Local-global divisibility on algebraic tori

Jessica Alessandrì

Università degli Studi dell'Aquila

Joint work with Rocco Chirivì and Laura Paladino

32èmes Journées Arithmétiques 2023

6 July 2023

The local-global divisibility problem

Let

- k be a number field;
- M_k be the set of places of k;
- k_v be the completion of k at $v \in M_k$;

The local-global divisibility problem

Let

- k be a number field;
- M_k be the set of places of k;
- k_v be the completion of k at $v \in M_k$;

Theorem (Hasse principle for quadratic forms, 1924)

A quadratic form $F(X_1, \ldots, X_n) \in k[X_1, \ldots, X_n]$ has nontrivial zeros in k if and only if it has nontrivial zeros in k_v, for every $v \in M_k$.

"for every $v \in M_k$" $\longrightarrow$ "for all but finitely many $v \in M_k$"

Question

With $k = \mathbb{Q}$ and $n = 2$: is it true that if $m \in \mathbb{Q}$ is a square modulo almost all primes, then it is a (perfect) square in $\mathbb{Q}$?

"for every $v \in M_k$" $\longrightarrow$ "for all but finitely many $v \in M_k$"

Question

With $k = \mathbb{Q}$ and $n = 2$: is it true that if $m \in \mathbb{Q}$ is a square modulo almost all primes, then it is a (perfect) square in $\mathbb{Q}$?

Question (revisited)

With q–powers and arbitrary k: is it true that if $P \in \mathbb{G}_m(k)$ is such that $P = R_v^q$ in $\mathbb{G}_m(k_v)$ for almost every v, then $P = R^q$ in $\mathbb{G}_m(k)$?

"for every $v \in M_k$" $\longrightarrow$ "for all but finitely many $v \in M_k$"

Question

With $k = \mathbb{Q}$ and $n = 2$: is it true that if $m \in \mathbb{Q}$ is a square modulo almost all primes, then it is a (perfect) square in $\mathbb{Q}$?

Question (revisited)

With q–powers and arbitrary k: is it true that if $P \in \mathbb{G}_m(k)$ is such that $P = R_v^q$ in $\mathbb{G}_m(k_v)$ for almost every v, then $P = R^q$ in $\mathbb{G}_m(k)$?

An answer is given by the Grunwald-Wang Theorem.

Let $\mathcal{G}$ be a commutative algebraic group defined over k and fix q a positive integer.

Problem (Dvornicich and Zannier, 2001)

If $P \in \mathcal{G}(k)$ is such that $P = qD_v$ for some $D_v \in \mathcal{G}(k_v)$, for all but finitely many $v \in M_k$, can we conclude that $P = qD$ for some $D \in \mathcal{G}(k)$?

Let $\mathcal{G}$ be a commutative algebraic group defined over k and fix q a positive integer.

Problem (Dvornicich and Zannier, 2001)

If $P \in \mathcal{G}(k)$ is such that $P = qD_v$ for some $D_v \in \mathcal{G}(k_v)$, for all but finitely many $v \in M_k$, can we conclude that $P = qD$ for some $D \in \mathcal{G}(k)$?

By the Bézout identity it is enough to answer when $q = p^r$, with p prime.

Cohomological interpretation

Fix $q = p^r$, with p prime number.

Cohomological interpretation

Fix $q = p^r$, with p prime number.
$K := k(\mathcal{G}[q])$ is finite Galois over k with $G := \mathrm{Gal}(K/k)$.

Cohomological interpretation

Fix $q = p^r$, with p prime number.
$K := k(\mathcal{G}[q])$ is finite Galois over k with $G := \mathrm{Gal}(K/k)$.

Definition

We say that the class of a cocycle $[c] = [\{Z_\sigma\}_{\sigma \in G}] \in \mathrm{H}^1(G, \mathcal{G}[q])$ **satisfies the local conditions** if

$$\forall \sigma \in G \; \exists W_\sigma \in \mathcal{G}[q] \text{ s.t. } Z_\sigma = (\sigma - 1) W_\sigma .$$

The subgroup of $\mathrm{H}^1(G, \mathcal{G}[q])$ of these classes is called the **first local cohomology group** $\mathrm{H}^1_{\mathrm{loc}}(G, \mathcal{G}[q])$.

Cohomological interpretation

Fix $q = p^r$, with p prime number.
$K := k(\mathcal{G}[q])$ is finite Galois over k with $G := \mathrm{Gal}(K/k)$.

Definition

We say that the class of a cocycle $[c] = [\{Z_\sigma\}_{\sigma \in G}] \in \mathrm{H}^1(G, \mathcal{G}[q])$ **satisfies the local conditions** if

$$\forall \sigma \in G \ \exists W_\sigma \in \mathcal{G}[q] \text{ s.t. } Z_\sigma = (\sigma - 1)W_\sigma.$$

The subgroup of $\mathrm{H}^1(G, \mathcal{G}[q])$ of these classes is called the **first local cohomology group** $\mathrm{H}^1_{\mathrm{loc}}(G, \mathcal{G}[q])$.

$$\mathrm{H}^1_{\mathrm{loc}}(G, \mathcal{G}[q]) = \bigcap_{\substack{C \leq G \\ C \text{ cyclic}}} \ker \left(\mathrm{H}^1(G, \mathcal{G}[q]) \xrightarrow{\mathrm{res}} \mathrm{H}^1(C, \mathcal{G}[q]) \right).$$

Cohomological interpretation

Fix $q = p^r$, with p prime number.
$K := k(\mathcal{G}[q])$ is finite Galois over k with $G := \mathrm{Gal}(K/k)$.

Definition

We say that the class of a cocycle $[c] = [\{Z_\sigma\}_{\sigma \in G}] \in \mathrm{H}^1(G, \mathcal{G}[q])$ **satisfies the local conditions** if

$$\forall \sigma \in G \; \exists W_\sigma \in \mathcal{G}[q] \text{ s.t. } Z_\sigma = (\sigma - 1)W_\sigma .$$

The subgroup of $\mathrm{H}^1(G, \mathcal{G}[q])$ of these classes is called the **first local cohomology group** $\mathrm{H}^1_{\mathrm{loc}}(G, \mathcal{G}[q])$.

$$\mathrm{H}^1_{\mathrm{loc}}(G, \mathcal{G}[q]) = \bigcap_{\substack{C \leq G \\ C \text{ cyclic}}} \ker \left(\mathrm{H}^1(G, \mathcal{G}[q]) \xrightarrow{\mathrm{res}} \mathrm{H}^1(C, \mathcal{G}[q]) \right).$$

Clearly, if G is cyclic then $\mathrm{H}^1_{\mathrm{loc}}(G, \mathcal{G}[q]) = 0$.

$$\Sigma = \{v \in M_k \mid v \text{ unramified in } K\}$$

If $v \in \Sigma$ and $w|v$, the group $G_v = \mathrm{Gal}(K_w/k_v)$ is cyclic.

$$\Sigma = \{v \in M_k \mid v \text{ unramified in } K\}$$

If $v \in \Sigma$ and $w|v$, the group $G_v = \mathrm{Gal}(K_w/k_v)$ is cyclic.
By the Čhebotarev Density Theorem, G_v varies over all cyclic subgroups of G, as v varies in Σ.

$$\Sigma = \{v \in M_k \mid v \text{ unramified in } K\}$$

If $v \in \Sigma$ and $w|v$, the group $G_v = \mathrm{Gal}(K_w/k_v)$ is cyclic.
By the Čhebotarev Density Theorem, G_v varies over all cyclic subgroups of G, as v varies in Σ.

$$\mathrm{H}^1_{\mathrm{loc}}(G, \mathcal{G}[q]) = \bigcap_{v \in \Sigma} \ker \left(\mathrm{H}^1(G, \mathcal{G}[q]) \xrightarrow{\mathrm{res}_v} \mathrm{H}^1(G_v, \mathcal{G}[q]) \right). \qquad (1)$$

Remark: if we take all places we get a group isomorphic to the Tate-Shafarevich group $Ш(k, \mathcal{G}[q])$.

Theorem (Dvornicich - Zannier, 2001)

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

Theorem (Dvornicich - Zannier, 2001)

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

Let G_p be a p–Sylow subgroup of G.

Theorem (Dvornicich - Zannier, 2001)

$$\mathrm{H}^1_{\mathrm{loc}}(G_p, \mathcal{G}[q]) = 0 \implies \mathrm{H}^1_{\mathrm{loc}}(G, \mathcal{G}[q]) = 0$$

Theorem (Dvornicich - Zannier, 2001)

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

Let G_p be a p–Sylow subgroup of G.

Theorem (Dvornicich - Zannier, 2001)

$$\mathrm{H}^1_{\mathrm{loc}}(G_p, \mathcal{G}[q]) = 0 \implies \mathrm{H}^1_{\mathrm{loc}}(G, \mathcal{G}[q]) = 0$$

Theorem (Dvornicich - Zannier, 2007)

If $\mathrm{H}^1_{\mathrm{loc}}(G, \mathcal{G}[q]) \neq 0$, *there exists a number field L such that the local-global divisibility by q does not hold for* $\mathcal{G}(L)$.

Known results

- Elliptic curves:
  - yes for $q = p$;
  - yes for $q = p^r$:
    - with $p \geq 5$ if $k = \mathbb{Q}$,
    - with $p > C([k : \mathbb{Q}])$ if k does not contain $\mathbb{Q}(\zeta_p + \overline{\zeta}_p)$;
  - no for $q = 2^m, 3^m$, with $m \geq 2$.

Known results

- Elliptic curves:
  - yes for $q = p$;
  - yes for $q = p^r$:
    - with $p \geq 5$ if $k = \mathbb{Q}$,
    - with $p > C([k : \mathbb{Q}])$ if k does not contain $\mathbb{Q}(\zeta_p + \overline{\zeta}_p)$;
  - no for $q = 2^m, 3^m$, with $m \geq 2$.
- Abelian varieties: conditions on $\mathcal{A}[q]$ for principally polarized abelian varieties, for $q = p^r$.

Known results

- Elliptic curves:
  - yes for $q = p$;
  - yes for $q = p^r$:
    - with $p \geq 5$ if $k = \mathbb{Q}$,
    - with $p > C([k : \mathbb{Q}])$ if k does not contain $\mathbb{Q}(\zeta_p + \overline{\zeta}_p)$;
  - no for $q = 2^m, 3^m$, with $m \geq 2$.
- Abelian varieties: conditions on $\mathcal{A}[q]$ for principally polarized abelian varieties, for $q = p^r$.
- General commutative groups: conditions for $q = p$.

Known results for algebraic tori

Classical case $T = \mathbb{G}_m$: we have a complete answer.

Known results for algebraic tori

Classical case $T = \mathbb{G}_m$: we have a complete answer.

Theorem (Grunwald-Wang Theorem)

Let $m = 2^t m'$ be an integer, with m' odd. If $\alpha \in k^\times$ is such that $\alpha \in k_p^m$ for all but finitely many primes and $k(\zeta_{2^t})/k$ is cyclic, then $\alpha \in k^m$.

Thus, for m odd, or divisible at most by 4, the answer is affirmative.

Known results for algebraic tori

Classical case $T = \mathbb{G}_m$: we have a complete answer.

Theorem (Grunwald-Wang Theorem)

Let $m = 2^t m'$ be an integer, with m' odd. If $\alpha \in k^\times$ is such that $\alpha \in k_p^m$ for all but finitely many primes and $k(\zeta_{2^t})/k$ is cyclic, then $\alpha \in k^m$.

Thus, for m odd, or divisible at most by 4, the answer is affirmative.
For $m = 2^t$, with $t \geq 3$, the answer is negative.

Known results for algebraic tori

Classical case $T = \mathbb{G}_m$: we have a complete answer.

Theorem (Grunwald-Wang Theorem)

Let $m = 2^t m'$ be an integer, with m' odd. If $\alpha \in k^\times$ is such that $\alpha \in k_p^m$ for all but finitely many primes and $k(\zeta_{2^t})/k$ is cyclic, then $\alpha \in k^m$.

Thus, for m odd, or divisible at most by 4, the answer is affirmative. For $m = 2^t$, with $t \geq 3$, the answer is negative.

Example (Trost, 1948)

The equation $x^8 - 16 = 0$ has solutions in $\mathbb{Q}_p$ for all odd primes p, but has no solution in $\mathbb{Q}$ (and $\mathbb{Q}_2$).

What about the non-split case?

What about the non-split case?

Theorem (Dvornicich - Zannier, 2001)

If T is an algebraic k–torus of dimension $n \leq \max(3, 2(p-1))$, then the local-global divisibility by p holds for $T(k)$.

What about the non-split case?

Theorem (Dvornicich - Zannier, 2001)

If T is an algebraic k–torus of dimension $n \leq \max(3, 2(p-1))$, then the local-global divisibility by p holds for $T(k)$.

Example (Dvornicich - Zannier, 2001)

There exists a torus T over $k = \mathbb{Q}(\zeta_{p^3})$, with $\dim(T) = p^4 - p^2 + 1$, and a point $P \in T(k)$ such that P locally p–divisible for all but finitely many $v \in M_k$, but not globally.

What about the non-split case?

Theorem (Dvornicich - Zannier, 2001)

If T is an algebraic k–torus of dimension $n \leq \max(3, 2(p-1))$, then the local-global divisibility by p holds for $T(k)$.

Example (Dvornicich - Zannier, 2001)

There exists a torus T over $k = \mathbb{Q}(\zeta_{p^3})$, with $\dim(T) = p^4 - p^2 + 1$, and a point $P \in T(k)$ such that P locally p–divisible for all but finitely many $v \in M_k$, but not globally.

The problem was left open for $2p - 1 \leq \dim(T) < p^4 - p^2 + 1$.

Theorem (Illengo, 2008)

Let $p \neq 2$ be a prime and T an algebraic k–torus of dimension $n < 3(p-1)$. Then the local-global divisibility by p holds for $T(k)$.

Theorem (Illengo, 2008)

Let $p \neq 2$ *be a prime and* T *an algebraic* k*–torus of dimension* $n < 3(p-1)$*. Then the local-global divisibility by* p *holds for* $T(k)$*.*

Proposition (Illengo, 2008)

There exists T *with* $\dim(T) = 3(p-1)$ *defined over some* k *and (possibly extending* k*) a* $P \in T(k)$ *for which the local-global divisibility by* $p \neq 2$ *fails.*

Thus the bound founded for the local-global divisibily by p is sharp.

The case $q = p$ on algebraic tori is completely solved.
What can we say for $q = p^r$?

The case $q = p$ on algebraic tori is completely solved.
What can we say for $q = p^r$?

Theorem 1 (A., Chirivì, Paladino)

Let $p \neq 2$ be a prime.

(a) *Let T be a torus defined over k. If $\dim(T) < p - 1$, then the local-global divisibility by every power p^r holds for $T(k)$.*

(b) *For each $n \geq p - 1$ there exists a torus T defined over a number field k with $\dim(T) = n$ and a finite extension L/k such that the local-global divisibility by p^r does not hold for $T(L)$ for any $r \geq 2$.*

The case $q = p$ on algebraic tori is completely solved.
What can we say for $q = p^r$?

Theorem 1 (A., Chirivì, Paladino)

Let $p \neq 2$ be a prime.

(a) *Let T be a torus defined over k. If $\dim(T) < p - 1$, then the local-global divisibility by every power p^r holds for $T(k)$.*

(b) *For each $n \geq p - 1$ there exists a torus T defined over a number field k with $\dim(T) = n$ and a finite extension L/k such that the local-global divisibility by p^r does not hold for $T(L)$ for any $r \geq 2$.*

To prove (a), we showed that if $\dim(T) < p - 1$ then G_p is cyclic
$\implies \mathrm{H}^1_{\mathrm{loc}}(G_p, T[p^r]) = 0$.

Sketch of proof of part (b)

Remark: $T[q] \simeq (\mathbb{Z}/q\mathbb{Z})^n$, with $n = \dim(T)$.
$\mathrm{Gal}\left(k(T[q])/k\right) \hookrightarrow \mathrm{GL}_n\left(\mathbb{Z}/q\mathbb{Z}\right)$.

Sketch of proof of part (b)

Remark: $T[q] \simeq (\mathbb{Z}/q\mathbb{Z})^n$, with $n = \dim(T)$.
$\mathrm{Gal}\,(k(T[q])/k) \hookrightarrow \mathrm{GL}_n\,(\mathbb{Z}/q\mathbb{Z})$.

Lemma 2 (A., Chirivì, Paladino)

There exists an algebraic torus T of dimension $r = p - 1$ defined over $\mathbb{Q}(\zeta_p)$ such that $G = \mathrm{Gal}\left(k(T[p^2])/k\right) \simeq \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ and is generated in $\mathrm{GL}_r(\mathbb{Z}/p^2\mathbb{Z})$ by

$$\gamma_1 = \begin{pmatrix} 0 & & & & -1 \\ 1 & 0 & & & -1 \\ & \ddots & \ddots & & \vdots \\ & & 1 & 0 & -1 \\ & & & 1 & -1 \end{pmatrix} \quad \textit{and} \quad \gamma_2 = \begin{pmatrix} p+1 & & \\ & \ddots & \\ & & p+1 \end{pmatrix}.$$

Lemma 3 (A., Chirivì, Paladino)

There exists a (unique) extension of

$$\gamma_1 \longmapsto v_1 = \begin{pmatrix} p-1 \\ 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix}, \quad \gamma_2 \longmapsto v_2 = \begin{pmatrix} p \\ \vdots \\ p \\ 0 \end{pmatrix}$$

to a non-trivial element of $\mathrm{H}^1_{\mathrm{loc}}\left(G, (\mathbb{Z}/p^2\mathbb{Z})^{p-1}\right)$.

$\mathrm{H}^1_{\mathrm{loc}}(G, T[p^2]) \neq 0 \implies$ local-global divisibility by p^2 fails (in a finite extension).

Lemma 3 (A., Chirivì, Paladino)

There exists a (unique) extension of

$$\gamma_1 \longmapsto v_1 = \begin{pmatrix} p-1 \\ 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix}, \quad \gamma_2 \longmapsto v_2 = \begin{pmatrix} p \\ \vdots \\ p \\ 0 \end{pmatrix}$$

to a non-trivial element of $\mathrm{H}^1_{\mathrm{loc}}\left(G, (\mathbb{Z}/p^2\mathbb{Z})^{p-1}\right)$.

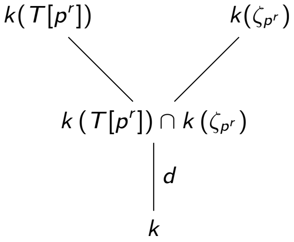
$\mathrm{H}^1_{\mathrm{loc}}(G, T[p^2]) \neq 0 \implies$ local-global divisibility by p^2 fails (in a finite extension).

For $r \geq 2$: p^2–divisibility fails $\implies$ p^r–divisibility fails.

If $\zeta_{p^r} \in k$ the local-global divisibility by every odd p^r still holds.

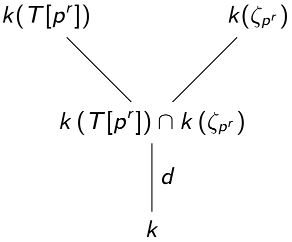
If $\zeta_{p^r} \in k$ the local-global divisibility by every odd p^r still holds.

$d := [k\,(T[p^r]) \cap k\,(\zeta_{p^r}) : k]$.



If $\zeta_{p^r} \in k$ the local-global divisibility by every odd p^r still holds.

$d := [k\,(T[p^r]) \cap k\,(\zeta_{p^r}) : k]$.



Theorem 4 (A., Chirivì, Paladino)

If T is a torus defined over k with $\dim(T) < 3(p-1)$ and $p \nmid d$, then the local-global divisibility by p^r holds for $T(k)$.

Sketch of proof

For $r = 1$, we have the results of Dvornicich-Zannier and Illengo.

Sketch of proof

For $r = 1$, we have the results of Dvornicich-Zannier and Illengo.

Assume $r \geq 2$ and $\mathrm{H}^1_{\mathrm{loc}}(\mathrm{Gal}(k\left(T[p^j]\right)/k), T[p^j]) = 0$ for $j < r$.

Sketch of proof

For $r = 1$, we have the results of Dvornicich-Zannier and Illengo.

Assume $r \geq 2$ and $\mathrm{H}^1_{\mathrm{loc}}(\mathrm{Gal}(k\left(T[p^j]\right)/k), T[p^j]) = 0$ for $j < r$.

We prove that $G = \mathrm{Gal}(k\left(T[p^r]\right)/k)$ acts on

$$1 \longrightarrow T[p] \xrightarrow{\iota} T[p^r] \xrightarrow{\varepsilon} T[p^{r-1}] \longrightarrow 1$$

Sketch of proof

For $r = 1$, we have the results of Dvornicich-Zannier and Illengo.

Assume $r \geq 2$ and $\mathrm{H}^1_{\mathrm{loc}}(\mathrm{Gal}(k\left(T[p^j]\right)/k), T[p^j]) = 0$ for $j < r$.

We prove that $G = \mathrm{Gal}(k\left(T[p^r]\right)/k)$ acts on

$$1 \longrightarrow T[p] \xrightarrow{\iota} T[p^r] \xrightarrow{\varepsilon} T[p^{r-1}] \longrightarrow 1$$

which induces

$$\mathrm{H}^1_{\mathrm{loc}}(G, T[p]) \longrightarrow \mathrm{H}^1_{\mathrm{loc}}(G, T[p^r]) \longrightarrow \mathrm{H}^1_{\mathrm{loc}}(G, T[p^{r-1}])$$

Sketch of proof

For $r = 1$, we have the results of Dvornicich-Zannier and Illengo.

Assume $r \geq 2$ and $\mathrm{H}^1_{\mathrm{loc}}(\mathrm{Gal}(k\left(T[p^j]\right)/k), T[p^j]) = 0$ for $j < r$.

We prove that $G = \mathrm{Gal}(k\left(T[p^r]\right)/k)$ acts on

$$1 \longrightarrow T[p] \xrightarrow{\iota} T[p^r] \xrightarrow{\varepsilon} T[p^{r-1}] \longrightarrow 1$$

which induces

$$\underset{=0}{\mathrm{H}^1_{\mathrm{loc}}(G, T[p])} \longrightarrow \mathrm{H}^1_{\mathrm{loc}}(G, T[p^r]) \longrightarrow \underset{=0}{\mathrm{H}^1_{\mathrm{loc}}(G, T[p^{r-1}])}$$

Sketch of proof

For $r = 1$, we have the results of Dvornicich-Zannier and Illengo.

Assume $r \geq 2$ and $\mathrm{H}^1_{\mathrm{loc}}(\mathrm{Gal}(k\left(T[p^j]\right)/k), T[p^j]) = 0$ for $j < r$.

We prove that $G = \mathrm{Gal}(k\left(T[p^r]\right)/k)$ acts on

$$1 \longrightarrow T[p] \xrightarrow{\iota} T[p^r] \xrightarrow{\varepsilon} T[p^{r-1}] \longrightarrow 1$$

which induces

$$\underset{=0}{\mathrm{H}^1_{\mathrm{loc}}(G, T[p])} \longrightarrow \mathrm{H}^1_{\mathrm{loc}}(G, T[p^r]) \longrightarrow \underset{=0}{\mathrm{H}^1_{\mathrm{loc}}(G, T[p^{r-1}])}$$

$$\Longrightarrow \mathrm{H}^1_{\mathrm{loc}}(G, T[p^r]) = 0.$$

Thank you for your attention!

References

- J. Alessandrì, R. Chirivì and L. Paladino, *Local-global divisibility on algebraic tori*, 2023, submitted.
- R. Dvornicich and U. Zannier, *Local-global divisibility of rational points in some commutative algebraic groups*, Bull. Soc. Math. France **129**, no. 3 (2001), 317–338.
- Dvornicich R. and Paladino L., *Local-global questions for divisibility in commutative algebraic groups*, Eur. J. Math., **8** (2022), 599–628.
- Dvornicich R. and Zannier U., *On a local-global principle for the divisibility of a rational point by a positive integer*, Bull. Lond. Math. Soc. **39** (2007), 27–34.
- M. Illengo, *Cohomology of integer matrices and local-global divisibility on the torus*, J. Théor. Nombres Bordeaux, **20** (2008), 327–334.