Lean for the curious Arithmetic Geometer

Alex J. Best

27/7/23 – Rational points 2023 in Schney

Unit fractions

In December 2021 Thomas Bloom posted a paper: On a Density Conjecture about Unit Fractions to arXiv (2112.03726)

> Abstract: We prove that any set $A \subset \mathbb{N}$ of positive upper density contains a finite $S \subset A$ such that $\sum_{n \in S} \frac{1}{n} = 1$, answering a question of Erdös and Graham.

18 pages, quickly recognized as correct and widely applauded in popular press (Quanta, etc), generalizes an older result of Croot.

Unit fractions

In December 2021 Thomas Bloom posted a paper: On a Density Conjecture about Unit Fractions to arXiv (2112.03726)

> Abstract: We prove that any set $A \subset \mathbb{N}$ of positive upper density contains a finite $S \subset A$ such that $\sum_{n \in S} \frac{1}{n} = 1$, answering a question of Erdös and Graham.

18 pages, quickly recognized as correct and widely applauded in popular press (Quanta, etc), generalizes an older result of Croot.

Bloom and Mehta formalized the paper, over the following summer (2022). This took place before the referee report was complete, and the paper is still not published

Unit fractions

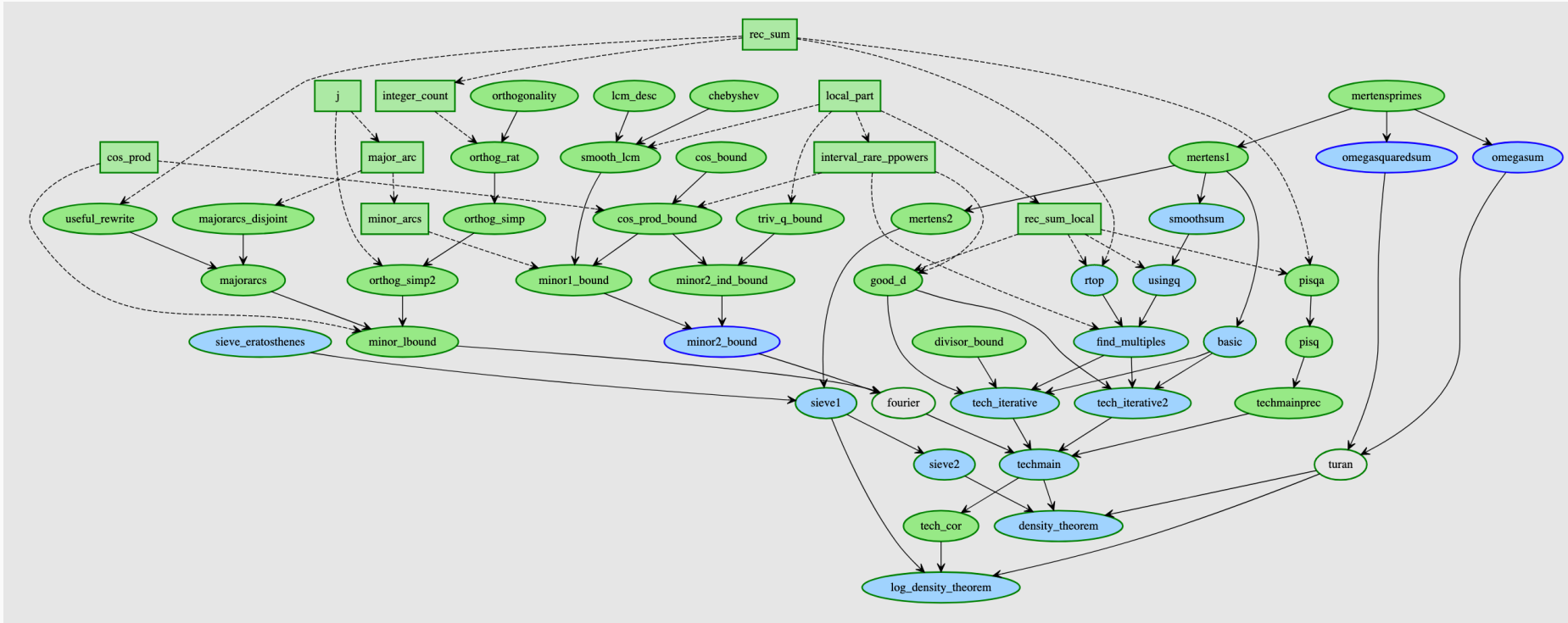
In December 2021 Thomas Bloom posted a paper: On a Density Conjecture about Unit Fractions to arXiv (2112.03726)

> Abstract: We prove that any set $A \subset \mathbb{N}$ of positive upper density contains a finite $S \subset A$ such that $\sum_{n \in S} \frac{1}{n} = 1$, answering a question of Erdös and Graham.

18 pages, quickly recognized as correct and widely applauded in popular press (Quanta, etc), generalizes an older result of Croot.

Bloom and Mehta formalized the paper, over the following summer (2022). This took place before the referee report was complete, and the paper is still not published

(Bloom and Yael Dillies are right now working on formalizing Bloom-Sisask's variant (Feb 2023) on the Kelley-Meka bound on Roth numbers (also Feb 2023), bounding the size of subsets of the integers containing no three term arithmetic progressions)


rec_sum
j
integer_count
orthogonality
lcm_desc
chebyshev
local_part
mertensprimes
cos_prod
major_arc
orthog_rat
smooth_lcm
cos_bound
interval_rare_ppowers
mertens1
omegasquaredsum
omegasum
useful_rewrite
majorarcs_disjoint
minor_arcs
orthog_simp
cos_prod_bound
triv_q_bound
mertens2
rec_sum_local
smoothsum
majorarcs
orthog_simp2
minor1_bound
minor2_ind_bound
good_d
rtop
usingq
pisqa
sieve_eratosthenes
minor_lbound
minor2_bound
divisor_bound
find_multiples
basic
pisq
sieve1
fourier
tech_iterative
tech_iterative2
techmainprec
sieve2
techmain
turan
tech_cor
density_theorem
log_density_theorem

December 5, 2020, Peter Scholze

I want to propose a challenge: Formalize the proof of the following theorem:

Theorem 1.1 (Clausen-S.): Let $0 < p' < p \leq 1$ be real numbers, let S be a profinite set, and let V be a p-Banach space. Let $\mathcal{M}_{p'}(S)$ be the space of p'-measures on S. Then $\mathrm{Ext}^i_{\mathrm{Cond(Ab)}}(\mathcal{M}_{p'}(S), V) = 0$ for $i \geq 1$.

Why do I want a formalization? ...

... I think the theorem is of utmost foundational importance, so being 99.9% sure is not enough. ... I spent much of 2019 obsessed with the proof of this theorem, almost getting crazy over it. In the end, we were able to get an argument pinned down on paper, but I think nobody else has dared to look at the details of this, and so I still have some small lingering doubts.

The Liquid Tensor Experiment - Resolution

Around 20 people contributed in some way or another directly to the experiment. Though Johan Commelin and Adam Topaz were some of the most prolific, several others made serious contributions.

In June 2021 the first "half" was completed, a technical analytical result, that was the heart of the difficulty of the proof.

And one year later in July 2022 the cohomological part was completed, finishing the challenge after a year and a half.

The Liquid Tensor Experiment - Resolution

In the course of the argument some of the mathematics was simplified, Commelin found a way to avoid the notion of Breen-Deligne resolutions, this was later found to be a reinvention of a complex introduced by Quillen.

Many errors in the manuscript, some nontrivial were found and fixed during the process

> Scholze: When I wrote the blog post half a year ago, I did not understand why the argument worked, and why we had to move from the reals to a certain ring of arithmetic Laurent series. But during the formalization, a significant amount of convex geometry had to be formalized, and this made me realize that actually the key thing happening is a reduction from a non-convex problem over the reals to a convex problem over the integers.

The Liquid Tensor Experiment - Future

Many people are still interested in working with Condensed mathematics in a proof assistant.

Dagur Asgeirsonn, a student of Clausen, is continuing to formalize new results from his thesis in a proof assistant.

Rational points - Descent

With Baanen, Coppola, Dahmen, we have been formalizing some Mordell-style descent to find integral points on elliptic curves: for example the non-existence of integral points on

$$y^2 = x^3 - 5$$

This required computing the class group of $\mathbf{Q}(\sqrt{-5})$ in a formally verified manner. (Baanen, Dahmen, Narayanan, Nuccio proved finiteness of the class group using a proof uniform in the number field and function field cases)

It should be possible to go further, maybe even find rational points on appropriate higher genus curves. Generalizing a proof using a proof assistant is usually a lot of fun, copy paste the proof and see what breaks, sometimes very little does.

What other sorts of things have been added to a proof assistant

- Buzzard, Commelin, Massot: Perfectoid spaces
- Sophie Bernard: Lindemann-Weierstrass
- Avigad, Donnelly, Gray, Raff: Prime number theorem
- Michael Stoll: Legendre symbols, a nice proof of Quadratic Reciprocity, reciprocity for Hilbert symbols (in progress)
- María Inés de Frutos-Fernández: Adeles and ideles, defining Fontaines period rings, statement of main theorem of CFT
- María Inés de Frutos-Fernández and Filippo Nuccio: DVRs, general local fields, completions, with a view towards LCFT
- Sophie Morel, formalization of half of her paper "Some combinatorial identities appearing in the calculation of the cohomology of Siegel modular varieties" (with Ehrenborg and Readdy)
- Bernard, Cohen, Mahboubi, Strub + Browning: Abel–Ruffini theorem

Continued...

- David Loeffler: Analytic continuation and functional equation of Riemann zeta, evaluation at negative integers
- Amelia Livingston: Group cohomology, Hilbert 90
- Lewis, Macbeth, Dupuis: Classify 1-d isocrystals
- Manuel Eberl, Chris Birkbeck: Modular forms
- Antoine Chambert-Loir and de Frutos-Fernández: divided power structures (link)
- David Angdinata and Junyan Xu: Group law on elliptic curves (in general), working on Mordell-Weil
- Brasca-B.-Birkbeck-Rodriguez: First case of FLT for regular primes.
- B.–Dahmen–Huriot-Tattegrain
- ... basics of schemes, Ostrowski's theorem...
- Your name here?: Your favourite moderately hard theorem

Lets Try!

First let's take a break.

Afterwards we will do another short demo, we will help anyone interested get started with one of:

Playing the Natural Number Game 4 (new and improved):
`https://adam.math.hhu.de/#/game/nng`

Going through the Mathematics in Lean 4 tutorial:

`https://github.com/leanprover-community/mathematics_in_lean`

(you will need some form of computer for both, though both can be accessed via an online interface without installing anything)

Implementing number theoretic algorithms

Alternatively we can implement algorithms within a proof assistant, as efficient functions that give the same output as what we want to compute

- Gives us a guaranteed correct implementation.
- We can experiment with modifying / improving the algorithm, and prove correctness or equality with the original one.
- We can prove properties, or "run" the algorithm in families, in ways normal code can't.

After writing the algorithm down, it is only accepted as a genuine mathematical function when it is shown to halt. With some functions this is obvious, but for algorithms that use recursion or unbounded loops, less so!

Tate's algorithm

Sacha Huriot-Tattegrain (+B.+Dahmen) has implemented Tate's algorithm in Lean(4).

- Complete algorithm to compute local invariants of an elliptic curve, including the $c_p(E), \mathrm{ord}_p(\Delta_E), \mathrm{ord}_p(N_E)$
- Works in characteristic 2 and 3.
- Based on Cohen's description of the algorithm, but at times consulting other sources and even the GP source code was necessary to get it right.
- It runs fast!
- Partly generalized to base rings beyond $\mathbf{Z}$.

Without an independent definition of the Kodaira types and conductor exponent we cannot actually check the algorithm does what it says. Nevertheless we could prove certain properties of the algorithm in future, such as invariance under

Closing thoughts

Formalization of mathematics (including number theory) is still slow and painful at times.

But we have several decades, even thousands of years of mathematics itself, learning how to think about mathematics, and to explain mathematics, to catch up on.

Thinking about these issues and finding clean arguments can be a lot of fun, and the tool may occasionally surprise you.