geminat; et sic sunt in secundo mense paria 3; ex quibus in uno mense duo pregnantur, et geminantur in tercio mense paria 2 coniculorum; et sic sunt paria 5 in ipso mense; ex quibus in ipso pregnantur paria 3; et sunt in quarto mense paria 8, ex quibus paria 5 geminant alia paria 5: quibus additis cum pariis 8, faciunt paria 13 in quinto mense; ex quibus paria 5, que geminata fuerunt in ipso mense, non concipiunt in ipso mense, sed alia 8 paria pregnantur; et sic sunt in sexto mense paria 21; cum quibus additis pariis 13, que geminantur in septimo, erunt in ipso paria 34; cum quibus additis pariis 21, que geminantur in octavo mense, erunt in ipso paria 55; cum quibus additis pariis 34, que geminantur in nono mense, erunt in ipso paria 89; cum quibus additis rursum pariis 55, que geminantur in decimo, erunt in ipso paria 144; cum quibus additis rursum pariis 89, que geminantur in undecimo mense, erunt in ipso paria 233. Cum quibus etiam additis pariis 144, que geminantur in ultimo mense, erunt paria 377; et tot paria peperit suprascriptum par in prefato loco in capite unius anni. Potes enim videre in hac margine, qualiter hoc operati fuimus, scilicet quod iunximus primum numerum cum secundo, videlicet 1 cum 2; et secundum cum tercio; et tercium cum quarto; et quartum cum quinto, et sic deinceps, donec iunximus decimum cum undecimo, videlicet 144 cum 233; et habuimus suprascriptorum cuniculorum summam, videlicet 377; et sic posses facere per ordinem de infinitis numeris mensibus.

parium	
1	primus
2	secundus
3	tercius
5	quartus
8	quintus
13	sextus
21	septimus
34	octavus
55	nonus
89	decimus
144	xi
233	xii
377	

1 cum 2 et secundum cum tercio et tercium cum quarto et quartum cum quinto et sic deinceps donec iunximus decimum cum undecimo videlicet 144

Quatuor homines sunt, quorum primus, secundus et tercius habent denarios; secundus itaque et tercius et quartus habent denarios 31; tercius et quartus et primus habent denarios 34; quartus vero et primus et secundus habent denarios 37. Queritur quot unusquisque habet. Adde hos .iiii. numeros in unum, erunt 129, qui numerus est triplum totius summe denariorum illorum .iiii. hominum. Ideo quod in ipsa summa unusquisque eorum ter computatus est; quare diviso ipso per 3 reddet 43 pro eorum summa. Ex qua si extraxeris denarios primi et secundi et tercii hominis, scilicet 27, remanebit quarto homini denarii 16. Item si ex ipsis denariis 43 extraxeris denarios 31 secundi et tercii et quarti hominis, remanebunt primo homini denarii 12. Rursum si de denariis 43 extraxeris 34, scilicet denarios tercii et quarti hominis et primi hominis, remanebunt secundo denarii 9. Et adhuc si de denariis 43 extraxeris denarios 37 quarti et primi et secundi hominis, remanebunt tercio denarii 6. Convenientis itaque denariis 12 primi hominis cum 9 secundi et cum 6 tercii et cum 16 quarti, nimirum summa reddet 43.

27
43
12
9
6
16

Item si propositum fuerit quod inter primum et secundum hominem habeant denarios 27; et inter secundum et tercium habent denarios 31; et inter tercium et quartum 34; inter quartum et primum 37; consimiles huius positionis quedam solvi possunt, quedam non. Unde ut ipse que solvi possunt ab hiis qui solvi non possunt cognoscantur, talem tradimus evidentiam: videlicet ut addas numerum primi et secundi cum numero tercii et quarti; et si eorum summa equalis fuerit numero secundi et tercii et quarti et primi, tunc solubilis erit questio. Si autem inequalis fuerit, tunc eam non posse solvi cognoscas, ut in hac questione in qua primi et secundi habent 27 et tercii et quarti habent 34, ergo inter omnes .iiii. habent denarios 61. Nam secundi et tercii

The "Why" of p-adic integration.

1. Skolem-Mahler-Lech.

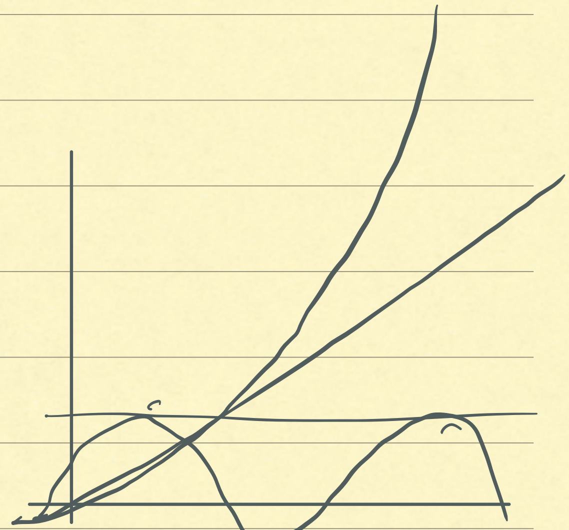
Consider linear recurrences with integer coefficients:

$a_n = a_{n-1}$ constant

$a_n = a_{n-1} + 1$ linear

$a_n = a_{n-1} + a_{n-2}$ Fibonacci

$a_n = a_{n-4}$ periodic



Can add, interleave, shift, change the start of such sequences.

Fundamental problem: Given a reccarence, describe the asymptotic nature of the zero set $\{n : a_n = 0\}$.

We can write

$$\begin{pmatrix} a_i \\ \vdots \\ a_{i+n} \end{pmatrix} = \begin{pmatrix} & & \\ & M & \\ & & \end{pmatrix}^i \begin{pmatrix} a_0 \\ \vdots \\ a_n \end{pmatrix} = (PJP^{-1})^i \begin{pmatrix} a_0 \\ \vdots \\ a_n \end{pmatrix}$$

$$= PJ^nP^{-1} \begin{pmatrix} a_0 \\ \vdots \\ a_n \end{pmatrix}$$

so $a_i = \sum_{j=0}^{n} \sum_{k=0}^{m_j} c_{jk} \lambda_j^i i^k$ polynomial exponential in i base λ_j

Ex: 1) Fibonacci sequence: F_n: $a_0 = 0$ $a_1 = 1$ $M = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$

$\lambda_1 = \frac{1+\sqrt{5}}{2}$, $\lambda_2 = \frac{1-\sqrt{5}}{2}$.

$$F_n = \frac{\lambda_1^n - \lambda_2^n}{\sqrt{5}} \quad (*)$$

Binet's formula

"Obvious" that $F_n = 0 \Rightarrow n = 0$.

One reason: $|\lambda_1| > 1$ $|\lambda_2| < 1$.

so eventually $F_n \gg 0$ by $(*)$

$$\frac{\lambda_1^n - \lambda_2^n}{\sqrt{5}} = 0 \iff \lambda_1^n = \lambda_2^n$$

$$\iff n \log\left(\frac{\lambda_1}{\lambda_2}\right) = 0.$$

2) Let $B_{2n} = F_n$, $B_{2n+1} = 0$

0, 0, 1, 0, 1, 0, 2, 0, ...

now λ_i are the $\pm\sqrt{\lambda_i}$ for F_n

No clear way to conclude in general.

Are there any other absolute value functions $|\cdot|$ we can control the vanishing of such a sequence with?

2 Theorem (Ostrowski): The only absolute value functions on $\mathbb{Q}$ are

$$\begin{cases} |x| := \operatorname{sgn}(x) \cdot x. \\ |x|_p := p^{-\operatorname{ord}_p(x)}, \end{cases}$$

$\operatorname{ord}_p\left(\frac{a}{b}\right) = \max\{n : p^n | a\} - \max\{n : p^n | b\}$

for p prime.

Ex: $\left|\frac{25}{7}\right|_7 = 7$ $\qquad$ $\left|\frac{25}{7}\right|_5 = \frac{1}{25}.$

$\mathbb{Q} \subseteq \mathbb{R} \qquad \mathbb{Q} \leq \mathbb{Q}_7$

For each prime p we can topologically complete $\mathbb{Q}$ to get a field $\mathbb{Q}_p$, analogous to $\mathbb{R}$.

Many familiar notions from $\mathbb{R}$ and $\mathbb{C}$ transfer to $\mathbb{Q}_p$, but often with strange differences.

$1 + 10^{-1}\cdot 8 + 10^{-2}3 + 10^{-3}\cdot 3.$

	3	$11/6$	$193/132$	$72097/50952$
In $\mathbb{R}$	3.0	$1.8\overline{3}$	$1.46\overline{21}$	$1.4149984\ldots$
In $\mathbb{Q}_7$	3.0	$3.\overline{6}$	$3.1260332\ldots$	$3.126121235\ldots$
	3	$3 + 7\cdot 6 + 7^2\cdot 6 + 7^3 6$		

$\sqrt{2} \approx \sqrt{9} = 3$

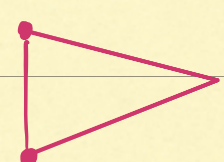
3. The p-adic topology

- Ultrametric:

  $|x+y| \leq \max\{|x|, |y|\} \quad (\leq |x| + |y|).$

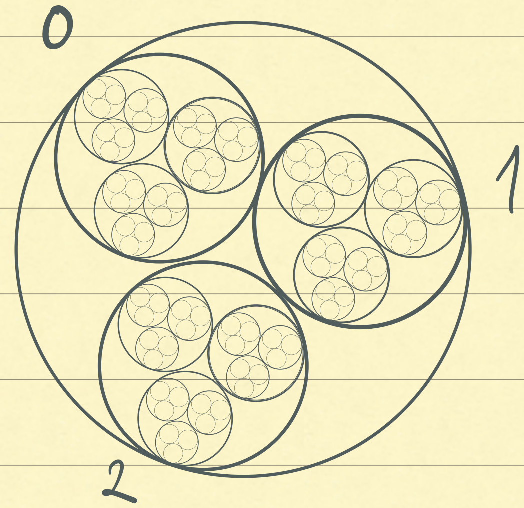
- Every point in a ball is the center

- Every triangle is isoceles



- p-adic topology is totally disconnected.

3-adic



4. Back to Recurrences

$$a_i = \sum_{k=1}^{m} A_k(i)\, \lambda_k^i$$

is almost a p-adic analytic function of i for any p such that $|\lambda_k|_p = 1$ for all k.

Problem: p-adic exponential has finite radius of convergence.

Instead:

Locally analytic so that on each set $\{r + (p-1)t : t \in \mathbb{Z}\}$ for some $0 \le r < p-1$ has

Fusion: $(p-1) \mid f$

$a_{r+(p-1)t}$ is a p-adic analytic function of t?

Conc $a_{r+(p-1)t} = 0$ then this function is identically zero.

The integers are bounded p-adically.

Thm: A linear recurrence a_i has zero set a union of arithmetic progressions (asymptotically)

What just happened?

Took a discrete object and p-adically continued the "time" step.

Then in small enough segments of time p-adic analyticity $\Rightarrow$ either $\equiv 0$ or finitely many zeroes.

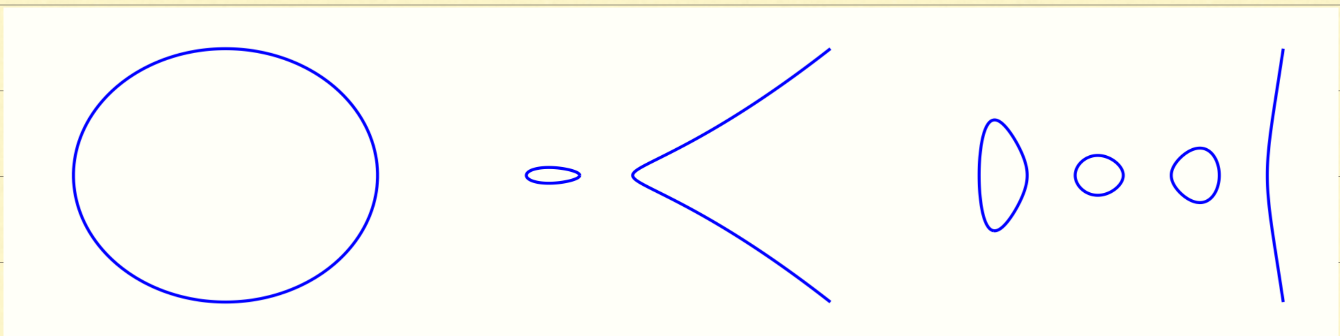
$$\begin{array}{ccc} \{n : a_n = 0\} & \subseteq & \{t \in \mathbb{Q}_p : a_t = 0\}. \\ \cap & & \cap \\ \mathbb{N} & \subseteq & \mathbb{Q}_p \end{array}$$

5. Rational points.

General Diophantine equations are undecidable. (Matiyasevich)

Q: But what about simpler classes / in practice.

Let C be an algebraic curve $/\mathbb{Q}$ (1-dimensional, defined by equations)



$x^2+y^2=1$ $\qquad$ $y^2=x(x-1)(x-2)$ $\qquad$ $y^2=x^5-3x+7$.

Then for complicated enough curves C we have only finitely many rational solutions $C(\mathbb{Q})$. Faltings

It is a fundamental open problem to give better control over this finite set:

- bound the number of solutions
- bound the size of each solution

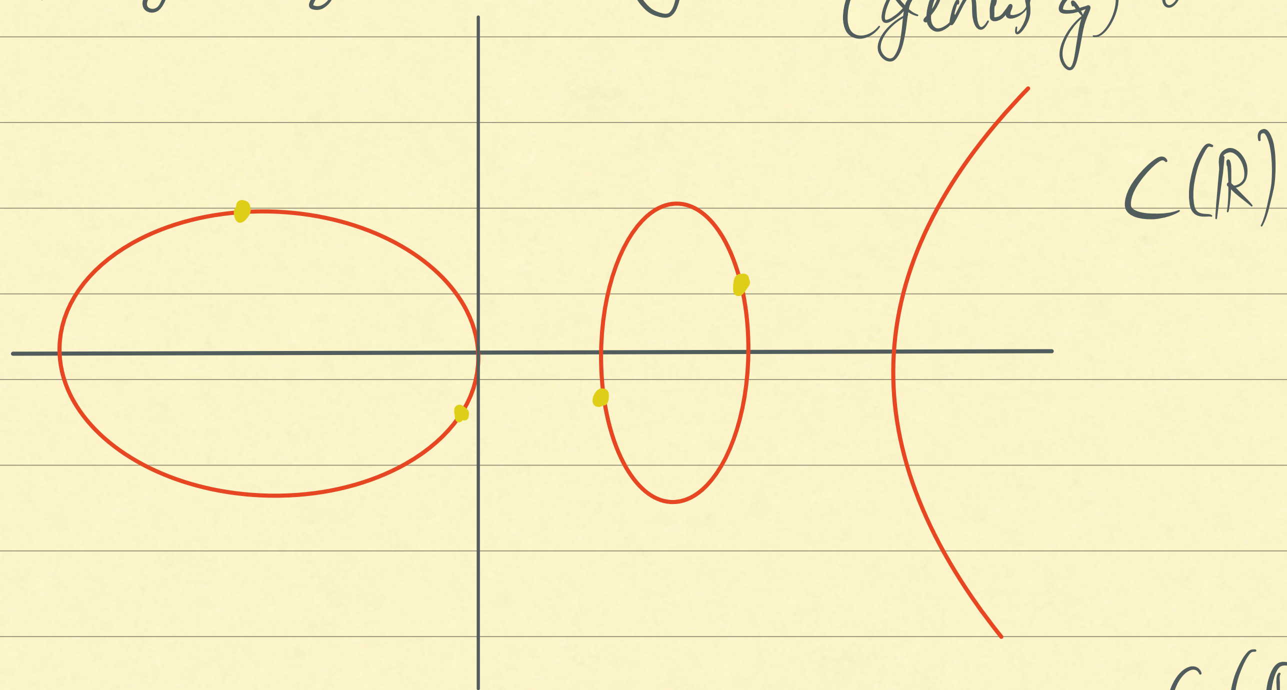
– provably find the set of solutions.

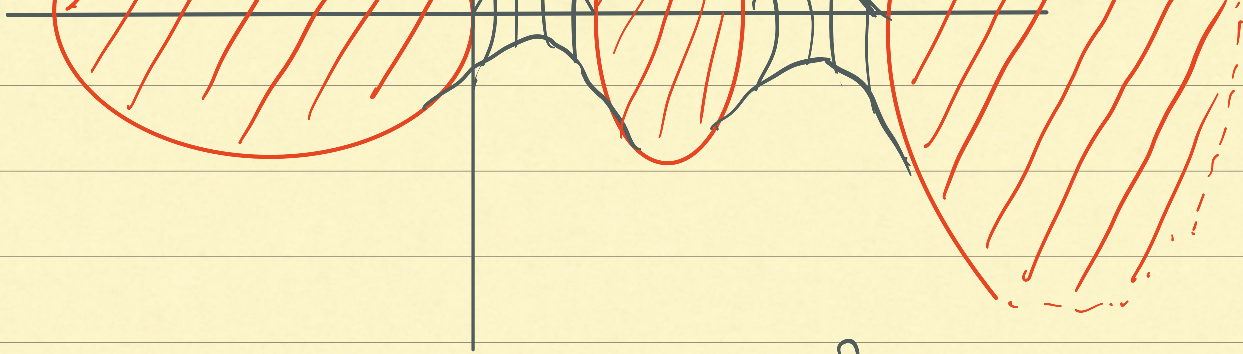
Can we use the ideas of Skolem - Mahler - Lech for this problem too?

$\boxed{\text{Need a source of p-adic analytic functions}}$

4. Embedding curves into groups.

Let C be a curve$/_{\mathbb{Q}}$ that over $\mathbb{C}$ is topologically a g-handled surface (genus g)





$g=2.$

Can't add points on C but we can add pairs of points.

By fixing a base point P we embed our algebraic curve into an algebraic group, its Jacobian. $J(C)$

5. p-adic integration

Can define

$$\int_P^Q \omega \quad \in \mathbb{Q}_p$$

$$y^2 = x^5 - 1$$

$$\frac{dx}{y} \qquad \frac{x\,dx}{y}$$

for $\omega \in \Omega^1_{J(C)}$ a translation invariant differential

defined by integrating locally using power series.

to analytically continue use group structure or the p-adic phenomenon of Frobenius

A lot of my work is about effectively computing these integrals in different contexts. Why?

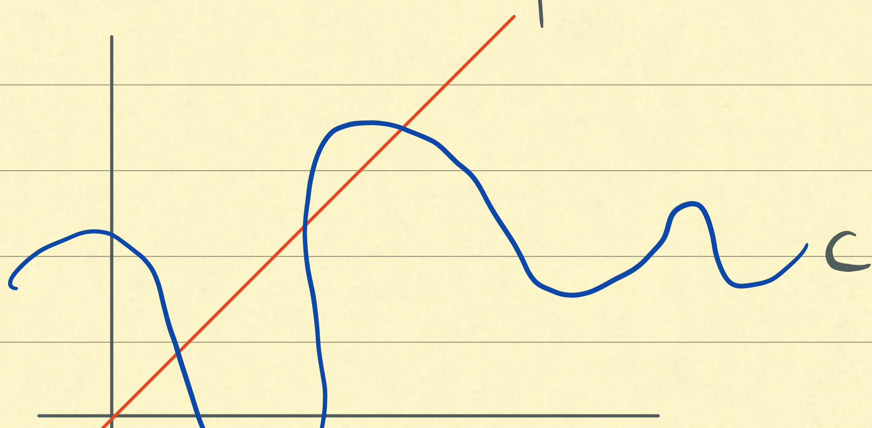
6. Chabauty's Method.

In order to find $C(\mathbb{Q})$ for a genus $g \geq 2$ curve we use

$$\begin{tikzcd}
C(\mathbb{Q}) \arrow[r, hook] \arrow[d, hook] & C(\mathbb{Q}_p) \arrow[d, hook] \arrow[dr, "(\int_p \omega_i)_i"] & \\
J(\mathbb{Q}) \arrow[r, hook] & J(\mathbb{Q}_p) \arrow[r, "(\int_p \omega_i)_i"'] & \operatorname{Lie} J(\mathbb{Q}_p)
\end{tikzcd}$$

$J(\mathbb{Q})$ is $\mathbb{Z}^r \times$ torsion

$J(\mathbb{Q}_p)$ g-dimensional p-adic lie group



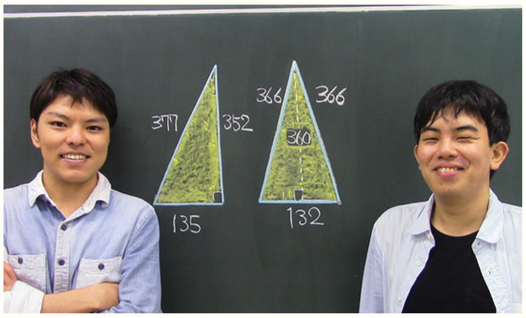
J

Bounds and algorithms

This method gives both bounds and algorithms e.g. for $p > 2r+1$, $r < g$ good reduction

$$\#C(\mathbb{Q}) \leq \#C(\mathbb{F}_p) + 2r \qquad \text{(Stoll)}$$

Theorem 2 (Hirakawa–Matsumura). *There exists a unique pair of a rational right triangle, and a rational isosceles triangle with equal areas and equal perimeters.*



Proof. The problem reduces to finding rational points on the genus 2 rank 1 curve

$$r^2 = (-3w^2 + 2w^2 - 6w + 4)^2 - 8w^6.$$

which has good reduction at 5, and 8 points over $\mathbf{F}_5$. Moreover we can find 10 rational points, most of which do not correspond to non-degenerate triangles. □

If we can explicitly calculate these integrals we can find the finite set of rational solutions!

Application to dynamics (Stoll)

Do there exist rational numbers x, c such that

$x \mapsto x^2 + c$ has period exactly n?

This problem defines a curve of solutions

$\Rightarrow$ finitely many for each n ($n \gg 0$)

for $n=6$ $g=4$ $r=3$.

Chabauty $\Rightarrow$ no solutions.

Theorem 11 (Balakrishnan–B.–Bianchi–Lawrence–Müller–Triantafillou–Vonk)**.** *The number of rational points on the Atkin–Lehner quotient modular curves $X_0(N)^+ := X_0(N)/w_N$, all of genus 2, rank 2 and Picard rank 2 for $N \in \{67, 73, 103\}$ are as follows:*

$$\#X_0(67)^+(\mathbf{Q}) = 10, \quad \#X_0(73)^+(\mathbf{Q}) = 10, \quad \#X_0(103)^+(\mathbf{Q}) = 8.$$

This involves non-abelian Chabauty and Mordell–Weil sieving at 31 and 137 in the $N = 67$ case.

$F=$