Nilmanifolds in number theory.

These notes were taken by A. Venkatesh and the speaker (B. Green) does not bear any responsibilities for errors contained herein.

Introduction.

Definition 1. *Let G be an s-step nilpotent Lie group, connected and simply connected, i.e. the* lower central series

$$G = G_0 \supset G_1 \supset G_2 = [G, G] \supset G_3 = [G, [G, G]] \supset \dots G_s = \{\mathrm{id}\}.$$

Example 1.

$$G = \begin{pmatrix} 1 & \mathbb{R} & \mathbb{R} \\ 0 & 1 & \mathbb{R} \\ 0 & 0 & 1 \end{pmatrix} \tag{1}$$

is 3-step nilpotent; $\mathbb{R}^d$ *is 1-step nilpotent.*

Let Γ be a discrete cocompact subgroup of G; in the example (1) above Γ can be taken to be matrices with integral entries. Topologically, in this instance, G/Γ is $[0, 1]^3$ with the faces identified, and G acts by right multiplication.

Definition 2. *A* nilsequence *is a function on $\mathbb{Z}$ of the form $n \mapsto F(g^n\Gamma)$ and $F : G/\Gamma \to [-1, 1]$ is nice-ish*[1] *function.*

<u>Why would we consider this?</u> In joint work with Terry Tao, we try to count configurations of primes. For example, we should like to have an asymptotic for

$$\sum_{\underline{n} \in K} \Lambda(\psi_1(\underline{n}) \dots \Lambda(\psi_t(\underline{n})), \tag{2}$$

where Λ is the van Mangoldt function; $\psi_i : \mathbb{Z}^d \to \mathbb{Z}$ are affine linear forms, and $\underline{n} \in \mathbb{Z}^d$; K is a "nice" large domain, e.g. $K \subset [-N, N]^d$. This formalism includes, for example, counting the number of arithmetic progressions of some fixed length.

Hardy and Littlewood already formulated a conjecture concerning the asymptotic of (2), which took into account "local obstructions", e.g. ψ_1 and ψ_2 should not always have opposite parity; or (archimedean obstruction) ψ_j should take positive values on the set K. More precisely,

$$(2) = \beta_\infty \prod_p \beta_p + o(N^d), \tag{3}$$

where

$$\beta_\infty = \mathrm{vol}(K \cap (\psi_1, \dots, \psi_j)^{-1}(\mathbb{R}_+)), \beta_p = p^{-d} \sum_{\underline{n} \in (\mathbb{Z}/p\mathbb{Z})^d} \prod_{j=1}^{t} \Lambda_{\mathbb{Z}/p\mathbb{Z}}(\psi_j(\underline{n})),$$

where $\Lambda_{\mathbb{Z}/p\mathbb{Z}}(n) = \begin{cases} 0, p|n. \\ \frac{p}{p-1}, \text{else} \end{cases}$ is a local analog of the von Mangoldt function. For example,

$$\frac{1}{N} \sum_{n \le N} \Lambda(n)\Lambda(n+2) \sim 2 \prod_{p \ge 3} \left(1 - (p-1)^{-2}\right)$$

[1] Lipschitz, or continuous...

Theorem 1. *(Green-Tao, 2006). Suppose the system* (ψ_j) *has complexity* s*. Assume also that:*

- $GI(s)$ *– inverse conjectures for Gowers norms, see below;*
- $MN(s)$ *– Möbius-Nilsequences conjectures, see below.*

Then the Hardy-Littlewood conjecture is true.

Known cass of the conjectures.: $GI(1), GI(2)$; finite field model (Tao-Ziegler, very recent!)[2]; $MN(s)$, all s.

Some ideas in the proof of the Theorem. We consider the multilinear functional:

$$T(f_1, \ldots, f_t) = N^{-d} \sum_{\underline{n}} \prod_{j=1}^{t} f_j(\psi_j(\underline{n}))$$

Here f_i are functions on $\mathbb{Z}$; (1) is the special case with f_j all equal to the von-Mangoldt function.

Convention: *Where not stated, sums over* $\underline{n}$ *range over* $[1,N]^d$*, and integer sums range over* $[1,N]$.

Now, one splits $\Lambda = \Lambda^\sharp + \Lambda^\flat$; here, for instance, we could obtain $\Lambda^\sharp$ by retaining all $d \leq R$ in the expression $\sum \mu(d) \log(n/d)$; here $R \sim N^{0.0001}$, where 0.0001 depends on the forms ψ_t. One may split, correspondingly,

$$T(\Lambda, \ldots, \Lambda) = T(\Lambda^\sharp, \ldots, \Lambda^\sharp) + (2^t - 1 \text{ other terms}),$$

The first term, which is roughly the analog of the "major arcs" in the Hardy-Littlewood method, contributes the main term. It remains to show the other terms are small; the hardest case is $T(\Lambda^\flat, \ldots, \Lambda^\flat)$.

Aside: the Gowers norms. .

Suppose $|f_i| \leq 1$ (less would be fine!). In that case, we have:

$$T(f_1, \ldots, f_t) = \frac{1}{N^d} \sum_{\underline{n} \in [N]^d} \prod_{j=1}^{t} f_i(\psi_i(\underline{n})),$$

satisfies (generalized von-Neumann = many applications of Cauchy-Schwarz):

$$|T(f_1, \ldots, f_t)| \leq \|f_i\|_{U^{s+1}}$$

for any i, where s is the complexity of the systm of forms. The first norms are defined thus:

$$\|f\|_{U^2}^4 = \frac{1}{N^3} \sum_{x, h_1, h_2} f(x) \overline{f(x+h_1) f(x+h_2)} f(x+h_1+h_2), \tag{4}$$

$$\|f\|_{U^3}^8 = \frac{1}{N^4} \left(\sum_{x, h_1, h_2, h_3} f(x) \ldots \overline{f(x+h_1+h_2+h_3)} \right). \tag{5}$$

Now, as remarked above, it suffices to control the Gowers norms $\|\Lambda^\flat, \ldots, \Lambda^\flat\|_{U^{s+1}} = o(1)$. Via the expression $\Lambda^\flat = \sum_{d \geq R, d|n} \mu(d) \log(n/d)$, this reduces, in substance, to verifying:

$$\|\mu\|_{U^s} = o(1). \tag{6}$$

[2]Remark: this uses a finite-field analogue of the correspondence principle!

The inverse conjectures.

Conjecture 1. *Let $f : \{1, \dots, N\} \to [-1, 1]$, where $\|f\|_{U^{s+1}} \geq \delta$. Then, there exists an s-step nilsequence, $n \mapsto F(g^n\Gamma)$ such that $\left|\frac{1}{N}\sum_{n\leq N} f(n)f(g^n\Gamma)\right| \geq \delta/2$, where $\|F\|_{Lip}, \dim(G/\Gamma) = O_\delta(1)$.*

Example 2. *If $G/\Gamma = \mathbb{R}/\mathbb{Z}$, a corresponding sequence would be $n \mapsto e^{in\theta}$.*

Why this conjecture?

(1) It is necessary: if $\frac{1}{N}\sum_n f(n)F(g^n\Gamma) \geq \delta/2$, then $\|f\|_{U^{s+1}} \geq \delta^c$.
(2) Ergodic theorists (Host and Kra) have proved an ergodic analogue.

The MN conjecture. It asserts that $\left|\frac{1}{N}\sum_{n=1}^N \mu(n)F(g^n\Gamma)\right| \ll_A \log^{-A} N$. (The power of log is necessary; $o(1)$ would not suffice for the application.)

Nilpotence and parallelograms. Due to Host and Kra; I call it the "Rubik's cube argument."

In the definition of Gowers norms we have "parallelpipeds", e.g.

$$(n, n + h_1, n + h_2, \dots, n + h_1 + h_2 + h_3).$$

Beautiful picture which could not be reproduced due to limitations of the scribe.

Take a set X, and suppose that G acts on X; we suppose that X has a notion of "three-dimensional parallelpipeds, " i.e. $P \subset X^8$. We suppose that 7 vertices of a parallelpiped determine the remaining one.

We should like, if P is a parallepiped with "faces" F, F' (both collections of four elements), then also (gF, F') is a parallelpiped, i.e. $(g, g, g, g, 1, 1, 1, 1)$ preserves P; similarly, $(h, h, 1, 1, h, h, 1, 1)$ preserves P. The commutator of these two, equals $([g, h], [g, h], 1, 1, 1, 1, 1, 1)$; it must also preserve P.

Proceeding once more, we arrive at the following conclusion:

(7) For $g_1, g_2, g_3 \in G$, $([g_1, [g_2, g_3]], 1, 1, 1, 1, 1, 1, 1)$ preserves P.

Since the latter seven vertices determine the first, it follows that $[g_1, [g_2, g_3]] = 1$. *Thus the automorphism group of the parallelpiped structure must be nilpotent.*