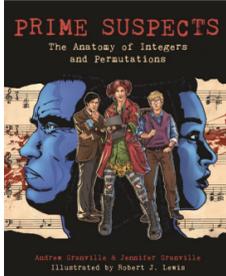


[Home](#)[Publications](#)[Activities](#)[Training](#)[Outreach](#)

Hiver / Winter 2022
*Elliptic curves and modular forms /
 Courbes elliptiques et formes modulaires*
 MAT6654: [Studium home page](#)

[Concours de Putnam: Atelier](#)[Number theory in Montreal](#)[Apply for a Montreal postdoc](#)[You need a reference letter?](#)[2019 Graphic novel; Advert](#)[Montreal Colloquium](#)[CRM-Fields-PIMS
prize lecture
\(December 2021\)](#)[CRM – Research center](#)[Preprint arXiv](#)[Calendrier des cours](#)[Address information](#)

Recent Preprints

[Do proofs yield objective truth, or are they culturally robust at best?](#)

In this article we explore what is accepted in the mathematical community as proof, how we deal with the Godel “crisis”, is there an objective standard for fully justified proof, how does computer proof change all that, etc.

[Three conjectures about character sums](#)

(with *Alexander (Sacha) Mangerel*), submitted

We establish that three well-known and rather different looking conjectures about Dirichlet characters and their (weighted) sums, (concerning the Polya-Vinogradov theorem for maximal character sums, the maximal admissible range in Burgess' estimate for short character sums, and upper bounds for $L(1, \chi)$ and $L(1 + it, \chi)$) are more-or-less “equivalent”. We also obtain a new mean value theorem for logarithmically weighted sums of 1-bounded multiplicative functions.

[Consecutive real quadratic fields with large class numbers](#)

(with *Giacomo Cherubini, Alessandro Fazzari, Vítězslav Kala, and Pavlo Yatsynal*), submitted

For a given positive integer k , we prove that there are at least $x^{1/2-o(1)}$ integers $d \leq x$ such that the real quadratic fields $\mathbb{Q}(\sqrt{d+1}), \dots, \mathbb{Q}(\sqrt{d+k})$ have class numbers essentially as large as possible, that is $\gg_k \sqrt{d} \frac{\log \log d}{\log d}$.

[The man who loved problems: Richard K Guy](#)

(with *Carl Pomerance*),

Notices of the American Mathematical Society (to appear)

A celebration of the life of one of the most colorful figures in contemporary mathematics. Richard Guy, popular author, columnist, educator, researcher, and avid mountain climber, passed away in 2020 at the age of 103.

[In mathematics, as in art,](#)

Journal of Humanistic Mathematics (to appear)

We compare appreciation of mathematics with appreciation of impressionist art

[Effective results on the size and structure of sumsets](#)

(with *George Shakan and Aled Walker*), submitted

Let $A \subset \mathbb{Z}^d$ be a finite set. It is known that NA has a particular size ($|NA| = P_A(N)$ for some $P_A(X) \in \mathbb{Q}[X]$) and structure (all of the lattice points in a cone other than certain exceptional sets), once N is larger than some threshold. In this article we give the first effective upper bounds for this threshold for arbitrary A . Such explicit results were only previously known in the special cases when $d = 1$, when the convex hull of A is a simplex or when $|A| = d + 2$, results which we improve.

[Large deviations of sums of random variables](#)

(with *Youness Lamzouri*)

Lithuanian Mathematics Journal **61** (2021), 345–372

In this paper, we investigate the large deviations of sums of weighted random variables that are *approximately independent*, generalizing and improving some of the results of Montgomery and Odlyzko. We are motivated by examples arising from number theory, including the sequences p^{it} , $\chi(p)$, $\chi_d(p)$, $\lambda_f(p)$, and $\text{Kl}_q(a - n, b)$; where p ranges over the primes, t varies in a large interval, χ varies among all characters modulo q , χ_d varies over quadratic characters attached to fundamental discriminants $|d| \leq x$, $\lambda_f(n)$ are the Fourier coefficients of holomorphic cusp forms f of (a large) weight k for the full modular group, and $\text{Kl}_q(a, b)$ are the normalized Kloosterman sums modulo a large prime q , where a, b vary in $(\mathbb{F}_q)^\times$.

[Exponential sums with multiplicative coefficients and applications](#)

(with *Régis de la Bréteche*)

Transactions of the American Mathematical Society (to appear)

We show that if an exponential sum with multiplicative coefficients is large then the associated multiplicative function is “pretentious”. This leads to applications in the circle method, and a natural interpretation of the local-global principle.

[Sieving intervals and Siegel zeros](#), submitted

Assuming that there exist (infinitely many) Siegel zeros, we show that the (Rosser-)Jurkat-Richert bounds in the linear sieve cannot be improved, and similarly look at Iwaniec's lower bound on Jacobsthal's problem, as well as minor improvements to the Brun-Titchmarsh Theorem. We also deduce an improved (though conditional) lower bound on the longest gaps between primes, and rework Cramér's heuristic in this situation to show that we would expect gaps around x that are significantly larger than $(\log x)^2$.

[Primes in short intervals: Heuristics and calculations](#)

(with *Allysa Lumley*)

Experimental Mathematics (online 1/7/21)

We formulate, using heuristic reasoning, precise conjectures for the range of the number of primes in intervals of length y around x , where $y \ll (\log x)^2$. In particular we conjecture that the maximum grows surprisingly slowly as y ranges from $\log x$ to $(\log x)^2$. We will show that our conjectures are somewhat supported by available data, though not so well that there may not be room for some modification.

[A tight structure theorem for sumsets](#)

(with *Aled Walker*)

Proceedings of the American Mathematical Society **149** (2021), 4073–4082

Let $A = \{0 = a_0 < a_1 < \dots < a_{\ell+1} = b\}$ be a finite set of non-negative integers. We prove that the sumset NA has a certain easily-described structure, provided that $N \geq b - \ell$, as recently conjectured by Granville and Shakan. We also classify those sets A for which this bound cannot be improved.

[The Frobenius postage stamp problem, and beyond](#)

(with *George Shakan*)

Acta Mathematica Hungarica **161** (2020), 700–718.

Let A be a finite subset of \mathbb{Z}^n , which generates \mathbb{Z}^n additively. We provide a precise description of the N -fold sumsets NA for N sufficiently large, with some explicit bounds on “sufficiently large.” For example if A has exactly three elements we provide a precise description of NA for all $N \geq 1$.

Number Theory Journals

[Acta Arithmetica](#)

[Algebra and Number Theory](#)

[Integers: Elect. J. Number theory](#)

[International J. Number theory](#)

[J. Number theory](#)

[J. Théorie de Nombres, Bordeaux](#)

[Ramanujan Journal](#)

[Research in Number Theory](#)

Number theory websites

[Number Theory Web](#)

[Number Theory listserv](#)

[Dickson's History: vol 1, vol 2, and vol 3.](#)

[Paul Erdos's papers](#)

[L-functions / Modular Forms database](#)

[Online encyclopaedia of integer sequences](#)

[Women in Number Theory](#)

Commentaries

[Best Professions in 2014?](#)

[Thanking our sponsors](#)

[Differences in pure and applied math and stats?](#)