_1 \cdot \mathcal{B}_2 \cdot \ldots \cdot \mathcal{B}_k \,,$$

then this is called a *multiplicative k-decomposition* of $\mathcal{A}$. (A decomposition will always mean a *non-trivial* one, i.e., a decomposition satisfying (1).)

H. H. Ostmann (1954, 1956) introduced some definitions on additive properties of sequences of non-negative *integers* and studied some related problems. The most interesting definitions are:

1. Introduction

We will need

Definition 1

Let $\mathcal{G}$ be an additive semigroup and $\mathcal{A}, \mathcal{B}_1, \dots, \mathcal{B}_k$ subsets of $\mathcal{G}$ with

$$|\mathcal{B}_i| \geq 2 \quad \text{for} \quad i = 1, 2, \dots, k. \tag{1}$$

If

$$\mathcal{A} = \mathcal{B}_1 + \mathcal{B}_2 + \dots + \mathcal{B}_k \,,$$

then this is called an (additive) *k-decomposition* of $\mathcal{A}$, while if

$$\mathcal{A} = \mathcal{B}_1 \cdot \mathcal{B}_2 \cdot \ldots \cdot \mathcal{B}_k \,,$$

then this is called a *multiplicative k-decomposition* of $\mathcal{A}$. (A decomposition will always mean a *non-trivial* one, i.e., a decomposition satisfying (1).)

H. H. Ostmann (1954, 1956) introduced some definitions on additive properties of sequences of non-negative *integers* and studied some related problems. The most interesting definitions are:

1. Introduction

We will need

Definition 1

Let $\mathcal{G}$ be an additive semigroup and $\mathcal{A}, \mathcal{B}_1, \dots, \mathcal{B}_k$ subsets of $\mathcal{G}$ with

$$|\mathcal{B}_i| \geq 2 \quad \text{for} \quad i = 1, 2, \dots, k. \tag{1}$$

If

$$\mathcal{A} = \mathcal{B}_1 + \mathcal{B}_2 + \cdots + \mathcal{B}_k \, ,$$

then this is called an (additive) *k-decomposition* of $\mathcal{A}$, while if

$$\mathcal{A} = \mathcal{B}_1 \cdot \mathcal{B}_2 \cdot \ldots \cdot \mathcal{B}_k \, ,$$

then this is called a *multiplicative k-decomposition* of $\mathcal{A}$. (A decomposition will always mean a *non-trivial* one, i.e., a decomposition satisfying (1).)

H. H. Ostmann (1954, 1956) introduced some definitions on additive properties of sequences of non-negative *integers* and studied some related problems. The most interesting definitions are:

Definition 2

A finite or infinite set $\mathcal{C}$ of non-negative integers is said to be *reducible* if it has an (additive) 2-decomposition

$$\mathcal{C} = \mathcal{A} + \mathcal{B}, \quad |\mathcal{A}| \geq 2, \quad |\mathcal{B}| \geq 2.$$

If there are no sets $\mathcal{A}$, $\mathcal{B}$ with these properties, then $\mathcal{C}$ is said to be *primitive* (or irreducible).

Definition 3

Two sets $\mathcal{A}$, $\mathcal{B}$ of non-negative integers are said to be *asymptotically equal* if there is a number K such that $\mathcal{A} \cap [K, +\infty) = \mathcal{B} \cap [K, +\infty)$, and then we write $\mathcal{A} \sim \mathcal{B}$.

Definition 4

An infinite set $\mathcal{C}$ of non-negative integers is said to be *totalprimitive* ("totally primitive") if every $\mathcal{C}'$ with $\mathcal{C}' \sim \mathcal{C}$ is primitive.

Ostmann also formulated the following beautiful conjecture:

Conjecture 1

The set $\mathcal{P}$ of the primes *is totalprimitive.*

Definition 2

A finite or infinite set $\mathcal{C}$ of non-negative integers is said to be *reducible* if it has an (additive) 2-decomposition

$$\mathcal{C} = \mathcal{A} + \mathcal{B}, \quad |\mathcal{A}| \geq 2, \quad |\mathcal{B}| \geq 2.$$

If there are no sets $\mathcal{A}$, $\mathcal{B}$ with these properties, then $\mathcal{C}$ is said to be *primitive* (or irreducible).

Definition 3

Two sets $\mathcal{A}$, $\mathcal{B}$ of non-negative integers are said to be *asymptotically equal* if there is a number K such that $\mathcal{A} \cap [K, +\infty) = \mathcal{B} \cap [K, +\infty)$, and then we write $\mathcal{A} \sim \mathcal{B}$.

Definition 4

An infinite set $\mathcal{C}$ of non-negative integers is said to be *totalprimitive* ("totally primitive") if every $\mathcal{C}'$ with $\mathcal{C}' \sim \mathcal{C}$ is primitive.

Ostmann also formulated the following beautiful conjecture:

Conjecture 1

The set $\mathcal{P}$ of the primes *is totalprimitive.*

Definition 2

A finite or infinite set $\mathcal{C}$ of non-negative integers is said to be *reducible* if it has an (additive) 2-decomposition

$$\mathcal{C} = \mathcal{A} + \mathcal{B}, \quad |\mathcal{A}| \geq 2, \quad |\mathcal{B}| \geq 2.$$

If there are no sets $\mathcal{A}$, $\mathcal{B}$ with these properties, then $\mathcal{C}$ is said to be *primitive* (or irreducible).

Definition 3

Two sets $\mathcal{A}$, $\mathcal{B}$ of non-negative integers are said to be *asymptotically equal* if there is a number K such that $\mathcal{A} \cap [K, +\infty) = \mathcal{B} \cap [K, +\infty)$, and then we write $\mathcal{A} \sim \mathcal{B}$.

Definition 4

An infinite set $\mathcal{C}$ of non-negative integers is said to be *totalprimitive* ("totally primitive") if every $\mathcal{C}'$ with $\mathcal{C}' \sim \mathcal{C}$ is primitive.

Ostmann also formulated the following beautiful conjecture:

Conjecture 1

The set $\mathcal{P}$ of the primes *is totalprimitive.*

Definition 2

A finite or infinite set $\mathcal{C}$ of non-negative integers is said to be *reducible* if it has an (additive) 2-decomposition

$$\mathcal{C} = \mathcal{A} + \mathcal{B}, \quad |\mathcal{A}| \geq 2, \quad |\mathcal{B}| \geq 2.$$

If there are no sets $\mathcal{A}$, $\mathcal{B}$ with these properties, then $\mathcal{C}$ is said to be *primitive* (or irreducible).

Definition 3

Two sets $\mathcal{A}$, $\mathcal{B}$ of non-negative integers are said to be *asymptotically equal* if there is a number K such that $\mathcal{A} \cap [K, +\infty) = \mathcal{B} \cap [K, +\infty)$, and then we write $\mathcal{A} \sim \mathcal{B}$.

Definition 4

An infinite set $\mathcal{C}$ of non-negative integers is said to be *totalprimitive* ("totally primitive") if every $\mathcal{C}'$ with $\mathcal{C}' \sim \mathcal{C}$ is primitive.

Ostmann also formulated the following beautiful conjecture:

Conjecture 1

The set $\mathcal{P}$ of the primes *is totalprimitive.*

I met these definitions and conjecture of Ostmann as a second year university student (in 1959) when I joined Paul Turán's seminar. As any new student in his seminar, I got a reading assignment from him: I was to read the first few chapters of Ostmann's book and then to give a survey of these chapters in the seminar. I gave 8-9 talks on this subject, and in the meantime Turán was asking related questions. I wrote a paper as an answer to one of his questions (which appeared in the Acta Arithmetica). Not much later I received the following letter:

"Dear Mr. Sárközy,

I have heard about your nice results on totalprimitive sequences from Paul Turán. Please, come and see me at the Mathematical Institute [of the Hungarian Academy of Sciences].

Paul Erdős"

I met these definitions and conjecture of Ostmann as a second year university student (in 1959) when I joined Paul Turán's seminar. As any new student in his seminar, I got a reading assignment from him: I was to read the first few chapters of Ostmann's book and then to give a survey of these chapters in the seminar. I gave 8-9 talks on this subject, and in the meantime Turán was asking related questions. I wrote a paper as an answer to one of his questions (which appeared in the Acta Arithmetica). Not much later I received the following letter:

"Dear Mr. Sárközy,

I have heard about your nice results on totalprimitive sequences from Paul Turán. Please, come and see me at the Mathematical Institute [of the Hungarian Academy of Sciences].

Paul Erdős"

I met these definitions and conjecture of Ostmann as a second year university student (in 1959) when I joined Paul Turán's seminar. As any new student in his seminar, I got a reading assignment from him: I was to read the first few chapters of Ostmann's book and then to give a survey of these chapters in the seminar. I gave 8-9 talks on this subject, and in the meantime Turán was asking related questions. I wrote a paper as an answer to one of his questions (which appeared in the Acta Arithmetica). Not much later I received the following letter:

"Dear Mr. Sárközy,

I have heard about your nice results on totalprimitive sequences from Paul Turán. Please, come and see me at the Mathematical Institute [of the Hungarian Academy of Sciences].

Paul Erdős"

I visited him soon. I told him my results. We had a nice discussion and he asked a related question (which was sort of converse of the problem asked earlier by Turán). Roughly, this question was: is it true that every “dense” sequence of non-negative integers is reducible? If the answer is affirmative, then how dense a sequence must be to guarantee reducibility? As an answer to this question, I soon published (again in the Acta Arithmetica) my first paper based on an Erdős problem.

This was the first “Uncle Paul session” that I attended, and it was followed by many others. During one of the next sessions Erdős asked the following question: “It is easy to see that the sequence of the squares is totalprimitive. Is it also true that if we change this sequence so that we change $o(\sqrt{n})$ elements up to n then the new sequence must be also totalprimitive?” Szemerédi and I settled this problem nearly completely, and we wrote a joint paper on this problem. Then I introduced Szemerédi to Erdős, and soon we published our first joint triple paper. This was followed by 61 further joint papers with Erdős (including 10 triple papers with Szemerédi).

I visited him soon. I told him my results. We had a nice discussion and he asked a related question (which was sort of converse of the problem asked earlier by Turán). Roughly, this question was: is it true that every "dense" sequence of non-negative integers is reducible? If the answer is affirmative, then how dense a sequence must be to guarantee reducibility? As an answer to this question, I soon published (again in the Acta Arithmetica) my first paper based on an Erdős problem.

This was the first "Uncle Paul session" that I attended, and it was followed by many others. During one of the next sessions Erdős asked the following question: "It is easy to see that the sequence of the squares is totalprimitive. Is it also true that if we change this sequence so that we change $o(\sqrt{n})$ elements up to n then the new sequence must be also totalprimitive?" Szemerédi and I settled this problem nearly completely, and we wrote a joint paper on this problem. Then I introduced Szemerédi to Erdős, and soon we published our first joint triple paper. This was followed by 61 further joint papers with Erdős (including 10 triple papers with Szemerédi).

I visited him soon. I told him my results. We had a nice discussion and he asked a related question (which was sort of converse of the problem asked earlier by Turán). Roughly, this question was: is it true that every "dense" sequence of non-negative integers is reducible? If the answer is affirmative, then how dense a sequence must be to guarantee reducibility? As an answer to this question, I soon published (again in the Acta Arithmetica) my first paper based on an Erdős problem.

This was the first "Uncle Paul session" that I attended, and it was followed by many others. During one of the next sessions Erdős asked the following question: "It is easy to see that the sequence of the squares is totalprimitive. Is it also true that if we change this sequence so that we change $o(\sqrt{n})$ elements up to n then the new sequence must be also totalprimitive?" Szemerédi and I settled this problem nearly completely, and we wrote a joint paper on this problem. Then I introduced Szemerédi to Erdős, and soon we published our first joint triple paper. This was followed by 61 further joint papers with Erdős (including 10 triple papers with Szemerédi).

These early days of my mathematical career explain that when the centennials of Erdős and Turán were approaching I decided to celebrate their centennials by returning to these Ostmann type problems, more precisely, to study *analogous problems in finite fields*.

But first let me complete the survey of the papers written on reducibility and primitivity of infinite sequences of non-negative integers. About 10–15 further papers have been written on questions of this type.

Volkmann, Wirsing and Sárközy estimated the Lebesgue measure, resp. Hausdorff dimension of the point set assigned to reducible sets.

Hornfeck, Hofmann and Wolke, Elsholtz (in 3 papers) and Puchta proved partial results towards Ostmann's Conjecture 1 on the totalprimitivity of the set $\mathcal{P}$ of the primes.

These early days of my mathematical career explain that when the centennials of Erdős and Turán were approaching I decided to celebrate their centennials by returning to these Ostmann type problems, more precisely, to study *analogous problems in finite fields*.

But first let me complete the survey of the papers written on reducibility and primitivity of infinite sequences of non-negative integers. About 10–15 further papers have been written on questions of this type.

Volkmann, Wirsing and Sárközy estimated the Lebesgue measure, resp. Hausdorff dimension of the point set assigned to reducible sets.

Hornfeck, Hofmann and Wolke, Elsholtz (in 3 papers) and Puchta proved partial results towards Ostmann's Conjecture 1 on the totalprimitivity of the set $\mathcal{P}$ of the primes.

These early days of my mathematical career explain that when the centennials of Erdős and Turán were approaching I decided to celebrate their centennials by returning to these Ostmann type problems, more precisely, to study *analogous problems in finite fields*.

But first let me complete the survey of the papers written on reducibility and primitivity of infinite sequences of non-negative integers. About 10–15 further papers have been written on questions of this type.

Volkmann, Wirsing and Sárközy estimated the Lebesgue measure, resp. Hausdorff dimension of the point set assigned to reducible sets.

Hornfeck, Hofmann and Wolke, Elsholtz (in 3 papers) and Puchta proved partial results towards Ostmann's Conjecture 1 on the totalprimitivity of the set $\mathcal{P}$ of the primes.

These early days of my mathematical career explain that when the centennials of Erdős and Turán were approaching I decided to celebrate their centennials by returning to these Ostmann type problems, more precisely, to study *analogous problems in finite fields*.

But first let me complete the survey of the papers written on reducibility and primitivity of infinite sequences of non-negative integers. About 10–15 further papers have been written on questions of this type.

Volkmann, Wirsing and Sárközy estimated the Lebesgue measure, resp. Hausdorff dimension of the point set assigned to reducible sets.

Hornfeck, Hofmann and Wolke, Elsholtz (in 3 papers) and Puchta proved partial results towards Ostmann's Conjecture 1 on the totalprimitivity of the set $\mathcal{P}$ of the primes.

In particular, it has been proved: if there are $\mathcal{P}' \sim \mathcal{P}$ and $\mathcal{A}$, $\mathcal{B}$ with

$$\mathcal{P}' = \mathcal{A} + \mathcal{B}, \qquad |\mathcal{A}|, |\mathcal{B}| \geq 2,$$

then we have

$$\frac{n^{1/2}}{(\log n)^{c_1}} < A(n), B(n) < n^{1/2}(\log n)^{c_2} \quad (\text{for } n > n_0)$$

where $A(n)$, $B(n)$ are the counting functions of $\mathcal{A}$ and $\mathcal{B}$, and c_1, c_2 are positive absolute constants, and Elsholtz also proved:

if

$$\mathcal{P}' \sim \mathcal{P},$$

then there are no $\mathcal{A}$, $\mathcal{B}$, $\mathcal{C}$ with

$$\mathcal{P}' = \mathcal{A} + \mathcal{B} + \mathcal{C}, \qquad |\mathcal{A}|, |\mathcal{B}|, |\mathcal{C}| \geq 2.$$

He also studied *multiplicative* decompositions of the set of the *shifted* primes, i.e., decompositions of the form

$$\mathcal{P}' + \{c\} = \mathcal{A} \cdot \mathcal{B} \quad (\text{with } c \neq 0).$$

In particular, it has been proved: if there are $\mathcal{P}' \sim \mathcal{P}$ and $\mathcal{A}$, $\mathcal{B}$ with

$$\mathcal{P}' = \mathcal{A} + \mathcal{B}, \qquad |\mathcal{A}|, |\mathcal{B}| \geq 2,$$

then we have

$$\frac{n^{1/2}}{(\log n)^{c_1}} < A(n), B(n) < n^{1/2}(\log n)^{c_2} \quad (\text{for } n > n_0)$$

where $A(n)$, $B(n)$ are the counting functions of $\mathcal{A}$ and $\mathcal{B}$, and c_1, c_2 are positive absolute constants, and Elsholtz also proved:

if

$$\mathcal{P}' \sim \mathcal{P},$$

then there are no $\mathcal{A}$, $\mathcal{B}$, $\mathcal{C}$ with

$$\mathcal{P}' = \mathcal{A} + \mathcal{B} + \mathcal{C}, \qquad |\mathcal{A}|, |\mathcal{B}|, |\mathcal{C}| \geq 2.$$

He also studied *multiplicative* decompositions of the set of the *shifted* primes, i.e., decompositions of the form

$$\mathcal{P}' + \{c\} = \mathcal{A} \cdot \mathcal{B} \quad (\text{with } c \neq 0).$$

In particular, it has been proved: if there are $\mathcal{P}' \sim \mathcal{P}$ and $\mathcal{A}$, $\mathcal{B}$ with

$$\mathcal{P}' = \mathcal{A} + \mathcal{B}, \qquad |\mathcal{A}|, |\mathcal{B}| \geq 2,$$

then we have

$$\frac{n^{1/2}}{(\log n)^{c_1}} < A(n), B(n) < n^{1/2}(\log n)^{c_2} \quad (\text{for } n > n_0)$$

where $A(n)$, $B(n)$ are the counting functions of $\mathcal{A}$ and $\mathcal{B}$, and c_1, c_2 are positive absolute constants, and Elsholtz also proved:

if

$$\mathcal{P}' \sim \mathcal{P},$$

then there are no $\mathcal{A}$, $\mathcal{B}$, $\mathcal{C}$ with

$$\mathcal{P}' = \mathcal{A} + \mathcal{B} + \mathcal{C}, \qquad |\mathcal{A}|, |\mathcal{B}|, |\mathcal{C}| \geq 2.$$

He also studied *multiplicative* decompositions of the set of the *shifted* primes, i.e., decompositions of the form

$$\mathcal{P}' + \{c\} = \mathcal{A} \cdot \mathcal{B} \quad (\text{with } c \neq 0).$$

2. On additive decompositions of the set of the quadratic residues modulo p

First (inspired partly by Erdős' problem and our result with Szemerédi on the sequence of squares) I formulated and studied the following conjecture (Acta Arithmetica, 2012):

Conjecture 2

For a prime p let $\mathcal{Q} = \mathcal{Q}(p)$ denote the set of the quadratic residues *modulo p. If p is large enough then $\mathcal{Q} = \mathcal{Q}(p)$ is* primitive, *i.e., it has no 2-decomposition.*

It turned out that here the situation is similar to Ostmann's conjecture: the conjecture seems to be beyond reach but I proved partial results similar to the results proved (by Elsholtz and others) in connection with Ostmann's conjecture.

2. On additive decompositions of the set of the quadratic residues modulo p

First (inspired partly by Erdős' problem and our result with Szemerédi on the sequence of squares) I formulated and studied the following conjecture (Acta Arithmetica, 2012):

Conjecture 2

For a prime p let $\mathcal{Q} = \mathcal{Q}(p)$ denote the set of the quadratic residues *modulo p. If p is large enough then $\mathcal{Q} = \mathcal{Q}(p)$ is* primitive, *i.e., it has no 2-decomposition.*

It turned out that here the situation is similar to Ostmann's conjecture: the conjecture seems to be beyond reach but I proved partial results similar to the results proved (by Elsholtz and others) in connection with Ostmann's conjecture.

2. On additive decompositions of the set of the quadratic residues modulo p

First (inspired partly by Erdős' problem and our result with Szemerédi on the sequence of squares) I formulated and studied the following conjecture (Acta Arithmetica, 2012):

Conjecture 2

For a prime p let $\mathcal{Q} = \mathcal{Q}(p)$ denote the set of the quadratic residues *modulo p. If p is large enough then $\mathcal{Q} = \mathcal{Q}(p)$ is* primitive, *i.e., it has no* 2*-decomposition.*

It turned out that here the situation is similar to Ostmann's conjecture: the conjecture seems to be beyond reach but I proved partial results similar to the results proved (by Elsholtz and others) in connection with Ostmann's conjecture.

First I proved

Theorem 1

If p is a prime large enough and

$$\mathcal{U}+\mathcal{V}=\mathcal{Q}$$

is a 2-decomposition *of $\mathcal{Q}=\mathcal{Q}(p)$, then we have*

$$\frac{1}{3}\frac{p^{1/2}}{\log p}<|\mathcal{U}|,|\mathcal{V}|<p^{1/2}\log p.$$

The crucial tool in the proof of Theorem 1 was Weil's theorem (on the estimate of character sums).

Next I proved

Theorem 2

If p is a prime large enough then $\mathcal{Q}=\mathcal{Q}(p)$ has no 3-decomposition

$$\mathcal{A}+\mathcal{B}+\mathcal{C}=\mathcal{Q}.$$

This theorem can be derived easily from Theorem 1 by using a result of Ruzsa:

If $\mathcal{X}$, $\mathcal{Y}$, $\mathcal{Z}$ are finite sets in a commutative group, then (using additive notation for the group operation) we have

$$|\mathcal{X}+\mathcal{Y}+\mathcal{Z}|^2\leq|\mathcal{X}+\mathcal{Y}|\,|\mathcal{Y}+\mathcal{Z}|\,|\mathcal{X}+\mathcal{Z}|.$$

First I proved

Theorem 1

If p is a prime large enough and

$$\mathcal{U}+\mathcal{V}=\mathcal{Q}$$

is a 2-decomposition *of $\mathcal{Q}=\mathcal{Q}(p)$, then we have*

$$\frac{1}{3}\frac{p^{1/2}}{\log p}<|\mathcal{U}|,|\mathcal{V}|<p^{1/2}\log p.$$

The crucial tool in the proof of Theorem 1 was Weil's theorem (on the estimate of character sums).

Next I proved

Theorem 2

If p is a prime large enough then $\mathcal{Q}=\mathcal{Q}(p)$ has no 3-decomposition

$$\mathcal{A}+\mathcal{B}+\mathcal{C}=\mathcal{Q}.$$

This theorem can be derived easily from Theorem 1 by using a result of Ruzsa:

If $\mathcal{X}$, $\mathcal{Y}$, $\mathcal{Z}$ are finite sets in a commutative group, then (using additive notation for the group operation) we have

$$|\mathcal{X}+\mathcal{Y}+\mathcal{Z}|^2\leq|\mathcal{X}+\mathcal{Y}|\,|\mathcal{Y}+\mathcal{Z}|\,|\mathcal{X}+\mathcal{Z}|.$$

First I proved

Theorem 1

If p is a prime large enough and

$$\mathcal{U}+\mathcal{V}=\mathcal{Q}$$

is a 2-decomposition *of $\mathcal{Q}=\mathcal{Q}(p)$, then we have*

$$\frac{1}{3}\frac{p^{1/2}}{\log p}<|\mathcal{U}|,|\mathcal{V}|<p^{1/2}\log p.$$

The crucial tool in the proof of Theorem 1 was Weil's theorem (on the estimate of character sums).

Next I proved

Theorem 2

If p is a prime large enough then $\mathcal{Q}=\mathcal{Q}(p)$ has no 3-decomposition

$$\mathcal{A}+\mathcal{B}+\mathcal{C}=\mathcal{Q}.$$

This theorem can be derived easily from Theorem 1 by using a result of Ruzsa:

If $\mathcal{X}$, $\mathcal{Y}$, $\mathcal{Z}$ are finite sets in a commutative group, then (using additive notation for the group operation) we have

$$|\mathcal{X}+\mathcal{Y}+\mathcal{Z}|^2\leq|\mathcal{X}+\mathcal{Y}|\,|\mathcal{Y}+\mathcal{Z}|\,|\mathcal{X}+\mathcal{Z}|.$$

First I proved

Theorem 1

If p is a prime large enough and

$$\mathcal{U} + \mathcal{V} = \mathcal{Q}$$

is a 2-decomposition *of $\mathcal{Q} = \mathcal{Q}(p)$, then we have*

$$\frac{1}{3} \frac{p^{1/2}}{\log p} < |\mathcal{U}|, |\mathcal{V}| < p^{1/2} \log p.$$

The crucial tool in the proof of Theorem 1 was Weil's theorem (on the estimate of character sums).

Next I proved

Theorem 2

If p is a prime large enough then $\mathcal{Q} = \mathcal{Q}(p)$ has no 3-decomposition

$$\mathcal{A} + \mathcal{B} + \mathcal{C} = \mathcal{Q}.$$

This theorem can be derived easily from Theorem 1 by using a result of Ruzsa:

If $\mathcal{X}$, $\mathcal{Y}$, $\mathcal{Z}$ are finite sets in a commutative group, then (using additive notation for the group operation) we have

$$|\mathcal{X} + \mathcal{Y} + \mathcal{Z}|^2 \leq |\mathcal{X} + \mathcal{Y}| \, |\mathcal{Y} + \mathcal{Z}| \, |\mathcal{X} + \mathcal{Z}|.$$

Recently Shkredov and Shparlinski have improved independently on Theorem 1: they proved that it follows from the same assumptions that

$$c_1 p^{1/2} < |\mathcal{U}|, |\mathcal{V}| < c_2 p^{1/2}$$

with some positive absolute constants $c_1 < 1$, $c_2 > 1$.

They used different approach: They used the fact that $\mathcal{Q}$ is a subgroup of the multiplicative group of $\mathbb{F}_p^*$. Shparlinski also proved similar results on additive 2-decompositions of other multiplicative subgroups $\mathcal{G}$ of $\mathbb{F}_p^*$.

While their methods use more special properties of the quadratic residues and thus they give sharper estimates, my method gives slightly weaker estimates but, on the other hand, it has the advantage that it also works in more general situations, e.g., it can be also used for studying additive properties of polynomial sets $\left\{ f(x^d) : \ x \in \mathbb{F}_p \right\}$ where f is a permutation polynomial.

For a set $\mathcal{A}$ write $\mathcal{A}\hat{+}\mathcal{A} = \{a + a' : \ a, a' \in \mathcal{A}, \ a \neq a'\}$. Shkredov also determined all the primes p for which $Q = Q(p)$ has a special additive decomposition of the form $\mathcal{A} + \mathcal{A}$ or $\mathcal{A}\hat{+}\mathcal{A}$.

Recently Shkredov and Shparlinski have improved independently on Theorem 1: they proved that it follows from the same assumptions that

$$c_1 p^{1/2} < |\mathcal{U}|, |\mathcal{V}| < c_2 p^{1/2}$$

with some positive absolute constants $c_1 < 1$, $c_2 > 1$.

They used different approach: They used the fact that $\mathcal{Q}$ is a subgroup of the multiplicative group of $\mathbb{F}_p^*$. Shparlinski also proved similar results on additive 2-decompositions of other multiplicative subgroups $\mathcal{G}$ of $\mathbb{F}_p^*$.

While their methods use more special properties of the quadratic residues and thus they give sharper estimates, my method gives slightly weaker estimates but, on the other hand, it has the advantage that it also works in more general situations, e.g., it can be also used for studying additive properties of polynomial sets $\left\{ f(x^d) : \ x \in \mathbb{F}_p \right\}$ where f is a permutation polynomial.

For a set $\mathcal{A}$ write $\mathcal{A} \hat{+} \mathcal{A} = \{a + a' : \ a, a' \in \mathcal{A}, \ a \neq a'\}$. Shkredov also determined all the primes p for which $Q = Q(p)$ has a special additive decomposition of the form $\mathcal{A} + \mathcal{A}$ or $\mathcal{A} \hat{+} \mathcal{A}$.

Recently Shkredov and Shparlinski have improved independently on Theorem 1: they proved that it follows from the same assumptions that

$$c_1 p^{1/2} < |\mathcal{U}|, |\mathcal{V}| < c_2 p^{1/2}$$

with some positive absolute constants $c_1 < 1$, $c_2 > 1$.

They used different approach: They used the fact that $\mathcal{Q}$ is a subgroup of the multiplicative group of $\mathbb{F}_p^*$. Shparlinski also proved similar results on additive 2-decompositions of other multiplicative subgroups $\mathcal{G}$ of $\mathbb{F}_p^*$.

While their methods use more special properties of the quadratic residues and thus they give sharper estimates, my method gives slightly weaker estimates but, on the other hand, it has the advantage that it also works in more general situations, e.g., it can be also used for studying additive properties of polynomial sets $\left\{ f(x^d) : \ x \in \mathbb{F}_p \right\}$ where f is a permutation polynomial.

For a set $\mathcal{A}$ write $\mathcal{A}\hat{+}\mathcal{A} = \{a + a' : \ a, a' \in \mathcal{A}, \ a \neq a'\}$. Shkredov also determined all the primes p for which $Q = Q(p)$ has a special additive decomposition of the form $\mathcal{A} + \mathcal{A}$ or $\mathcal{A}\hat{+}\mathcal{A}$.

Recently Shkredov and Shparlinski have improved independently on Theorem 1: they proved that it follows from the same assumptions that

$$c_1 p^{1/2} < |\mathcal{U}|, |\mathcal{V}| < c_2 p^{1/2}$$

with some positive absolute constants $c_1 < 1$, $c_2 > 1$.

They used different approach: They used the fact that $\mathcal{Q}$ is a subgroup of the multiplicative group of $\mathbb{F}_p^*$. Shparlinski also proved similar results on additive 2-decompositions of other multiplicative subgroups $\mathcal{G}$ of $\mathbb{F}_p^*$.

While their methods use more special properties of the quadratic residues and thus they give sharper estimates, my method gives slightly weaker estimates but, on the other hand, it has the advantage that it also works in more general situations, e.g., it can be also used for studying additive properties of polynomial sets $\left\{ f(x^d) : \ x \in \mathbb{F}_p \right\}$ where f is a permutation polynomial.

For a set $\mathcal{A}$ write $\mathcal{A}\hat{+}\mathcal{A} = \{a + a' : \ a, a' \in \mathcal{A}, \ a \neq a'\}$. Shkredov also determined all the primes p for which $Q = Q(p)$ has a special additive decomposition of the form $\mathcal{A} + \mathcal{A}$ or $\mathcal{A}\hat{+}\mathcal{A}$.

3. On additive decompositions of the set of the primitive roots modulo p

In a joint paper (Monatshefte Math., 2013) with C. Dartyge we studied the set $\mathcal{G}(p) = \{g : \ g \in \mathbb{F}_p, \ g$ is a *primitive root* modulo $p\}$. We conjectured:

Conjecture 3

If $p > p_0$ then $\mathcal{G} = \mathcal{G}(p)$ is primitive *(i.e., it has no 2-decomposition).*

Again, the conjecture seems to be beyond reach but we proved partial results similar to the results proved in case of the quadratic residues:

Theorem 3

If p is a prime large enough and

$$\mathcal{U} + \mathcal{V} = \mathcal{G}$$

is a 2-decomposition of $\mathcal{G} = \mathcal{G}(p)$, then we have

$$\frac{\varphi(p-1)}{\tau(p-1)p^{1/2}\log p} < |\mathcal{U}|, |\mathcal{V}| < \tau(p-1)p^{1/2}\log p$$

where $\varphi(n)$ is Euler's function and $\tau(n)$ denotes the divisor function.

3. On additive decompositions of the set of the primitive roots modulo p

In a joint paper (Monatshefte Math., 2013) with C. Dartyge we studied the set $\mathcal{G}(p) = \{g : \ g \in \mathbb{F}_p,\, g$ is a *primitive root* modulo $p\}$. We conjectured:

Conjecture 3

If $p > p_0$ then $\mathcal{G} = \mathcal{G}(p)$ is primitive *(i.e., it has no 2-decomposition).*

Again, the conjecture seems to be beyond reach but we proved partial results similar to the results proved in case of the quadratic residues:

Theorem 3

If p is a prime large enough and

$$\mathcal{U} + \mathcal{V} = \mathcal{G}$$

is a 2-decomposition of $\mathcal{G} = \mathcal{G}(p)$, then we have

$$\frac{\varphi(p-1)}{\tau(p-1)p^{1/2}\log p} < |\mathcal{U}|, |\mathcal{V}| < \tau(p-1)p^{1/2}\log p$$

where $\varphi(n)$ is Euler's function and $\tau(n)$ denotes the divisor function.

3. On additive decompositions of the set of the primitive roots modulo p

In a joint paper (Monatshefte Math., 2013) with C. Dartyge we studied the set $\mathcal{G}(p) = \{g : \ g \in \mathbb{F}_p, \, g$ is a *primitive root* modulo $p\}$. We conjectured:

Conjecture 3

If $p > p_0$ then $\mathcal{G} = \mathcal{G}(p)$ is primitive *(i.e., it has no 2-decomposition).*

Again, the conjecture seems to be beyond reach but we proved partial results similar to the results proved in case of the quadratic residues:

Theorem 3

If p is a prime large enough and

$$\mathcal{U} + \mathcal{V} = \mathcal{G}$$

is a 2-decomposition of $\mathcal{G} = \mathcal{G}(p)$, then we have

$$\frac{\varphi(p-1)}{\tau(p-1)p^{1/2}\log p} < |\mathcal{U}|, |\mathcal{V}| < \tau(p-1)p^{1/2}\log p$$

where $\varphi(n)$ is Euler's function and $\tau(n)$ denotes the divisor function.

3. On additive decompositions of the set of the primitive roots modulo p

In a joint paper (Monatshefte Math., 2013) with C. Dartyge we studied the set $\mathcal{G}(p) = \{g : \ g \in \mathbb{F}_p,\ g$ is a *primitive root* modulo $p\}$. We conjectured:

Conjecture 3

If $p > p_0$ then $\mathcal{G} = \mathcal{G}(p)$ is primitive *(i.e., it has no 2-decomposition).*

Again, the conjecture seems to be beyond reach but we proved partial results similar to the results proved in case of the quadratic residues:

Theorem 3

If p is a prime large enough and

$$\mathcal{U} + \mathcal{V} = \mathcal{G}$$

is a 2-decomposition of $\mathcal{G} = \mathcal{G}(p)$, then we have

$$\frac{\varphi(p-1)}{\tau(p-1)p^{1/2}\log p} < |\mathcal{U}|, |\mathcal{V}| < \tau(p-1)p^{1/2}\log p$$

where $\varphi(n)$ is Euler's function and $\tau(n)$ denotes the divisor function.

The crucial tool in our proof was an estimate (based on Weil's theorem) for sums $\sum_{g \in \mathcal{G}} \chi(f(g))$, where χ is a multiplicative character, $f(x) \in \mathbb{F}_p[x]$, and we used some ideas from my paper on the quadratic residues, but we also needed some further ideas.

From the last theorem we derived (using again Ruzsa's theorem):

Theorem 4

If p is large enough then $\mathcal{G}$ has no 3-decomposition

$$\mathcal{A} + \mathcal{B} + \mathcal{C} = \mathcal{G}.$$

Recently Shparlinski has improved on Theorem 3 by removing the factors $\tau(p-1)$ and $\log p$ apart from constant factors: under the assumptions of Theorem 3 we have

$$c_1 \frac{\varphi(p-1)}{p^{1/2}} < |\mathcal{U}|, |\mathcal{V}| < c_2 p^{1/2}.$$

The crucial tool in our proof was an estimate (based on Weil's theorem) for sums $\sum\limits_{g\in\mathcal{G}}\chi(f(g))$, where χ is a multiplicative character, $f(x)\in\mathbb{F}_p[x]$, and we used some ideas from my paper on the quadratic residues, but we also needed some further ideas.

From the last theorem we derived (using again Ruzsa's theorem):

Theorem 4

If p is large enough then $\mathcal{G}$ has no 3-decomposition

$$\mathcal{A}+\mathcal{B}+\mathcal{C}=\mathcal{G}.$$

Recently Shparlinski has improved on Theorem 3 by removing the factors $\tau(p-1)$ and $\log p$ apart from constant factors: under the assumptions of Theorem 3 we have

$$c_1\frac{\varphi(p-1)}{p^{1/2}}<|\mathcal{U}|,|\mathcal{V}|<c_2p^{1/2}.$$

The crucial tool in our proof was an estimate (based on Weil's theorem) for sums $\sum_{g \in \mathcal{G}} \chi(f(g))$, where χ is a multiplicative character, $f(x) \in \mathbb{F}_p[x]$, and we used some ideas from my paper on the quadratic residues, but we also needed some further ideas.

From the last theorem we derived (using again Ruzsa's theorem):

Theorem 4

If p is large enough then $\mathcal{G}$ has no 3-decomposition

$$\mathcal{A} + \mathcal{B} + \mathcal{C} = \mathcal{G}.$$

Recently Shparlinski has improved on Theorem 3 by removing the factors $\tau(p-1)$ and $\log p$ apart from constant factors: under the assumptions of Theorem 3 we have

$$c_1 \frac{\varphi(p-1)}{p^{1/2}} < |\mathcal{U}|, |\mathcal{V}| < c_2 p^{1/2}.$$

The crucial tool in our proof was an estimate (based on Weil's theorem) for sums $\sum_{g\in\mathcal{G}}\chi(f(g))$, where χ is a multiplicative character, $f(x)\in\mathbb{F}_p[x]$, and we used some ideas from my paper on the quadratic residues, but we also needed some further ideas.

From the last theorem we derived (using again Ruzsa's theorem):

Theorem 4

If p is large enough then $\mathcal{G}$ has no 3-decomposition

$$\mathcal{A}+\mathcal{B}+\mathcal{C}=\mathcal{G}.$$

Recently Shparlinski has improved on Theorem 3 by removing the factors $\tau(p-1)$ and $\log p$ apart from constant factors: under the assumptions of Theorem 3 we have

$$c_1\frac{\varphi(p-1)}{p^{1/2}}<|\mathcal{U}|,|\mathcal{V}|<c_2p^{1/2}.$$

4. On multiplicative decompositions of the set of the shifted quadratic residues modulo p

In Theorems 1 and 2 I studied *additive* 2- and 3-decompositions of the set $\mathcal{Q} = \{x^2 : \ x \in \mathbb{F}_p^*\}$. One might like to study the *multiplicative* analogues of these results by considering (non-trivial) 2- and 3-decompositions $\mathcal{A} \cdot \mathcal{B}$, resp. $\mathcal{A} \cdot \mathcal{B} \cdot \mathcal{C}$ with $|\mathcal{A}|$, $|\mathcal{B}|$, $|\mathcal{C}| \geq 2$. However, some caution is needed:

First, if $p > 3$, then clearly

$$\mathcal{Q} = \mathcal{Q} \cdot \mathcal{Q}$$

is a (non-trivial) multiplicative 2-decomposition of $\mathcal{Q}$. Thus to make the problem non-trivial we have to replace $\mathcal{Q}$ by $\mathcal{Q} + c$ (with $c \neq 0$).

Next, observe that if $\mathcal{A} \subset \mathbb{F}_p$, $0 \in \mathcal{A}$ and $|\mathcal{A}| \geq 2$, then

$$\mathcal{A} = \{0, 1\} \cdot \mathcal{A}$$

is a non-trivial 2-decomposition of $\mathcal{A}$; thus we have to remove 0 from $\mathcal{Q} + c$. In a recent paper (to appear in the Turán memorial volume) I formulated the conjecture that there are no further exemptions, more precisely,

4. On multiplicative decompositions of the set of the shifted quadratic residues modulo p

In Theorems 1 and 2 I studied *additive* 2- and 3-decompositions of the set $\mathcal{Q} = \{x^2 : \ x \in \mathbb{F}_p^*\}$. One might like to study the *multiplicative* analogues of these results by considering (non-trivial) 2- and 3-decompositions $\mathcal{A} \cdot \mathcal{B}$, resp. $\mathcal{A} \cdot \mathcal{B} \cdot \mathcal{C}$ with $|\mathcal{A}|$, $|\mathcal{B}|$, $|\mathcal{C}| \geq 2$. However, some caution is needed:

First, if $p > 3$, then clearly

$$\mathcal{Q} = \mathcal{Q} \cdot \mathcal{Q}$$

is a (non-trivial) multiplicative 2-decomposition of $\mathcal{Q}$. Thus to make the problem non-trivial we have to replace $\mathcal{Q}$ by $\mathcal{Q} + c$ (with $c \neq 0$).

Next, observe that if $\mathcal{A} \subset \mathbb{F}_p$, $0 \in \mathcal{A}$ and $|\mathcal{A}| \geq 2$, then

$$\mathcal{A} = \{0, 1\} \cdot \mathcal{A}$$

is a non-trivial 2-decomposition of $\mathcal{A}$; thus we have to remove 0 from $\mathcal{Q} + c$. In a recent paper (to appear in the Turán memorial volume) I formulated the conjecture that there are no further exemptions, more precisely,

4. On multiplicative decompositions of the set of the shifted quadratic residues modulo p

In Theorems 1 and 2 I studied *additive* 2- and 3-decompositions of the set $\mathcal{Q} = \{x^2 : \ x \in \mathbb{F}_p^*\}$. One might like to study the *multiplicative* analogues of these results by considering (non-trivial) 2- and 3-decompositions $\mathcal{A} \cdot \mathcal{B}$, resp. $\mathcal{A} \cdot \mathcal{B} \cdot \mathcal{C}$ with $|\mathcal{A}|$, $|\mathcal{B}|$, $|\mathcal{C}| \geq 2$. However, some caution is needed:

First, if $p > 3$, then clearly

$$\mathcal{Q} = \mathcal{Q} \cdot \mathcal{Q}$$

is a (non-trivial) multiplicative 2-decomposition of $\mathcal{Q}$. Thus to make the problem non-trivial we have to replace $\mathcal{Q}$ by $\mathcal{Q} + c$ (with $c \neq 0$).

Next, observe that if $\mathcal{A} \subset \mathbb{F}_p$, $0 \in \mathcal{A}$ and $|\mathcal{A}| \geq 2$, then

$$\mathcal{A} = \{0, 1\} \cdot \mathcal{A}$$

is a non-trivial 2-decomposition of $\mathcal{A}$; thus we have to remove 0 from $\mathcal{Q} + c$. In a recent paper (to appear in the Turán memorial volume) I formulated the conjecture that there are no further exemptions, more precisely,

4. On multiplicative decompositions of the set of the shifted quadratic residues modulo p

In Theorems 1 and 2 I studied *additive* 2- and 3-decompositions of the set $\mathcal{Q} = \{x^2 : \ x \in \mathbb{F}_p^*\}$. One might like to study the *multiplicative* analogues of these results by considering (non-trivial) 2- and 3-decompositions $\mathcal{A} \cdot \mathcal{B}$, resp. $\mathcal{A} \cdot \mathcal{B} \cdot \mathcal{C}$ with $|\mathcal{A}|$, $|\mathcal{B}|$, $|\mathcal{C}| \geq 2$. However, some caution is needed:

First, if $p > 3$, then clearly

$$\mathcal{Q} = \mathcal{Q} \cdot \mathcal{Q}$$

is a (non-trivial) multiplicative 2-decomposition of $\mathcal{Q}$. Thus to make the problem non-trivial we have to replace $\mathcal{Q}$ by $\mathcal{Q} + c$ (with $c \neq 0$).

Next, observe that if $\mathcal{A} \subset \mathbb{F}_p$, $0 \in \mathcal{A}$ and $|\mathcal{A}| \geq 2$, then

$$\mathcal{A} = \{0, 1\} \cdot \mathcal{A}$$

is a non-trivial 2-decomposition of $\mathcal{A}$; thus we have to remove 0 from $\mathcal{Q} + c$. In a recent paper (to appear in the Turán memorial volume) I formulated the conjecture that there are no further exemptions, more precisely,

Conjecture 4

If $c \neq 0$, and we write

$$\mathcal{Q}_c = \mathcal{Q} + \{c\} = \left\{x^2 + c : \ x \in \mathbb{F}_p^*\right\}$$

and

$$\mathcal{Q}'_c = \mathcal{Q}_c \setminus \{0\},$$

then the set $\mathcal{Q}'_c$ has no non-trivial multiplicative 2-decomposition.

Again, this conjecture seems to be beyond reach, however, I proved partial results similar to Theorems 1 and 2 proved in the case of additive decompositions of $\mathcal{Q}$:

Theorem 5

If p is large enough, $c \in \mathbb{F}_p$, $c \neq 0$ and

$$\mathcal{U} \cdot \mathcal{V} = \mathcal{Q}'_c$$

is a (non-trivial) multiplicative 2-decomposition of $\mathcal{Q}'_c$, then we have

$$\frac{1}{3}\frac{p^{1/2}}{\log p} < |\mathcal{U}|, |\mathcal{V}| < p^{1/2}\log p.$$

Conjecture 4

If $c \neq 0$, and we write

$$\mathcal{Q}_c = \mathcal{Q} + \{c\} = \left\{x^2 + c : \ x \in \mathbb{F}_p^*\right\}$$

and

$$\mathcal{Q}'_c = \mathcal{Q}_c \setminus \{0\},$$

then the set $\mathcal{Q}'_c$ has no non-trivial multiplicative 2-decomposition.

Again, this conjecture seems to be beyond reach, however, I proved partial results similar to Theorems 1 and 2 proved in the case of additive decompositions of $\mathcal{Q}$:

Theorem 5

If p is large enough, $c \in \mathbb{F}_p$, $c \neq 0$ and

$$\mathcal{U} \cdot \mathcal{V} = \mathcal{Q}'_c$$

is a (non-trivial) multiplicative 2-decomposition of $\mathcal{Q}'_c$, then we have

$$\frac{1}{3}\frac{p^{1/2}}{\log p} < |\mathcal{U}|, |\mathcal{V}| < p^{1/2} \log p.$$

Conjecture 4

If $c \neq 0$, and we write

$$\mathcal{Q}_c = \mathcal{Q} + \{c\} = \left\{x^2 + c : \ x \in \mathbb{F}_p^*\right\}$$

and

$$\mathcal{Q}'_c = \mathcal{Q}_c \setminus \{0\},$$

then the set $\mathcal{Q}'_c$ has no non-trivial multiplicative 2-decomposition.

Again, this conjecture seems to be beyond reach, however, I proved partial results similar to Theorems 1 and 2 proved in the case of additive decompositions of $\mathcal{Q}$:

Theorem 5

If p is large enough, $c \in \mathbb{F}_p$, $c \neq 0$ and

$$\mathcal{U} \cdot \mathcal{V} = \mathcal{Q}'_c$$

is a (non-trivial) multiplicative 2-decomposition of $\mathcal{Q}'_c$, then we have

$$\frac{1}{3}\frac{p^{1/2}}{\log p} < |\mathcal{U}|, |\mathcal{V}| < p^{1/2}\log p.$$

Conjecture 4

If $c \neq 0$, and we write

$$\mathcal{Q}_c = \mathcal{Q} + \{c\} = \left\{x^2 + c : \ x \in \mathbb{F}_p^*\right\}$$

and

$$\mathcal{Q}'_c = \mathcal{Q}_c \setminus \{0\},$$

then the set $\mathcal{Q}'_c$ has no non-trivial multiplicative 2-decomposition.

Again, this conjecture seems to be beyond reach, however, I proved partial results similar to Theorems 1 and 2 proved in the case of additive decompositions of $\mathcal{Q}$:

Theorem 5

If p is large enough, $c \in \mathbb{F}_p$, $c \neq 0$ and

$$\mathcal{U} \cdot \mathcal{V} = \mathcal{Q}'_c$$

is a (non-trivial) multiplicative 2-decomposition of $\mathcal{Q}'_c$, then we have

$$\frac{1}{3} \frac{p^{1/2}}{\log p} < |\mathcal{U}|, |\mathcal{V}| < p^{1/2} \log p.$$

Theorem 6

If p is large enough, $c \in \mathbb{F}_p$ and $c \neq 0$ then $\mathcal{Q}'_c$ has no nontrivial multiplicative 3*-decomposition*

$$\mathcal{A} \cdot \mathcal{B} \cdot \mathcal{C} = \mathcal{Q}'_c.$$

The tools used in this paper are the same as in the additive case (Weil's theorem on the estimate of character sums and Ruzsa's lemma on sumsets). However, some new ideas are also needed and, in particular, the special role of the number 0 leads to certain complications.

Shparlinski also studied *multiplicative* 2-decompositions of sets of form $\{m+1, m+2, \ldots, m+n\} \subset \mathbb{F}_p^*$.

Theorem 6

If p is large enough, $c \in \mathbb{F}_p$ and $c \neq 0$ then $\mathcal{Q}'_c$ has no nontrivial multiplicative 3-decomposition

$$\mathcal{A} \cdot \mathcal{B} \cdot \mathcal{C} = \mathcal{Q}'_c.$$

The tools used in this paper are the same as in the additive case (Weil's theorem on the estimate of character sums and Ruzsa's lemma on sumsets). However, some new ideas are also needed and, in particular, the special role of the number 0 leads to certain complications.

Shparlinski also studied *multiplicative* 2-decompositions of sets of form $\{m+1, m+2, \ldots, m+n\} \subset \mathbb{F}_p^*$.

Theorem 6

If p is large enough, $c \in \mathbb{F}_p$ and $c \neq 0$ then $\mathcal{Q}'_c$ has no nontrivial multiplicative 3-decomposition

$$\mathcal{A} \cdot \mathcal{B} \cdot \mathcal{C} = \mathcal{Q}'_c.$$

The tools used in this paper are the same as in the additive case (Weil's theorem on the estimate of character sums and Ruzsa's lemma on sumsets). However, some new ideas are also needed and, in particular, the special role of the number 0 leads to certain complications.

Shparlinski also studied *multiplicative* 2-decompositions of sets of form $\{m+1, m+2, \dots, m+n\} \subset \mathbb{F}_p^*$.

Theorem 6

If p is large enough, $c \in \mathbb{F}_p$ and $c \neq 0$ then $\mathcal{Q}'_c$ has no nontrivial multiplicative 3*-decomposition*

$$\mathcal{A} \cdot \mathcal{B} \cdot \mathcal{C} = \mathcal{Q}'_c.$$

The tools used in this paper are the same as in the additive case (Weil's theorem on the estimate of character sums and Ruzsa's lemma on sumsets). However, some new ideas are also needed and, in particular, the special role of the number 0 leads to certain complications.

Shparlinski also studied *multiplicative* 2-decompositions of sets of form $\{m+1, m+2, \ldots, m+n\} \subset \mathbb{F}_p^*$.

5. On the reducibility of large subsets of $\mathbb{F}_p$

I mentioned my early papers answering the questions of Turán and Erdős on the reducibility of dense sets of non-negative integers. In a recent joint paper with K. Gyarmati and S. Konyagin (Journal of Number Theory, 2013) we studied the finite analogues of these old results of mine: we estimated *the cardinality $f(p)$ of the largest primitive subset of $\mathbb{F}_p$.*

Note that Green, Gowers and Green, and Alon studied a closely related problem: they studied representations of large subsets $\mathcal{C}$ of $\mathbb{F}_p$ in form

$$\mathcal{A} + \mathcal{A} = \mathcal{C}.$$

Let $g(p)$ denote the cardinality of the largest subset $\mathcal{C}$ of $\mathbb{F}_p$ which cannot be represented in this form. Clearly $f(p) \leq g(p)$. Improving on results of Gowers and Green, Alon proved that

$$p - c_1 \frac{p^{2/3}}{(\log p)^{1/3}} < g(p) < p - c_2 \frac{p^{1/2}}{\log p}.$$

By $f(p) \leq g(p)$ it follows from the upper bound here that

$$f(p) < p - c_2 \frac{p^{1/2}}{\log p}. \qquad (2)$$

5. On the reducibility of large subsets of $\mathbb{F}_p$

I mentioned my early papers answering the questions of Turán and Erdős on the reducibility of dense sets of non-negative integers. In a recent joint paper with K. Gyarmati and S. Konyagin (Journal of Number Theory, 2013) we studied the finite analogues of these old results of mine: we estimated *the cardinality $f(p)$ of the largest primitive subset of $\mathbb{F}_p$.*

Note that Green, Gowers and Green, and Alon studied a closely related problem: they studied representations of large subsets $\mathcal{C}$ of $\mathbb{F}_p$ in form

$$\mathcal{A} + \mathcal{A} = \mathcal{C}.$$

Let $g(p)$ denote the cardinality of the largest subset $\mathcal{C}$ of $\mathbb{F}_p$ which cannot be represented in this form. Clearly $f(p) \leq g(p)$. Improving on results of Gowers and Green, Alon proved that

$$p - c_1 \frac{p^{2/3}}{(\log p)^{1/3}} < g(p) < p - c_2 \frac{p^{1/2}}{\log p}.$$

By $f(p) \leq g(p)$ it follows from the upper bound here that

$$f(p) < p - c_2 \frac{p^{1/2}}{\log p}. \tag{2}$$

5. On the reducibility of large subsets of $\mathbb{F}_p$

I mentioned my early papers answering the questions of Turán and Erdős on the reducibility of dense sets of non-negative integers. In a recent joint paper with K. Gyarmati and S. Konyagin (Journal of Number Theory, 2013) we studied the finite analogues of these old results of mine: we estimated *the cardinality $f(p)$ of the largest primitive subset of $\mathbb{F}_p$.*

Note that Green, Gowers and Green, and Alon studied a closely related problem: they studied representations of large subsets $\mathcal{C}$ of $\mathbb{F}_p$ in form

$$\mathcal{A} + \mathcal{A} = \mathcal{C}.$$

Let $g(p)$ denote the cardinality of the largest subset $\mathcal{C}$ of $\mathbb{F}_p$ which cannot be represented in this form. Clearly $f(p) \le g(p)$. Improving on results of Gowers and Green, Alon proved that

$$p - c_1 \frac{p^{2/3}}{(\log p)^{1/3}} < g(p) < p - c_2 \frac{p^{1/2}}{\log p}.$$

By $f(p) \le g(p)$ it follows from the upper bound here that

$$f(p) < p - c_2 \frac{p^{1/2}}{\log p}. \tag{2}$$

Gyarmati, Konyagin and I first proved:

Theorem 7

If p is a prime, $p > 2$, $\ell \in \mathbb{F}_p$ and

$$|\mathcal{C}| \geq p - p^{1/2},$$

then $\mathcal{C}$ can be represented in the form

$$\mathcal{A} + \mathcal{B} = \mathcal{C} \quad \textit{with} \quad |\mathcal{B}| = 2. \tag{3}$$

Our proof is an existence proof using a rather simple counting argument.

(Note that Alon, Granville and Ubis gave an estimate for the number of the sets $\mathcal{C} \subset \mathbb{F}_p$ having a representation of form (3).)

It follows from Theorem 7 that

Corollary 1

For $p > 2$ we have

$$f(p) < p - p^{1/2}.$$

This improves slightly (by a $\log p$ factor) on the upper bound (2) which follows from Alon's result. Replacing $|\mathcal{B}| = 2$ in (3) by $|\mathcal{B}| \geq 2$ we could prove much more:

Gyarmati, Konyagin and I first proved:

Theorem 7

If p is a prime, $p > 2$, $\ell \in \mathbb{F}_p$ and

$$|\mathcal{C}| \geq p - p^{1/2},$$

then $\mathcal{C}$ can be represented in the form

$$\mathcal{A} + \mathcal{B} = \mathcal{C} \quad \textit{with} \quad |\mathcal{B}| = 2. \tag{3}$$

Our proof is an existence proof using a rather simple counting argument.

(Note that Alon, Granville and Ubis gave an estimate for the number of the sets $\mathcal{C} \subset \mathbb{F}_p$ having a representation of form (3).)

It follows from Theorem 7 that

Corollary 1

For $p > 2$ we have

$$f(p) < p - p^{1/2}.$$

This improves slightly (by a $\log p$ factor) on the upper bound (2) which follows from Alon's result. Replacing $|\mathcal{B}| = 2$ in (3) by $|\mathcal{B}| \geq 2$ we could prove much more:

Gyarmati, Konyagin and I first proved:

Theorem 7

If p is a prime, $p > 2$, $\ell \in \mathbb{F}_p$ and

$$|\mathcal{C}| \geq p - p^{1/2},$$

then $\mathcal{C}$ can be represented in the form

$$\mathcal{A} + \mathcal{B} = \mathcal{C} \quad \textit{with} \quad |\mathcal{B}| = 2. \tag{3}$$

Our proof is an existence proof using a rather simple counting argument.

(Note that Alon, Granville and Ubis gave an estimate for the number of the sets $\mathcal{C} \subset \mathbb{F}_p$ having a representation of form (3).)

It follows from Theorem 7 that

Corollary 1

For $p > 2$ we have

$$f(p) < p - p^{1/2}.$$

This improves slightly (by a $\log p$ factor) on the upper bound (2) which follows from Alon's result. Replacing $|\mathcal{B}| = 2$ in (3) by $|\mathcal{B}| \geq 2$ we could prove much more:

Gyarmati, Konyagin and I first proved:

Theorem 7

If p is a prime, $p > 2$, $\ell \in \mathbb{F}_p$ and

$$|\mathcal{C}| \geq p - p^{1/2},$$

then $\mathcal{C}$ can be represented in the form

$$\mathcal{A} + \mathcal{B} = \mathcal{C} \quad \textit{with} \quad |\mathcal{B}| = 2. \tag{3}$$

Our proof is an existence proof using a rather simple counting argument.

(Note that Alon, Granville and Ubis gave an estimate for the number of the sets $\mathcal{C} \subset \mathbb{F}_p$ having a representation of form (3).)

It follows from Theorem 7 that

Corollary 1

For $p > 2$ we have

$$f(p) < p - p^{1/2}.$$

This improves slightly (by a $\log p$ factor) on the upper bound (2) which follows from Alon's result. Replacing $|\mathcal{B}| = 2$ in (3) by $|\mathcal{B}| \geq 2$ we could prove much more:

Theorem 8

For $p > p_0$ we have

$$f(p) < p - c_3 \frac{p}{\log p}.$$

This is proved by a rather tricky and complicated counting argument using graph theory.

From the opposite side we proved:

Theorem 9

For $p > p_1$ we have

$$f(p) > p - c_4 \frac{\log \log p}{(\log p)^{1/2}} p.$$

This is also proved by a rather tricky and complicated counting argument which also involved the set of the quadratic residues modulo p and the use of Weil's theorem.

Theorem 8

For $p > p_0$ we have

$$f(p) < p - c_3 \frac{p}{\log p}.$$

This is proved by a rather tricky and complicated counting argument using graph theory.

From the opposite side we proved:

Theorem 9

For $p > p_1$ we have

$$f(p) > p - c_4 \frac{\log \log p}{(\log p)^{1/2}} p.$$

This is also proved by a rather tricky and complicated counting argument which also involved the set of the quadratic residues modulo p and the use of Weil's theorem.

Theorem 8

For $p > p_0$ we have

$$f(p) < p - c_3 \frac{p}{\log p}.$$

This is proved by a rather tricky and complicated counting argument using graph theory.

From the opposite side we proved:

Theorem 9

For $p > p_1$ we have

$$f(p) > p - c_4 \frac{\log \log p}{(\log p)^{1/2}} p.$$

This is also proved by a rather tricky and complicated counting argument which also involved the set of the quadratic residues modulo p and the use of Weil's theorem.

6. On primitive, k-primitive, reducible and k-reducible subsets of $\mathbb{F}_p$

In two papers to be completed soon K. Gyarmati and I studied primitive and reducible subsets of $\mathbb{F}_p$, the connections between them, and we also introduced and studied further related definitions. First we presented *three criteria for primitivity* of subsets of $\mathbb{F}_p$ (note that while there are several criteria for primitivity of *sequences of integers*, no criteria have been proved for primitivity of *subsets of* $\mathbb{F}_p$).

Theorem 10

Assume that $\mathcal{A} = \{a_1, a_2, \dots, a_t\}$ is a subset of $\mathbb{F}_p$, and there are i, j with $1 \le i < j \le t$ such that

$$a_i + a_j - a_k \notin \mathcal{A} \quad \textit{for every} \quad k \quad \textit{with} \quad 1 \le k \le t, \ \ k \ne i, \ \ k \ne j$$

and

$$a_i - a_j + a_k \notin \mathcal{A} \quad \textit{for every} \quad k \quad \textit{with} \quad 1 \le k \le t, \ \ k \ne j.$$

Then $\mathcal{A}$ is primitive.

6. On primitive, k-primitive, reducible and k-reducible subsets of $\mathbb{F}_p$

In two papers to be completed soon K. Gyarmati and I studied primitive and reducible subsets of $\mathbb{F}_p$, the connections between them, and we also introduced and studied further related definitions. First we presented *three criteria for primitivity* of subsets of $\mathbb{F}_p$ (note that while there are several criteria for primitivity of *sequences of integers*, no criteria have been proved for primitivity of *subsets of* $\mathbb{F}_p$).

Theorem 10

Assume that $\mathcal{A} = \{a_1, a_2, \dots, a_t\}$ is a subset of $\mathbb{F}_p$, and there are i, j with $1 \leq i < j \leq t$ such that

$$a_i + a_j - a_k \notin \mathcal{A} \quad \text{for every} \quad k \quad \text{with} \quad 1 \leq k \leq t, \;\; k \neq i, \;\; k \neq j$$

and

$$a_i - a_j + a_k \notin \mathcal{A} \quad \text{for every} \quad k \quad \text{with} \quad 1 \leq k \leq t, \;\; k \neq j.$$

Then $\mathcal{A}$ is primitive.

6. On primitive, k-primitive, reducible and k-reducible subsets of $\mathbb{F}_p$

In two papers to be completed soon K. Gyarmati and I studied primitive and reducible subsets of $\mathbb{F}_p$, the connections between them, and we also introduced and studied further related definitions. First we presented *three criteria for primitivity* of subsets of $\mathbb{F}_p$ (note that while there are several criteria for primitivity of *sequences of integers*, no criteria have been proved for primitivity of *subsets of* $\mathbb{F}_p$).

Theorem 10

Assume that $\mathcal{A} = \{a_1, a_2, \dots, a_t\}$ *is a subset of* $\mathbb{F}_p$, *and there are* i, j *with* $1 \le i < j \le t$ *such that*

$$a_i + a_j - a_k \notin \mathcal{A} \ \ \textit{for every} \ \ k \ \ \textit{with} \ \ 1 \le k \le t, \ \ k \ne i, \ \ k \ne j$$

and

$$a_i - a_j + a_k \notin \mathcal{A} \ \ \textit{for every} \ \ k \ \ \textit{with} \ \ 1 \le k \le t, \ \ k \ne j.$$

Then $\mathcal{A}$ *is primitive.*

To illustrate the applicability of this criterion we showed

Corollary 2

If p is a prime of form $p = 4k+1$ and $\mathcal{A} \subset \mathbb{F}_p$ is defined by

$$\mathcal{A} = \{0,1\} \cup \left\{ a \in \mathbb{F}_p : \left(\frac{a}{p}\right) = 1,\ \left(\frac{a-1}{p}\right) = -1,\ a \neq -1,\ a \neq 2 \right\},$$

then $\mathcal{A}$ is primitive.

It also follows from Theorem 10 that

Corollary 3

If $\mathcal{A} \subset \mathbb{F}_p$ is a Sidon set, *then it is primitive.*

(A set $\mathcal{A} = \{a_1, a_2, \dots, a_t\}$ is called Sidon set if the sums $a_i + a_j$ with $1 \leq i < j \leq t$ are distinct.)

The second criterion for primitivity is

Theorem 11

If $\mathcal{A} \subset \mathbb{F}_p$ is of the form

$$\mathcal{A} = \{0\} \cup \mathcal{A}_0 \ \ \textit{with} \ \ \mathcal{A}_0 \subset [p/3, 2p/3),$$

then $\mathcal{A}$ is primitive.

To illustrate the applicability of this criterion we showed

Corollary 2

If p is a prime of form $p = 4k + 1$ and $\mathcal{A} \subset \mathbb{F}_p$ is defined by

$$\mathcal{A} = \{0, 1\} \cup \left\{ a \in \mathbb{F}_p : \ \left(\frac{a}{p}\right) = 1, \ \left(\frac{a-1}{p}\right) = -1, \ a \neq -1, \ a \neq 2 \right\},$$

then $\mathcal{A}$ is primitive.

It also follows from Theorem 10 that

Corollary 3

If $\mathcal{A} \subset \mathbb{F}_p$ is a Sidon set, *then it is primitive.*

(A set $\mathcal{A} = \{a_1, a_2, \dots, a_t\}$ is called Sidon set if the sums $a_i + a_j$ with $1 \le i < j \le t$ are distinct.)

The second criterion for primitivity is

Theorem 11

If $\mathcal{A} \subset \mathbb{F}_p$ is of the form

$$\mathcal{A} = \{0\} \cup \mathcal{A}_0 \quad \textit{with} \quad \mathcal{A}_0 \subset [p/3, 2p/3),$$

then $\mathcal{A}$ is primitive.

To illustrate the applicability of this criterion we showed

Corollary 2

If p is a prime of form $p = 4k + 1$ and $\mathcal{A} \subset \mathbb{F}_p$ is defined by

$$\mathcal{A} = \{0, 1\} \cup \left\{ a \in \mathbb{F}_p : \left(\frac{a}{p}\right) = 1, \left(\frac{a-1}{p}\right) = -1, \ a \neq -1, \ a \neq 2 \right\},$$

then $\mathcal{A}$ is primitive.

It also follows from Theorem 10 that

Corollary 3

If $\mathcal{A} \subset \mathbb{F}_p$ is a Sidon set, *then it is primitive.*

(A set $\mathcal{A} = \{a_1, a_2, \ldots, a_t\}$ is called Sidon set if the sums $a_i + a_j$ with $1 \leq i < j \leq t$ are distinct.)

The second criterion for primitivity is

Theorem 11

If $\mathcal{A} \subset \mathbb{F}_p$ is of the form

$$\mathcal{A} = \{0\} \cup \mathcal{A}_0 \quad \textit{with} \quad \mathcal{A}_0 \subset [p/3, 2p/3),$$

then $\mathcal{A}$ is primitive.

To illustrate the applicability of this criterion we showed

Corollary 2

If p is a prime of form $p = 4k + 1$ and $\mathcal{A} \subset \mathbb{F}_p$ is defined by

$$\mathcal{A} = \{0, 1\} \cup \left\{ a \in \mathbb{F}_p : \left(\frac{a}{p}\right) = 1, \left(\frac{a-1}{p}\right) = -1, \ a \neq -1, \ a \neq 2 \right\},$$

then $\mathcal{A}$ is primitive.

It also follows from Theorem 10 that

Corollary 3

If $\mathcal{A} \subset \mathbb{F}_p$ is a Sidon set, *then it is primitive.*

(A set $\mathcal{A} = \{a_1, a_2, \ldots, a_t\}$ is called Sidon set if the sums $a_i + a_j$ with $1 \leq i < j \leq t$ are distinct.)

The second criterion for primitivity is

Theorem 11

If $\mathcal{A} \subset \mathbb{F}_p$ is of the form

$$\mathcal{A} = \{0\} \cup \mathcal{A}_0 \quad \textit{with} \quad \mathcal{A}_0 \subset [p/3, 2p/3),$$

then $\mathcal{A}$ is primitive.

The third criterion is:

Theorem 12

Let $\mathcal{A} \subset \mathbb{F}_p$ and for $d \in \mathbb{F}_p^*$ denote the number of solutions of

$$a - a' = d, \quad a \in \mathcal{A},\ a' \in \mathcal{A}$$

by $f(\mathcal{A}, d)$. If

$$\max_{d \in \mathbb{F}_p^*} f(\mathcal{A}, d) < |\mathcal{A}|^{1/2},$$

then $\mathcal{A}$ is primitive.

Note that Corollary 3 (the primitivity of Sidon sets) also follows from this criterion.

We also proved that Theorem 12 is sharp in the range $0 < |\mathcal{A}| \ll p^{1/2}$:

Theorem 13

If p is large enough and k is a positive integer with $k_0 < k < \frac{1}{2}p^{1/4}$, then there is a set $\mathcal{A} \subset \mathbb{F}_p$ such that $|\mathcal{A}| = k^2$,

$$\max_{d \in \mathbb{F}_p^*} f(\mathcal{A}, d) = |\mathcal{A}|^{1/2}$$

and $\mathcal{A}$ is reducible.

Each of the three criteria can be proved in an elementary way. We also showed that these criteria are independent, i.e., for each criterion there is a primitive subset which satisfies it, but it does not satisfy the conditions in the two other criteria.

The third criterion is:

Theorem 12

Let $\mathcal{A} \subset \mathbb{F}_p$ and for $d \in \mathbb{F}_p^*$ denote the number of solutions of

$$a - a' = d, \quad a \in \mathcal{A},\ a' \in \mathcal{A}$$

by $f(\mathcal{A}, d)$. If

$$\max_{d \in \mathbb{F}_p^*} f(\mathcal{A}, d) < |\mathcal{A}|^{1/2},$$

then $\mathcal{A}$ is primitive.

Note that Corollary 3 (the primitivity of Sidon sets) also follows from this criterion.

We also proved that Theorem 12 is sharp in the range $0 < |\mathcal{A}| \ll p^{1/2}$:

Theorem 13

If p is large enough and k is a positive integer with $k_0 < k < \frac{1}{2}p^{1/4}$, then there is a set $\mathcal{A} \subset \mathbb{F}_p$ such that $|\mathcal{A}| = k^2$,

$$\max_{d \in \mathbb{F}_p^*} f(\mathcal{A}, d) = |\mathcal{A}|^{1/2}$$

and $\mathcal{A}$ is reducible.

Each of the three criteria can be proved in an elementary way. We also showed that these criteria are independent, i.e., for each criterion there is a primitive subset which satisfies it, but it does not satisfy the conditions in the two other criteria.

The third criterion is:

Theorem 12

Let $\mathcal{A} \subset \mathbb{F}_p$ and for $d \in \mathbb{F}_p^*$ denote the number of solutions of

$$a - a' = d, \quad a \in \mathcal{A},\ a' \in \mathcal{A}$$

by $f(\mathcal{A}, d)$. If

$$\max_{d \in \mathbb{F}_p^*} f(\mathcal{A}, d) < |\mathcal{A}|^{1/2},$$

then $\mathcal{A}$ is primitive.

Note that Corollary 3 (the primitivity of Sidon sets) also follows from this criterion.

We also proved that Theorem 12 is sharp in the range $0 < |\mathcal{A}| \ll p^{1/2}$:

Theorem 13

If p is large enough and k is a positive integer with $k_0 < k < \frac{1}{2}p^{1/4}$, then there is a set $\mathcal{A} \subset \mathbb{F}_p$ such that $|\mathcal{A}| = k^2$,

$$\max_{d \in \mathbb{F}_p^*} f(\mathcal{A}, d) = |\mathcal{A}|^{1/2}$$

and $\mathcal{A}$ is reducible.

Each of the three criteria can be proved in an elementary way. We also showed that these criteria are independent, i.e., for each criterion there is a primitive subset which satisfies it, but it does not satisfy the conditions in the two other criteria.

The third criterion is:

Theorem 12

Let $\mathcal{A} \subset \mathbb{F}_p$ and for $d \in \mathbb{F}_p^*$ denote the number of solutions of

$$a - a' = d, \quad a \in \mathcal{A},\ a' \in \mathcal{A}$$

by $f(\mathcal{A}, d)$. If

$$\max_{d \in \mathbb{F}_p^*} f(\mathcal{A}, d) < |\mathcal{A}|^{1/2},$$

then $\mathcal{A}$ is primitive.

Note that Corollary 3 (the primitivity of Sidon sets) also follows from this criterion.

We also proved that Theorem 12 is sharp in the range $0 < |\mathcal{A}| \ll p^{1/2}$:

Theorem 13

If p is large enough and k is a positive integer with $k_0 < k < \frac{1}{2}p^{1/4}$, then there is a set $\mathcal{A} \subset \mathbb{F}_p$ such that $|\mathcal{A}| = k^2$,

$$\max_{d \in \mathbb{F}_p^*} f(\mathcal{A}, d) = |\mathcal{A}|^{1/2}$$

and $\mathcal{A}$ is reducible.

Each of the three criteria can be proved in an elementary way. We also showed that these criteria are independent, i.e., for each criterion there is a primitive subset which satisfies it, but it does not satisfy the conditions in the two other criteria.

As we have seen, Ostmann's definitions for reducibility and primitivity can be extended to $\mathbb{F}_p$ (indeed, these definitions can be used in any additive semigroup). On the other hand, the situation is very much different in case of the definition of *totalprimitivity*: clearly, this definition cannot be used in its original form in case of finite sets. Instead, we introduced the following definitions:

Definition 5

If $\mathcal{A}, \mathcal{B} \subset \mathbb{F}_p$, then their *distance* is defined as the cardinality of their symmetric difference and it is denoted by $D(\mathcal{A}, \mathcal{B})$:

$$D(\mathcal{A}, \mathcal{B}) = \big|(\mathcal{A} \setminus \mathcal{B}) \cup (\mathcal{B} \setminus \mathcal{A})\big|.$$

Definition 6

For $k \in \mathbb{N}$ a set $\mathcal{A} \subset \mathbb{F}_p$ is said to be *k-primitive* if every set $\mathcal{A}' \subset \mathbb{F}_p$ with $D(\mathcal{A}, \mathcal{A}') \leq k$ is primitive.

(In other words, $\mathcal{A}$ is k-primitive if changing at most k elements of it we always get a primitive set.)

As we have seen, Ostmann's definitions for reducibility and primitivity can be extended to $\mathbb{F}_p$ (indeed, these definitions can be used in any additive semigroup). On the other hand, the situation is very much different in case of the definition of *totalprimitivity*: clearly, this definition cannot be used in its original form in case of finite sets. Instead, we introduced the following definitions:

Definition 5

If $\mathcal{A}, \mathcal{B} \subset \mathbb{F}_p$, then their *distance* is defined as the cardinality of their symmetric difference and it is denoted by $D(\mathcal{A}, \mathcal{B})$:

$$D(\mathcal{A}, \mathcal{B}) = \big|(\mathcal{A} \setminus \mathcal{B}) \cup (\mathcal{B} \setminus \mathcal{A})\big|.$$

Definition 6

For $k \in \mathbb{N}$ a set $\mathcal{A} \subset \mathbb{F}_p$ is said to be *k-primitive* if every set $\mathcal{A}' \subset \mathbb{F}_p$ with $D(\mathcal{A}, \mathcal{A}') \le k$ is primitive.

(In other words, $\mathcal{A}$ is k-primitive if changing at most k elements of it we always get a primitive set.)

As we have seen, Ostmann's definitions for reducibility and primitivity can be extended to $\mathbb{F}_p$ (indeed, these definitions can be used in any additive semigroup). On the other hand, the situation is very much different in case of the definition of *totalprimitivity*: clearly, this definition cannot be used in its original form in case of finite sets. Instead, we introduced the following definitions:

Definition 5

If $\mathcal{A}, \mathcal{B} \subset \mathbb{F}_p$, then their *distance* is defined as the cardinality of their symmetric difference and it is denoted by $D(\mathcal{A}, \mathcal{B})$:

$$D(\mathcal{A}, \mathcal{B}) = \big|(\mathcal{A} \setminus \mathcal{B}) \cup (\mathcal{B} \setminus \mathcal{A})\big|.$$

Definition 6

For $k \in \mathbb{N}$ a set $\mathcal{A} \subset \mathbb{F}_p$ is said to be *k-primitive* if every set $\mathcal{A}' \subset \mathbb{F}_p$ with $D(\mathcal{A}, \mathcal{A}') \leq k$ is primitive.

(In other words, $\mathcal{A}$ is k-primitive if changing at most k elements of it we always get a primitive set.)

From Theorem 12 (the third criterion for primitivity) we derived the following criterion for k-primitivity:

Theorem 14

Let $\mathcal{A} \subset \mathbb{F}_p$ and define $f(\mathcal{A}, d)$ again by $f(\mathcal{A}, d) = \left|\{(a, a') : \ a \in \mathcal{A}, \ a' \in \mathcal{A}, \ a - a' = d\}\right|$.
If

$$\max_{d \in \mathbb{F}_p^*} f(\mathcal{A}, d) < \frac{1}{2}|\mathcal{A}|^{1/2}$$

and $k \in \mathbb{N}$ with

$$k \leq \frac{1}{4}|\mathcal{A}|^{1/2},$$

then $\mathcal{A}$ is k-primitive.

It follows from this theorem that

Corollary 4

If $\mathcal{A} \subset \mathbb{F}_p$ is a Sidon set and $k = \left[\frac{1}{4}|\mathcal{A}|^{1/2}\right]$, then $\mathcal{A}$ is k-primitive.

If p is a prime then let $M(p)$ denote the greatest integer k such that there is a k-primitive set $\mathcal{A}$ in $\mathbb{F}_p$. Our next goal was to estimate $M(p)$. We proved:

Theorem 15

For $p \to \infty$ we have

$$(c + o(1))p < M(p) < \left(\frac{1}{2} + o(1)\right) p$$

where $c = 0.119\ldots$ is the smaller zero of the function $\frac{\log 2}{2} + \big(x \log x + (1 - x) \log(1 - x)\big)$ in $(0, 1)$.

From Theorem 12 (the third criterion for primitivity) we derived the following criterion for k-primitivity:

Theorem 14

Let $\mathcal{A} \subset \mathbb{F}_p$ and define $f(\mathcal{A}, d)$ again by $f(\mathcal{A}, d) = \big|\{(a, a') : \ a \in \mathcal{A},\ a' \in \mathcal{A},\ a - a' = d\}\big|$.
If

$$\max_{d \in \mathbb{F}_p^*} f(\mathcal{A}, d) < \frac{1}{2}|\mathcal{A}|^{1/2}$$

and $k \in \mathbb{N}$ with

$$k \leq \frac{1}{4}|\mathcal{A}|^{1/2},$$

then $\mathcal{A}$ is k-primitive.

It follows from this theorem that

Corollary 4

If $\mathcal{A} \subset \mathbb{F}_p$ is a Sidon set and $k = \left[\frac{1}{4}|\mathcal{A}|^{1/2}\right]$, then $\mathcal{A}$ is k-primitive.

If p is a prime then let $M(p)$ denote the greatest integer k such that there is a k-primitive set $\mathcal{A}$ in $\mathbb{F}_p$. Our next goal was to estimate $M(p)$. We proved:

Theorem 15

For $p \to \infty$ we have

$$(c + o(1))p < M(p) < \left(\frac{1}{2} + o(1)\right) p$$

where $c = 0.119\ldots$ is the smaller zero of the function $\frac{\log 2}{2} + \big(x \log x + (1-x)\log(1-x)\big)$ in $(0, 1)$.

From Theorem 12 (the third criterion for primitivity) we derived the following criterion for k-primitivity:

Theorem 14

Let $\mathcal{A} \subset \mathbb{F}_p$ and define $f(\mathcal{A}, d)$ again by $f(\mathcal{A}, d) = \left|\{(a, a') : \ a \in \mathcal{A}, \ a' \in \mathcal{A}, \ a - a' = d\}\right|$.
If

$$\max_{d \in \mathbb{F}_p^*} f(\mathcal{A}, d) < \frac{1}{2}|\mathcal{A}|^{1/2}$$

and $k \in \mathbb{N}$ with

$$k \leq \frac{1}{4}|\mathcal{A}|^{1/2},$$

then $\mathcal{A}$ is k-primitive.

It follows from this theorem that

Corollary 4

If $\mathcal{A} \subset \mathbb{F}_p$ is a Sidon set and $k = \left[\frac{1}{4}|\mathcal{A}|^{1/2}\right]$, then $\mathcal{A}$ is k-primitive.

If p is a prime then let $M(p)$ denote the greatest integer k such that there is a k-primitive set $\mathcal{A}$ in $\mathbb{F}_p$. Our next goal was to estimate $M(p)$. We proved:

Theorem 15

For $p \to \infty$ we have

$$(c + o(1))p < M(p) < \left(\frac{1}{2} + o(1)\right) p$$

where $c = 0.119\ldots$ is the smaller zero of the function $\frac{\log 2}{2} + \big(x \log x + (1-x)\log(1-x)\big)$ in $(0, 1)$.

From Theorem 12 (the third criterion for primitivity) we derived the following criterion for k-primitivity:

Theorem 14

Let $\mathcal{A} \subset \mathbb{F}_p$ and define $f(\mathcal{A}, d)$ again by $f(\mathcal{A}, d) = \left|\{(a, a') : \ a \in \mathcal{A}, \ a' \in \mathcal{A}, \ a - a' = d\}\right|$.
If

$$\max_{d \in \mathbb{F}_p^*} f(\mathcal{A}, d) < \frac{1}{2}|\mathcal{A}|^{1/2}$$

and $k \in \mathbb{N}$ with

$$k \leq \frac{1}{4}|\mathcal{A}|^{1/2},$$

then $\mathcal{A}$ is k-primitive.

It follows from this theorem that

Corollary 4

If $\mathcal{A} \subset \mathbb{F}_p$ is a Sidon set and $k = \left[\frac{1}{4}|\mathcal{A}|^{1/2}\right]$, then $\mathcal{A}$ is k-primitive.

If p is a prime then let $M(p)$ denote the greatest integer k such that there is a k-primitive set $\mathcal{A}$ in $\mathbb{F}_p$. Our next goal was to estimate $M(p)$. We proved:

Theorem 15

For $p \to \infty$ we have

$$(c + o(1))p < M(p) < \left(\frac{1}{2} + o(1)\right) p$$

where $c = 0.119\ldots$ is the smaller zero of the function $\frac{\log 2}{2} + \left(x \log x + (1-x)\log(1-x)\right)$ in $(0, 1)$.

Here the upper bound is trivial while the lower bound is based on a result of Alon, Granville and Ubis: they proved that the number of the reducible subsets of $\mathbb{F}_p$ is $2^{p/2+o(p)}$.

Next we studied the following problem: if $\mathcal{A}$ is a subset of $\mathbb{F}_p$ then, depending on the cardinality of $\mathcal{A}$, what can be said about the *size of the greatest reducible subset* of $\mathcal{A}$?

If $\mathcal{A}$ is a Sidon set, then its subsets are also Sidon sets, thus by Corollary 3 they are primitive so that $\mathcal{A}$ has no reducible subset. Since the cardinality of a Sidon set in $\mathbb{F}_p$ can be $\gg p^{1/2}$, thus a subset $\mathcal{A} \subset \mathbb{F}_p$ of cardinality $\ll p^{1/2}$ need not contain a reducible subset. On the other hand, we proved that a subset of cardinality $\gg p^{1/2}$ must contain a reducible set. This follows from

Theorem 16

If $\mathcal{A}$ is a subset of $\mathbb{F}_p$ with

$$|\mathcal{A}|^2 - |\mathcal{A}| > p - 1,$$

then it contains a reducible subset of form

$$\mathcal{B} + \mathcal{C} \quad \textit{with} \quad |\mathcal{B} + \mathcal{C}| \geq \min\left\{\frac{|\mathcal{A}|^2 - |\mathcal{A}|}{p-1}, p\right\}, \ |\mathcal{C}| = 2. \tag{4}$$

Here the upper bound is trivial while the lower bound is based on a result of Alon, Granville and Ubis: they proved that the number of the reducible subsets of $\mathbb{F}_p$ is $2^{p/2+o(p)}$.

Next we studied the following problem: if $\mathcal{A}$ is a subset of $\mathbb{F}_p$ then, depending on the cardinality of $\mathcal{A}$, what can be said about the *size of the greatest reducible subset* of $\mathcal{A}$?

If $\mathcal{A}$ is a Sidon set, then its subsets are also Sidon sets, thus by Corollary 3 they are primitive so that $\mathcal{A}$ has no reducible subset. Since the cardinality of a Sidon set in $\mathbb{F}_p$ can be $\gg p^{1/2}$, thus a subset $\mathcal{A} \subset \mathbb{F}_p$ of cardinality $\ll p^{1/2}$ need not contain a reducible subset. On the other hand, we proved that a subset of cardinality $\gg p^{1/2}$ must contain a reducible set. This follows from

Theorem 16

If $\mathcal{A}$ is a subset of $\mathbb{F}_p$ with

$$|\mathcal{A}|^2 - |\mathcal{A}| > p - 1,$$

then it contains a reducible subset of form

$$\mathcal{B} + \mathcal{C} \quad \textit{with} \quad |\mathcal{B} + \mathcal{C}| \geq \min\left\{\frac{|\mathcal{A}|^2 - |\mathcal{A}|}{p-1}, p\right\}, \ |\mathcal{C}| = 2. \tag{4}$$

Here the upper bound is trivial while the lower bound is based on a result of Alon, Granville and Ubis: they proved that the number of the reducible subsets of $\mathbb{F}_p$ is $2^{p/2+o(p)}$.

Next we studied the following problem: if $\mathcal{A}$ is a subset of $\mathbb{F}_p$ then, depending on the cardinality of $\mathcal{A}$, what can be said about the *size of the greatest reducible subset* of $\mathcal{A}$?

If $\mathcal{A}$ is a Sidon set, then its subsets are also Sidon sets, thus by Corollary 3 they are primitive so that $\mathcal{A}$ has no reducible subset. Since the cardinality of a Sidon set in $\mathbb{F}_p$ can be $\gg p^{1/2}$, thus a subset $\mathcal{A} \subset \mathbb{F}_p$ of cardinality $\ll p^{1/2}$ need not contain a reducible subset. On the other hand, we proved that a subset of cardinality $\gg p^{1/2}$ must contain a reducible set. This follows from

Theorem 16

If $\mathcal{A}$ is a subset of $\mathbb{F}_p$ with

$$|\mathcal{A}|^2 - |\mathcal{A}| > p - 1,$$

then it contains a reducible subset of form

$$\mathcal{B} + \mathcal{C} \quad \textit{with} \quad |\mathcal{B} + \mathcal{C}| \geq \min\left\{\frac{|\mathcal{A}|^2 - |\mathcal{A}|}{p-1}, p\right\}, \; |\mathcal{C}| = 2. \tag{4}$$

Here the upper bound is trivial while the lower bound is based on a result of Alon, Granville and Ubis: they proved that the number of the reducible subsets of $\mathbb{F}_p$ is $2^{p/2+o(p)}$.

Next we studied the following problem: if $\mathcal{A}$ is a subset of $\mathbb{F}_p$ then, depending on the cardinality of $\mathcal{A}$, what can be said about the *size of the greatest reducible subset* of $\mathcal{A}$?

If $\mathcal{A}$ is a Sidon set, then its subsets are also Sidon sets, thus by Corollary 3 they are primitive so that $\mathcal{A}$ has no reducible subset. Since the cardinality of a Sidon set in $\mathbb{F}_p$ can be $\gg p^{1/2}$, thus a subset $\mathcal{A} \subset \mathbb{F}_p$ of cardinality $\ll p^{1/2}$ need not contain a reducible subset. On the other hand, we proved that a subset of cardinality $\gg p^{1/2}$ must contain a reducible set. This follows from

Theorem 16

If $\mathcal{A}$ is a subset of $\mathbb{F}_p$ with

$$|\mathcal{A}|^2 - |\mathcal{A}| > p - 1,$$

then it contains a reducible subset of form

$$\mathcal{B} + \mathcal{C} \quad \text{with} \quad |\mathcal{B} + \mathcal{C}| \geq \min\left\{\frac{|\mathcal{A}|^2 - |\mathcal{A}|}{p-1}, p\right\}, \ |\mathcal{C}| = 2. \tag{4}$$

Here the upper bound is trivial while the lower bound is based on a result of Alon, Granville and Ubis: they proved that the number of the reducible subsets of $\mathbb{F}_p$ is $2^{p/2+o(p)}$.

Next we studied the following problem: if $\mathcal{A}$ is a subset of $\mathbb{F}_p$ then, depending on the cardinality of $\mathcal{A}$, what can be said about the *size of the greatest reducible subset* of $\mathcal{A}$?

If $\mathcal{A}$ is a Sidon set, then its subsets are also Sidon sets, thus by Corollary 3 they are primitive so that $\mathcal{A}$ has no reducible subset. Since the cardinality of a Sidon set in $\mathbb{F}_p$ can be $\gg p^{1/2}$, thus a subset $\mathcal{A} \subset \mathbb{F}_p$ of cardinality $\ll p^{1/2}$ need not contain a reducible subset. On the other hand, we proved that a subset of cardinality $\gg p^{1/2}$ must contain a reducible set. This follows from

Theorem 16

If $\mathcal{A}$ is a subset of $\mathbb{F}_p$ with

$$|\mathcal{A}|^2 - |\mathcal{A}| > p - 1,$$

then it contains a reducible subset of form

$$\mathcal{B} + \mathcal{C} \quad \textit{with} \quad |\mathcal{B} + \mathcal{C}| \geq \min\left\{ \frac{|\mathcal{A}|^2 - |\mathcal{A}|}{p-1}, p \right\}, \; |\mathcal{C}| = 2. \tag{4}$$

A simple counting argument is used to prove the result.

Observe that the decomposition $\mathcal{B}+\mathcal{C}$ in the last theorem is of very special type: one of two summands is a 2-element subset. One may expect that if $|\mathcal{A}|$ increases, then there are also better balanced decompositions where both $|\mathcal{B}|$ and $|\mathcal{C}|$ are large. Indeed, we have proved such a theorem but before presenting it we need a further definition.

Definition 7

If k is a positive integer and the set $\mathcal{A} \subset \mathbb{F}_p$ has a k-decomposition

$$\mathcal{A} = \mathcal{B}_1 + \mathcal{B}_2 + \cdots + \mathcal{B}_k \quad (\text{with } |\mathcal{B}_1|, |\mathcal{B}_2|, \dots, |\mathcal{B}_k| \geq 2),$$

then $\mathcal{A}$ is said to be *k-reducible*.

We raised two problems on k-reducibility.

(i) Recall that I conjectured that the set of the quadratic residues and the set of the primitive roots are primitive, i.e., they are not 2-reducible, and as a partial result it has been proved that they are not 3-reducible. Does it not follow from this partial result that they are not 2-reducible either? We gave a negative answer by constructing subsets of $\mathbb{F}_p$ which are 2-reducible but they are not 3-reducible.

A simple counting argument is used to prove the result.

Observe that the decomposition $\mathcal{B}+\mathcal{C}$ in the last theorem is of very special type: one of two summands is a 2-element subset. One may expect that if $|\mathcal{A}|$ increases, then there are also better balanced decompositions where both $|\mathcal{B}|$ and $|\mathcal{C}|$ are large. Indeed, we have proved such a theorem but before presenting it we need a further definition.

Definition 7

If k is a positive integer and the set $\mathcal{A} \subset \mathbb{F}_p$ has a k-decomposition

$$\mathcal{A} = \mathcal{B}_1 + \mathcal{B}_2 + \cdots + \mathcal{B}_k \quad (\text{with } |\mathcal{B}_1|, |\mathcal{B}_2|, \ldots, |\mathcal{B}_k| \geq 2),$$

then $\mathcal{A}$ is said to be *k-reducible.*

We raised two problems on k-reducibility.

(i) Recall that I conjectured that the set of the quadratic residues and the set of the primitive roots are primitive, i.e., they are not 2-reducible, and as a partial result it has been proved that they are not 3-reducible. Does it not follow from this partial result that they are not 2-reducible either? We gave a negative answer by constructing subsets of $\mathbb{F}_p$ which are 2-reducible but they are not 3-reducible.

A simple counting argument is used to prove the result.

Observe that the decomposition $\mathcal{B}+\mathcal{C}$ in the last theorem is of very special type: one of two summands is a 2-element subset. One may expect that if $|\mathcal{A}|$ increases, then there are also better balanced decompositions where both $|\mathcal{B}|$ and $|\mathcal{C}|$ are large. Indeed, we have proved such a theorem but before presenting it we need a further definition.

Definition 7

If k is a positive integer and the set $\mathcal{A} \subset \mathbb{F}_p$ has a k-decomposition

$$\mathcal{A} = \mathcal{B}_1 + \mathcal{B}_2 + \cdots + \mathcal{B}_k \quad (\text{with } |\mathcal{B}_1|, |\mathcal{B}_2|, \dots, |\mathcal{B}_k| \geq 2),$$

then $\mathcal{A}$ is said to be *k-reducible*.

We raised two problems on k-reducibility.

(i) Recall that I conjectured that the set of the quadratic residues and the set of the primitive roots are primitive, i.e., they are not 2-reducible, and as a partial result it has been proved that they are not 3-reducible. Does it not follow from this partial result that they are not 2-reducible either? We gave a negative answer by constructing subsets of $\mathbb{F}_p$ which are 2-reducible but they are not 3-reducible.

A simple counting argument is used to prove the result.

Observe that the decomposition $\mathcal{B} + \mathcal{C}$ in the last theorem is of very special type: one of two summands is a 2-element subset. One may expect that if $|\mathcal{A}|$ increases, then there are also better balanced decompositions where both $|\mathcal{B}|$ and $|\mathcal{C}|$ are large. Indeed, we have proved such a theorem but before presenting it we need a further definition.

Definition 7

If k is a positive integer and the set $\mathcal{A} \subset \mathbb{F}_p$ has a k-decomposition

$$\mathcal{A} = \mathcal{B}_1 + \mathcal{B}_2 + \cdots + \mathcal{B}_k \quad (\text{with } |\mathcal{B}_1|, |\mathcal{B}_2|, \ldots, |\mathcal{B}_k| \geq 2),$$

then $\mathcal{A}$ is said to be *k-reducible*.

We raised two problems on k-reducibility.

(i) Recall that I conjectured that the set of the quadratic residues and the set of the primitive roots are primitive, i.e., they are not 2-reducible, and as a partial result it has been proved that they are not 3-reducible. Does it not follow from this partial result that they are not 2-reducible either? We gave a negative answer by constructing subsets of $\mathbb{F}_p$ which are 2-reducible but they are not 3-reducible.

(ii) Is it true that large subsets of $\mathbb{F}_p$ must contain a k-reducible subset for some large k? We proved that the answer to this question is affirmative, and simultaneously we also proved the existence of reducible subsets in large subsets of $\mathbb{F}_p$ with balanced 2-decompositions into large subsets:

Theorem 17

If p is a prime large enough, $\mathcal{A} \subset \mathbb{F}_p$, $d \in \mathbb{N}$ and

$$|\mathcal{A}| \geq 3p^{1-2^{-d}}, \tag{5}$$

then

(i) *$\mathcal{A}$ contains a reducible subset of form $\mathcal{B} + \mathcal{C}$ with $\min\{|\mathcal{B}|, |\mathcal{C}|\} \geq [d/2]$,*

(ii) *$\mathcal{A}$ contains a d-reducible subset.*

Note that if p is large enough and $|\mathcal{A}| \geq 2$, then (5) holds with

$$d = \left[\frac{1}{\log 2} \log \frac{\log p}{\log(3p/|\mathcal{A}|)}\right],$$

thus we may take this d value in the conclusions (i) and (ii).

(ii) Is it true that large subsets of $\mathbb{F}_p$ must contain a k-reducible subset for some large k? We proved that the answer to this question is affirmative, and simultaneously we also proved the existence of reducible subsets in large subsets of $\mathbb{F}_p$ with balanced 2-decompositions into large subsets:

Theorem 17

If p is a prime large enough, $\mathcal{A} \subset \mathbb{F}_p$, $d \in \mathbb{N}$ and

$$|\mathcal{A}| \geq 3p^{1-2^{-d}}, \tag{5}$$

then

(i) *$\mathcal{A}$ contains a reducible subset of form $\mathcal{B} + \mathcal{C}$ with $\min\{|\mathcal{B}|, |\mathcal{C}|\} \geq [d/2]$,*

(ii) *$\mathcal{A}$ contains a d-reducible subset.*

Note that if p is large enough and $|\mathcal{A}| \geq 2$, then (5) holds with

$$d = \left[\frac{1}{\log 2} \log \frac{\log p}{\log(3p/|\mathcal{A}|)} \right],$$

thus we may take this d value in the conclusions (i) and (ii).

(ii) Is it true that large subsets of $\mathbb{F}_p$ must contain a k-reducible subset for some large k? We proved that the answer to this question is affirmative, and simultaneously we also proved the existence of reducible subsets in large subsets of $\mathbb{F}_p$ with balanced 2-decompositions into large subsets:

Theorem 17

If p is a prime large enough, $\mathcal{A} \subset \mathbb{F}_p$, $d \in \mathbb{N}$ and

$$|\mathcal{A}| \geq 3p^{1-2^{-d}}, \tag{5}$$

then

(i) *$\mathcal{A}$ contains a reducible subset of form $\mathcal{B}+\mathcal{C}$ with* $\min\{|\mathcal{B}|, |\mathcal{C}|\} \geq [d/2]$,

(ii) *$\mathcal{A}$ contains a d-reducible subset.*

Note that if p is large enough and $|\mathcal{A}| \geq 2$, then (5) holds with

$$d = \left[\frac{1}{\log 2} \log \frac{\log p}{\log(3p/|\mathcal{A}|)}\right],$$

thus we may take this d value in the conclusions (i) and (ii).

(ii) Is it true that large subsets of $\mathbb{F}_p$ must contain a k-reducible subset for some large k? We proved that the answer to this question is affirmative, and simultaneously we also proved the existence of reducible subsets in large subsets of $\mathbb{F}_p$ with balanced 2-decompositions into large subsets:

Theorem 17

If p is a prime large enough, $\mathcal{A} \subset \mathbb{F}_p$, $d \in \mathbb{N}$ and

$$|\mathcal{A}| \geq 3p^{1-2^{-d}}, \tag{5}$$

then

(i) *$\mathcal{A}$ contains a reducible subset of form $\mathcal{B} + \mathcal{C}$ with* $\min\{|\mathcal{B}|, |\mathcal{C}|\} \geq [d/2]$,

(ii) *$\mathcal{A}$ contains a d-reducible subset.*

Note that if p is large enough and $|\mathcal{A}| \geq 2$, then (5) holds with

$$d = \left[\frac{1}{\log 2} \log \frac{\log p}{\log(3p/|\mathcal{A}|)}\right],$$

thus we may take this d value in the conclusions (i) and (ii).

* * *

All the results I was speaking about (and also their proofs) can be extended from $\mathbb{F}_p$ to $\mathbb{F}_q$ with $q = p^r$ (but *not* to $\mathbb{Z}_m$).

$$* \quad * \quad *$$

All the results I was speaking about (and also their proofs) can be extended from $\mathbb{F}_p$ to $\mathbb{F}_q$ with $q = p^r$ (but *not* to $\mathbb{Z}_m$).