7. Counting congruence subgroups and the congruence subgroup problem

Let k be a global field, i.e., k is a finite extension of $\mathbb{Q}$, in case $char(k) = 0$, or of $\mathbb{F}_p(x)$, in case $char(k) = p > 0$ Let $\mathcal{O}$ be the ring of integers of k and S a finite set of valuations ("primes") of k and $\mathcal{O}_S = \{x \in k | v(x) \geq 0, \forall v \notin S\}$. Let G be a connected, simply-connected simple, algebraic group defined over k with a fixed embedding $G \hookrightarrow GL_r$. Let $\Gamma = G \cap GL_r(\mathcal{O}_S)$ the S-arithmetic subgroup of G. We will always assume that Γ is infinite (or equivalently that $\prod\limits_{v \in S} G(k_v)$ is not compact). Every ideal $\mathcal{J} \neq 0$ of $\mathcal{O}_S$ defines a *principal congruence subgroup* $\Gamma(\mathcal{J})$ of Γ:

$$\Gamma(\mathcal{J}) = Ker\big(\Gamma \to GL_r(\mathcal{O}_S/\mathcal{J})\big)$$

A subgroup of Γ containing $\Gamma(\mathcal{J})$ for some $\mathcal{J}$ is called a *congruence subgroup.*

Let $C_n(\Gamma) = \#$ congruence subgroups of Γ of index $\leq n$.

Theorem 7.1. *Assume $char(k) = 0$. Then there exists positive constants a and b such that*

$$n^{a \log n / \log \log n} \leq C_n(\Gamma) \leq n^{b \log n / \log \log n}$$

Theorem 7.2. *Assume $char(k) = p > 0$* (Assume also ???). *Then there exist positive constants a and b such that $n^{a \log n} \leq C_n(\Gamma) \leq n^{b (\log n)^2}$.*

Let $\hat{\Gamma}$ be the profinite completion of Γ and $\tilde{\Gamma}$ the completion of Γ with respect to the topology induced on Γ by the congruence subgroups (see WINDOW on STRONG APPROXIMATION). The identity map from Γ to Γ extends to a continuous epimorphism $\pi : \hat{\Gamma} \to \tilde{\Gamma}$ whose kernel $C = C(G, S)$ is called the *congruence kernel* of Γ. Γ is said to have the *congruence subgroup property* if C is finite.

Corollary 7.3. *If $char(k) = 0$ and Γ has the congruence subgroup property then the subgroup growth of Γ is of type $n^{\log n / \log \log n}$.*

The precise growth in characteristic p is not known as of now. In any event and any characteristic such Γ's have "intermediate subgroup growth" (i.e., more than polynomial less than exponential). In chapter 9 it will be shown that there are plenty of such possibilities, including many that are slower than $n^{\log n / \log \log n}$ and yet non-polynomial. On the other hand Theorem 7.1 will be used to show in chapter 8 that this is impossible among the linear groups.

Theorem 7.1 will be proved in section 7.1, while Theorem 7.2 will be dealt with in section 7.2. In section 7.3 we will relate the congruence subgroup problem and subgroup growth:

Theorem 7.4. *Assume char$(k) = 0$ and that G satisfies the Platonov-Margulis conjecture (see §7.3). Then Γ has the congruence subgroup property if and only if for every $\varepsilon > 0$, $s_n(\Gamma) = O_\varepsilon(n^{\varepsilon \log n})$, i.e. if and only if the subgroup growth type of Γ is strictly less than $n^{\log n}$.*

Corollary 7.5. *Assume char$(k) = 0$ and Γ as before. If Γ fails to have the congruence subgroup property then the subgroup growth type of Γ is at least as large as $n^{\log n}$.*

The last corollary shows that when Γ fails to have the congruence subgroup property, it has plenty of non-congruence subgroups – by far more than congruence subgroups; the congruence subgroup growth is $n^{\log n/\log\log n}$ while the subgroup growth is at least $n^{\log n}$. We actually believe (and many known examples support this) that when the congruence subgroup property fails the subgroup growth is in fact even faster than $n^{\log n}$ (probably exponential or even super exponential).

Theorem 7.4 has another important application: it enables us to formulate the congruence subgroup problem by abstract group theoretic terms making no reference to the arithmetic structure of Γ:

Generalized congruence subgroup problem: Let Γ be a finitely generated group. Is the subgroup growth type of Γ strictly smaller than $n^{\log n}$?

The classical congruence subgroup problem is asked for S-arithmetic groups as above. Every such S-arithmetic group is a lattice (i.e., a discrete subgroup of finite covolume) in a suitable semi-simple group H. Here by semi-simple group H we mean a product $\prod_{i=1}^{r} G_i(K_i)$ when for each $1 \le i \le r$, K_i is a local field and G_i is a simple algebraic group defined over K_i. By the celebrated arithmeticity result of Margulis [ ], under some assumptions on H, every lattice in H is S-arithmetic. On the other hand, when $H = G(K)$, K a local field and G a simple, connected, algebraic group defined over K and of K-rank one, it is possible (sometimes) that H has non-arithmetic lattices. It is of special interest to extend the congruence subgroup problem and to study it in the more general framework of lattices in semi-simple groups and not merely for S-arithmetic lattices.

Serre conjecture, which is largely proved by now, asserts, loosely speaking, that an S-arithmetic lattice in a semi-simple group H has the congruence subgroup property if and only if rank$(H) \ge 2$ (see section 7.3 for a precise formulation). In particular, the conjecture says that the validity of the congruence subgroup property for lattices Γ in H, depends only on H and not on Γ. This is compatible with the experience with other properties of lattices. Extending this philosophy to arbitrary lattices in H, it is natural to extend Serre's conjecture and to add the conjecture that all non-arithmetic lattices (in rank one groups, and as mentioned above, by Margulis' result only in rank one group, non-arithmetic lattices exist) fail to satisfy the generalized congruence subgroup property.

Theorem 7.6. *Let $H = G(K)$ when K is a local field and G a simple, connected algebraic group defined over K. Let Γ be a lattice in H. Then:*

(1) *If K is non-archimedean then Γ has a negative answer to the generalized congruence subgroup problem.*
(2) *If H is locally isomorphic to $SO(n,1), n = 2$ or 3 then Γ has a negative answer to the generalized congruence subgroup problem.*
(3) *If H is locally isomorphic to $SO(n,1), n \geq 4$ and Γ is one of the known non-arithmetic lattices (i.e., either generated by reflections or the ones constructed by Gromov and Piatezki-Shapiro [GPS]) then Γ has negative answer to the generalized congruence subgroup problem.*

The proof of Theorem 7.6 uses hyperbolic geometry. As a byproduct of the subgroup growth consideration, the following result is deduced:

Theorem 7.7. *Let $n \geq 4$, $0 < r \in \mathbb{R}$ and $\rho_n(r)$ be the number of isomorphism classes on n-dimensional hyperbolic manifolds of volume at most r. Then there exist two constants $a = a(n)$ and $b = b(n)$ such that*

$$ar \log r \leq \log \rho_n(v) \leq br \log r$$

The lower bound of Theorem 7.7, (which is based on subgroup growth is proved in section 7.5. (For the upper bound – see [BGLM]). We also compare there Theorem 7.7 and Theorem 7.1 and present some conjectures about the rate of growth of other types of manifolds.

We end the chapter with some conjectures and speculations on subgroup growth of groups with Kazhdan property (T) and of amenable groups. (???)

7.1. **Counting congruence subgroups: the characteristic O case.**

In this section we determine precisely the congruence subgroup growth type of S-arithmetic groups over number fields and prove Theorem 7.1.

Keeping the notations of the introduction, we assume k is a finite extension of $\mathbb{Q}$. So S is a finite set of prime ideals in $\mathcal{O}$-the ring of integers in k. For such S let $S_{\mathbb{Q}}$ be the set of all the rational primes lying below S, i.e. $S_{\mathbb{Q}} = \{p \in \mathbb{Z}_{+} | \mathcal{P} \cap \mathbb{Z} = (p)$ for some $\mathcal{P} \in S\}$ and let $\overline{S}$ be the set of all primes in $\mathcal{O}$ lying above $S_{\mathbb{Q}}$. Then $S \subseteq \overline{S}$ and clearly $G(\mathcal{O}) \subseteq G(\mathcal{O}_S) \subseteq G(\mathcal{O}_{\overline{S}})$, we also have surjective maps $G(\hat{\mathcal{O}}) \twoheadrightarrow G(\hat{\mathcal{O}}_S) \twoheadrightarrow G(\hat{\mathcal{O}}_{\overline{S}})$. Now if H is $Res^k_{\mathbb{Q}}(G)$ the restriction of scalars from k to $\mathbb{Q}$, then $H(\mathbb{Z}) = G(\mathcal{O})$ and $H(\mathbb{Z}_{S_{\mathbb{Q}}}) = G(\mathcal{O}_{\overline{S}})$. Thus if we prove the upper bound of Theorem 7.1 for $H(\mathbb{Z})$ and the lower bound for $H(\mathbb{Z}_{S_{\mathbb{Q}}})$ the Theorem will be proved. This shows that it suffices to prove the Theorem for $k = \mathbb{Q}$. We therefore assume $k = \mathbb{Q}$, an assumption that will simplify the notations.

So let $\Gamma = G(\mathbb{Z}_S)$ and $M = G(\hat{\mathbb{Z}}_S)$ its congruence completion. There is one to one correspondence between index n subgroups of M and congruence subgroups of index n of Γ. It will be sometimes more convenient to work with M rather than Γ. We will move freely between the two.

Proof of the lower bound: Let x be a large real number. Bombieri's theorem (which is "Riemann hypothesis on the average") implies (see [Window, Prime number theorem]) that for every $\rho < \frac{1}{2}$ there exists at least one prime q with $q \sim x^{\rho}$ such that $\#\mathcal{O}(x,q) \sim \frac{L_i(x)}{\phi(q)}$ where $L_i(x) = \int_0^x \frac{\log t}{t} dt$, ϕ is the Euler function (so $\phi(q) = q-1$) and $\mathcal{O}(x,q) = \{p | \, p \text{ prime } \leq x \text{ and } p \equiv 1(\mod q)\}$.
So we have:

$$P := \prod_{p \in \mathcal{O}(x,q)} p \sim e^{x/\phi(q)} \sim e^{x^{1-\rho}}$$

and

$$L := \#\mathcal{O}(x,q) \sim \frac{x}{\phi(q)\log x} \sim \frac{x^{1-\rho}}{\log x}$$

Let's now look at the congruence subgroups $\Gamma(P)$ of Γ. From the Strong Approximation Theorem for arithmetic groups (see[Window, Strong Approximation]) it follows that $\Gamma/\Gamma(P) = G(\mathbb{Z}/P\mathbb{Z})$ and by the Chinese Reminder Theorem

$$G(\mathbb{Z}/P\mathbb{Z}) = \prod_{p \in \mathcal{O}(x,q)} G(\mathbb{F}_p).$$

By Lang's Theorem (see [Window, Algebraic groups]) G is quasi split over the finite field $\mathbb{F}_p$, so it has a one dimensional split torus, i.e., $G(\mathbb{F}_p)$ contains a subgroup isomorphic to $\mathbb{F}_p^*$ which is a cyclic subgroup of order $p-1$. As $p \in \mathcal{O}(x,q)$, $q | p-1$ and so $\mathbb{F}_p^*$ and hence $G(\mathbb{F}_p)$ has a cyclic subgroup of order q, and $G(\mathbb{Z}/P\mathbb{Z})$ has an elementary abelian q-group A of dimension $L = \#\mathcal{O}(x,q)$. Now by [Basic Counting] A has at least $q^{L^2/4}$ subgroups. Each of them when pulled back to Γ give rise to a subgroup of Γ containing $\Gamma(P)$ and hence of index at most $\#G(\mathbb{Z}/P\mathbb{Z}) \sim P^d$ when $d = \dim(G)$.

So Γ has at least $q^{L^2/4}$ subgroups of index at most P^d. Taking log we get:

$$\log(q^{1/4L^2}) = \tfrac{1}{4}L^2 \log q \sim \tfrac{1}{4}\frac{x^{2(1-\rho)}}{\log^2 x} \cdot \rho \log x = \tfrac{\rho}{4}\frac{x^{2(1-\rho)}}{\log x}$$

while $\log(P^d) = d \log P \sim dx^{1-\rho}$ Hence:

$$\log(q^{1/4\,L^2}) \geq \tfrac{\rho(1-\rho)}{4d^2} \tfrac{\log^2(P^d)}{\log\log(P^d)}$$

Let $\rho \to \frac{1}{2}$, we get the lower bound for the theorem with $a = \frac{1}{16d^2}$.

Remark. One can improve the result to get a better estimate of a - see[GL]. For example for $\Gamma = SL_2(\mathbb{Z})$ we get ??? *Should we start with* $SL_2(\mathbb{Z})$ *as an example*???

Proof of the upper bound

Proposition 7.8. *("level ≤ index") Let* $\Gamma = G(\mathbb{Z})$ *as before and* H *a congruence subgroup of* Γ. *Then* $H \geq \Gamma(m)$ *for some* $m \leq [\Gamma : H]$.

Proof. To be given [*can Babai-Cameron-Palfy replace the original proof???*] □

Corollary 7.9.

$$C_n(\Gamma) \leq \sum_{m=1}^{n} s\big(G(\mathbb{Z}/m\mathbb{Z})\big)$$

The problem is therefore transformed now to a problem on finite groups. We need the following Proposition, which is of independent interest:

Proposition 7.10. $rank\big(G(\mathbb{Z}/p^\alpha\mathbb{Z})\big)$ *is bounded by a constant* C *independent of* p *and* α.

Proof. Here or in a window????? Note: the case $\alpha = 1$, needs (as far as I know) the CFSG-Pyber has an argument without (see [Lub]). Anyway, C can made explicit. What is better: without CFSG but *worse constant???*

We can now complete the proof of the upper bound; by (7.9) we should estimate $s\big(G(\mathbb{Z}/m\mathbb{Z})\big)$. If $m = \prod_{i=1}^{r} p_i^{e_i}$ is a decomposition of m into a product of distinct prime powers then $r \leq \frac{\log m}{\log\log m}$ (see [Window on Prime Number Theorem]). Thus

$$rank\big(G(\mathbb{Z}/m\mathbb{Z})\big) = rank\Big(\prod_{i=1}^{r} G(\mathbb{Z}/p_i^{e_i}\mathbb{Z})\Big) \leq rC \leq C\frac{\log m}{\log\log m}$$

where C is the constant from (7.10). By [Basic counting])

$$s\big(G(\mathbb{Z}/m\mathbb{Z})\big) \leq |G(\mathbb{Z}/m\mathbb{Z})|^{rank\left(G(\mathbb{Z}/m\mathbb{Z})\right)} \leq m^{dC\frac{\log m}{\log\log m}}$$

when $d = dim(G)$. So altogether $C_n(\Gamma) \leq n \cdot n^{dC\frac{\log n}{\log\log n}}$ as promised. $\square$

7.2. **Counting congruence subgroups: the positive characteristic case.**

Let k be a global field of characteristic $p > 0$, θ its ring of integers, S a finite set of (finite) valuations of k and $\theta_s = \{x \in k | v(x) \geq 0 \forall v \notin S\}$. Let G be a connected, simply connected, simple k-group with a fixed embedding $G \hookrightarrow GL_r$. Let $\Gamma = G(\theta_s) = G \cap GL_r(\theta_s)$. As before, a subgroup Δ of Γ is called a **congruence subgroup** if there exists an ideal $0 \neq \mathfrak{A} \triangleleft \theta_s$ such that Δ contains the **principal congruence subgroup** $\Gamma(\mathfrak{A}) = \{g \in \Gamma | g \equiv I_r(\mod \mathfrak{A})\}$.

Let $\tau_n(\Gamma)$ denote the number of congruence subgroups of Γ of index at most n.

Theorem 7.11. *There exist two positive constant a and b such that for all large n,*

$$n^{a \log n} \leq \tau_n(\Gamma) \leq n^{b(\log n)^2}.$$

Remark 7.12. *Unfortunately, we cannot determine the rate of growth if $\tau_n(\Gamma)$: it is somewhere between $n^{\log n}$ to $n^{(\log n)^2}$.*

The proof of the lower bound is quite easy: Note that $\tau_n(\Gamma) = s_n\big(G(\hat{\theta}_s)\big)$ when $\hat{\theta}_s$ is the profinite completion of θ_s and $G(\hat{\theta}_s)$ is the congruence completion of Γ. Now, $G(\hat{\theta}_s) = \underset{v \notin s}{\pi} G(\theta_v)$ where θ_v is the $v - adic$ completion of θ, i.e., the completion with respect to a maximal ideal $m = m_v$. In particular, $K = G(\theta_v)$ is a quotient of $G(\hat{\theta}_s)$. The subgroup growth rate of $G(\theta_v)$ is at least $n^{\log n}$ (in fact, equal to $n^{\log n}$, see §4.4). Indeed, let $\bar{m}_v$ be the maximal ideal of θ_v, and $\bar{m}_v$ be the maximal ideal of θ_v, and $\bar{m}_v^i$ its i-th power. Denote $K_i = Ker\big(G(\theta_v) \to G)theta_v/\bar{m}_v^i)\big)$, then one can easily check that:

(i) $\log_p[K : K_i] \sim\subset i$ for some constant c.
(ii) $[K_i, K_i] \subseteq K_{2i}$
(iii) $K_i^p \subseteq k_{pi}$

This implies that k_i/K_{2i} is an elementary abelian p-group of rank approximately $c\dot{i}$. Thus there are at least $p^{\frac{1}{4}c^2 i^2}$ subgroups between K_i and K_{2i} all whose index in K is at most p^{2ci}. This proves the lower bound.

To prove the upper bound we note first that as $G(\hat{\theta})$ is mapped onto $G(\hat{\theta}_s)$, we can assume $S = \emptyset$, so assume $\Gamma = G(\theta)$. As G is simple over k, it is the restriction of scalars of an absolutely simple group defined over a finite extension of k. We can therefore, without loss of generality, assume that G is absolutely simple. As before $\tau_n(\Gamma) = s_n\big(G(\hat{\theta})\big)$ and we will work with $G(\hat{\theta})$.

Proposition 7.13. *Every open subgroup H of $L = G(\hat{\theta})$ of index n has a subgroup H_L subnormal in L and of index at most n^c in L, for a suitable constant c.*

Proof. The Proposition actually says that L satisfies the "polynomial subnormal core condition". As shown in Window , a profinite group satisfying the Babai-Cameron-Palfy (BCP) condition also satisfies the polynomial subnormal core condition. It is easy to see that L satisfies BCP since every non-abelian upper composition factor of L is a quotient of $G(\mathbb{F}_q)$ for some q a power of p. $\square$

Proposition 7.14. *Every subnormal subgroup of $L = G(\hat{\theta})$ of index n contains a principal congruence subgroup of index at most $n^{c' \log n}$ in L, for a suitable constant c'.*

Before proving Proposition 3, let us show how Propositions 2 and 3 imply Theorem 1. If H is a subgroup of K of index n, it contains a subnormal subgroup H_L of index at most n^c and the latter contains a principal congruence subgroup of index at most $n^{cc'(\log n^c)} = n^{c^2c' \log n} = n^{c_1 \log n}$ for $c_1 = c^2c'$.

Now the number of ideals of index m in θ is at most m^{c_2} and if $\mathfrak{A} \lhd \theta$ is an ideal of index m then the principal congruence subgroup $\Gamma(\mathfrak{A})$ is of index approximately m^{c_3} when $c_3 = \dim G$. Thus the number of principal congruence subgroups of index at most $n^{c_1 \log n}$ is at most the number of ideals of index at most $n^{c_4 \log n}$.

Hence $\Delta_n(K) \leq n^{c_4 \log n} s_n\big(G(\theta/\mathfrak{A})\big)$ where $\mathfrak{A}$ is an ideal in θ of index at most $n^{c_1 \log n}$ and so $G(\theta/\mathfrak{A})$ is a finite group of index at most $n^{c_5 \log n}$.

By (Window   ) the number of subgroups of index n in a group of order g is at most $g^{2 \log n}$. Hence $s_n\big(G(\theta/\mathfrak{A})\big) \leq n^{(2c_5(\log n)^2}$ and so $\tau_n(\Gamma)$ is at most $n^{b(\log n)^2}$ for a suitable constant b.

We turn now to the proof of Proposition 3. let us refresh our notations:

Let $V = V_k$ be the set of (finite) valuations of k. For $v \in V$, there is a maximal ideal $\underline{\mathrm{m}}_v$ of θ inducing v. Let θ_r be the completion of θ with respect to v (or equivalently with respect to $\underline{\mathrm{m}}_v$, i.e. $\theta_v = \underset{\leftarrow}{\rightarrow} \lim \theta/\underline{\mathrm{m}}_v^i$) and let m_v be the unique maximal ideal of θ_v. Denote $L_v = G(\theta_v)$ and

$$L_v(i) = Ker\big(G(\theta_v) \to G(\theta_v/m_v^i)\big).$$

So, $L = G(\hat{\theta}) = \underset{v \in V}{\pi} L_v$.

Let $W(L_v)$ be the weak-Frattini of L_v, i.e., the intersection of the maximal open normal subgroups of L_v. Then for almost every $v \in V, W(L_v)$ contains $L_v(1)$. In fact, it is almost always equal to Z_v, where Z_v is the preimage in $L_v = G(\theta_v)$ of the center $Z = Z\big(G(\theta_v/m_v)\big)$, since $G(\theta_v/m_v)/z$ is a finite simple group, for every v outside a finite set S.

Let now H be a subnormal subgroup of L, so $H_v = H \cap L_v$ is a subnormal subgroup of L_v. We claim that for $v \notin s$, either $H_v = L_v$ or $H_v \subseteq W(L_v)$. Indeed, the image of $H_v \mod W(L_v)$ is a subnormal subgroup of the simple group $L/W(L_v)$ and hence it is either onto, in which case $H = L_v$, or trivial, in which case $H_v \leq W(L_v)$.

Let $V_0(H) = \{v \in V | H \cap L_v \neq L_v\}$. We claim that if $v \in V_0(H)$, then $\pi_v(H) \leq Z_v$ where π_v is the projection from L to L_v. Again, it suffices to prove this under the assumption that $\pi_v(H) \lhd L_v$, which is then clear.

This shows that H is contained in the group $\underset{v}{\notin} V_0(H) \to \pi L_v \times \underset{v}{\in} V_0(H) \to$ $|PIZ_v$. Now, if H is of index n, then it follows that $|V_0(H)| = 0\left(\frac{\log n}{\log \log n}\right)$ by the Prime Number Theorem (for characteristic p) since $[L_v : Z_v]$ is of order approximately $[\theta_v : m_v]^d$ where d is a constant (the dimension of G).

Moreover, if $V(H) = V_0(H) \cup S$, then for every $v \notin V(H)$, H contains L_v (since $H \cap L_v = L_v$). We can therefore consider H as a subgroup of index n in $\underset{v}{\in} V(H) \to \pi L_v$. The results and methods of §4.4 now show that H contains a principal congruence subgroup corresponding to $\underset{v}{\in} V(H) \to \pi m_v^{c \log n}$, where c is some constant. As the index of $\underset{v}{\in} V(H) \to \pi m_v$ in $\underset{v}{\in} V(H) \to \pi \theta_v$ is at most $n^{c'}$, Proposition 3 is now proved.

Warning to Dan: (1) There is something to complete here. §4.4 is under the assumption of "perfect". Thios is almost always true, but when not something should be said (I am sure the result is basically still correct – maybe c will be larger). In my Invent. paper, I made assumptions on G, but we prefer not to, as we want to use the theorem for a lower bound on all linear groups in *charp*.

(2) There is also a notational problem: The ring of integers in k is defined w.r.t. a choice of a "valuation at ∞". How to write this? I meant here that θ is the integral closure in k of $\mathbb{F}_p[t]$, if k is a finite extension of $\mathbb{F}_p(t)$.