On strong approximation for algebraic groups

Rapinchuk

Goal: given an affine alg. grp. $G/\mathbb{Z}$, when is it true that

$G(\mathbb{Z}) \to G(\mathbb{Z}/N\mathbb{Z})$ is surjective for (almost) all N?

Examples:

- $\mathbb{G}_a(\mathbb{R}) = \mathbb{R}$, $\mathbb{G}_a = \mathbb{A}^1_{\mathbb{Z}}$. $\mathbb{G}_a(\mathbb{Z}) = \mathbb{Z}$, $\mathbb{G}_a(\mathbb{Z}/N\mathbb{Z}) = \mathbb{Z}/N\mathbb{Z}$
  $\rightsquigarrow$ Yes ✓
- $\mathbb{G}_m(\mathbb{R}) = \mathbb{R}^\times$, $\mathbb{G}_m = \mathbb{A}^1_{\mathbb{Z}} \setminus \{0\}$. $\mathbb{G}_m(\mathbb{Z}) = \mathbb{Z}^\times = \{\pm 1\}$, $\mathbb{G}_m(\mathbb{Z}/N\mathbb{Z}) = (\mathbb{Z}/N\mathbb{Z})^\times$ $\rightsquigarrow$ No ✗.
- $\mathbb{G}_2$: one can show that
  - $|\mathbb{G}_2(\mathbb{Z})| = 8$
  - $|\mathbb{G}_2(\mathbb{F}_p)| = \begin{cases} 2(p-1) & p \equiv 1 \bmod 4 \\ 2(p+1) & p \equiv 3 \bmod 4 \end{cases}$.

  $\rightsquigarrow$ No ✗.

I SL_r, GL_r

Claim: For $N \geq 2$, $SL_r(\mathbb{Z}) \to SL_r(\mathbb{Z}/N\mathbb{Z})$ is surj.

Case $r=2$:

- Observe that $\begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ * & 1 \end{pmatrix}$ (shear), $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ (permutation) are in the image of $SL_2(\mathbb{Z})$

  We show these generate $SL_2(\mathbb{Z}/N\mathbb{Z})$.
- Starting from $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}/N\mathbb{Z})$, act on it by shear/permutation, reduce to $\begin{pmatrix} \alpha & 0 \\ 0 & \alpha^{-1} \end{pmatrix} \in SL_2(\mathbb{Z}/N\mathbb{Z})$
- Conclude with

$$\begin{pmatrix} \alpha & 0 \\ 0 & \alpha^{-1} \end{pmatrix} = \begin{pmatrix} 1 & \alpha \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & \alpha^{-1} \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ -\alpha & 1 \end{pmatrix}$$

Claim: For $N \geq 5$, $GL_r(\mathbb{Z}) \to GL_r(\mathbb{Z}/N\mathbb{Z})$ is NOT surj.

The problem is the determinant!

- if $M \in GL_r(\mathbb{Z})$, $\det M \in \mathbb{Z}^\times = \{\pm 1\}$
- if $N \geq 5$, take $x \in (\mathbb{Z}/N\mathbb{Z})^\times$ s.t. $x \neq \pm 1$, then $\operatorname{diag}(x, 1, \dots, 1)$ is not in the image of $GL_r(\mathbb{Z})$.

Generalization:

Prop: Let $X/\mathbb{Z}$ be affine s.t. $X(\mathbb{Z})$ is not Zariski dense in $X_{\mathbb{Q}}$. Then for ∞-many primes p, the map
$X(\mathbb{Z}) \to X(\mathbb{F}_p)$
is not surjective.

$\rightsquigarrow GL_r, \mathbb{G}_r, U_r$, any G s.t. $G(\mathbb{R})$ is infinite compact

Q: What if we allow ourselves to invert some primes?

$G = \mathbb{G}_m$ $\quad \mathbb{Z}[\frac{1}{2}]^\times \to (\mathbb{Z}/N\mathbb{Z})^\times \quad 2 \nmid N$

$G = O_r$ $\quad O_r(\mathbb{Z}[\frac{1}{6}]) \to O_r(\mathbb{Z}/N\mathbb{Z})^\times \quad 6 \nmid N$

?

II Strong approximation

Recall the adèles: $\mathbb{A}_{\mathbb{Q}} = \mathbb{R} \times \prod_p{}' \mathbb{Q}_p$

$= \{(x_\infty, (x_p)) \mid x_p \in \mathbb{Z}_p \text{ for almost all } p\}$

Let S be a finite set of places of $\mathbb{Q}$, with $\infty \in S$.

$\mathbb{A}^S_{\mathbb{Q}} = \prod_{p \notin S}{}' \mathbb{Q}_p$ is a $\mathbb{Q}$-algebra $[\mathbb{Q} \hookrightarrow \mathbb{A}^S_{\mathbb{Q}}]$

Def: We say that $X/\mathbb{Q}$ has "strong (S-) approximation" if
$X(\mathbb{Q}) \longrightarrow X(\mathbb{A}^S_{\mathbb{Q}})$
has dense image.

Claim: if $G/\mathbb{Z}[\frac{1}{m}]$ smooth alg. group, $\infty \in S$. Let $m = \prod_{p \in S \setminus \{\infty\}} p$.
Then:

(P) $G(\mathbb{Z}[\frac{1}{m}]) \to G(\mathbb{Z}/N\mathbb{Z})$ is surj $\forall N \geq 2$, $m \nmid N$

$\Updownarrow$

G has strong (S-) approximation.

Proof for $S = \{\infty\}$:

- Recall $\hat{\mathbb{Z}} = \prod_p \mathbb{Z}_p$ is an open nbhd of 0 in $\mathbb{A}^S_{\mathbb{Q}}$

  $\rightsquigarrow G(\hat{\mathbb{Z}})$ is a nbhd of $1 \in G(\mathbb{A}^S_{\mathbb{Q}})$.
- By smoothness of G, any $M \in G(\mathbb{Z}/N\mathbb{Z})$ lifts to $G(\mathbb{Z}/N'\mathbb{Z})$ for $N \mid N'$. Hence a lift

$$G(\hat{\mathbb{Z}}) = \varprojlim_{N \mid N'} G(\mathbb{Z}/N'\mathbb{Z}).$$

So far:

$$G(\hat{\mathbb{Z}}) \xrightarrow{f_N} G(\mathbb{Z}/N\mathbb{Z})$$
$$\cup \mathrel{|}$$
$$G(\mathbb{Z})$$

(arrow from $G(\mathbb{Z})$ to $G(\mathbb{Z}/N\mathbb{Z})$: surj?)

Key point: as N varies, the fibers of f_N form a basis of the topology of $G(\hat{\mathbb{Z}})$.

(P) $\iff$ $G(\mathbb{Z})$ intersect all fibers of f_N $\forall N \geq 2$

$\overset{\text{key point}}{\iff}$ $G(\mathbb{Z})$ is dense in $G(\hat{\mathbb{Z}})$

($G(\mathbb{Z}) = G(\mathbb{Q}) \cap G(\hat{\mathbb{Z}})$; $G(\hat{\mathbb{Z}})$ open nbhd of 1 in $G(\mathbb{A}^S_{\mathbb{Q}})$)

$\overset{G \text{ is a group}}{\iff}$ $G(\mathbb{Q})$ is dense in $G(\mathbb{A}^S_{\mathbb{Q}})$. "strong S-approx" ☒

Cor: For $G = \mathbb{G}_m$, $S = \{\infty\}$, $\mathbb{Q}^\times \to (\mathbb{A}^{\{\infty\}}_{\mathbb{Q}})^\times$ not dense image.
(finite idèles(?))

Thm: [Kneser, Platonov, Margulis, Prasad]
Let $G/\mathbb{Q}$ be a connected, absolutely almost simple alg. grp, S finite set of places of $\mathbb{Q}$.

Then G has strong S-approx iff

(1) G is simply connected [no nontrivial central isogeny]

(2) $\prod_{p \in S} G(\mathbb{Q}_p)$ is non compact $[\mathbb{Q}_\infty = \mathbb{R}]$

"almost simple": non commutative + the only proper normal subgroups are finite.

Examples: $S = \{\infty\}$ [(2) $\Leftrightarrow G(\mathbb{R})$ non compact $\Leftrightarrow G(\mathbb{Z})$ Zar. dense in $G_{\mathbb{Q}}$]

G	(1) simply connected?	(2) $G(\mathbb{R})$ non compact?	strong approx?
SL_r	✓	✓	✓
PSL_r	✗	✓	✗
SU_r	✓	✗	✗
Sp_{2r}	✓	✓	✓
SO_r	✗	✗	✗
$Spin_r$	✓	✗	✗
$SO(p,q)$ $p,q \geq 1$	✗	✓	✗
$Spin(p,q)$	✓	✓	✓

Link with $\mathcal{A}_{g,n}/\mathbb{C}$

Analitically:

$\mathcal{H}$ = Siegel upper half ~~plane~~ space $\quad \circlearrowleft Sp_{2g}$

$= \{$p.p. ab. var. w/ symplectic basis of $H_1(A, \mathbb{Z})\}$ (not algebraic)

$\mathcal{H}/\Gamma'(N) = \{$p.p. ab. var. w/ (sym. basis of $H_1(A, \mathbb{Z})$) mod $N\}$

$\updownarrow$

Algebraically

$\mathcal{A}_{g,N} = \{$p.p. ab. var. w/ sym. basis $(H_1(A, \mathbb{Z}) \bmod N)\}$

These coincide bc $\operatorname{Im}(Sp_{2g}(\mathbb{Z})) = Sp_{2g}(\mathbb{Z}/N\mathbb{Z})$.