Local-global problems

Laura Paladino

paladino@mat.unical.it

UNIVERSITÀ DELLA CALABRIA

4th Number Theory Meeting
Torino, October 25 2019

Local-global problems

Definition.

A *global field* is a finite extension of $\mathbb{Q}$ or a finite extension of $\mathbb{F}_p(t)$.

Definition.

A *number field* k is a finite extension of $\mathbb{Q}$.

Definition.

An *absolute value* of a number field k is a function $|\ | : k \longrightarrow \mathbb{R}$ satisfying the following properties, for all $x, y \in k$.

(i) $|x| \geq 0$, e $|x| = 0$ if and only if $x = 0$

(ii) $|xy| = |x||y|$

(iii) $|x + y| \leq |x| + |y|$

Definition.

A *global field* is a finite extension of $\mathbb{Q}$ or a finite extension of $\mathbb{F}_p(t)$.

Definition.

A *number field* k is a finite extension of $\mathbb{Q}$.

Definition.

An *absolute value* of a number field k is a function $|\ | : k \longrightarrow \mathbb{R}$ satisfying the following properties, for all $x, y \in k$.

(I) $|x| \geq 0$, e $|x| = 0$ if and only if $x = 0$

(II) $|xy| = |x||y|$

(III) $|x + y| \leq |x| + |y|$

Definition.

A *global field* is a finite extension of $\mathbb{Q}$ or a finite extension of $\mathbb{F}_p(t)$.

Definition.

A *number field* k is a finite extension of $\mathbb{Q}$.

Definition.

An *absolute value* of a number field k is a function $|\ | : k \longrightarrow \mathbb{R}$ satisfying the following properties, for all $x, y \in k$.

(I) $|x| \geq 0$, e $|x| = 0$ if and only if $x = 0$

(II) $|xy| = |x||y|$

(III) $|x + y| \leq |x| + |y|$

Examples.

- $|\ \ |_\infty$ the usual absolute value over $\mathbb{Q}$
- Let $a = \frac{b}{c}$, with $b, c \in \mathbb{Z}$, coprime. Let p be a prime number. Assume

$$a = p^l \frac{b'}{c'}, \quad (b'c', p) = 1$$

The function $|\ \ |_p$, defined by $|a|_p := \frac{1}{p^l}$, is an absolute value of $\mathbb{Q}$, named the *p-adic absolute value*.

Examples.

- $|\ \ |_\infty$ the usual absolute value over $\mathbb{Q}$
- Let $a = \frac{b}{c}$, with $b, c \in \mathbb{Z}$, coprime. Let p be a prime number. Assume

$$a = p^l \frac{b'}{c'}, \quad (b'c', p) = 1$$

The function $|\ \ |_p$, defined by $|a|_p := \frac{1}{p^l}$, is an absolute value of $\mathbb{Q}$, named the *p-adic absolute value.*

Examples.

- $|\ \ |_\infty$ the usual absolute value over $\mathbb{Q}$
- Let $a = \frac{b}{c}$, with $b, c \in \mathbb{Z}$, coprime. Let p be a prime number. Assume

$$a = p^l \frac{b'}{c'}, \qquad (b'c', p) = 1$$

The function $|\ \ |_p$, defined by $|a|_p := \frac{1}{p^l}$, is an absolute value of $\mathbb{Q}$, named the *p-adic absolute value*.

DEFINITION.

We say that two *absolute values* of k are equivalent if they induce the same topology over k.

OSTROWSKI'S THEOREM.

Every absolute value of $\mathbb{Q}$ is equivalent to one of the absolute values $|\ |_\infty$ or $|\ |_p$.

DEFINITION.

The field obtained as a completion of $\mathbb{Q}$ by the absolute value $|\ |_p$ is called *p-adic field* and it is denoted by $\mathbb{Q}_p$. The elements of $\mathbb{Q}_p$ are called *p-adic numbers*.

DEFINITION.

We say that two *absolute values* of k are equivalent if they induce the same topology over k.

OSTROWSKI'S THEOREM.

Every absolute value of $\mathbb{Q}$ is equivalent to one of the absolute values $|\ |_\infty$ or $|\ |_p$.

DEFINITION.

The field obtained as a completion of $\mathbb{Q}$ by the absolute value $|\ |_p$ is called *p-adic field* and it is denoted by $\mathbb{Q}_p$. The elements of $\mathbb{Q}_p$ are called *p-adic numbers.*

Definition.

We say that two *absolute values* of k are equivalent if they induce the same topology over k.

Ostrowski's Theorem.

Every absolute value of $\mathbb{Q}$ is equivalent to one of the absolute values $|\ \ |_\infty$ or $|\ \ |_p$.

Definition.

The field obtained as a completion of $\mathbb{Q}$ by the absolute value $|\ \ |_p$ is called *p-adic field* and it is denoted by $\mathbb{Q}_p$. The elements of $\mathbb{Q}_p$ are called *p-adic numbers.*

Definition.

We say that two *absolute values* of k are equivalent if they induce the same topology over k.

Ostrowski's Theorem.

Every absolute value of $\mathbb{Q}$ is equivalent to one of the absolute values $|\ |_\infty$ or $|\ |_p$.

Definition.

The field obtained as a completion of $\mathbb{Q}$ by the absolute value $|\ |_p$ is called *p-adic field* and it is denoted by $\mathbb{Q}_p$. The elements of $\mathbb{Q}_p$ are called *p-adic numbers*.

Local-global problems

Definition.

A *local field* is a field obtained as a completion of a global field by one of its absolute values.

In particular the fields $\mathbb{Q}_p$ are local fields.

Definition.

A *local field* is a field obtained as a completion of a global field by one of its absolute values.

In particular the fields $\mathbb{Q}_p$ are local fields.

Definition.

A *local field* is a field obtained as a completion of a global field by one of its absolute values.

In particular the fields $\mathbb{Q}_p$ are local fields.

Hasse Principle, 1923-1924.

Let k be a number field and let $F(X_1, ..., X_n) \in k[X_1, ..., X_n]$ be a quadratic form. If $F = 0$ has a non-trivial solution in k_v, for all completions k_v of k, where v is a place of k, then $F = 0$ has a non-trivial solution in k.

The assumption that F is isotropic in k_v *for all but finitely many completions* implies the same conclusion.

Since then, many mathematicians have been concerned with similar so-called *local-global problems*, i.e. they have been questioning if, given a global field k, the validity of some properties for all but finitely many local fields k_v could ensure the validity of the same properties for k.

Hasse Principle, 1923-1924.

Let k be a number field and let $F(X_1, ..., X_n) \in k[X_1, ..., X_n]$ be a quadratic form. If $F = 0$ has a non-trivial solution in k_v, for all completions k_v of k, where v is a place of k, then $F = 0$ has a non-trivial solution in k.

The assumption that F is isotropic in k_v *for all but finitely many completions* implies the same conclusion.

Since then, many mathematicians have been concerned with similar so-called *local-global problems*, i.e. they have been questioning if, given a global field k, the validity of some properties for all but finitely many local fields k_v could ensure the validity of the same properties for k.

Hasse Principle, 1923-1924.

Let k be a number field and let $F(X_1, ..., X_n) \in k[X_1, ..., X_n]$ be a quadratic form. If $F = 0$ has a non-trivial solution in k_v, for all completions k_v of k, where v is a place of k, then $F = 0$ has a non-trivial solution in k.

The assumption that F is isotropic in k_v *for all but finitely many completions* implies the same conclusion.

Since then, many mathematicians have been concerned with similar so-called *local-global problems*, i.e. they have been questioning if, given a global field k, the validity of some properties for all but finitely many local fields k_v could ensure the validity of the same properties for k.

Notation

$\bar{k}$ the algebraic closure of k

G_k the absolute Galois group $\mathrm{Gal}(\bar{k}/k)$

$$G_k = \{\sigma \in \mathrm{Aut}(\bar{k}) | \sigma(x) = x, \text{ for every } x \in k\}$$

M_k the set of places $v \in k$

$\bar{k}$ the algebraic closure of k

G_k the absolute Galois group $\mathrm{Gal}(\bar{k}/k)$

$$G_k = \{\sigma \in \mathrm{Aut}(\bar{k}) | \sigma(x) = x, \text{ for every } x \in k\}$$

M_k the set of places $v \in k$

$\bar{k}$	the algebraic closure of k
G_k	the absolute Galois group $\mathrm{Gal}(\bar{k}/k)$
	$G_k = \{\sigma \in \mathrm{Aut}(\bar{k}) \mid \sigma(x) = x, \text{ for every } x \in k\}$
M_k	the set of places $v \in k$

$\mathcal{A}$	a commutative algebraic group defined over k
$\mathcal{A}[p^l]$	the p^l-torsion subgroup of $\mathcal{A}$
	$\mathcal{A}[p^l] = \{P \in \mathcal{A} \mid p^l P = 0\}$
$k(\mathcal{A}[p^l])$	the number field obtained by adding to k the coordinates of the points in $\mathcal{A}[p^l]$

$\mathcal{A}$	a commutative algebraic group defined over k
$\mathcal{A}[p^l]$	the p^l-torsion subgroup of $\mathcal{A}$
	$\mathcal{A}[p^l] = \{P \in \mathcal{A} \mid p^l P = 0\}$
$k(\mathcal{A}[p^l])$	the number field obtained by adding to k the coordinates of the points in $\mathcal{A}[p^l]$

Notation

$\mathcal{A}$	a commutative algebraic group defined over k
$\mathcal{A}[p^l]$	the p^l-torsion subgroup of $\mathcal{A}$
	$\mathcal{A}[p^l] = \{P \in \mathcal{A} \mid p^l P = 0\}$
$k(\mathcal{A}[p^l])$	the number field obtained by adding to k the coordinates of the points in $\mathcal{A}[p^l]$

The Local-Global Divisibility Problem

LOCAL-GLOBAL DIVISIBILITY PROBLEM. (DVORNICICH, ZANNIER, 2001)

Let $P \in \mathcal{A}(k)$. Suppose for all but finitely many $v \in M_k$, there exists $D_v \in \mathcal{A}(k_v)$ such that $P = p^l D_v$. Is it possible to conclude that there exists $D \in \mathcal{A}(k)$ such that $P = p^l D$?

This problem has a cohomological interpretation.

Local-Global Divisibility Problem. (Dvornicich, Zannier, 2001)

Let $P \in \mathcal{A}(k)$. Suppose for all but finitely many $v \in M_k$, there exists $D_v \in \mathcal{A}(k_v)$ such that $P = p^l D_v$. Is it possible to conclude that there exists $D \in \mathcal{A}(k)$ such that $P = p^l D$?

This problem has a cohomological interpretation.

Local-Global Divisibility Problem. (Dvornicich, Zannier, 2001)

Let $P \in \mathcal{A}(k)$. Suppose for all but finitely many $v \in M_k$, there exists $D_v \in \mathcal{A}(k_v)$ such that $P = p^l D_v$. Is it possible to conclude that there exists $D \in \mathcal{A}(k)$ such that $P = p^l D$?

This problem has a cohomological interpretation.

Local-Global Divisibility Problem. (Dvornicich, Zannier, 2001)

Let $P \in \mathcal{A}(k)$. Suppose for all but finitely many $v \in M_k$, there exists $D_v \in \mathcal{A}(k_v)$ such that $P = p^l D_v$. Is it possible to conclude that there exists $D \in \mathcal{A}(k)$ such that $P = p^l D$?

This problem has a cohomological interpretation.

Local-Global Divisibility Problem. (Dvornicich, Zannier, 2001)

Let $P \in \mathcal{A}(k)$. Suppose for all but finitely many $v \in M_k$, there exists $D_v \in \mathcal{A}(k_v)$ such that $P = p^l D_v$. Is it possible to conclude that there exists $D \in \mathcal{A}(k)$ such that $P = p^l D$?

This problem has a cohomological interpretation.

Definition.

Let G be a group and let M be a G-module. A *cocycle* of G with values in M (or a *crossed homomorphism* of G in M) is a map

$$Z : G \longrightarrow M$$
$$\sigma \mapsto Z_\sigma$$

such that

$$Z_{\sigma\tau} = Z_\sigma + \sigma(Z_\tau),$$

for every $\sigma, \tau \in G$.

The cocycles of G with values in M form a group denoted by $Z(G, M)$.

Definition.

Let G be a group and let M be a G-module. A *cocycle* of G with values in M (or a *crossed homomorphism* of G in M) is a map

$$Z : G \longrightarrow M$$
$$\sigma \mapsto Z_\sigma$$

such that

$$Z_{\sigma\tau} = Z_\sigma + \sigma(Z_\tau),$$

for every $\sigma, \tau \in G$.

The cocycles of G with values in M form a group denoted by $Z(G, M)$.

Definition.

Let G be a group and let M be a G-module. A *coboundary* of G with value in M is a cocycle Z of G with value in M such that

$$Z_\sigma = (\sigma - 1)A,$$

for some $A \in M$.

The coboundaries of G with values in M form a group denoted by $B(G, M)$.

Definition.

Let G be a group and let M be a G-module. A *coboundary* of G with value in M is a cocycle Z of G with value in M such that

$$Z_\sigma = (\sigma - 1)A,$$

for some $A \in M$.

The coboundaries of G with values in M form a group denoted by $B(G, M)$.

Definition.

Let G be a group and let M be a G-module. The *first cohomology group* of G with values in M is defined as the quotient $Z(G,M)/B(G,M)$ and it is denoted by $H^1(G,M)$.

Let $D \in \mathcal{A}(\bar{k})$ such that $p^l D = P$. We can define a cocycle of G_k with values in $\mathcal{A}[p^l]$ by setting

$$Z_\sigma := \sigma(D) - D, \quad \sigma \in G_k.$$

Proposition.

The class of Z is 0 in $H^1(G_k, \mathcal{A}[p^l])$, if and only if there exists $D' \in \mathcal{A}(k)$ such that $p^l D' = P$.

Corollary

If $H^1(G_k, \mathcal{A}[p^l]) = 0$, then the local-global divisibility by p^l holds in $\mathcal{A}$ over k.

Let $\Sigma \subseteq M_k$, containing all the places v, for which the hypotheses of the problem hold. Then Z vanishes in $H^1(G_{k_v}, \mathcal{A}[p^l])$, for every $v \in \Sigma$.

Let $D \in \mathcal{A}(\bar{k})$ such that $p^l D = P$. We can define a cocycle of G_k with values in $\mathcal{A}[p^l]$ by setting

$$Z_\sigma := \sigma(D) - D, \quad \sigma \in G_k.$$

Proposition.

The class of Z is 0 in $H^1(G_k, \mathcal{A}[p^l])$, if and only if there exists $D' \in \mathcal{A}(k)$ such that $p^l D' = P$.

Corollary

If $H^1(G_k, \mathcal{A}[p^l]) = 0$, then the local-global divisibility by p^l holds in $\mathcal{A}$ over k.

Let $\Sigma \subseteq M_k$, containing all the places v, for which the hypotheses of the problem hold. Then Z vanishes in $H^1(G_{k_v}, \mathcal{A}[p^l])$, for every $v \in \Sigma$.

Let $D \in \mathcal{A}(\bar{k})$ such that $p^l D = P$. We can define a cocycle of G_k with values in $\mathcal{A}[p^l]$ by setting

$$Z_\sigma := \sigma(D) - D, \quad \sigma \in G_k.$$

Proposition.

The class of Z is 0 in $H^1(G_k, \mathcal{A}[p^l])$, if and only if there exists $D' \in \mathcal{A}(k)$ such that $p^l D' = P$.

Corollary

If $H^1(G_k, \mathcal{A}[p^l]) = 0$, then the local-global divisibility by p^l holds in $\mathcal{A}$ over k.

Let $\Sigma \subseteq M_k$, containing all the places v, for which the hypotheses of the problem hold. Then Z vanishes in $H^1(G_{k_v}, \mathcal{A}[p^l])$, for every $v \in \Sigma$.

Let $D \in \mathcal{A}(\bar{k})$ such that $p^l D = P$. We can define a cocycle of G_k with values in $\mathcal{A}[p^l]$ by setting

$$Z_\sigma := \sigma(D) - D, \quad \sigma \in G_k.$$

Proposition.

The class of Z is 0 in $H^1(G_k, \mathcal{A}[p^l])$, if and only if there exists $D' \in \mathcal{A}(k)$ such that $p^l D' = P$.

Corollary

If $H^1(G_k, \mathcal{A}[p^l]) = 0$, then the local-global divisibility by p^l holds in $\mathcal{A}$ over k.

Let $\Sigma \subseteq M_k$, containing all the places v, for which the hypotheses of the problem hold. Then Z vanishes in $H^1(G_{k_v}, \mathcal{A}[p^l])$, for every $v \in \Sigma$.

Let $D \in \mathcal{A}(\bar{k})$ such that $p^l D = P$. We can define a cocycle of G_k with values in $\mathcal{A}[p^l]$ by setting

$$Z_\sigma := \sigma(D) - D, \quad \sigma \in G_k.$$

Proposition.

The class of Z is 0 in $H^1(G_k, \mathcal{A}[p^l])$, if and only if there exists $D' \in \mathcal{A}(k)$ such that $p^l D' = P$.

Corollary

If $H^1(G_k, \mathcal{A}[p^l]) = 0$, then the local-global divisibility by p^l holds in $\mathcal{A}$ over k.

Let $\Sigma \subseteq M_k$, containing all the places v, for which the hypotheses of the problem hold. Then Z vanishes in $H^1(G_{k_v}, \mathcal{A}[p^l])$, for every $v \in \Sigma$.

The *first local cohomology group of* $\mathcal{A}$ over k is defined as

$$H^1_{\mathrm{loc}}(G, \mathcal{A}[p^l]) := \bigcap_{v \in \Sigma} \ker\{H^1(G_k, \mathcal{A}[p^l]) \xrightarrow{res_v} H^1(G_{k_v}, \mathcal{A}[p^l])\}.$$

where res_v is the usual restriction map and $G = \mathrm{Gal}(k(\mathcal{A}[p^l])/k)$.

Proposition. (Dvornicich, Zannier, 2001)

If $H^1_{\mathrm{loc}}(G, \mathcal{A}[p^l]) = 0$, then the local-global divisibility by p^l holds in $\mathcal{A}$ over k.

The *first local cohomology group of* $\mathcal{A}$ over k is defined as

$$H^1_{\mathrm{loc}}(G,\mathcal{A}[p^l]) := \bigcap_{v\in\Sigma} \ker\{H^1(G_k,\mathcal{A}[p^l]) \xrightarrow{res_v} H^1(G_{k_v},\mathcal{A}[p^l])\}.$$

where res_v is the usual restriction map and $G = \mathrm{Gal}(k(\mathcal{A}[p^l])/k)$.

Proposition. (Dvornicich, Zannier, 2001)

If $H^1_{\mathrm{loc}}(G,\mathcal{A}[p^l]) = 0$, then the local-global divisibility by p^l holds in $\mathcal{A}$ over k.

The *first local cohomology group of* $\mathcal{A}$ over k is defined as

$$H^1_{\mathrm{loc}}(G, \mathcal{A}[p^l]) := \bigcap_{v \in \Sigma} \ker\{H^1(G_k, \mathcal{A}[p^l]) \xrightarrow{res_v} H^1(G_{k_v}, \mathcal{A}[p^l])\}.$$

where res_v is the usual restriction map and $G = \mathrm{Gal}(k(\mathcal{A}[p^l])/k)$.

Proposition. (Dvornicich, Zannier, 2001)

If $H^1_{\mathrm{loc}}(G, \mathcal{A}[p^l]) = 0$, then the local-global divisibility by p^l holds in $\mathcal{A}$ over k.

$$H^1_{\mathrm{loc}}(G, \mathcal{A}[p^l]) = \bigcap_{v \in \Sigma} \ker\{H^1(G_k, \mathcal{A}[p^l]) \xrightarrow{res_v} H^1(G_{k_v}, \mathcal{A}[p^l])\}.$$

This definition is very similar to the one of the Tate-Shafarevich group

$$\text{Ш}(k, \mathcal{A}[p^l]) := \bigcap_{v \in M_k} \ker\{H^1(G_k, \mathcal{A}[p^l]) \xrightarrow{res_v} H^1(G_{k_v}, \mathcal{A}[p^l])\}.$$

$$H^1_{\mathrm{loc}}(G, \mathcal{A}[p^l]) = \bigcap_{v\in\Sigma} \ker\{H^1(G_k, \mathcal{A}[p^l]) \xrightarrow{res_v} H^1(G_{k_v}, \mathcal{A}[p^l])\}.$$

This definition is very similar to the one of the Tate-Shafarevich group

$$Ш(k, \mathcal{A}[p^l]) := \bigcap_{v\in M_k} \ker\{H^1(G_k, \mathcal{A}[p^l]) \xrightarrow{res_v} H^1(G_{k_v}, \mathcal{A}[p^l])\}.$$

Cassels' question

Cassels' Question, 1962.

Let k be a number field and $\mathcal{E} : y^2 = x^3 + bx + c$ an elliptic curve defined over k. Are the elements of $Ш(k, \mathcal{E})$ infinitely divisible by a prime p when considered as elements of the group $H^1(G_k, \mathcal{E})$?

Proposition.

If $Ш(k, \mathcal{E}[p^l]) = 0$, for every l, then Cassels' question has an affirmative answer for p.

Cassels' Question, 1962.

Let k be a number field and $\mathcal{E} : y^2 = x^3 + bx + c$ an elliptic curve defined over k. Are the elements of $\text{Ш}(k, \mathcal{E})$ infinitely divisible by a prime p when considered as elements of the group $H^1(G_k, \mathcal{E})$?

Proposition.

If $\text{Ш}(k, \mathcal{E}[p^l]) = 0$, for every l, then Cassels' question has an affirmative answer for p.

Solutions

(TATE, 1962)

Cassels' question has an affirmative answer for the divisibility by p (one time).

The question for the divisibility by powers of p remained open for decades, for every p.

(Tate, 1962)

Cassels' question has an affirmative answer for the divisibility by p (one time).

The question for the divisibility by powers of p remained open for decades, for every p.

Theorem. (P., Ranieri, Viada, 2012)

The local-global divisibility by p^l holds in $\mathcal{E}$ over k, for all $p > (3^{[k:\mathbb{Q}]/2} + 1)^2$ and $l \geq 1$.

Corollary. (P., Ranieri, Viada, 2012)

Cassels' question has an affirmative answer over k for all $p > (3^{[k:\mathbb{Q}]/2} + 1)^2$.

Theorem. (P., Ranieri, Viada, 2012)

The local-global divisibility by p^l holds in $\mathcal{E}$ over k, for all $p > (3^{[k:\mathbb{Q}]/2} + 1)^2$ and $l \geq 1$.

Corollary. (P., Ranieri, Viada, 2012)

Cassels' question has an affirmative answer over k for all $p > (3^{[k:\mathbb{Q}]/2} + 1)^2$.

THEOREM. (P., RANIERI, VIADA, 2012-2014)

The local-global divisibility by p^l holds in $\mathcal{E}$ over $\mathbb{Q}$, for all $p \geq 5$ and $l \geq 1$.

COROLLARY. (P., RANIERI, VIADA, 2012-2014)

Cassels' question has an affirmative answer over $\mathbb{Q}$ for all $p \geq 5$.

A second proof.

THEOREM. (ÇIPERIANI, STIX, 2015)

Cassels' question has an affirmative answer in elliptic curves defined over $\mathbb{Q}$, for all $p \geq 11$.

Theorem. (P., Ranieri, Viada, 2012-2014)

The local-global divisibility by p^l holds in $\mathcal{E}$ over $\mathbb{Q}$, for all $p \geq 5$ and $l \geq 1$.

Corollary. (P., Ranieri, Viada, 2012-2014)

Cassels' question has an affirmative answer over $\mathbb{Q}$ for all $p \geq 5$.

A second proof.

Theorem. (Çiperiani, Stix, 2015)

Cassels' question has an affirmative answer in elliptic curves defined over $\mathbb{Q}$, for all $p \geq 11$.

THEOREM. (P., RANIERI, VIADA, 2012-2014)

The local-global divisibility by p^l holds in $\mathcal{E}$ over $\mathbb{Q}$, for all $p \geq 5$ and $l \geq 1$.

COROLLARY. (P., RANIERI, VIADA, 2012-2014)

Cassels' question has an affirmative answer over $\mathbb{Q}$ for all $p \geq 5$.

A second proof.

THEOREM. (ÇIPERIANI, STIX, 2015)

Cassels' question has an affirmative answer in elliptic curves defined over $\mathbb{Q}$, for all $p \geq 11$.

Counterexamples

in elliptic curves over $\mathbb{Q}$ for all 2^n, with $n \geq 2$ (P., 2011);

in elliptic curves over $\mathbb{Q}$ for all 3^n, with $n \geq 2$ (Creutz, 2016).

Counterexamples

in elliptic curves over $\mathbb{Q}$ for all 2^n, with $n \geq 2$ (P., 2011);

in elliptic curves over $\mathbb{Q}$ for all 3^n, with $n \geq 2$ (Creutz, 2016).

Counterexamples

in elliptic curves over $\mathbb{Q}$ for all 2^n, with $n \geq 2$ (P., 2011);

in elliptic curves over $\mathbb{Q}$ for all 3^n, with $n \geq 2$ (Creutz, 2016).

THEOREM. (P., 2019)

Let p be a prime number. Let k be a number field and let $\mathcal{A}$ be a commutative algebraic group defined over k, with $\mathcal{A}[p] \simeq (\mathbb{Z}/p\mathbb{Z})^n$.

Assume that $\mathcal{A}[p]$ is an irreducible N-module or a direct sum of irreducible N-modules, for every subnormal subgroup N of $\mathrm{Gal}(k(\mathcal{A}[p^l])/k)$.

If $p > \frac{n}{2} + 1$, then the local-global divisibility by p holds in $\mathcal{A}$ over k and $\text{Ш}(k, \mathcal{A}[p]) = 0$.

THEOREM. (P., 2019)

Let p be a prime number. Let k be a number field and let $\mathcal{A}$ be a commutative algebraic group defined over k, with $\mathcal{A}[p] \simeq (\mathbb{Z}/p\mathbb{Z})^n$.

Assume that $\mathcal{A}[p]$ is an irreducible N-module or a direct sum of irreducible N-modules, for every subnormal subgroup N of $\mathrm{Gal}(k(\mathcal{A}[p^l])/k)$.

If $p > \frac{n}{2} + 1$, then the local-global divisibility by p holds in $\mathcal{A}$ over k and $\text{Ш}(k, \mathcal{A}[p]) = 0$.

Theorem. (P., 2019)

Let p be a prime number. Let k be a number field and let $\mathcal{A}$ be a commutative algebraic group defined over k, with $\mathcal{A}[p] \simeq (\mathbb{Z}/p\mathbb{Z})^n$.

Assume that $\mathcal{A}[p]$ is an irreducible N-module or a direct sum of irreducible N-modules, for every subnormal subgroup N of $\mathrm{Gal}(k(\mathcal{A}[p^l])/k)$.

If $p > \frac{n}{2} + 1$, then the local-global divisibility by p holds in $\mathcal{A}$ over k and $\text{Ш}(k, \mathcal{A}[p]) = 0$.

Theorem. (P., 2019)

Let p be a prime number. Let G be a group and let $M = (\mathbb{Z}/p\mathbb{Z})^n$ a G-module.

Assume that M is an irreducible N-module or a direct sum of irreducible N-modules, for every subnormal subgroup N of G.

If $p > \left(\frac{n}{2} + 1\right)^2$, then $H^1(G, M) = 0$.

THEOREM. (P., 2019)

Let p be a prime number. Let G be a group and let $M = (\mathbb{Z}/p\mathbb{Z})^n$ a G-module.

Assume that M is an irreducible N-module or a direct sum of irreducible N-modules, for every subnormal subgroup N of G.

If $p > \left(\frac{n}{2} + 1\right)^2$, then $H^1(G, M) = 0$.

Theorem. (P., 2019)

Let p be a prime number. Let G be a group and let $M = (\mathbb{Z}/p\mathbb{Z})^n$ a G-module.

Assume that M is an irreducible N-module or a direct sum of irreducible N-modules, for every subnormal subgroup N of G.

If $p > \left(\frac{n}{2} + 1\right)^2$, then $H^1(G, M) = 0$.

Thank you for your attention!