The curious case of Congruence Subgroups

Giancarlo Castellano

17 March 2018

In the classical study of modular forms, the notion of congruence subgroups is ubiquitous. This is in sharp contrast with the adelic treatment of automorphic forms, where congruence subgroups are either entirely missing or only appear in the vague statement that "passing to the adelic setting has the advantage that one can now look at all congruence subgroups at once". In this note, we attempt to find out:

(Q1) What happened to congruence subgroups upon adelization?

(Q2) How do we get them back?

The short answers are (see §0 for the notations):

(A1) *The suitable adelic substitute for congruence subgroups of $G(F)$ are open compact subgroups of $G(\mathbb{A}_f)$.*

(A2) *Congruence subgroups $\Gamma \subset G(F)$ are obtained from open compact subgroups $L \subset G(\mathbb{A}_f)$ by intersecting with $G(F)$. If G has "strong approximation" (cf. §6), then for each Γ there exists precisely one L with $\Gamma = L \cap G(F)$.*

Let us now go into more details. After fixing some notation in §0, we give the classical and modern definitions of (principal) congruence subgroups in §1 and §2, respectively. Then, in §3 and in §4, we prove (A2), putting emphasis on why strong approximation is needed, and in §5 we conclude with an observation on automorphic forms. The appendix (§§A-C) is merely a collection of easy topological facts that are used in §2.

§0. We first fix some notation. Let F be a number field, and let $\mathbb{A}_f = \prod'_{\nu<\infty} F_\nu$ denote the ring of finite adeles of F. As usual, F is embedded diagonally into $\mathbb{A}_f$ via $r \mapsto (r)_{\nu<\infty} = (r, r, ...)$; recall that the image of F is dense in $\mathbb{A}_f$, cf. e.g. [5, Thm. 1.5].

Next, let G be a reductive algebraic group defined over F; for most intents and purposes, we will have to fix an embedding $G \hookrightarrow \mathrm{GL}_n$ for some n. (Thus, for each F-algebra A, we regard the group $G(A)$ of A-points as a subgroup of $\mathrm{GL}_n(A)$.)

§1. Let us recall the definition of congruence subgroups in the classical setting ($F = \mathbb{Q}$, $G = \mathrm{SL}_2$). A *principal congruence subgroup* of $\mathrm{SL}_2(\mathbb{Z})$ is a subgroup of the form

$$\Gamma(N) := \{\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z}) : a \equiv d \equiv 1 \pmod N, b \equiv c \equiv 0 \pmod N\}$$

for some integer $N \geq 1$. More generally, $\Gamma \subseteq \mathrm{SL}_2(\mathbb{Z})$ is called a *congruence subgroup* of $\mathrm{SL}_2(\mathbb{Z})$ if it contains some principal congruence subgroup $\Gamma(N)$. (In this case, the index $[\Gamma : \Gamma(N)]$ is necessarily finite.)

Example. For any $N \geq 1$,

$$\Gamma_0(N) := \{\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z}) : c \equiv 0 \pmod N\}$$

(sometimes called the *Hecke subgroup*) and

$$\Gamma_1(N) := \{\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z}) : a \equiv d \equiv 1 \pmod N, c \equiv 0 \pmod N\}$$

are congruence subgroups of $\mathrm{SL}_2(\mathbb{Z})$.

Analogously, for general F and G (and a fixed embedding $G \hookrightarrow \mathrm{GL}_n$), we may define a principal congruence subgroup of $G(F)$ to be a subgroup of the form

$$\Gamma(\mathfrak{a}) := G(F) \cap \ker\left(\mathrm{GL}_n(\mathcal{O}_F) \to \mathrm{GL}_n(\mathcal{O}_F/\mathfrak{a})\right),$$

where $\mathcal{O}_F$ is the ring of integers of F and $\mathfrak{a}$ is a nonzero ideal of $\mathcal{O}_F$. At this point, it would seem natural to define congruence subgroups as those $\Gamma \subset G(F)$ such that

Γ *contains a principal congruence subgroup* $\Gamma(\mathfrak{a})$ *as a subgroup of finite index.* (*)

We want to keep this in the back of our minds, but this is not the definition we (or anyone else, for that matter) shall be working with.

§2. The modern notion of congruence subgroups is as follows: we call $\Gamma \subset G(F)$ a *congruence subgroup* of $G(F)$ if it is of the form

$$\Gamma = G(F) \cap L$$

for some open compact subgroup L of $G(\mathbb{A}_f)$.

This definition may feel a bit like it fell from the sky. Let us provide arguments to remedy this. On the one hand, the link with the classical definition from §1 is contained in the two following facts (which are proved in §C below):

Fact 2.1. Let $\Gamma = \Gamma(\mathfrak{a})$ be a principal congruence subgroup of $G(F)$, cf. §1. Then there exists an open compact subgroup $L(\mathfrak{a})$ of $G(\mathbb{A}_f)$ such that $\Gamma = G(F) \cap L(\mathfrak{a})$.

Fact 2.2. Let Γ be a congruence subgroup of G according to the new definition. Then Γ contains a principal congruence subgroup $\Gamma(\mathfrak{a}) = G(F) \cap L(\mathfrak{a})$ as a subgroup of finite index. (That is, Γ satisfies (*).)

On the other hand, it is not at all clear whether every Γ satisfying (*) is a congruence subgroup. Thus, our fancy new definition has the advantage that it automatically makes the (set-theoretic) function

$$\{\text{open compact subgroups of } G(\mathbb{A}_f)\} \to \{\text{congruence subgroups of } G(\mathbb{Q})\},$$
$$L \mapsto G(F) \cap L$$

(well-defined and) surjective. This will come in handy later (in §4).

§3. Our shiny new definition of congruence subgroups (see §2) raises a natural question, which is related to (Q1) from the introduction:

(Q1') Given a concrete congruence subgroup Γ of $G(F)$, how do we obtain or construct an open compact subgroup L of $G(\mathbb{A}_f)$ such that $\Gamma = G(F) \cap L$?

Of course Fact 2.1 already answers this question for principal congruence subgroups $\Gamma = \Gamma(\mathfrak{a})$, but even in this special case there may be more than one $L(\mathfrak{a})$ with $\Gamma = G(F) \cap L(\mathfrak{a})$ – as a matter of fact, there may even be *more than one* $\mathfrak{a}$ such that Γ is of the form $\Gamma(\mathfrak{a})$, as illustrated nicely (or horribly) by the following example.

Example. Let $F = \mathbb{Q}$ and let $G = \mathrm{GL}_1$, embedded into itself. Since $\mathcal{O}_F = \mathbb{Z}$ is a PID, we can simplify the notation by considering positive integers N in lieu of nonzero ideals $\mathfrak{a} \subseteq \mathcal{O}_F$.

Now, as N ranges over the positive integers, all $L(N)$'s are pairwise distinct. (This is apparent by their definition, see §B.) However, $G(\mathbb{Q})$ only has two distinct congruence subgroups, one being all of $G(\mathbb{Z}) = \mathrm{GL}_1(\mathbb{Z}) = \{\pm 1\}$ and the other one being the trivial subgroup $\{1\}$.

Accordingly, in order to obtain a nice correspondence and a satisfactory answer to (Q1'), we have to impose additional assumptions on G.

§4. The decisive assumption on G is that $G(F)$ (or rather, its image under the diagonal embedding) be dense in $G(\mathbb{A}_f)$; if this is the case, we say that G has *strong approximation*. The need for this definition is shown by the following example:

Example. Let $F = \mathbb{Q}$ and let G be the multiplicative group $\mathbb{G}_m = \mathrm{GL}_1$. We claim that $G(F) = \mathbb{Q}^\times$ is *not* dense in $G(\mathbb{A}_f) = \mathbb{A}_f^\times$. Since a dense subset must meet every non-empty open subset, it suffices to find $U \subset G(\mathbb{A}_f)$ open such that $U \cap \mathbb{Q}^\times = \emptyset$.

First, let $O := \prod_p \mathbb{Z}_p^\times$. Since $\mathbb{A}_f^\times$ is precisely the restricted product of the $\mathbb{Q}_p^\times$ with respect to $\mathbb{Z}_p^\times$ as p ranges over the primes (cf. footnote 4), O is open by definition of the restricted product topology. On the other hand, O intersects $\mathbb{Q}^\times$ in the two-point set $\{\pm 1\}$. Hence $U = O \setminus \{\pm 1\}$ is an open subset of $\mathbb{A}_f^\times$ which does not meet $\mathbb{Q}^\times$.

(On the other hand, the well-known fact that F is dense in $\mathbb{A}_f$ tells us precisely that the additive group $G = \mathbb{G}_a$ has strong approximation. Moreover, the special linear group $G = \mathrm{SL}_n$ has strong approximation, see [2, Thm 3.3.1.(i)].)

Without further ado, let us present our main result, which makes up the bulk of (A2) from the introduction.

Theorem. *Suppose that G has strong approximation. Then the congruence subgroups of $G(F)$ are in one-to-one correspondence with the open compact subgroups of $G(\mathbb{A}_f)$, the bijection being given by*

$$\Gamma \mapsto \overline{\Gamma},$$
$$L \cap G(F) \leftarrow\!\shortmid L;$$

here $\overline{\Gamma}$ denotes the closure of Γ in the topology of $G(\mathbb{A}_f)$.

Proof. It suffices[1] to show that, for any open compact $L \subseteq G(\mathbb{A}_f)$,

$$\overline{G(F) \cap L} = L,$$

i.e. that for each $g \in L$ there exists a sequence $(g_n)_{n\in\mathbb{N}}$ in $G(F) \cap L$ converging to g.

Hence, let $g \in L$. Since $L \subseteq G(\mathbb{A}_f)$, by strong approximation there exists a sequence $(g_n)_{n\in\mathbb{N}}$ in $G(F)$ converging to g. But L is open, so g_n will eventually lie in L for large

[1] The argument is purely set-theoretical. As we observed in §2, the assignment $L \mapsto G(F) \cap L$ is surjective; in particular it has a right inverse. On the other hand, we now claim that it has a left inverse, namely the closure operator. But if both a left and a right inverse exist, they must coincide, so the closure operator and the given assignment are inverse to each other.

enough n. Thus, discarding finitely many terms if necessary, we can assume that each g_n lies in $G(F) \cap L$, which means that $(g_n)_{n\in\mathbb{N}}$ has the desired property. □

To conclude this paragraph, let us remark that Kneser [3] provided a complete classification of (reductive) algebraic groups which have strong approximation; this topic is treated in detail in [5, §7.4]. As Borel and Jacquet remark in [1, 4.7], for G semisimple and almost simple over F to have strong approximation it is (necessary and) sufficient that G be simply connected and G_∞ be noncompact; check [5, 2.1.13] for some of the definitions.

§5. We wish to round out this note with an observation on the spaces of automorphic forms which helps build a bridge between the classical and the adelic worlds; we have resolved to keep the rigour and technical details to a minimum because, after all, we are not writing a textbook. We follow the notations and terminology of [1]; and the details may be looked up there.

Let L be an open compact subgroup of $G(\mathbb{A}_f)$, let ξ_L denote the corresponding idempotent of the Hecke algebra $\mathscr{H}_f$ (cf. [1, 3.1-3.2]), and let $\mathscr{A}(\xi_\infty \otimes \xi_L, J, K_\infty)$ denote the space of "(adelic) automorphic forms for G of type $(\xi_\infty \otimes \xi_L, J, K_\infty)$", i.e. smooth functions $f : G(\mathbb{A}_F) \to \mathbb{C}$ such that

(i) $f(\gamma x) = f(x)$ for all $\gamma \in G(F)$;

(ii) $f * \xi_L = f$, which by [1, 3.2] means precisely that f is right invariant under L;

(iii) f is annihilated by J which is an ideal of finite codimension in ... (you know the drill);

(iv) f is slowly increasing.

On the other hand, let Γ be a congruence subgroup of $G(F)$, and let $\mathscr{A}(\Gamma, \xi_\infty, J, K_\infty)$ denote the space of "(classical) automorphic forms for (Γ, K_∞) of type (ξ_∞, J)", i.e. smooth functions $f : G_\infty \to \mathbb{C}$ such that

(i) $f(\gamma x) = f(x)$ for all $\gamma \in \Gamma$;

(ii) $f * \xi_\infty = f$, which by [1, 1.5] means precisely that f is right K_∞-finite;

(iii) f is annihilated by J which is again an ideal of finite codimension yadda yadda yadda;

(iv) f is slowly increasing.

If G has strong approximation, and if Γ and L correspond to one another via the bijection from Thm. §4, then we have an isomorphism

$$\mathscr{A}(\xi_\infty \otimes \xi_L, J, K_\infty) \xrightarrow{\sim} \mathscr{A}(\Gamma, \xi_\infty, J, K_\infty).$$

Note that, for varying L, the spaces on the left-hand side form a directed system: an inclusion $L \supset L'$ yields an inclusion $\mathscr{A}(\xi_\infty \otimes \xi_L, ...) \subset \mathscr{A}(\xi_\infty \otimes \xi_{L'}, ...)$. The corresponding direct (or inductive) limit shall be denoted by $\mathscr{A}(\xi_\infty, J, K_\infty)$. Similarly, if Σ denotes the family of congruence subgroups of $G(F)$, then we can form the direct limit $\mathscr{A}(\Sigma, \xi_\infty, J, K_\infty)$ as Γ runs over the elements of Σ. Perhaps unsurprisingly, we get an isomorphism

$$\mathscr{A}(\xi_\infty, J, K_\infty) \xrightarrow{\sim} \mathscr{A}(\Sigma, \xi_\infty, J, K_\infty).$$

But more importantly (at least, I believe so), $G(\mathbb{A}_f)$ *acts on both spaces, and the isomorphism commutes with these actions*! On the one hand, the action of $G(\mathbb{A}_f)$ on the "adelic space" is defined in [1, 4.7]. On the other hand, in [1, 1.9] the authors define an action of a certain[2] topological group $G(F)_\Sigma$ on $\mathscr{A}(\Sigma, \xi_\infty, J, K_\infty)$, and later argue that, since G has strong approximation, the group $G(F)_\Sigma$ is precisely $G(\mathbb{A}_f)$. (They also spend a few words on the general case, where $G(F)_\Sigma$ is merely a subgroup of $G(\mathbb{A}_f)$.) In my limited view and understanding, this makes automorphic representations look "more natural", or at least more rooted in the classical theory. I hope it was also somewhat interesting for the reader.

Appendix

§A. We start by asking the question: what do open compact subgroups of $\mathbb{A}_f$ look like?

Fact A.1. In the local field F_ν, a neighbourhood base around 0 is given by the open subgroups $\varpi^k \mathcal{O}_\nu$ as k ranges over $\mathbb{N}$. Each $\varpi^k \mathcal{O}_\nu$ is also compact.

Indeed, $\varpi^k \mathcal{O}_\nu$ coincides with the open ball of radius ρ^{k-1} around 0, where $\rho = |\varpi|_\nu < 1$. As for the second claim, $\varpi^k \mathcal{O}_\nu$ is compact as it coincides with the closed ball of radius ρ^k around 0.

Fact A.2. Let $\mathfrak{a}$ be a nonzero ideal of $\mathcal{O}_F$ with prime ideal decomposition[3] $\mathfrak{a} = \prod_{\nu<\infty} \mathfrak{p}_\nu^{k_\nu}$, and let

$$K(\mathfrak{a}) := \prod_{\nu<\infty} \varpi_\nu^{k_\nu} \mathcal{O}_\nu.$$

Then $K(\mathfrak{a})$ is an open compact subgroup of $\mathbb{A}_f$.

[2] I have some half-assed notes on (completions of) topological groups where I meant to mention stuff like $G(F)_\Sigma$ in much more detail. If I ever get around to finishing those, I will also make them available to anyone who cares.

[3] Recall that the finite places of F are in one-to-one correspondence with the nonzero prime ideals of the Dedekind domain $\mathcal{O}_F$. For a place ν, we denote the corresponding prime by $\mathfrak{p}_\nu$.

Indeed, the given subgroup is open by definition of the restricted product topology on $\mathbb{A}_f$, and it is compact by Tychonoff's theorem. (In both cases we are using Fact A.1.)

Fact A.3. Let K be any open compact subgroup of $\mathbb{A}_f$. Then there exists a nonzero ideal $\mathfrak{a} \subseteq \mathcal{O}_F$ such that $K \supseteq K(\mathfrak{a})$.

Indeed, by using Fact A.1 together with the definition of the restricted product topology, we obtain that the $K(\mathfrak{a})$'s form a neighbourhood base around 0 in $\mathbb{A}_f$.

§B. We now try to use §A to infer some results on open compact subgroups of $G(\mathbb{A}_f)$.

The point here is, that for topological purposes, the elements of $G(\mathbb{A}_f) \subseteq \mathrm{GL}_n(\mathbb{A}_f)$ are regarded as points (resp., vectors) in some high-dimensional[4] affine space $\mathbb{A}_f^N$, with the entries as components; thus, topological statements over the underlying ring $\mathbb{A}_f$ carry over to the group $G(\mathbb{A}_f)$ because "they are true entry-wise". (This is analogous to classical observations such as: $\mathrm{SL}_2(\mathbb{Z})$ is discrete in $\mathrm{SL}_2(\mathbb{R})$ precisely because $\mathbb{Z}$ is discrete in $\mathbb{R}$.)[5]

With this idea in mind and some elbow grease, it should be possible to prove the following analogues of Facts A.1-A.3.

Fact B.1. Let $\nu < \infty$ and $k \in \mathbb{N}$, and let

$$H_{k,\nu} := \begin{cases} \mathrm{GL}_n(\mathcal{O}_\nu), & \text{if } k = 0; \\ \mathbf{1}_n + \varpi^k M_n(\mathcal{O}_\nu), & \text{if } k > 0, \end{cases}$$

where $M_n(\mathcal{O}_\nu)$ is the space of $(n \times n)$-matrices with entries in $\mathcal{O}_\nu$. Then $H_{k,\nu}$ is an open compact subgroup of $\mathrm{GL}_n(F_\nu)$, and its intersection with $G(F_\nu)$ is an open compact subgroup of $G(F_\nu)$. Moreover, as k ranges over $\mathbb{N}$, these subgroups form a neighbourhood base around $\mathbf{1}_n$ in the topology of $\mathrm{GL}_n(F_\nu)$, resp. $G(F_\nu)$.

[4] As is often the case in our field, the exact nature of this embedding becomes *less* clear as one consults *more* reference texts. We have chosen to follow [2, §3.3] and thus identify $\mathrm{GL}_n(\mathbb{A}_f)$ with a subset X of $\mathbb{A}_f^{n^2+1}$, namely

$$X = \{(a_{11}, a_{12}, ..., a_{nn}, d) \in \mathbb{A}_f^{n^2} \times \mathbb{A}_f : \det(a_{ij}) \cdot d = 1\} \subset \mathbb{A}_f^{n^2+1},$$

and equip it (and subsequently also $G(\mathbb{A}_f)$) with the subspace topology. Alternatively, $G(\mathbb{A}_f)$ is the restricted product of the $G(F_\nu)$ with respect to the $G(\mathcal{O}_\nu)$, where each $G(F_\nu)$ is topologized as a subspace of $F_\nu^{n^2+1}$ in a similar way as above.

[5] Obviously, we are cheating a little here. For instance, even though F is dense in $\mathbb{A}_f$, it is not true for general reductive G that $G(F)$ is dense in $G(\mathbb{A}_f)$, as we saw in §4.

Fact B.2. Let $\mathfrak{a} = \prod_{\nu<\infty} \mathfrak{p}_\nu^{k_\nu}$ be a nonzero ideal of $\mathcal{O}_F$, and let

$$L(\mathfrak{a}) := \prod_{\nu<\infty} \big(H_{k_\nu,\nu} \cap G(F_\nu)\big) \subset G(\mathbb{A}_f).$$

Then $L(\mathfrak{a})$ is an open compact subgroup of $G(\mathbb{A}_f)$.

Fact B.3. Let L be any open compact subgroup of $G(\mathbb{A}_f)$. Then there exists a nonzero ideal $\mathfrak{a} \subseteq \mathcal{O}_F$ such that $L \supseteq L(\mathfrak{a})$.

§C. Let us finally prove Facts 2.1 and 2.2.

It is more or less evident that $L(\mathfrak{a}) \cap G(F)$ coincides with the principal congruence subgroup $\Gamma(\mathfrak{a})$ defined in §1. This proves Fact 2.1.

Now let $\Gamma = G(F) \cap L$ be an arbitrary congruence subgroup as in §2. By Fact B.3, there exists some $\mathfrak{a}$ such that $L(\mathfrak{a}) \subseteq L$. Since L is compact and $L(\mathfrak{a})$ is open, L can be covered by finitely many translates of $L(\mathfrak{a})$; in other words, the index of $L(\mathfrak{a})$ in L is finite. But then so is $[\Gamma : \Gamma(\mathfrak{a})] \leq [L : L(\mathfrak{a})]$, and Fact 2.2 is proved.

References

[1] A. Borel, H. Jacquet, *Automorphic forms and automorphic representations*, in: Proc. Sympos. Pure Math., Vol. XXXIII, part I, AMS, Providence, R.I., (1977) pp. 189–202.

[2] D. Bump, *Automorphic forms and representations*, Cambridge Studies in Advanced Mathematics, vol. 55, Cambridge University Press, Cambridge, 1997.

[3] M. Kneser, Starke Approximation in algebraischen Gruppen I, *J. Reine Angew. Math.* **218** (1965), pp. 190–203.

[4] J. S. Milne, *Introduction to Shimura Varieties*, expository notes, available at http://jmilne.org/math/xnotes/svi.html.

[5] V. Platonov, A. Rapinchuk, *Algebraic Groups and Number Theory*, translated by Rachel Rowen, Academic Press, Inc., 1993.