Strong Approximation

John Mangual

1 The Pigeonhole Principle

> The chinese remainder theorem for $SL(n, \mathbb{Z})$ asserts, among other things that for $q > 1$ the reduction $SL(n, \mathbb{Z}) \to SL(n, \mathbb{Z}/q\mathbb{Z})$ is onto. Far less elementary is the extension of this feature to $G(\mathbb{Z})$ where G is a suitable matrix algebraic group defined over $\mathbb{Q}$. The general form of this phenomenon is known as Strong Approximation...
>
> There is a quantification of the above that is not as well known as it should be, as it turns out to be very powerful in many contexts. We call this "superstrong" approximation and it asserts that if we choose a finite symmetric generating set S (such that $s, s^{-1} \in S$) then the congruence Cayley graphs $X_q(S)$ form an expander family as $q \to \infty$.

In this striking paragraph, Peter Sarnak sketches expansion from the Chinese Remainder Theorem to Strong Approxmation and even to Super-Strong Appproximation. I can't hold back my surprise.

Ex Chinese Remainder Theorem is a way to solve simultaneous congruences. Let $(p, q) = 1$ then:

$$\mathbb{Z}_p \times \mathbb{Z}_q \simeq \mathbb{Z}_{pq}$$

This isomorphism looks obvious to me since $p \times q = pq$. In order to `prove` this isomorphism we need either the continued fraction of $\frac{p}{q}$ or the pigeonhole principle in order to ensure ourselves a solution to the congruence:

$$\begin{aligned} x &\equiv 1 \mod p \\ x &\equiv 0 \mod q \end{aligned}$$

It is quite reasonable this factorization should extend to matrix groups. Withouth commutativity there is more work.

$$SL(2, \mathbb{Z}/pq\mathbb{Z}) \simeq SL(2, \mathbb{Z}/p\mathbb{Z}) \times SL(2, \mathbb{Z}/q\mathbb{Z})$$

There also seems to be some kind of connection to Hasse principle.

Ex It's hard to think of how strong Strong Approximation actually is. The Adeles are the product of infinitely many completions of the rational numbers[1] (not too much permitted after the decimal point):

$$\mathbb{A} = \mathbb{R} \times \hat{\prod_{p \in \mathbb{Z}}} \mathbb{Q}_p$$

[1] Categorical description of the restricted product (Adeles) `http://mathoverflow.net/a/96138/1358`

However, the maximally compact subgroup $\hat{\mathbb{Z}}$ is the product of all possible p-adic integers (everything before the decimal is permissible).

$$\widehat{\mathbb{Z}} = \prod_{p \in \mathbb{Z}} \mathbb{Z}_p$$

Note it is really surprising that $\mathbb{R}$ just appears out of nowhere in the completion. The adeles seem to be a very formal way of thinking about the Chinese Remainder Theorem. The beat goes on:

$$\mathrm{SO}_3(\mathbb{Z})\backslash\mathrm{SO}_3(\mathbb{R}) \simeq \mathrm{SO}_3(\mathbb{Q})\backslash\mathrm{SO}_3(\mathbb{A})/\mathrm{SO}_3(\widehat{\mathbb{Z}})$$

This is an “Adelic” way of looking at the rotation group in 3 dimensions. They even get the 3-sphere. Let:

$$K_f[q] := \ker\Big(SO_3(\widehat{\mathbb{Z}}) \to SO_3(\mathbb{Z}/q\mathbb{Z}) \Big)$$

The transitive action of $SO_3(\mathbb{R})$ is transitive, they use the stabilizer $K_\infty \simeq SO_2(\mathbb{R})$ the sphere is

$$S^2 \simeq \mathrm{SO}_3(\mathbb{Q})\backslash\mathrm{SO}_3(\mathbb{A})/K_\infty . K_f[3]$$

Here what are the rotation over the adeles? Do they preserve $x^2 + y^2 + z^2 = 1$ in $\mathbb{A}$?

$$\mathrm{SO}_3(\mathbb{A}) = \hat{\prod_{p \in \mathbb{Z}}} \mathrm{SO}_3(\mathbb{Q}_p)$$

Ex Next and more difficult to articulate are the extension to Cayley graphs and super-strong approximation. How does the expansion property of Ramanujan graphs generalize the Pigeonhole Principle or the Chinese Remainder Theorem??

$$\mathcal{H}_d(q) \simeq \Gamma_{(3,q)}\backslash\mathrm{SO}_3(\mathbb{Q}_5)/\mathrm{SO}_3(\mathbb{Z}_5)$$

Ex Sarnak's article start with the case of “thin” subgroups of algebraic groups $G(\mathbb{Z})$ of infinite index and checking that strong/superstrong approximation still applies there. [3, 4]

References

[1] Peter Sarnak. *Notes on Thin Matrix Groups.* `http://web.math.princeton.edu/sarnak/NotesOnThinGroups.pdf`

[2] Jordan S. Ellenberg, Philippe Michel, Akshay Venkatesh. *Linnik's ergodic method and the distribution of integer points on spheres* `arXiv:1001.0897v1`

[3] Jean Bourgain, Alex Gamburd, Peter Sarnak. *Generalization of Selberg's 3/16 Theorem and Affine Sieve* `arXiv:0912.5021`

[4] Harald Helfgott *Growth and generation in* $SL_2(\mathbb{Z}/p\mathbb{Z})$ `arXiv:math/0509024`