On the strong approximation for Zariski-dense subgroups

A. Rapinchuk

The goal of this talk is to give a survey of known results about strong approximation in algebraic groups. The most elementary way to think about strong approximation is to ask if one can lift solutions of integer polynomial equations mod m to integer solutions

Suppose we have a family of polynomial equations $f_\alpha(x_1, \dots x_d) \in \mathbb{Z}[x_1, \dots, x_d]$, and we let $X \subset \mathbb{A}^d$ denote the affine variety (scheme) defined by these polynomials. Thus, for a $\mathbb{Z}$-algebra R, we have

$$X(R) = \{ (a_1, \dots, a_d) \in R^d \mid f_\alpha(a_1, \dots, a_d) = 0 \}$$

For any $m \geq 1$, we have a natural map

$$\rho_m : X(\mathbb{Z}) \longrightarrow X(\mathbb{Z}/m\mathbb{Z}),$$

and the question is whether this map is surjective for all $m \geq 1$. (Of course, for this question to be meaningful, we need to assume that $X(\mathbb{Z}/m\mathbb{Z}) \neq \emptyset$ for all m). We can assemble all $X(\mathbb{Z}/m\mathbb{Z})$ into a single object by taking the inverse limit:

$$\varprojlim X(\mathbb{Z}/m\mathbb{Z}) = X(\hat{\mathbb{Z}}),$$

where $\hat{\mathbb{Z}} = \varprojlim \mathbb{Z}/m\mathbb{Z}$; by the Chinese remainder theorem, $\hat{\mathbb{Z}} = \prod_p \mathbb{Z}_p$. There is a natural map

$$\iota : X(\mathbb{Z}) \longrightarrow X(\hat{\mathbb{Z}}).$$

For any $m \geq 1$, there is a natural map

$$\hat{\rho}_m : X(\hat{\mathbb{Z}}) \longrightarrow X(\hat{\mathbb{Z}}/m\hat{\mathbb{Z}}) = X(\mathbb{Z}/m\mathbb{Z}).$$

The pullbacks of points under the $\hat{\rho}_m$'s form a basis of the topology on $X(\hat{\mathbb{Z}})$ (which is also the topology of $\varprojlim X(\mathbb{Z}/m\mathbb{Z})$, or the topology induced by the embedding $X(\hat{\mathbb{Z}}) \hookrightarrow \hat{\mathbb{Z}}^d$, or the topology of the direct product $\prod_p X(\mathbb{Z}_p)$.

Clearly,

ρ_m is surjective for all $m \geq 1 \iff \iota : X(\mathbb{Z}) \to X(\hat{\mathbb{Z}})$ is dense.
We say that X has strong approximation if this is the case.

Intuitively, this should not happen very often as there are plentiful examples where $X(\hat{\mathbb{Z}}) \neq \emptyset$ but $X(\mathbb{Z}) = \emptyset$. However, it is very difficult to figure out for general varieties when exactly this is the case – one can only give some necessary conditions. In this talk, we will deal exclusively with algebraic groups.

Let us start with two elementary examples:

$$G_1 = SL_2 \quad \text{and} \quad G_2 = GL_2$$

One doesn't see much of a difference between these examples just by looking at the defining equations:

$$G_1 \subset \mathbb{A}^4 \,, \qquad x_{11}x_{22} - x_{12}x_{21} = 1$$

$$G_2 \subset \mathbb{A}^5 \,, \qquad y(x_{11}x_{22} - x_{12}x_{21}) = 1$$

However, G_1 has strong approximation and G_2 doesn't.

<u>Lemma 1.</u> For any $m \geq 1$,

$$\rho_m : SL_2(\mathbb{Z}) \to SL_2(\mathbb{Z}/m\mathbb{Z})$$

is surjective

<u>Proof</u> does not use equations (in fact, it is not easy to prove this using the defining equation – which is a quadric; see later). The crucial observation is that any $\bar{g} \in SL_2(\mathbb{Z}/m\mathbb{Z})$ can be written as a product of elementaries:

$$\bar{g} = \prod e_{i_k j_k}(\bar{a}_k) \,, \quad \bar{a}_k \in \mathbb{Z}/m\mathbb{Z}. \qquad (1)$$

(For this, one needs to observe that if $m = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ then $\mathbb{Z}/m\mathbb{Z} = \mathbb{Z}/p_1^{\alpha_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_r^{\alpha_r}\mathbb{Z}$, and therefore

$$SL_2(\mathbb{Z}/m\mathbb{Z}) = SL_2(\mathbb{Z}/p_1^{\alpha_1}\mathbb{Z}) \times \cdots \times SL_2(\mathbb{Z}/p_r^{\alpha_r}).$$

This reduces the proof to the case where $m = p^{\alpha}$.

Then, given $\overline{g} = \begin{pmatrix} x_{11} & x_{12} \\ x_{21} & x_{22} \end{pmatrix} \in SL_2(\mathbb{Z}/p^\alpha\mathbb{Z})$, either x_{11} or x_{12} is invertible mod p^α, and then using Gaussian elimination one can easily write $\overline{g}$ as a product of elementaries.)
Pick any $a_k \in \mathbb{Z}$ such that $a_k \in \overline{a}_k$, and let

$$g = \prod e_{i_k j_k}(a_k).$$

Then clearly $\rho_m(g) = \overline{g}$. □

So, the argument is based on the consideration of unipotent elements, and what is interesting is that in most known cases strong approximation is achieved by using unipotent elements in some form (even when unipotent elements are not present in the original group).

The case of $G_2 = GL_2$ is even simpler: the map

$$\rho_5 : GL_2(\mathbb{Z}) \longrightarrow GL_2(\mathbb{Z}/5\mathbb{Z})$$

already fails to be surjective (because all matrices in $\rho_5(GL_2(\mathbb{Z}))$ will have determinant ±1 (mod 5)). One can articulate this obstruction in a more conceptual way by saying that in order for X to have strong approximation,

$$X(\mathbb{Z}) \quad \text{must be Zariski-dense in } X$$

Indeed, if $Y \subset X$ is a proper Zariski-closed subset then one can find infinitely many primes p such that $Y(\mathbb{Z}_p) \neq X(\mathbb{Z}_p)$, and then $Y(\mathbb{Z}/p^\alpha\mathbb{Z}) \neq X(\mathbb{Z}/p^\alpha\mathbb{Z})$ for sufficietly large α. [In fact, this is true for almost all prime: it is easy to see that for X to have strong approximation, it need to be irreducible; then $\dim Y < \dim X$, so $|\underline{Y}^{(p)}(\mathbb{F}_p)| \approx$ (number of irr. comp. of Y) $\cdot\, p^{\dim Y}$, and $|\underline{X}^{(p)}(\mathbb{F}_p)| \approx p^{\dim X}$. It follows that $\underline{Y}^{(p)}(\mathbb{F}_p)$ is much smaller than $\underline{X}^{(p)}(\mathbb{F}_p)$. On the other hand, removing a proper subvariety, we can assume X to be smooth, and then $X(\mathbb{Z}_p) \longrightarrow \underline{X}^{(p)}(\mathbb{F}_p)$ is surjective for almost all p. So, if $X(\mathbb{Z}) \subset Y$ then $X(\mathbb{Z}) \to X(\mathbb{F}_p)$ is not surjective for almost all p.

Since $GL_2(\mathbb{Z})$ is not Zariski-dense in GL_2, we see that GL_2 cannot possibly have strong approximation. Let us slightly change the set-up by replacing the ring of integers with the ring of S-integers, e.g. with $\mathbb{Z}[\frac{1}{2}]$. Then $GL_2(\mathbb{Z}[\frac{1}{2}])$ is already Zariski-dense in GL_2, and in fact the map

$$\rho_5 : GL_2(\mathbb{Z}[\tfrac{1}{2}]) \to GL_2(\mathbb{Z}/5\mathbb{Z})$$

is already surjective, but the map

$$\rho_{17} : GL_2(\mathbb{Z}[\tfrac{1}{2}]) \to GL_2(\mathbb{Z}/17\mathbb{Z})$$

is not. (In fact, one can find infinitely many primes p with this property.)

Thus, Zariski-density is certainly not enough for strong approximation in the general case. At the same time let us consider the following example in the case of SL_2. We have

$$SL_2(\mathbb{Z}) := \Gamma_0 = \left\langle \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \right\rangle$$

For $\ell \geq 1$, consider

$$\Gamma_\ell = \left\langle \begin{pmatrix} 1 & 2^\ell \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 2^\ell & 1 \end{pmatrix} \right\rangle.$$

We have the following inclusions

$$\Gamma_0 \overset{12}{\supset} \Gamma_1 \overset{\infty}{\supset} \Gamma_2 \overset{\infty}{\supset} \Gamma_3 \supset \ldots$$

So, for larg ℓ, Γ_ℓ is very "thin" in Γ_0, and the only property it retains is Zariski-density.

Nevertheless, for any ODD m, we have

$$\rho_m(\Gamma_\ell) = \rho_m(\Gamma_0) = SL_2(\mathbb{Z}/m\mathbb{Z}).$$

So, if we ignore $p=2$ (more precisely, the component $\mathbb{Z}_2$ of $\hat{\mathbb{Z}}$), then we still have strong approximation for Γ_ℓ, for any $\ell \geq 1$. At the same time, the closure of Γ_ℓ in $SL_2(\mathbb{Z}_2)$ is open. So, eventually we obtain that the closure of Γ_ℓ in $SL_2(\hat{\mathbb{Z}})$ is open. – this is the next best thing to strong approximation. Note that for a general variety X, the openness of the closure of $X(\mathbb{Z})$ in $X(\hat{\mathbb{Z}})$ implies that the reduction maps $\rho_m : X(\mathbb{Z}) \to X(\mathbb{Z}/m\mathbb{Z})$ are surjective for all m prime to some fixed exceptional number $N_0 = N_0(X)$.

So, generally speaking, the idea that Zariski-density should (or may) imply strong approximation in some sense, at least for subgroups, appears to be sound (by and large), but we need to figure out what is wrong with GL_2 (compared to SL_2).

But before we do this, let us describe a more general approach to strong approximation. The thing is that typically an algebraic group does not come with a fixed geometric (or linear) realization, and different realizations $G \hookrightarrow GL_n$ may result in different groups of integral points. So, it makes sense to reformulate strong approximation in terms of the group of rational points.

So, let G be an algebraic group defined over a global field K, S be a nonempty set of places of K (it is often assumed that S contains all archimedean places and is finite). For now, fix a matrix realization $G \subset GL_n$, which enables us to speak unambiguously about the group $G(\mathcal{O}_v)$ for any nonarchimedean place v of K, where $\mathcal{O}_v$ is the valuation ring in the completion K_v. We let A_S define the ring of S-adeles, and let

$$G(A_S) = \left\{ g \in \prod_{v \notin S} G(K_v) \;\middle|\; g \in G(\mathcal{O}_v) \text{ for almost all } v \notin S \right\}$$

The topology on $G(A_S)$ is defined by taking all open subgroups of $\prod_{v \notin S} G(\mathcal{O}_v)$ for a fundamental system of neighborhoods of the identity (so, the topology on $G(A_S)$ is the "natural extension" of the product topology on $\prod_{v \notin S} G(\mathcal{O}_v)$). Then the topological group $G(A_S)$ is independent of the embedding $G \hookrightarrow GL_n$. Also, there is an embedding $G(K) \hookrightarrow G(A_S)$, and we give the following

<u>Definition</u> G has strong approximation with respect to S if $G(K)$ is dense in $G(A_S)$.

This property is independent of the realization $G \hookrightarrow GL_n$. On the other hand, if it holds then for any realization $G(\mathcal{O}(S)) = G(K) \cap \prod_{v \notin S} G(\mathcal{O}_v)$ in dense in $\prod_{v \notin S} G(\mathcal{O}_v)$ in the case where S contains all archimedean places, where $\mathcal{O}(S)$ is the ring of S-integers.

Now, let us discuss why GL_2 has no chance to possess strong approximation. It is the easiest to pin down the reason by working with the 1-dimensional split torus $T = G_m$ — we will show that it does not have strong approximation with respect to any finite S.

Let us start with $K = \mathbb{Q}$.

If $S = \{\infty\}$ then $T(\mathbb{Z}) = \{\pm 1\}$ which is not even Zariski-dense.

For $S = \{\infty, 2\}$, we have $T(\mathbb{Z}) = \pm\langle 2\rangle$, so it is already Zariski-dense, but it still does not have strong approximation. Indeed, take any prime p of the form $8k+1$. Then $-1, 2$ are squares mod p. So, the map

$$\pm\langle 2\rangle \longrightarrow (\mathbb{Z}/p\mathbb{Z})^{\times}$$

is NOT surjective. What really happens here is that T has a 2-sheeted cover

$$\pi : T \to T, \quad t \mapsto t^2,$$

and then there exist infinitely many primes p such that

$$T(\mathbb{Z}[\tfrac{1}{2}]) \subset \pi(T(\mathbb{Z}_p)) \neq T(\mathbb{Z}_p).$$

Thus, given a finite collection of such primes $p_1, \ldots, p_r$ $(\equiv 1 \pmod 8)$, the image of

$$\pm\langle 2\rangle \longrightarrow (\mathbb{Z}/p_1\cdots p_r\mathbb{Z})^{\times\cancel{2}}_{2}$$

is contained in $(\mathbb{Z}/p_1\cdots p_r\mathbb{Z})^{\times 2}$, which has index 2^r in $(\mathbb{Z}/p_1\cdots p_r\mathbb{Z})^{\times}$. Since there are infinitely many primes $\equiv 1 \pmod 8$, we see that the closure of $\overline{T(\mathbb{Z}[\frac{1}{2}])}$ in $T(\hat{\mathbb{Z}}) = \prod_p T(\mathbb{Z}_p)$ has infinite index.

This is a very general phenomenon. It was observed by Minchev (1989) that if X is an irreducible normal variety over a number field K, and there exists a nontrivial unramified covering

$$f : Y \to X$$

defined over $\overline{K}$, then X does not have strong approximation with respect to <u>any finite</u> S. Namely, in this situation there exists an <u>infinite</u> set V of nonarchimedean places, disjoint from S, such that for any $v \in V$ we have

$$X(\mathcal{O}(S)) \subset f(Y(\mathcal{O}_v)) \subsetneqq X(\mathcal{O}_v);$$

in fact, $f(Y(\mathcal{O}_v))$ is a "small" closed subset of $X(\mathcal{O}_v)$ (e.g. $\underline{f}(\underline{Y}^{(v)}(k_v)) \neq \underline{X}^{(v)}(k_v)$, where k_v is the residue field). This implies that $\overline{X(\mathcal{O}(S))}^{(S)} \subset \prod_{v \notin S} X(\mathcal{O}_v)$ has "measure zero" for any reasonable measure (so, the closure is very thin).

For general varieties, this requires some arithmetic algebraic geometry, but for algebraic groups it is much simpler. For example, consider

$$SL_2 = \widetilde{G} \xrightarrow{\pi} G = PSL_2$$

(one can think of G as the special orthogonal group $SO_3(q)$ where $q = xy + z^2$). Then for any field extension F/K, where K is the base field, we have

$$G(F) = PGL_2(F)$$

(by the Skolem-Noether theorem, one can think of G as $\mathrm{Aut}(M_2)$, where M_2 is the degree two matrix algebra, and then again by the Skolem-Noether, $G(F) = PGL_2(F)$).

Then there is an exact sequence

$$\tilde{G}(F) \xrightarrow{\pi} G(F) \xrightarrow{\theta_F} F^{\times}/F^{\times 2} \longrightarrow 0 \qquad (2)$$

where θ_F is induced by det, viz. $gF^{\times} \to (\det g)F^{\times 2}$ (if one thinks of G as $SO_3(q)$ then θ_F is simply the spinor norm on $SO_3(q)(F)$.

The point is that given any finitely generated subgroup $\Gamma \subset G(K)$, its image $\Delta = \theta_K(\Gamma)$ is a finite group. So, it follows from Tchebotarev's Density Theorem that there are infinitely many nonarchimedean places v of K such that the image of Δ under $K^{\times}/K^{\times 2} \longrightarrow K_v^{\times}/K_v^{\times 2}$ is trivial. From the exactness of (2), we see that for these v we have

$$\Gamma \subset \pi\left(\tilde{G}(K_v)\right) \neq G(K_v)$$

In fact, for almost all such v, we have

$$\Gamma \subset \pi\left(\tilde{G}(\mathcal{O}_v)\right) \neq G(\mathcal{O}_v),$$

and eventually the closure of Γ in $\prod_{v \notin S} G(\mathcal{O}_v)$ has infinite index.

This shows that if G is not simply connected (i.e. there exists a nontrivial isogeny $\pi : \tilde{G} \longrightarrow G$ with connected $\tilde{G}$) then strong approximation in G fails

Example. If $G = GL_2$, we can take $\tilde{G} = SL_2 \times G_m$, and then the product map gives an isogeny of degree 2. (Furthermore, the map $GL_2 \to GL_2$, $g \mapsto (\det g)\, g$, is an isogeny of degree three.

So, we have two necessary conditions for strong approximation: our S-arithmetic subgroup must be Zariski-dense, and the algebraic group must be simply connected. It turns out that for absolutely almost simple groups, these conditions are also sufficient.

__Theorem__ (Kneser, Platonov in char 0, Margulis, Prasad in char $p>0$)

Let G be an absolutely almost simple algebraic group over a global field K, and let S be a finite set of places of K. Then G has strong approximation with respect to S (i.e. $G(K)$ is dense in $G(\mathbb{A}_S)$) if and only if

(1) G is simply connected

(2) $G_S = \prod_{v \in S} G(K_v)$ is noncompact

(Condition (2) for an absolutely almost simple group G is equivalent to the fact that $G(\mathcal{O}(S))$ is Zariski-dense (equivalently, infinite).)

__Remarks.__ 1. The fact that G is simply connected is used in the proof in a very peculiar way. More precisely, what we need is that $G(K_v)$ does not have proper subgroups of finite index. This is proved by establishing that $G(K_v)$ is generated by unipotents (more precisely, that $G(K_v) = G(K_v)^+$ in Tits' notations), and this is where simply connected is essential.

2. For certain infinite S, G may have strong approximation without being simply connected. For example, in a work with G. Prasad, we considered strong approximation for tori. To avoid technicalities, I will just state the result for $T = \mathbb{G}_m / \mathbb{Q}$: If S contains an arithmetic progression then $\overline{T(\mathbb{Q})}^{(S)} \subset T(\mathbb{A}_S)$ is of finite index (the general result is a bit more technical as one needs to impose some additional conditions on the arithmetic progression, dealing with the splitting field of T - these conditions are necessary). We applied this result to the congruence subgroup problem

3. For general varieties, (1) and (2) are not sufficient, even for homogeneous spaces.

Example. Let $f(x,y,z) = ax^2+by^2+cz^2$, $a,b,c \in K^\times$, and let X be defined by $ax^2+by^2+cz^2=a$. Set $g(y,z)=by^2+cz^2$. Let $S \subset V^K$ be a finite set of places such that X_S is noncompact. Then X has strong approximation with respect to S if and only if one of the following conditions holds

(a) g is K-isotropic;

(b) g is anisotropic and there exists $v \in S$ such that g is anisotropic over K_v, and either v is nonarchimedean and f is K_v-isotropic.

In particular, X defined by $x_1^2+x_2^2-2x_3^2=1$ $/\mathbb{Q}$ does not have strong approximation w.r.t. $S=\{\infty\}$. (but quadrics of higher dimension always have strong approximation).

If $X=G/H$ where G is simply connected and H is connected, then X has strong approximation for sufficiently large S.

We will not prove the theorem because it treats S-arithmetic groups, and our main interest is general Zariski-dense subgroups, but in fact its proof does give us something that applies to arbitrary Zariski-dense subgroups (this argument goes back to Kneser and Platonov).

<u>Lemma</u> Let G be an absolutely almost simple algebraic $\mathbb{Q}$-group, and let $\Gamma \subset G(\mathbb{Z})$ be a Zariski-dense subgroup. Then for any prime p, the closure $\overline{\Gamma}^{(p)} \subset G(\mathbb{Z}_p)$ is open.

<u>Proof</u>. Let $\mathfrak{g} = L(G)$, $\Delta = \overline{\Gamma}^{(p)}$. By a theorem of Cartan, Δ is a p-adic Lie group, of positive dimension as Γ is Zariski-dense. So, we can consider the Lie algebra $\mathfrak{h} \subset \mathfrak{g}_{\mathbb{Q}_p}$ of Δ. Clearly, $\mathfrak{h}$ is invariant under $Ad\, \Gamma$. But then ~~it~~ $\mathfrak{h} \otimes \overline{\mathbb{Q}}_p$ is ~~also~~ invariant under $Ad\, \overline{\Gamma}^{(Zar)}$. So, $\mathfrak{h} \otimes \overline{\mathbb{Q}}_p$ is inveriant under G. But G acts on $\mathfrak{g}$ irreducibly. So, $\mathfrak{h} = \mathfrak{g}_{\mathbb{Q}_p}$, and Δ is open in $G(\mathbb{Z}_p)$. □

Since $\overline{\Gamma}^{(p)}$ is a virtual pro-p group, given a finite collection $\{p_1, -, p_r\}$ of distinct primes, we can deduce from the lemma that the closure

$$\overline{\Gamma} \subset \prod_{i=1}^{r} G(\mathbb{Z}_{p_i})$$

is open. This is sufficient for some applications, for example, for the existence of generic elements (Prasad will discuss this in his talk).

If we take ALL primes, we obtain the following:

the closure $\hat{\Gamma} \subset G(\hat{\mathbb{Z}})$ contains $\prod W_p$, where $W_p \subset G(\mathbb{Z}_p)$ is open for each p.

Of course, this does <u>not</u> imply that $\hat{\Gamma}$ is open in $G(\hat{\mathbb{Z}})$: for this we need to show that actually $W_p = G(\mathbb{Z}_p)$ for almost all p.

The first general result in this direction was the following.

Theorem (Matthews, Vaserstein, Weisfeiler)
Let G be an absolutely almost simple simply connected algebraic group over $\mathbb{Q}$

(1) If $\Gamma \subset G(\mathbb{Z})$ is a Zariski-dense subgroup then the closure $\hat{\Gamma} \subset G(\hat{\mathbb{Z}})$ is open;

(2) If $\Gamma \subset G(\mathbb{Q})$ is a finitely generated Zariski-dense subgroup then for some finite set S of places of $\mathbb{Q}$ containing ∞, the closure of Γ in $G(A_S)$ is open.

The paper of MVW appeared in 1984, but the interest to this sort of questions arose at least 20 years earlier in connection with the study of Galois representations on torsion points of elliptic curves. In particular, in his book on ℓ-adic representations, Serre pretty much has this theorem for $G = SL_2$

Parts (1) and (2) are proved in the same way, so let us focus on (1). A purely group-theoretic argument reduces the openness claim to proving that the closure $\overline{\Gamma}^{(p)} \subset G(\mathbb{Z}_p)$ (which is known to be open) in fact coincides with $G(\mathbb{Z}_p)$ for almost all p. It turns out that for almost all p this reduces to showing that for the reduction map $\rho_p : G(\mathbb{Z}_p) \to G(\mathbb{F}_p)$, we have $\rho_p(\Gamma) = G(\mathbb{F}_p)$ (for almost all p!

<u>Proposition</u> (MVW) For almost all p, if $\Delta \subset G(\mathbb{Z}_p)$ is a closed subgroup such that $\rho_p(\Delta) = \underline{G}^{(p)}(\mathbb{F}_p)$ then $\Delta = G(\mathbb{Z}_p)$.

The proof for the case $G = SL_2$, was given by Serre.

<u>Lemma</u> Let $\Delta \subset SL_2(\mathbb{Z}_p)$ $(p>2)$ be a closed subgroup such that for the reduction mod p map $\rho_p : SL_2(\mathbb{Z}_p) \to SL_2(\mathbb{F}_p)$ we have $\rho_p(\Delta) = SL_2(\mathbb{F}_p)$. Then $\Delta = SL_2(\mathbb{Z}_p)$.

<u>Proof</u> By assumption, there exists $g \in \Delta$ such that

$$g = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} + ps, \qquad s \in M_2(\mathbb{Z}_p).$$

We claim that

$$\Delta \ni g^p = \begin{pmatrix} 1 & p \\ 0 & 1 \end{pmatrix} + p^2 t, \qquad t \in M_2(\mathbb{Z}_p). \qquad (*)$$

Indeed,

$$g^p = \left(I + \left(\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} + ps\right)\right)^p = I + p\left(\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} + ps\right) + \binom{p}{2}\left(\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} + ps\right)^2 + \dots + \left(\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} + ps\right)^p.$$

But clearly

$$\left(\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} + pS\right)^k \equiv 0 \pmod{p} \quad \text{for any } k \geq 2,$$

and in fact

$$\left(\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} + pS\right)^k \equiv 0 \pmod{p^2} \quad \text{for any } k \geq 3$$

as $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}^2 = 0$. So, $(*)$ follows.

Thus, the image of $\Delta \cap SL_2(\mathbb{Z}_p, p)$ in $SL_2(\mathbb{Z}_p, p)/SL_2(\mathbb{Z}_p, p^2)$ is nontrivial. But since $p>2$, the group $SL_2(\mathbb{F}_p) \simeq sl_2(\mathbb{F}_p)$ acts on $sl_2(\mathbb{F}_p)$ irreducibly, implying that $\Delta \cap SL_2(\mathbb{Z}_p, p)$ surjectively maps onto $SL_2(\mathbb{Z}_p, p)/SL_2(\mathbb{Z}_p, p^2)$. Since

$SL_2(\mathbb{Z}_p, p^2)$ is the Frattini subgroup of the pro-p group $SL_2(\mathbb{Z}_p, p)$, we obtain that $\Delta \cap SL_2(\mathbb{Z}_p, p) = SL_2(\mathbb{Z}_p, p)$, and our claim follows.

The general case is obtain by reduction to the case of SL_2. More precisely, for almost all p, ~~[illegible]~~ G is quasi-split over $\mathbb{Q}_p$, and therefore $G(\mathbb{Z}_p)$ contains $H = SL_2(\mathbb{Z}_p)$ for almost all p. However, one needs to argue a bit more carefully than in MVW, p. 529, to make sure that $\Delta \cap H$ maps onto $SL_2(\mathbb{F}_p)$ surjectively. This can be achieved by choosing a special H.

So, to complete the proof of strong approximation, one needs to prove the following

<u>Theorem</u>. Let G be a connected absolutely almost simple, simply connected algebraic group over $\mathbb{Q}$, and let $\Gamma \subset G(\mathbb{Q})$ be a finitely generated Zariski-dense subgroup. Then there exists a finite set of primes $\Pi = \{p_1, \dots, p_r\}$ such that

(1) for $p \notin \Pi$, there exists a smooth reduction $\underline{G}^{(p)}$

(2) $\Gamma < G(\mathbb{Z}[\frac{1}{p_1}, \dots, \frac{1}{p_r}])$;

(3) if $\rho_p : G(\mathbb{Z}_p) \to \underline{G}^{(p)}(\mathbb{F}_p)$ is the reduction map for $p \notin \Pi$, then $\rho_p(\Gamma) = \underline{G}^{(p}(\mathbb{F}_p)$.

(It is clear how to ensure (1) and (2), and in fact (2) holds automatically if $\Gamma \subset G(\mathbb{Z})$, so the main point is condition (3)).

The general idea is the following. Since Γ is Zariski-dense in G, $\mathrm{Ad}\,\Gamma$ acts on $\mathfrak{g}_{\mathbb{Q}}$, where $\mathfrak{g} = L(G)$, absolutely irreducibly. Then a standard argument shows that for almost all p, $\rho_p(\Gamma)$ acts on $\mathfrak{g}^{(p)}_{\mathbb{F}_p}$ absolutely irreducibly. This eventually implies that $\rho_p(\Gamma) = \underline{G}_p^{(p)}(\mathbb{F}_p)$ (this is obvious if we could say that $\rho_p(\Gamma) = H(\mathbb{F}_p)$ there $H \subset \underline{G}^{(p)}$ is some proper algebraic subgroup (assuming that $\underline{G}^{(p)}$ is connected)), and this is indeed what we can basically do using Nori's theorem.

Theorem of Nori (1987)

Let H be a subgroup of $GL_n(\mathbb{F}_p)$, and let

$$X = \{x \in H \mid x^p = 1\}.$$

Note that if we assume that $p > n$ (which we will do throughout this section), then the condition $x^p = 1$ characterizes precisely unipotent elements, and then $(x-1)^n = 0$.

We can define $\log x = -\sum_{i=1}^{p-1} \frac{(1-x)^i}{i}$, and for any $t \in \overline{\mathbb{F}}_p$, we can define

$$x^t := \exp(t \log x),$$

where $\exp z = \sum_{i=0}^{p-1} \frac{z^i}{i!}$. Set

$$H^+ = \langle X \rangle \subset H,$$

and let $\widetilde{H}$ denote the connected algebraic $\mathbb{F}_p$-subgroup of GL_n generated by the 1-parameter subgroups x^t for $x \in X$.

Then if p is large enough (for a given n) then

$$H^+ = \widetilde{H}(\mathbb{F}_p)^+$$

(subgroup of $\widetilde{H}(\mathbb{F}_p)$ generated by all unipotents).

Actually, Nori does a lot more, viz. he shows that log and exp define bijections between nilpotently generated Lie subalgebras of $M_n(F)$, where F is a field of characteristic p which is large enough, and exponentially generated subgroups of $GL_n(F)$.

A different proof of Nori's theorem was given by Hrushovsky and Pillay using model-theoretic techniques

Proof for subgroups of $GL_2(\mathbb{F}_p)$, $p>3$.

Lemma. Let $H \subset SL_2(\mathbb{F}_p)$ be a subgroup of order divisible by p, and let $H_p \subset H$ be a Sylow p-subgroup. Then either $H_p \trianglelefteq H$, or $H = SL_2(\mathbb{F}_p)$.

Proof. We can assume that $H_p = U = \left\{\begin{pmatrix}1&\alpha\\0&1\end{pmatrix} \mid \alpha\in\mathbb{F}_p\right\}$. Let $T=\left\{\begin{pmatrix}\alpha&0\\0&\alpha^{-1}\end{pmatrix} \mid \alpha\in\mathbb{F}_p^\times\right\}$, $B=TU$ and $w=\begin{pmatrix}0&1\\-1&0\end{pmatrix}$. Then we have the Bruhat decomposition

$$SL_2(\mathbb{F}_p) = B \cup BwB.$$

If $H_p \ntrianglelefteq H$ then H contains a nontrivial conjugate U' of U. It is well-known that U has 2 orbits on $\mathbb{P}^1(\mathbb{F}_p)$, of sizes 1 and p. If $U'\neq U$, then U' does not fix the point which is fixed by U, which implies that $V=\langle U, U'\rangle \subset H$ acts on $\mathbb{P}^1(\mathbb{F}_p)$ transitively. So, $|V|$ is divisible by $p(p+1)$. Since $|B|=p(p-1)$, we have $V \not\subset B$ (in fact, it is easy to see that $U' \not\subset B$ as B normalizes U). It follows from the Bruhat decompotition that V contains an element of the form tw, $t\in T$. Then V contains

$$U^- = (tw)^{-1}U(tw) = \left\{\begin{pmatrix}1&1\\\alpha&0\end{pmatrix} \mid \alpha\in\mathbb{F}_p\right\}.$$

But $\langle U, U^-\rangle = SL_2(\mathbb{F}_p)$.

So, for a subgroup $H \subset GL_2(\mathbb{F}_p)$, we only have the following possibilities

(i) $H^+=\{1\}$

(ii) H^+ is conjugate to U

(iii) $H^+ = SL_2(\mathbb{F}_p)$

In either case, the assertion of Nori's theorem is valid.

Proof of the theorem. We can assume that $G \subset GL_n$. Then there exists $j = j(n)$ such that if $\mathcal{G} \subset GL_n(\mathbb{F}_p)$ is a subgroup of order prime to p then $\mathcal{G}$ has an abelian normal subgroup $\mathcal{L} \subset \mathcal{G}$ with $[\mathcal{G} : \mathcal{L}]$ dividing j. (This is a consequence of the usual Jordan Theorem in characteristic zero: Indeed, consider the reduction map $GL_n(\mathbb{Z}_p) \to GL_n(\mathbb{F}_p)$. Since the kernel is a pro-p group, $\mathcal{G}$ lifts to a subgroup $\tilde{\mathcal{G}} \subset GL_n(\mathbb{Z}_p)$, and Jordan's theorem applies.)

Let $\Gamma^{(j)}$ be the subgroup of Γ generated by γ^j for $\gamma \in \Gamma$, and let $\Phi = [\Gamma^{(j)}, \Gamma^{(j)}]$. Since the map $G \to G$, $x \mapsto x^j$, is dominant, Γ^j, hence $\Gamma^{(j)}$ is Zariski-dense, and then so is Φ. In particular, $\Phi \neq \{1\}$, so by expanding Π we may assume that $\rho_p(\Phi) \neq \{1\}$ for all $p \notin \Pi$.

As we said earlier, we may enlarge Π so that for $p \notin \Pi$, $\mathrm{Ad}\,\rho_p(\Gamma)$ acts absolutely trivial on $\underline{g}^{(p)}_{\mathbb{F}_p}$, which is the Lie algebra of $\underline{G}^{(p)}$ over $\mathbb{F}_p$.

Let $p \notin \Pi$, and set $H = \rho_p(\Gamma)$. Then p divides $|H|$. Indeed, otherwise H would have an abelian normal subgroup of index dividing j, and $\rho_p(\Phi)$ would be trivial, a contradiction.

Construct H^+ as in Nori's Theorem. By Nori's theorem there exists a connected algebraic group $\tilde{H}$, which in fact is contained in $\underline{G}^{(p)}$, such that $H^+ = \tilde{H}(\mathbb{F}_p)^+$; in particular, $\tilde{H} \neq \{1\}$. By construction, $\tilde{H}$ is normalised by $\mathrm{Ad}\,\rho_p(\Gamma)$, so $\mathfrak{h}$ is nontrivial and invariant under $\mathrm{Ad}\,\rho_p(\Gamma)$. Since the latter acts on $\underline{\mathfrak{g}}^{(p)}$ irreducibly, we conclude that $\mathfrak{h} = \underline{\mathfrak{g}}^{(p)}$, hence $H = \underline{G}^{(p)}$. But since $\underline{G}^{(p)}$ is simply connected we have

$$\underline{G}^{(p)}(\mathbb{F}_p)^+ = \underline{G}^{(p)}(\mathbb{F}_p),$$

and $\rho_p(\Gamma) = \underline{G}^{(p)}(\mathbb{F}_p)$.

(Thus, here again the simply connectedness condition is used to conclude that the relevant group of rational points is generated by unipotent elements, i.e the Kneser-Tits conjecture holds. This connection with the Kneser-Tits conjecture goes back to Platonov's argument.).

A vast generalization of the theorem of MVW is the following theorem of Weisfeiler

Theorem. Let k be an algebraically closed field of characteristic different from 2 and 3, and let G be an almost simple, connected and simply connected algebraic group defined over k. Let Γ be a Zariski-dense finitely generated subgroup of $G(k)$, and let A be the subring of k generated by the traces $\operatorname{tr} \operatorname{Ad}\gamma$, $\gamma \in \Gamma$. Then there exists $b \in A$, a subgroup of finite index $\Gamma' \subset \Gamma$, and a structure G_{A_b} of a group scheme over A_b on G such that $\Gamma' \subseteq G_{A_b}(A_b)$ and Γ' is dense in $G_{A_b}(\hat{A}_b)$.

(Additional problems in characteristic 2 and 3 can arise from the existence of exceptional isogenies)

The final word in the strong approximation saga is the work of Pink: he included characteristics 2 and 3 and also proved an appropriate version of the openness statement for semi-simple, and not just simple groups.