On almost strong approximation in reductive groups

Andrei S. Rapinchuk
Univerity of Virginia (USA)

June 19, 2025

Basic example: Let K be a field equipped with a valuation v. Then embedding $K \hookrightarrow K_v$ into completion is *dense*.

However, here we get *more* than we could expect:

Theorem 1 (WEAK APPROXIMATION)

Let K be a field, and let $v_1, \ldots, v_r$ be pairwise inequivalent valuations of K. Then diagonal embedding

$$K \hookrightarrow K_{v_1} \times \cdots \times K_{v_r}$$

is dense.

Informally: one can always find $a \in K$ having *prescribed* arithmetic properties at each v_i.

E.g., given primes $p_1, \ldots, p_r$, one can find $q \in \mathbb{Q}^\times$ such that

$$q \notin \mathbb{Q}_{p_i}^{\times 2} \text{ for all } i = 1, \ldots, r.$$

But WA does not allow to recover Chinese Remainder Theorem. Viz., given $a_1, \ldots, a_r \in \mathbb{Z}$, by WA one finds $q \in \mathbb{Q}$ such that

$$q \equiv a_i (\mathrm{mod}\, p_i \mathbb{Z}_{p_i}) \quad \text{for all} \quad i = 1, \ldots, r.$$

However, WA does not guarantee that one can choose $q \in \mathbb{Z}$.

For this, we need to be able to approximate w.r.t. a finite number of nonarchimedean valuations AND satisfy *integrality* conditions at all other nonarchimedean valuations!

Thus, we need an adequate extension of WA to *infinite* sets of valuations – and strong approximation does provide such an extension.

First, let us see what elements of *infinite* products can or cannot be approximated.

E.g., let $K = \mathbb{Q}$, and $V = \{v_p\}$ be set of all p-adic valuations.

For any $q \in \mathbb{Q}$, we have $q \in \mathbb{Z}_p$ for *almost all* p. So,

$$\mathbf{q} = (q_p) \in \prod_p \mathbb{Q}_p$$

cannot be "reasonably well" approximated by $q \in \mathbb{Q}$ unless $q_p \in \mathbb{Z}_p$ for almost all p.

SA says that this is the *only* obstruction to approximation.

Conceptually, this leads to notion of adeles.

In this talk, K is a number field.

- V^K = set of (pairwise inequivalent) valuations of K;
- V^K_∞ (resp., V^K_f) = subset of archimedean (resp., nonarchimedean) valuations;
- $S \subset V^K$ = a subset (possibly, empty).

Adeles

Ring of S-adeles $\mathbb{A}_S$ is restricted product of K_v for $v \in V^K \setminus S$ w.r.t. valuation rings $O_v \subset K_v$ for $v \in V^K \setminus (V^K_\infty \cup S)$. Thus,

$$\mathbb{A}_S := \left\{ (x_v) \in \prod_{v \notin S} K_v \;\middle|\; x_v \in O_v \text{ for almost all } v \notin S \cup V^K_\infty \right\}.$$

$\mathbb{A}_S$ is a locally compact topological ring for *S-adelic topology*.

For this topology, *subring of integral adeles*

$$\mathbb{A}_S(\infty) := \prod_{v \in V^K_\infty \setminus S} K_v \times \prod_{v \in V^K_f \setminus S} O_v$$

is *open*, and on it S-adelic topology coincides with product topology.

We have diagonal embedding $\iota_S \colon K \hookrightarrow \mathbb{A}_S$.

Strong approximation

Definition (preliminary)

We say that K has strong approximation w.r.t S if $\iota_S \colon K \hookrightarrow \mathbb{A}_S$ is dense.

If S is co-finite (i.e., $V = V^K \setminus S$ is finite), then SA w.r.t S reduces to WA w.r.t. V, hence always holds.

Another extreme: $S = \varnothing$. Then $\iota_S(K)$ is *discrete* in $\mathbb{A}_S$, hence **not** dense.

Theorem 2 (strong approximation for K)

For any $S \neq \varnothing$, embedding $\iota_S \colon K \hookrightarrow \mathbb{A}_S$ is dense.

This statement subsumes CRT and is useful in other situations, **but** most arithmetic applications require more sophisticated versions of SA.

Let $X \subset \mathbf{A}^n$ be an affine algebraic variety defined over K.

For K-algebra R, we let $X(R)$ set of R-points of X.

Then $X(\mathbb{A}_S)$ is a topological space for topology induced by S-adelic topology, and we have diagonal embedding

$$\iota_{X,S} \colon X(K) \hookrightarrow X(\mathbb{A}_S).$$

Definition.

X has strong approximation w.r.t. S if embedding $\iota_{X,S}$ is dense.

Identifying $X(K)$ with image of $\iota_{X,S}$, we see that SA for X amounts to

$$\overline{X(K)}^{(S)} = X(\mathbb{A}_S)$$

where $\overline{}^{(S)}$ denotes closure in S-adelic topology.

Integral adeles

$$X(\mathbb{A}_S(\infty)) = \prod_{v \in V_\infty^K \setminus S} X(K_v) \times \prod_{v \in V_f^K \setminus S} X(O_v)$$

form an open subspace on which S-adelic topology coincides with product topology.

Note that SA implies that

$$\overline{X(K) \cap X(\mathbb{A}_S(\infty))}^{(S)} = X(\mathbb{A}_S(\infty)).$$

This can be used to show that X does not have SA.

In fact, there are various obstructions to SA, but there is a criterion for SA for algebraic groups.

Significance of SA for arithmetic of algebraic groups was understood already by M. Eichler in the late 1930s. Since then number of applications has grown considerably, but today I will briefly discuss just two examples.

Let q be a nondegenerate quadratic form in n variables with integer coefficients. Gauss defined the number $c(q)$ of classes in genus of q. What are values of $c(q)$?

- (Kneser, 1956) If $n \geqslant 3$ and q is *indefinite*, then $c(q)$ is always 2^ℓ, and if we fix q then for every $\ell \geqslant 0$ there exists a quadratic form q_ℓ which is rationally equivalent to q with $c(q_\ell) = 2^\ell$.
- (A.R., 1981) If $n \geqslant 2$ and q is *positive definite* then for every $r \geqslant 1$ there exists a quadratic form q_r which is rationally equivalent to q with $c(q_r)$ is divisible by r.

Why such difference?

The reason is that when $n \geqslant 3$ and q is indefinite, $G = \mathrm{Spin}_n(q)$ has SA w.r.t. $S = \{\infty\}$, and when q is positive definite, it doesn't.

Now, let $X \subset \mathbf{A}^n$ be a smooth $\mathbb{Q}$-defined affine algebraic variety, and suppose $f_1, \ldots, f_m \in \mathbb{Z}[x_1, \ldots, x_n]$ generate ideal of polynomials that vanish on X.

For every prime p, we can consider *reduction* $X^{(p)} \subset \mathbf{A}^n$ which is $\mathbb{F}_p$-variety given by

$$\bar{f}_i^{(p)}(x_1, \ldots, x_n) = 0 \quad \text{for} \quad i = 1, \ldots, m,$$

where $\bar{f}_i^{(p)}$ is reduction of f_i mod p.

There exists a finite set of primes Π such that for $p \notin \Pi$, reduction $X^{(p)}$ is smooth. Then by Hensel's Lemma

$$X(\mathbb{Z}_p) \to X(\mathbb{Z}/p^\ell\mathbb{Z})$$

is surjective for all $\ell \geqslant 1$.

Set $\widehat{\mathbb{Z}}_\Pi = \prod_{p \notin \Pi} \mathbb{Z}_p$. Then for any d not involving primes from Π,

$$X(\widehat{\mathbb{Z}}_\Pi) \to X(\widehat{\mathbb{Z}}_\Pi/d\widehat{\mathbb{Z}}_\Pi) = X(\mathbb{Z}/d\mathbb{Z})$$

is surjective.

On the other hand,

$$X(\widehat{\mathbb{Z}}_\Pi) = X(\mathbb{A}_S(\infty)) \quad \text{for} \quad S = \{\infty\} \cup \{v_p \,|\, p \in \Pi\}$$

in our previous notations.

So, if X has SA w.r.t. S, then

$$X(\mathbb{Q}) \cap X(\widehat{\mathbb{Z}}_\Pi) = X(\mathbb{Z}_\Pi)$$

is dense in $X(\widehat{\mathbb{Z}}_\Pi)$ where $\mathbb{Z}_\Pi$ is localization of $\mathbb{Z}$.

This and surjectivity of $X(\widehat{\mathbb{Z}}_\Pi) \to X(\mathbb{Z}/d\mathbb{Z})$ implies that already

$$X(\mathbb{Z}_\Pi) \to X(\mathbb{Z}/d\mathbb{Z})$$

is surjective, for all d not involving primes from Π.

Thus, SA in appropriate set-up allows to lift solutions of congruences to solutions of equations over a suitable localization.

Note that lifting solutions of congruences is a difficult problem.

E.g., lifting is not always possible for $G = \mathrm{GL}_2$, which can be realized as a hypersurface in $\mathbf{A}^5$.

However, lifting is always possible for $G = \mathrm{SL}_2$, which is a hypersurface in $\mathbf{A}^4$.

Criterion for SA explains these phenomena.

There are many more important applications of SA.

This motivated Eichler, Shimura, Weil, Kneser and others to investigate various aspects of SA.

Final criterion for SA for algebraic groups over number fields was obtained by V.P. Platonov.

Theorem 3 (PLATONOV, 1969)

Let G be a connected reductive algebraic group over a number field K, and S be a finite set of valuations of K. Then G has strong approximation w.r.t. S if and only if

(1) *G is simply connected;*

(2) *for every nontrivial K-simple normal K-subgroup $H \subset G$, the group $H_S := \prod_{v \in S} H(K_v)$ is noncompact.*

Platonov proved sufficiency of (1) & (2) by linking SA to Kneser-Tits conjecture, which he established over local fields.

Other ingredients included reduction theory for S-arithmetic groups and theory of p-adic Lie groups.

A proof of SA over global fields of *positive* characteristic was obtained by G.A. Margulis and G. Prasad in 1977. Their argument also used Kneser-Tits conjecture over local fields, **but** instead of p-adic Lie theory relied on measure theory and ergodic theory.

Condition (1) explains absence of SA in GL_2, and (2) in spinor groups of positive definite forms.

On other hand, criterion yields SA for SL_2 (which can be established by elementary means).

Note that (1) is necessary for strong approximation for *finite* S not only in class of algebraic groups but (under minor assumption) in class of all algebraic varieties.

Proposition (MINCHEV, 1989)

Let X be an irreducible normal variety over a number field K. If X is not simply connected (i.e., there exists a nontrivial connected etale cover $Y \to X$ defined over an algebraic closure $\overline{K}$) then X does not have SA w.r.t. any finite set S of valuations of K.

In particular, (nontrivial) algebraic tori **never** have SA w.r.t. any finite S.

In this talk: situation changes if we consider *infinite* S.

Extreme case: S is co-finite (i.e., $V^K \setminus S$ is finite).

Then SA "degenerates" into WA, making this case not very interesting in our context.

Goal: identify situations where SA (almost) holds for tori and general reductive groups for infinite but "small" S (in terms of Dirichlet's density)

This will be the case for sets that we will call *tractable* (to be defined later)

First, we will describe results for tori, and then for arbitrary connected reductive groups.

At the end, we will apply results for tori to the *Congruence Subgroup Problem*.

First, let $T = \mathbb{G}_m$ (multiplicative group = 1-dimensional split torus).

Example 1.

Let $K = \mathbb{Q}$, $S = \{v_\infty\}$. Then

$$T(\mathbb{Q}) = \mathbb{Q}^\times, \quad T(\mathbb{A}_S(\infty)) = \prod_p \mathbb{Z}_p^\times.$$

So, $T(\mathbb{Q}) \cap T(\mathbb{A}_S(\infty)) = \{\pm 1\}$, **not** dense in $T(\mathbb{A}_S(\infty))$, hence T does not have SA w.r.t. S.

Example 2.

Let $K = \mathbb{Q}$, $S = \{v_\infty, v_2\}$. Then

$$T(\mathbb{A}_S(\infty)) = \prod_{p \neq 2} \mathbb{Z}_p^\times \quad \text{and} \quad \Gamma := T(\mathbb{Q}) \cap T(\mathbb{A}_S(\infty)) = \{\pm 2^i\}.$$

There are infinitely many primes $p \equiv 1 (\mathrm{mod}\, 8)$, and for each such p we have $\Gamma \subset \mathbb{Z}_p^{\times 2} \subsetneq \mathbb{Z}_p^\times$. So, Γ is **not** dense in $T(\mathbb{A}_S(\infty))$ (in fact, closure has infinite index), hence T fails to have SA w.r.t. S.

Argument in Example 2 extends to any finite set

$$S = \{v_\infty, v_{q_1}, \dots, v_{q_r}\}$$

as by applying Chebotarev's to $L = \mathbb{Q}(\sqrt{-1}, \sqrt{q_1}, \dots, \sqrt{q_r})$ one finds infinitely many primes p such that

$$-1, q_1, \dots, q_r \in \mathbb{Z}_p^{\times 2} \subsetneq \mathbb{Z}_p^\times,$$

implying that $[T(\mathbb{A}_S) : \overline{T(\mathbb{Q})}^{(S)}] = \infty$ (thus, **no** SA w.r.t. S).

Note: this argument fails for S *infinite* as then $L/\mathbb{Q}$ is infinite and Chebotarev's doesn't apply.

Does this mean that T will have SA for any infinite S?

Example 3.

One can construct an infinite S for which SA fails.

Example 4.

Let $S = \{v_\infty\} \cup \{v_p \mid p \equiv 1 (\mathrm{mod}\, 4)\}$. Then $T = \mathbb{G}_m$ has SA w.r.t. S.

Proof uses CRT and Dirichlet's Theorem on Primes in Arithmetic Progressions.

This can be partially generalized: For any integers a, m with $(a, m) = 1$ and

$$S = \{v_\infty\} \cup \{v_p \mid p \equiv a (\mathrm{mod}\, m)\},$$

$[T(\mathbb{A}_S) : \overline{T(\mathbb{Q})}^{(S)}] < \infty$.

Example 5.

Pick a prime $q \equiv 1 (\mathrm{mod}\, 4)$ and let $S = \{v_\infty\} \cup \{v_p \mid p \equiv 1 (\mathrm{mod}\, q)\}$.

Then $[T(\mathbb{A}_S) : \overline{T(\mathbb{Q})}^{(S)}] > 1$. (In fact, index can be arbitrarily large.)

TAKE-AWAYS: 1. Primes in arithmetic progressions appear to be "good" sets for SA.

2. Instead of asking whether $\overline{T(\mathbb{Q})}^{(S)} = T(\mathbb{A}_S)$, one should ask if $[T(\mathbb{A}_S) : \overline{T(\mathbb{Q})}^{(S)}] < \infty$.

Definitions.

1. Let L/K be a finite Galois extension, and $\mathcal{C}$ be a conjugacy class in $\mathrm{Gal}(L/K)$. A generalized arithmetic progression $\mathcal{P}(L/K, \mathcal{C})$ consists of all $v \in V_f^K$ that are *unramified* in L/K and for which $\mathrm{Fr}(w|v) \in \mathcal{C}$ for some (equivalently, any) extension $w|v$.

2. A subset $S \subset V^K$ is tractable if it contains

$$V_\infty^K \cup (\mathcal{P}(L/K, \mathcal{C}) \setminus \mathcal{P}_0)$$

where $\mathcal{P}_0$ has Dirichlet density zero.

3. A K-group G has almost strong approximation w.r.t. $S \subset V^K$ if

$$[G(\mathbb{A}_S) : \overline{G(K)}^{(S)}] < \infty.$$

Remark. If G has almost strong approximation w.r.t. S then there exists $S' \subset V^K$ with $S' \setminus S$ finite such that

$$\overline{G(K)}^{(S')} = G(\mathbb{A}_{S'}).$$

Example 6.

Let $K = \mathbb{Q}$ and $L = \mathbb{Q}(i)$. Set

$$S = \{v_\infty\} \cup \{v_p \mid p \equiv 3 (\mathrm{mod}\, 4)\}$$

noting that $S = \{v_\infty\} \cup \mathcal{P}(L/K, \sigma)$ for nontrivial $\sigma \in \mathrm{Gal}(L/K)$.

Set $T = \mathrm{R}^{(1)}_{L/K}(\mathbb{G}_m)$ (norm 1 torus associated with L/K).

One shows that $[T(\mathbb{A}_S) : \overline{T(\mathbb{Q})}^{(S)}] = \infty$, (i.e., T does not have almost strong approximation w.r.t. S).

Here splitting field of T coincides with field used to define generalized arithmetic progression. In this case, there are *additional arithmetic obstructions* to almost strong approximation.

Theorem 4 (A.R., W. TRALLE)

Let T be a K-torus with minimal splitting field P, and let $S \subset V^K$ be a tractable set containing $V_\infty^K \cup (\mathcal{P}(L/K, \mathcal{C}) \setminus \mathcal{P}_0)$. Assume that

$$\sigma|(P \cap L) = \mathrm{id}_{P \cap L} \quad \text{for some} \quad \sigma \in \mathcal{C}.$$

Then T has almost strong approximation w.r.t. S.

Proof consists of two parts. First, we treat quasi-split tori using CFT and Chebotarev's Theorem, and then consider general case using Nakayama-Tate Theorem.

Index $[T(\mathbb{A}_S) : \overline{T(K)}^{(S)}]$ is bounded by an explicit constant that depends only on $\dim T$ and $[L : K]$.

Theorem 5.

Let $G = T \cdot H$ (almost direct product) where T is a K-torus and H a connected semisimple K-group.

Set $E = PM$ where P is minimal splitting field of T and M minimal Galois extension of K over which H becomes an inner form.

Then G has ASA w.r.t. any tractable set S containing $V_\infty^K \cup (\mathcal{P}(L/K, \mathcal{C}) \setminus \mathcal{P}_0)$ provided that

$$\sigma|(E \cap L) = \mathrm{id}_{E \cap L} \quad \text{for some} \quad \sigma \in \mathcal{C}. \qquad (*)$$

In fact, $\overline{G(K)}^{(S)}$ is a *normal subgroup* of $G(\mathbb{A}_S)$, of index bounded by a constant depending only on K, absolute rank of G, and $[L : K]$.

Proof combines classical SA theorem for semisimple simply connected groups with ASA for tori.

Corollary.

Let G be a semisimple K-group which is an inner form of a split group. Then G has ASA w.r.t. any tractable set S.

Condition $(*)$ cannot be omitted. We construct an adjoint outer form of type A_n which fails to have ASA w.r.t. to a tractable set.

Question. *Do semisimple inner forms have ASA w.r.t. any set of positive Dirichlet density?*

Let

- $G \subset \mathrm{GL}_n$ be a linear algebraic group defined over a number field K,
- $S \subset V^K$ be a subset containing V_∞^K,
- $O_S \subset K$ be the ring of S-integers,
- $\Gamma = G(O_S)$.

For a nonzero ideal $\mathfrak{a} \subset O_S$, we have *congruence subgroup*

$$\Gamma(\mathfrak{a}) = \{A \in \Gamma \mid A \equiv I_n (\mathrm{mod}\, \mathfrak{a})\},$$

which is a finite index normal subgroup of Γ.

Congruence Subgroup Problem (CSP) asks if, conversely, every finite index normal subgroup $\Delta \subset \Gamma$ contains a suitable congruence subgroup $\Gamma(\mathfrak{a})$.

Serre pointed out that one should view (CSP) as problem of computing a *profinite group* $C^S(G)$, called the congruence kernel.

$C^S(G) = \{1\}$ is equivalent to positive answer to (CSP).

There are situations which by many characteristics are close to such situations, but where $C^S(G)$ is *not trivial*, but rather *finite*. So, focus shifts to proving finiteness of $C^S(G)$.

In main case of absolutely almost simple simply connected G, if $C^S(G)$ is finite then its *precise* description is given by computations of *metaplectic kernel* (G. Prasad, A.R, 1996).

Congruence Subgroup Conjecture (SERRE, 1970)

Let G be an absolutely almost simple simply connected algebraic group over a number field K, and let $S \subset V^K$ be a finite set containing V_∞^K.

Then $C^S(G)$ is finite if $\mathrm{rk}_S G := \sum_{v \in S} \mathrm{rk}_{K_v} G \geqslant 2$ and $\mathrm{rk}_{K_v} G > 0$ for all $v \in S \setminus V_\infty^K$, and is infinite if $\mathrm{rk}_S G = 1$.

While higher rank case of Serre's conjecture has been confirmed in a number of cases, but it remains open in other cases, in particular, for most anisotropic forms of type A_n.

One can obtain supporting evidence for Serre's conjecture in those cases by considering (CSP) for *infinite* S.

More precisely, truth of Serre's conjecture combined with computations of metaplectic kernel would imply that

$C^S(G) = \{1\}$ for *any* infinite S such that $\mathrm{rk}_{K_v} G > 0$ for all $v \in S \setminus V_\infty^K$, and this is what one would like to prove.

We used our results on ASA for tori to do this for tractable sets (under appropriate assumptions).

The argument does not use any case-by-case considerations, so potentially it may lead to a uniform proof of Serre's conjecture.

It follows from SA that positive results on (CSP) should be preceded by results on normal subgroup structure of groups of rational points.

So, we will now formulate expected result in latter case as Margulis-Platonov conjecture (MP), and will then include (MP) as an assumption in our theorem.

Margulis-Platonov conjecture

Set $\mathcal{A} = \{v \in V_f^K \mid \mathrm{rk}_{K_v} G = 0\}$, and let $\delta\colon G(K) \to G_{\mathcal{A}} := \prod_{v\in\mathcal{A}} G(K_v)$ be diagonal embedding. Then for every noncentral normal subgroup $N \subset G(K)$ there exists an open normal subgroup $W \subset G_{\mathcal{A}}$ such that $N = \delta^{-1}(W)$. In particular, if $\mathcal{A} = \varnothing$ (which is always true if G is not of type A_n), then $G(K)$ does not proper noncentral normal subgroups.

Theorem 6.

Let G be an absolutely almost simple simply connected algebraic group over a number field K, and let M/K be minimal Galois extension over which G becomes an inner form. Assume that (MP) holds for $G(K)$.

Let $S \subset V^K$ be a tractable set containing $V_\infty^K \cup (\mathcal{P}(L/K, \mathcal{C}) \setminus \mathcal{P}_0)$ where

$$\sigma|(M \cap L) = \mathrm{id}_{M \cap L} \quad \text{for some} \quad \sigma \in \mathcal{C},$$

and such that $\mathrm{rk}_{K_v} G > 0$ for $v \in S \setminus V_\infty^K$.

Then $C^S(G) = 1$.

Historical remarks. For those S that contain

$$V_\infty^K \cup (\mathcal{P}(L/K, \mathcal{C}) \setminus \mathcal{P}_0)$$

where $\mathcal{P}_0$ is finite, theorem was proved by Prasad, A.R. (2016).

Radhika and Raghunathan (2020) showed that result remains valid for inner forms of type A_n for any $\mathcal{P}_0$ of Dirichlet density zero.

Our theorem generalizes results of Radhika-Raghunathan to all types.