Computational Number Theory, Past, Present, and Future

Henri Cohen

COMPUTATIONAL NUMBER THEORY, PAST, PRESENT, AND FUTURE

HENRI COHEN

For Catriona Byrne, with thanks

Abstract. A survey of computational number theory viewed through the prism of my own experience and the `Pari/GP` software.

1. Introduction

This paper is a *very personal* account of some computational aspects of number theory, especially in relation to the `Pari/GP` computer algebra system [104]. It is in no way exhaustive, but highlights significant advances that I have personally encountered.

Without going back too far in time, one of the pioneering figures in the subject was D. H. Lehmer (and to a lesser extent his father D. N. Lehmer) who introduced a number of methods some of which are still in use today. He is probably best known for the Lehmer conjecture dealing with finding a polynomial with smallest nonzero logarithmic Mahler measure [87] (see also [123] for recent work). I had the privilege of meeting him once in Berkeley when I was still in high school. Although not a number theorist per se, one can also mention A. Turing [133] who made extensive computations on the Riemann Hypothesis using a method that is still used and bears his name, see also [30].

More recently, in the 1960's and 1970's D. Shanks, who by training was not a professional mathematician, made a number of very significant contributions to computational number theory, see for instance [117]. To name a few, the baby-step giant step method, which allows to find a given element in a group of size N in time $O(N^{1/2})$, the infrastructure of real quadratic fields, which was in some sense a precursor to Arakelov theory, and an essential piece in the development of algorithms for computing class and unit groups, the Tonelli–Shanks algorithm for computing square roots modulo p, as well as less important but still interesting 6-letter methods (coming from FORTRAN) such as NUCOMP and SQUFOF, the latter allowing to factor 18-digit numbers on a pocket calculator using only 10 digits. I refer to [37] for details on all these methods.

In parallel and during the same period, more "serious" computational mathematics was being done: first and foremost, the computations of B. Birch and P. Swinnerton-Dyer in the 1960's on the Mordell–Weil group of rational elliptic curves, leading to the famous BSD conjecture [28], which is one of the most outstanding conjecture in number theory, on par with the Riemann Hypothesis; the work of D. Tingley [132] leading to tables of modular elliptic curves in Antwerp IV [29]; and later the work of J. Buhler proving the existence of an icosahedral

weight 1 modular form in level 800 [35]; work of O. Atkin on many computational aspects of modular forms such as the Atkin–Lehner operators [8], non-congruence subgroups [10], congruences between modular forms, etc.; work of H. Stark on Stark units, leading to the Stark conjectures [124], as well as the first explicit (although at the time non-rigorous) computation of cuspidal Maass forms in level 1 [125] and also [31] for a modern and rigorous treatment; this was followed by extensive work of D. Hejhal on this subject [81]; work of A. Odlyzko on verifying the Riemann Hypothesis at very large heights and relations with the GUE hypothesis, and in particular the Odlyzko–Schönhage algorithm for computing $\zeta(s)$ for large $\Im(s)$ [103].

In the late 1970's and early 1980's, a flurry of activity took place around primality testing and factoring. This ultimately led to the two leading practical primality tests, the APRCL (Adleman–Pomerance–Rumely–Cohen–Lenstra) test using Jacobi sums and cyclotomic fields [48] and [49], and the ECPP (Elliptic Curve Primality Proving) algorithm using elliptic curves by O. Atkin and F. Morain [9]. Later, the AKS (Agrawal–Kayal–Saxena) test [1] proved that primality proving is polynomial-time, but this test is less practical than the previous ones.

For factoring, the decisive step was taken by J. Pollard (again a nonprofessional mathematician) which led to the NFS (Number Field Sieve) algorithm [90], other important algorithms being the MPQS (Multiple Polynomial Quadratic Sieve), in large part due to C. Pomerance [108], and the ECM (Elliptic Curve Method), due to H. W. Lenstra, Jr. [89]. All these algorithms are still in use today.

In parallel, R. Schoof used "ℓ-adic" techniques to create a polynomial time algorithm for counting points on elliptic curves over prime finite fields [116], which was later improved by O. Atkin and N. Elkies into the SEA (Schoof–Elkies–Atkin) algorithm [63]. For elliptic curves over fields of small characteristic, J.-F. Mestre [98] and T. Satoh [115] invented incredibly simple algorithms for this task (only a few lines of programming necessary, see for instance Algorithm 17.58 in [47] for Mestre's AGM based algorithm in characteristic 2). Later, this was largely generalized to all hyperelliptic curves (and other varieties) by K. Kedlaya [85]. These algorithms are "p-adic" in nature, as opposed to ℓ-adic above.

2. The Development of Pari/GP and Computational Number Theory Books

There are two ways of doing number theory on a computer: either program in a standard low-level computer language such as C or even directly in assembly, or use high-level software such as Maple or Mathematica. The first method is by far the most efficient, but is extremely cumbersome, since for instance multiprecision operations are not available, at least directly, in these languages. In the early 1980's, there existed a few Computer Algebra Systems, but first they were mostly tailored to perform computations in applied mathematics and numerical analysis and not number theory, and second they were very slow for the little number theory that they could do.

With the help of a few colleagues, first F. Dress, then C. Batut, D. Bernardi, and M. Olivier, in 1985 we embarked on the daunting task of writing a complete computer algebra system with two goals in mind: first speed and efficiency, second specifically tailored to number-theoretic computations, although we also included some numerical analysis tools. Once the basic functionality written (which required

two years of hard work, including tens of thousands of lines of assembly language code), we included algorithms for working with common mathematical objects, and recent groundbreaking algorithms such as the LLL (Lenstra–Lenstra–Lovász) algorithm [91] (see [100] and [101] for later work), one of the most useful algorithms invented at the end of the twentieth century. In friendly competition with the KANT group led by M. Pohst, we also completed H. Zassenhaus' program consisting in computing rings of integers, unit groups, and class groups of algebraic number fields. The pioneering work of Hafner–McCurley [77], followed by that of J. Buchmann [33], led us to the first program able to compute class and unit groups of general number fields in reasonable time and at the simple press of a keystroke. I still recall our elation in seeing the class groups of several thousand cubic fields being computed in the blink of an eye, since previously, computing even a few could constitute a Masters thesis. Later, with the help of D. Bernardi and J.-F. Mestre, we also wrote a number of programs for working with elliptic curves over the rationals, not including rank computations.

In parallel with the writing of these programs, I decided to write down explicitly the algorithms used, since they were either scattered in the literature, or completely new such as Buchmann's algorithm. This resulted in quite a large manuscript (more than 500 pages), and on the occasion of the 1991 Arbeitstagung in Bonn I was introduced to Catriona Byrne, who after sending the book to a number of referees, accepted the manuscript, which was published with the title "A Course in Computational Number Theory" as Springer GTM 138 [37]. Since then we stayed in professional contact, at ICMs and on the occasion of the publication of my later books, and I was very pleased that she attended the conference given in Bordeaux for my 60th birthday in 2007.

I was of course very happy by the success of this book (I believe it has now reached a circulation of more than 10000 copies, Springer can confirm this), but evidently almost 30 years later a large part is outdated since computational methods change much faster than mathematical theories do.

Note that previously almost all books on computational number theory were mostly conference proceedings such as [92] and [109], and/or devoted to a specific subject, with the exception of [140] in 1972, and [106] which appeared essentially at the same time as [37] in 1993.

Shortly after the book appeared, J. Martinet (who was both my thesis advisor and the chairman of our department) gave a course on class field theory, using the classical language of *moduli*, instead of the more modern language of adèles and idèles. That modern language had always frightened me, and I considered class field theory as a difficult subject. Martinet's course opened my eyes, and I soon realized that class field theory could, with some effort, be included in computer packages. For this purpose I had to develop some elementary but apparently new machinery for dealing with relative extensions, and also I rewrote Martinet's course (omitting many proofs) in a way which was more suited to computer implementation. Exactly as in the beginning of `Pari/GP`, this led both to an extensive `Pari` library for computing in relative extensions, computing ray class groups and ray class fields (helped by F. Diaz y Diaz and M. Olivier [43]), and to the writing of a new book, naturally called "Advanced topics" in computational algebraic number

theory, published in 2000 as Springer GTM 193 [38]. This book contains in particular a very understandable description of class field theory in classical language, in large part based on Martinet's course.

For completeness (and self-advertising) I also mention my two other books [39] and [40] which are much less computationally oriented but contain a very large amount of material and exercises on modern number theory.

3. Arithmetic Statistics

A considerable number of additional algorithmic methods for number fields have since been found. In particular, in the domain of making *tables* of number fields, in addition to the brute force methods using theorems of Hunter and Martinet, class-field theoretic methods have been used to compute certain classes of number fields, in particular quartic fields [45] and [46], very elegant methods for computing cubic fields based on the Delone–Fadeev correspondence have been devised by K. Belabas [15], and much more recently the work of M. Bhargava [22] and [23] has led to much more efficient methods for computing S_4 quartic fields [138].

The rest of this section is more theoretical, but intimately connected to computational number theory.

The problem of *enumerating* number fields (usually, but not always, ordered by discriminant) has attracted a lot of attention. Denote by $N_n(G, X)$ the number of isomorphism classes of number fields of degree n, absolute discriminant less than X, and Galois group of their Galois closure isomorphic to G, and by $N_n(X)$ if G is not specified. The case $n = 2$ is trivial, The case $G = C_3$ is easy and first published by H. Cohn [52], $G = C_4$ and $G = C_2 \times C_2$ are due to A. Baily [11], although his formulas need to be corrected, and the general case where G is abelian has been treated by S. Mäki in her thesis (Helsinki, 1985), see also [96].

Non-abelian groups are much more difficult. The case of S_3 cubic fields was solved by Davenport and Heilbronn using the Delone–Fadeev correspondence [58], the case of D_4 quartic fields is due to F. Diaz y Diaz, M. Olivier, and the author [45], and S_4 quartic and S_5 quintic fields are due to the fundamental pioneering work of M. Bhargava [23], [24] using prehomogeneous vector spaces and a careful point counting inside multidimensional fundamental domains.

A folk conjecture predicts that the total number of number fields of absolute discriminant less than X should be asymptotic to $c \cdot X$ for a suitable positive constant c. A much more precise general conjecture due to G. Malle predicts that $N_n(G, X) \sim c(G) \cdot X^{a(G)} \log(X)^{b(G)}$ for explicit constants $a(G)$ and $b(G)$ and a nonexplicit positive constant $c(G)$ (his initial conjectured value of $b(G)$ needs to be corrected in certain cases; note that this conjecture implies that $N_n(G, X) > 0$ for sufficiently large X, i.e., the truth of the inverse Galois problem, which is also conjectural), and in particular that $N_n(X) \sim c_n \cdot X$ for $n \geq 2$ for some $c_n > 0$.

Malle's conjecture is known to be true in a number of cases in addition to the ones already mentioned, but is far from being proved in general. For instance it predicts that $N_4(A_4, X) \sim c\, X^{1/2} \log(X)$, but the best known unconditional upper bound is $N_4(A_4, X) = O(X^{0.7785})$ [25] (even conditionally, the best known is $O(X^{2/3})$ [139]). For another example, it is not known whether $N_6(X) = O(X)$, the trivial bound being $O(X^2)$; it is only recently (April 2022) that several authors [6], [26] succeeded in improving on this trivial bound, the best result being $O(X^{61/32+\epsilon})$ for any $\epsilon > 0$, still far from the conjectured result. Even more frustrating, it is widely

conjectured that the number of cubic fields with *given* discriminant X is $O(X^\epsilon)$ for any $\epsilon > 0$, but the trivial class-field theoretic bound only gives $O(X^{1/2})$, and the current best bound is $O(X^{1/3})$ [65].

On the other hand, an important step towards the folk conjecture was made by J.-M. Couveignes [54], later slightly improved by other authors in [88], who show that $N_n(X) = O_n(X^{c\cdot\log(n)^2})$ for a suitable constant c.

Another aspect of arithmetic statistics, closely linked to the above-mentioned works via class field theory, is to study the distribution of class groups of number fields. The basic conjectures were proposed by Lenstra, Martinet, and the author in [50] and [51], although the latter should be modified in the presence of roots of unity, see for instance [134] and [13] for recent approaches and references.

These conjectures have been proved only in a very small number of cases: the theorems of Davenport-Heilbronn and the works of Bhargava et al. already mentioned, and in the special case $p = 2$ for quadratic fields in the remarkable work of A. Smith [122], following work of F. Gerth [73] and Fouvry–Klüners [72].

In a different direction, the so-called Odlyzko bounds, due in fact to many people (H. Stark, A. Odlyzko, G. Poitou, J.-P.-Serre, F. Diaz y Diaz, see the references in Odlyzko's survey [102]) led to considerable work towards finding number fields with smallest possible absolute discriminant for given degree and signature, see for instance [44].

A considerable amount of work has also been done on statistics for elliptic curves. Without going into too much detail, probably the most spectacular heuristic is due to B. Poonen and E. Rains [111], predicting in particular that there should exist only a finite number of (isomorphism classes of) elliptic curves defined over $\mathbb{Q}$ with Mordell–Weil rank strictly larger than 21 (the current record is due to N. Elkies with a curve of rank 28, see [64]), see [110] for additional references. Note that 21 would be very close to optimal since another result of Elkies shows that there are infinitely many elliptic curves defined over $\mathbb{Q}$ with rank greater or equal to 19, see again [64]. A different heuristic due to A. Granville and M. Watkins [135] also gives 21 as an upper bound.

4. Automorphic Forms, L-Functions, and `Pari/GP` Implementations

Notwithstanding all this work, in the past 25 years, the emphasis has turned away from number fields, and more toward more algebro-geometric objects and automorphic forms, in particular related to the Langlands program.

Already in the early 1990's, J. Cremona launched an extensive computation to tabulate elliptic curves defined over $\mathbb{Q}$ (he has reached conductor 500000), and has written a very nice book giving all the details [56]. In addition, he provided the number-theoretic community with the `mwrank` program, which in many cases is able to compute the Mordell–Weil group of a rational elliptic curve.

Cremona's computation of elliptic curves defined over $\mathbb{Q}$ is based on the use of modular symbols for computing spaces of modular forms of weight 2 with trivial character. In collaboration with N. Skoruppa and D. Zagier, we developed algorithms for computing spaces of modular forms of any even weight with trivial character, later generalized by Skoruppa to forms with character (Nebentypus). The method was completely different since based on the Eichler–Selberg trace formula. We computed and even printed large tables, which were used by a small circle but were never published, but see below.

Since the 1990's a large number of papers appeared containing new or improved algorithms and programs in computational number theory. In particular, the ANTS (Algorithmic Number Theory Symposia) series held every two years since 1994 holds a wealth of information, see the 14 volumes of [3], and see also [47], which is more oriented towards cryptographic applications.

I will now focus on what I know best, without minimizing the importance of subjects that I do not mention.

The appearance of the Computer Algebra Systems `magma` [32] (headed by J. Cannon) and `Sage` [114] (headed by W. Stein) gave the (non-numerical) mathematical community powerful additional tools, although the strictly number-theoretic part of `Sage` mostly comes from the use of `Pari/GP`. One of the initial ingredients of `Sage` was a package written by W. Stein for computing spaces of modular forms using modular symbols, which is very nicely explained in his book [126]. Many of the implementations that I will now describe are also available in `magma` (and of course also in `Sage` since it contains the `Pari` code).

In the `Pari/GP` system [104], a number of very important new implementations have been included, which can be roughly divided into five categories, although almost all these improvements are interwoven. This is the main strength of the `Pari` library: so many arithmetic functions are available and used internally in so many places that even localized improvements or better design concepts quickly have major impacts elsewhere.

4.1. **Algebraic Number Fields.**

- A considerably more efficient computation of the class and unit groups of algebraic number fields due to the work of B. Allombert, K. Belabas and L. Grenié over 20 years [19] and [76].
- The systematic use of compact representations of elements and in particular of S-units in number fields by K. Belabas following H. Williams' original ideas, absolutely essential for many applications, see [34] and [120].
- A Thue equation solver, by G. Hanrot [27].
- A fast polynomial factorization engine over number fields by K. Belabas building on earlier work of X. Roblot and the revolutionary ideas introduced in the LLL method by M. van Hoeij [16] and [21].
- A large number of Galois-theoretic functions by B. Allombert [4].
- A complete rewrite of basic finite fields arithmetic (including polynomial factorization and many multimodular methods) by B. Allombert [5] and asymptotically fast linear algebra by P. Bruijn, including fast linear algebra over cyclotomic rings by B. Allombert [84].
- On the fly computation of number fields with given Galois group and local data by K. Belabas and the author, see in particular [46].
- A much more efficient program for Kummer extensions and computing class fields by K. Belabas, L. Grenié and A. Page using C. Fieker's ideas.

4.2. **Elliptic and hyperelliptic curves.**

- Many new algorithms for elliptic curves over number fields and p-adic fields by B. Allombert, K. Belabas, and B. Perrin-Riou.
- Isogenies by H. Ivey-Law and B. Allombert.

- Modular and class polynomial computations by A. Enge, H. Ivey-Law, and A. Sutherland, see [66], [68], [129], and [128].
- Pairings by J. Milan and B. Allombert.
- ECPP implementation by J. Asuncion.
- Mordell–Weil group of elliptic curves by B. Allombert, K. Belabas and D. Simon, extending D. Simon's original `GP` scripts and considerably more efficient than J. Cremona's initial very useful `mwrank` program.
- Improvements of the Heegner point method using ideas of J. Cremona and M. Watkins by B. Allombert [135].
- Implementation of the SEA point-counting algorithm by B. Allombert, C. Doche, and S. Duquesne.
- Kedlaya's algorithm [85] to compute the characteristic polynomial of the Frobenius automorphism on a hyperelliptic curve by B. Allombert.
- Reduction of genus 2 curves by K. Belabas and Q. Liu [94].
- A port by B. Allombert of the `ratpoints` program written by M. Stoll [127] which searches for rational points of small height on hyperelliptic curves.

4.3. **L-Functions and Automorphic Forms.**

- Numerical computation of arbitrary (motivic) L-functions, initially based on a paper and a `GP` script due to T. Dokchitser [61], but largely enhanced thanks to ideas of A. Booker, P. Molin, and the `Pari` group, see [41], [42], and [18].
- Computation of modular form spaces by K. Belabas and the author, again using the Eichler–Selberg trace formula, but enormously enhanced: in particular, it can compute modular forms of weight 1, of half-integral weight, expansions at arbitrary cusps, Petersson products, etc., see [17] for complete details.
- Isomorphisms of lattices by B. Allombert, porting B. Souvignier's implementation of the Plesken and Souvignier algorithm [105].
- Modular symbols by K. Belabas and B. Perrin-Riou [20] (after R. Pollack and G. Stevens [107]), analogous to W. Stein's initial one and more tailored towards the computation of p-adic L-functions attached to modular forms.
- Associative and central simple algebras due to A. Page, complementing similar work done by J. Voight.
- Hypergeometric motives and their L-functions by K. Belabas and the author, based on ideas of N. Katz, F. Rodriguez-Villegas and M. Watkins, see [14] and [113].
- Implementation of arbitrary Hecke Grössencharacters by P. Molin and A. Page [99].

4.4. **Numerical Methods.** A large number of arbitrary precision numerical methods, many of them new, have been implemented:

- A. Schönhage's polynomial root finding method, which guarantees to find all complex polynomial roots to a given accuracy, as implemented by X. Gourdon [75].
- A port by B. Allombert of the `fplll` software written by D. Stehlé implementing very efficient floating point versions of the LLL algorithm due to D. Stehlé and P. Nguyen [100].

- Numerous methods for numerical summation (in particular discrete Euler–McLaurin and Monien summation), numerical integration (in particular Gauss–Legendre integration and doubly-exponential methods), extrapolation (in particular Lagrange and Sidi extrapolation), asymptotic expansions, and efficient evaluation of continued fractions. All of these algorithms are explained in great detail (including `GP` code) in the recent book [18] of K. Belabas and the author.
- Computation of transcendental functions, both elementary, and higher transcendental functions, in particular hypergeometric functions, as well as p-adic transcendental functions.
- Multiple zeta values and multiple polylogarithms, based on work of P. Akhilesh [2] and the author.
- Computation of Dirichlet L-functions for large imaginary part of the argument, using either K. Fischer's `zetafast` algorithm [70] or the Riemann–Siegel formula, see [7] for $\zeta(s)$ and [119] for Dirichlet characters.

4.5. **Software Enhancements.** On the non-mathematical side, one can mention the following:

- The use of the highly optimized `gmp` multiprecision library to replace most of the integer arithmetic, in particular our own assembly code.
- The `GP2C` compiler written by B. Allombert which translates `GP` scripts into pure C code which can be 3 or 4 times faster and can be incorporated into standalone programs or be used to learn `libpari` programming.
- The possibility of using parallelism in `Pari/GP` programs (POSIX threads or MPI) with essentially no effort nor additional programming, also due to B. Allombert. The underlying mechanism is also heavily used internally in many algorithms, without user intervention, to benefit from the now ubiquitous multicore machines (pthreads) or launch massive jobs on computing clusters (MPI).

5. Additional Available Software and Algorithms

As already mentioned, both `magma` and `Sage` are very large systems containing much more than computational number theory. But in addition to the programs provided by these systems, the most important additional resource is the `LMFDB` (L-function and Modular Form Database) [93] and [57], which contains a huge amount of interconnected tables related to computational number theory, which can be trivially downloaded and used in `Pari/GP`, `magma`, or `Sage`. This is a collaborative effort by almost a hundred people, and has become an essential tool for working on the subject.

Unrelated but also very useful is the `arb` system [83] developed by F. Johansson which guarantees the accuracy of numerical results by working in ball arithmetic, and which in particular contains a very large number of transcendental functions. Not only are the results *guaranteed*, but in addition the implementations are considerably more efficient than in other systems. Note also the `paritwine` package [67] which allows easy access to many `arb` functions inside a `Pari/GP` session.

I would also like to mention the following additional works, again far from being exhaustive:

- Implementations of Hilbert modular forms by L. Dembelé, J. Voight [59], as well as later work.
- Implementation of Bianchi modular forms by J. Cremona [55] as well as later work, see the LMFDB [93] and [57] for further references.
- Implementation of certain types of Siegel modular forms by many people.
- Implementation of p-adic L-functions by R. Pollack and C. Wuthrich.
- Work of D. Farmer's group on creating L-functions "out of thin air", and in particular in making tables of GL_3 and GL_4 Maass forms [69].
- Work of Poor and Yuen on paramodular forms, and in parallel of A. Brumer on abelian surfaces, in the direction of the paramodular conjecture [112] and [36].
- The very efficient use of the p-adic Gross–Koblitz formula for counting points over finite fields by several people, see for instance [18].
- Quasi-linear time computation of coefficients of motivic L-functions by D. Harvey, K. Kedlaya, A. Sutherland et al., and application to classification of Sato–Tate groups, as well as other important contributions of these authors, see for instance [78], [79], [130], [131], and [71].
- Chabauty–Coleman methods [95] to compute all rational points on curves and certain other varieties, and generalizations such as Kim's non-abelian Chabauty [53],
- Generalizing Schoof's algorithm, the *polynomial time* (but not practical) algorithm of J.-M. Couveignes, B. Edixhoven[1] et al. [62], for computing the Ramanujan tau function and more generally Hecke eigenvalues.
- The work of K. Khuri-Makdisi on efficient computations on Jacobians of curves [86].
- The recent proof by D. Harvey and J. van der Hoeven [80] of the existence of a $O(n\log(n))$ algorithm for multiplying n-bit numbers, which had been conjectured for more than 50 years.

6. The Future

In the same way that fundamental research is essential for practical applications, theoretical progress on mathematical conjectures is often essential for computational uses, but conversely, not only computational experiments often lead to important conjectures (I have already mentioned BSD and the Stark conjecures, but there are many other examples), but in conjunction with theoretical advances can lead to *proofs*. Let me specialize to number theory.

Many theorems in number theory are *non-effective*, in that one knows that some property is true for a "sufficiently large" (but unspecified) number, or that some quantity is larger than $C \cdot f(x)$ for a known function x but an unspecified constant C, or similar. It is then useless to do computations since we will never know when the "sufficiently large" is attained. Some other theorems are effective, but the implied constants are so large that the computations become unfeasible.

In these cases, computational methods can be applied *only* after some *theoretical* progress is made. Let me give a few examples.

[1]My friend and colleague Bas Edixhoven died suddenly and very prematurely on January 16, 2022.

(1) A special case of a well-known theorem of Brauer–Siegel implies that for any $\varepsilon > 0$ the class number $h(D)$ of an imaginary quadratic field of discriminant D is greater than $|D|^{1/2-\varepsilon}$ for $|D|$ sufficiently large, but *non-effectively*. In particular $h(D) \to \infty$ with $|D|$. The class number 1 problem ($h(D) > 1$ for $|D| > 163$) was famously solved by Heegner–Stark and Baker, and the class number 2 problem ($h(D) > 2$ for $|D| > 427$) by Stark and Baker using Baker's lower bounds for linear forms in logarithms. But it wasn't until the combined work of D. Goldfeld and B. Gross–D. Zagier that a very weak but explicit lower bound tending to infinity for $h(D)$ was found, using a very clever method, see [74] for an overview of all this. Computational methods could then be applied, and in this way M. Watkins [137] was able to solve the class number h problem for all $h \leq 100$ (one could go further if desired).

(2) A theorem of Siegel states that the number of *integral* points on any model of an elliptic curve defined over $\mathbb{Q}$ is finite, but non-effectively. Progress on this was made thanks to two advances, the main one being theoretical: thanks to Baker-type theorems on linear forms in *elliptic* logarithms, Siegel's theorem could be made effective, but with bounds of the type 10^{10^A}. The second advance was the crucial use of the LLL algorithm to reduce in 2 or 3 steps the bound to something manageable, so that finding all integral points on an elliptic curve is now routine (as long as the Mordell–Weil group is known), see [121] or Section 8.7 of [39].

(3) A theorem of Faltings (previously known as Mordell's conjecture) tells us that the number of rational points on a curve of genus $g \geq 2$ is finite, again non-effectively. In this case, theoretical advances have been constant, but slow. When the rank r of the Mordell–Weil group of the Jacobian of the curve satisfies $r < g$, Faltings' result is in fact effective and due to C. Chabauty and R. Coleman. In the past few years, considerable progress has been made when $r = g$ and in some cases $r > g$, but we are still far from a satisfactory situation analogous to integral points on elliptic curves, see [53] for a survey.

(4) Several theorems in analytic number theory are effective, but with implied constants that would a priori seem inaccessible to computation. Once again, it is thanks to theoretical advances such as a very careful analysis of the so-called "minor arcs" or similar, that the theorems have been completed, usually after a very large computation. Two examples: Waring's problem for 4th powers (every integer $n > 13792$ is a sum of 16 4th powers [60], and every integer is a sum of 19 such [12]) and Goldbach's conjecture for odd integers (every odd integer $n > 5$ is a sum of at most three primes) by H. Helfgott [82].

Therefore it seems reasonable to believe that future important progress in computational number theory will come from theoretical advances.

For instance, a very important problem (which may never be solved) is to find efficient algorithms for finding Euler factors and local conductors of motivic L-functions at `bad` primes. Apart from brute force searches (the search domain being finite), one of the most general methods consists in writing systems of linear or nonlinear equations and trying to solve them using the functional equation of the L-function, but these methods fail as soon as the problems get large.

For specific types of L-functions, one has specific theorems and/or algorithms, the most famous being Tate's algorithm for elliptic curves. One also has algorithms for curves of genus 2 and partial results in higher genus, for certain other varieties, for symmetric powers of modular forms, for Hecke L-functions, and for Artin L-functions.

A general algorithm would involve computing explicitly ℓ-adic cohomology groups, which for now seems out of reach except in special cases including those mentioned above.

Other future goals may be the generalization of the Riemann–Siegel formula to L-functions of degree larger than 1, for instance attached to classical modular forms, a rigorous understanding of Dokchitser's heuristic continued fraction method for computing inverse Mellin transforms, obtaining more efficient methods for finding L-functions knowing only their functional equation and arithmetic properties by building on the work of D. Farmer, algorithmic methods for more general automorphic forms, improvement in the computation of Mordell–Weil groups of abelian varieties including the use of n-descent for $n \geq 3$, and improvements of Chabauty-like methods for finding rational points.

One can also have even more inaccessible dreams: first, of finding a polynomial time algorithm for factoring, or at least faster than the number field sieve. But perhaps less inaccessible, it is quite frustrating that on the one hand, given a rational elliptic curve of rank 1, the Heegner point method can find a generator very efficiently, while if the curve has rank 2, say, and one rational point is known, there is no efficient general method for finding a second independent rational point. This is intimately linked to the fact that the BSD conjecture is totally open for curves of rank greater than or equal to 2.

One can also consider paradigm shifts in computational problems. Until rather recently, the Graal was to find polynomial time algorithms (possibly probablilistic or depending on unproved hypotheses such as GRH) for computational problems. Since then, the emphasis is sometimes more on finding quasi-linear algorithms (with respect to the input and output size). In view of the possible existence of quantum computers, the possibilities of quantum computability opens also a wide scope for research, the prototypical example being Shor's factoring algorithm [118], but many other applications of quantum computing have since been found.

References

[1] M. Agrawal, N. Kayal, and N. Saxena, *PRIMES is in P*, Ann. Math. **160** (2004), 781–793.

[2] P. Akhilesh, *Double tails of multiple zeta values*, J. Number Theory **170** (2017), 228–249.

[3] Algorithmic Number Theory Symposia I to IX, Lecture Notes in Computer Science **877** (1994), **1122** (1996), **1423** (1998), **1838** (2000), **2369** (2002), **3076** (2004), **4076** (2006), **5011** (2008), **6197** (2010), Springer-Verlag; X, XIII, and XIV, Open Book Series **1** (2012), **2** (2018), **4** (2020), XI and XII, J. of Computation and Math. **17A** (2014), **19A** (2016), London Math. Soc.

[4] B. Allombert, *An efficient algorithm for the computation of Galois automorphisms*, Math. Comp. **73** (2001), 359–375.

[5] B. Allombert, *Explicit computation of isomorphisms between finite fields*, Finite fields **8** (2002), 332-342.

[6] T. Anderson et al., *Improved bounds on number fields of small degree*, arXiv:2204.01651 (2022).

[7] J. Arias de Reyna, *High precision computation of Riemann's zeta function by the Riemann–Siegel formula, I*, Math. Comp. **80** (2011), 995–1009, and *II*, arXiv:2201.00342 (2022).

[8] O. Atkin and J. Lehner, *Hecke operators on* $\Gamma_0(m)$, Math. Annalen **185** (1970), 134–160.
[9] O. Atkin and F. Morain, *Elliptic curves and primality proving*, Math. Comp. **61** (1993), 29–68.
[10] O. Atkin and P. Swinnerton-Dyer, *Modular forms on congruence subgroups*, Proc. Sympos. Pure Math. **19**, American Math. Soc. (1971), 1–25.
[11] A. Baily, *On the density of discriminants of quartic fields*, J. reine angew. Math. **315** (1980), 190–210.
[12] R. Balasubramanian, J.-M. Deshouillers, and F. Dress, *Problème de Waring pour les bicarrés. I* Comptes Rendus Acad. Sci Paris **303** (1986) 85–88, and *II* 161–163.
[13] A. Bartel, H. Johnston, and H. W. Lenstra, Jr., *Galois module structure of oriented Arakelov class groups*, arXiv:2005.11533 (2020).
[14] F. Beukers, H. Cohen, and A. Mellit, *Finite hypergeometric functions*, Pure Appl. Math. Q. **11** (2015), 559–589.
[15] K. Belabas, *A fast algorithm to compute cubic fields*, Math. Comp. **66** (1997), 1213–1237.
[16] K. Belabas, *A relative van Hoeij algorithm over number fields*, J. Symbolic Computation **37** (2004), 641–668.
[17] K. Belabas and H. Cohen, *Modular forms in Pari/GP*, in Research in the Math. Sciences **5** (2018), 46–64.
[18] K. Belabas and H. Cohen, *Numerical Algorithms for Number Theory Using Pari/GP*, Math. surveys and monographs **254**, American Math. Soc. (2021).
[19] K. Belabas, F. Diaz y Diaz, and E. Friedman, *Small generators of the ideal class group*, Math. Comp. **77** (2008), 1185–1197.
[20] K. Belabas and B. Perrin-Riou, *Overconvergent modular symbols and p-adic L-functions*, arXiv:2101.06960 (2021).
[21] K. Belabas, M. Van Hoeij, J. Klüners, and A. Steel, *Factoring polynomials over global fields*, J. Théor. Nombres Bordeaux **21** (2009), 15–39.
[22] M. Bhargava, *Higher composition laws I, II, III, and IV*, Ann. Math. **159** (2004), 217–250, 865–886, 1329–1360, and **172** (2010), 1559–1591.
[23] M. Bhargava, *The density of discriminants of quartic rings and fields*, Ann. Math. **162** (2005), 1031–1063.
[24] M. Bhargava, *The density of discriminants of quintic rings and fields*, Ann. Math. **172** (2010), 1559–1591.
[25] M. Bhargava, A. Shankar, T. Taniguchi, F. Thorne, J. Tsimerman, and Y. Zhao, *Bounds on 2-torsion in class groups of number fields and integral points on elliptic curves*, J. Amer. Math. Soc. **33** (2020), 1087–1099.
[26] M Bhargava, A. Shankar, and X. Wang, *An improvement on Schmidt's bound on the number of number fields of bounded discriminant and small degree*, arXiv:2204.01331 (2022).
[27] Y. Bilu and G. Hanrot, *Solving Thue equations of high degree*, J. Number Theory **60** (1996), 373–392.
[28] B. Birch and P. Swinnerton-Dyer, *Notes on elliptic curves I and II*, J. reine angew. Math. **212** (1963), 7–25, **218** (1965), 79–108.
[29] B. Birch and W. Kuyk (eds), *Modular forms in one variable IV*, Lecture Notes in Math. **476**, Springer-Verlag (1975).
[30] A. Booker, *Artin's conjecture, Turing's method, and the Riemann hypothesis*, Experiment. Math. **15** (2006), 385–407.
[31] A. Booker, A. Strömbergsson, and A. Venkatesh, *Effective computation of Maass cusp forms*, Int. Math. Res. Not. (2006), Art. ID 71281, 34.
[32] W. Bosma, J. Cannon, and C. Playoust, *The Magma algebra system I. The user language*, J. Symbolic Comput. **24** (1997), 235–265.
[33] J. Buchmann, *On the computation of units and class numbers by a generalization of Lagrange's algorithm*, J. Number Theory **26** (1987), 8–30.
[34] J. Buchmann, C. Thiel, and H. Williams, *Short representations of quadratic integers*, Math. and its applications **325**, Kluwer (1995), 159–185.
[35] J. Buhler, *Icosahedral Galois representations*, Lecture Notes in Math. **654**, Springer–Verlag (1978).
[36] A. Brumer and K. Kramer, *Paramodular abelian varieties of odd conductor*, Trans. Amer. Math. Soc. **366** (2014), 2463–2516.

[37] H. Cohen, *A Course in Computational Algebraic Number Theory (fourth corrected printing)*, Graduate Texts in Math. **138**, Springer-Verlag, 2000.
[38] H. Cohen, *Advanced Topics in Computational Number Theory*, Graduate Texts in Math. **193**, Springer-Verlag, 2000.
[39] H. Cohen, *Number Theory I, Tools and Diophantine Equations*, Graduate Texts in Math. **239**, Springer-Verlag, 2007.
[40] H. Cohen, *Number Theory II, Analytic and Modern Tools*, Graduate Texts in Math. **240**, Springer-Verlag, 2007.
[41] H. Cohen, *Computing L-functions: A survey*, J. Th. Nombres Bordeaux **27** (2015), 699–726.
[42] H. Cohen, *Computational number theory in relation with L-functions*, in I. Inam and E. Büyükaşik (eds.), International Autumn School on Computational Number Theory, Birkhäuser (2019), 171–266.
[43] H. Cohen, F. Diaz y Diaz, and M. Olivier, *Computing ray class groups, conductors, and discriminants*, Math. Comp. **67** (1998), 773–795.
[44] H. Cohen, F. Diaz y Diaz, and M. Olivier, *A table of totally complex number fields of small discriminant*, Proceedings ANTS XIII, Lecture Notes in Computer Science **1423**, Springer-Verlag (1998), 381–391.
[45] H. Cohen, F. Diaz y Diaz, and M. Olivier, *Enumerating quartic dihedral extensions of* $\mathbb{Q}$, Compositio Math. **133** (2002), 65–93.
[46] H. Cohen, F. Diaz y Diaz, and M. Olivier, *Constructing complete tables of quartic fields using Kummer theory*, Math. Comp. **72** (2003), 941–951.
[47] H. Cohen and G. Frey (eds), *Handbook of elliptic and elliptic and hyperelliptic curve cryptography*, CRC Press (2006).
[48] H. Cohen and H. W. Lenstra, Jr., *Primality testing and Jacobi sums*, Math. Comp. **42** (1984), 297–330.
[49] H. Cohen and A. K. Lenstra, *Implementation of a new primality test*, Math. Comp. **48** (1987), 103–121 and S1–S4.
[50] H. Cohen and H. W. Lenstra, Jr., *Heuristics on class groups of number fields*, Lecture Notes in Math. **1068** Springer-Verlag (1984), 33–62.
[51] H. Cohen and J. Martinet, *Étude heuristique des groupes de classes des corps de nombres*, J. für die reine und angew. Math. **404** (1990), 39–76.
[52] H. Cohn, *The density of abelian cubic fields*, Proc. Amer. Math. Soc. **5** (1954), 476–477.
[53] D. Corwin, *From Chabauty's method to Kim's non-abelian Chabauty's method*, unpublished manuscript (2021), 41 p.
[54] J.-M. Couveignes, *Enumerating number fields*, Ann. Math. **192** (2020), 487–497 and arXiv:1907.13617 (2019).
[55] J. Cremona, *Hyperbolic tessellations, modular symbols, and elliptic curves over complex quadratic fields*, Compositio Math. **51** (1984), 275–324.
[56] J. Cremona, *Algorithms for modular elliptic curves (2nd ed.)*, Cambridge Univ. Press (1997).
[57] J. Cremona, *The L-functions and modular forms database project*, Found. Comp. Math. **16** (2016), 1541–1553.
[58] H. Davenport and H. Heilbronn, *On the density of discriminants of cubic fields I*, Bull. London Math. Soc. **1** (1969), 345–348, and *II*, Proc. Royal Soc. A **322** (1971), 405–420.
[59] L. Dembélé and J. Voight, *Explicit methods for Hilbert modular forms*, Elliptic curves, Hilbert modular forms, and Galois deformations, Birkhäuser (2013), 135–198.
[60] J.-M. Deshouillers, F. Hennecart, and B. Landreau, *Waring's problem for sixteen biquadrates - Numerical results*, J. Th. Nombres Bordeaux **12** (2000), 411–422.
[61] T. Dokchitser, *Computing special values of motivic L-functions*, Exp. Math. **13** (2004), 137–149.
[62] B. Edixhoven and J.-M. Couveignes (eds.), *Computational aspects of modular forms and Galois representations*, Annals of Math. Studies **176**, Princeton Univ. Press (2011).
[63] N. Elkies, *Elliptic and modular curves over finite fields and related computational issues*, in Computational perspectives in number theory **7**, American Math. Soc. (1998), 21–76.
[64] N. Elkies, *Three lectures on elliptic surfaces and curves of high rank*, arXiv:0709.2908 (2007).
[65] J. Ellenberg and A. Venkatesh, *Reflection principles and bounds for class group torsion*, Int. Math. Res. Not. **1** (2007).
[66] A. Enge, *Computing modular polynomials in quasi-linear time*, Math. Comp. **78** (2009), 1809–1824.

[67] A. Enge and F. Johansson, `paritwine 0.1`, INRIA (2019) `https://www.multiprecision.org/paritwine/`.
[68] A. Enge and A. Sutherland, *Class invariants by the CRT method*, Proceedings ANTS IX, Lecture Notes in Comp. Science **6197** (2010), 142–156.
[69] D. Farmer. S. Koutsioliotas, and S. Lemurell, *Maass forms on* GL(3) *and* GL(4), Int. research notices **22** and arXiv:1212.4544 (2012).
[70] K. Fischer, *The Zetafast algorithm for computing zeta functions*, arXiv:1703.01414v7 (2017).
[71] F. Fité, K. Kedlaya, and A. Sutherland, *Sato–Tate groups of abelian threefolds: a preview of the classification*, Contemp. Math. **770** (2021), 103–129.
[72] E. Fouvry and J. Klüners, *On the* 4*-rank of class groups of quadratic number fields*, Invent. Math. **167** (2007), 455–513.
[73] F. Gerth, *The* 4*-class ranks of quadratic fields*, Invent. Math. **77** (1984), 489–515.
[74] D. Goldfeld, *Gauss' class number problem for imaginary quadratic fields*, Bull. Amer. Math. Soc. **13** (1985), 23–37.
[75] X. Gourdon, *Algorithmique du théorème fondamental de l'algèbre*, Rapport de recherche **1852** INRIA (1993).
[76] L. Grenié and G. Molteni, *Explicit versions of the prime ideal theorem for Dedekind zeta functions under GRH*, Math. Comp. **85** (2016), 889–906.
[77] J. Hafner and K. McCurley, *A rigorous subexponential algorithm for computation of class groups*, J. American Math. Soc. **2** (1989), 837–850.
[78] D. Harvey, *Counting points on hyperelliptic curves in average polynomial time*, Ann. Math. **179** (2014), 783–803.
[79] D. Harvey, *Computing zeta functions of arithmetic schemes*, Proc. London Math. Soc. **111** (2015), 1379–1401.
[80] D. Harvey and J. van der Hoeven, *Integer multiplication in time* $O(n \log(n))$, Annals of Math. **193** (2021), 563–617.
[81] D. Hejhal, *The Selberg trace formula for* $\mathrm{PSL}_2(\mathbb{R})$ I and II, Lecture Notes in Math. **548** and **1001**, Springer-Verlag (1976 and 1983).
[82] H. Helfgott *The ternary Goldbach problem*, arXiv:1501.05438v2 (2015).
[83] F. Johansson, *Arb: efficient arbitrary-precision midpoint-radius interval arithmetic*, IEEE Trans. on Computers **66** (2017), 1281–1292.
[84] C. Jeannerod, C. Pernet, and A. Storjohann, *Rank-profile revealing Gaussian elimination and the CUP matrix decomposition*, J. Symbolic Comput. **56** (2013), 46–68.
[85] K. Kedlaya, *Counting points on hyperelliptic curves using Monsky–Washnitzer cohomology*, J. Ramanujan Math. Soc. **16** (2001), 318–330 and **18** (2003), 417–418.
[86] K. Khuri-Makdisi, *Asymptotically fast group operations on Jacobians of general curves*, Math. Comp. **76** (2007), 2213–2239.
[87] D. H. Lehmer, *Factorization of certain cyclotomic functions*, Ann. Math. 2 **34** (1933), 461–479.
[88] R. Lemke Oliver and F. Thorne, *Upper bounds on number fields of given degree and bounded discriminant*, arXiv:2005.14110v2 (2020).
[89] H. W. Lenstra, Jr., *Factoring integers with elliptic curves*, Annals of Math. **126** (1987), 649–673.
[90] A. K. Lenstra and H. W. Lenstra, Jr. (eds.), *The development of the number field sieve*, Lecture Notes in Math. **1554**, Springer-Verlag (1993).
[91] A. K. Lenstra, H. W. Lenstra, Jr., and L. Lovász, *Factoring polynomials with rational coefficients*, Math. Ann. **261** (1982), 515–534.
[92] H. W. Lenstra and R. Tijdeman (eds), *Computational methods in number theory*, Math. Center Tracts **154/155**, Math. Centrum Amsterdam (1982).
[93] The LMFDB collaboration, *The L-function and modular form database*, `http://www.lmfdb.org` and `http://beta.lmfdb.org`.
[94] Q. Liu, *Modèles minimaux des courbes de genre deux*, J. für die reine und angew. Math. **453** (1994), 137–164.
[95] W. McCallum and B. Poonen, *The method of Chabauty and Coleman*, Panoramas et synthèses **36**, Soc. Math. de France (2012), 99-117.
[96] S. Mäki, *The conductor density of abelian number fields*, J. London Math. Soc. (2) **47** (1993), 18–30.

[97] G. Malle, *On the distribution of Galois groups I*, J. Number Theory **92** (2002), 315–322, and *II*, Exp. Math. **13** (2004), 129–135.
[98] J.-F. Mestre, unpublished, but see Section 17.3.2.b in [47].
[99] P. Molin and A. Page, *Computing groups of Hecke characters*, arXiv (2022), in preparation.
[100] P. Nguyen and D. Stehlé, *Floating-point LLL revisited*, in Proceedings Eurocrypt '2005, Springer-Verlag.
[101] P. Nguyen and B. Vallée (eds), *The LLL algorithm: Survey and applications*, Information Security and Cryptography, Springer (2010).
[102] A. Odlyzko, *Bounds for discriminants and related estimates for class numbers, regulators, and zeros of zeta functions: a survey of recent results*, J. Th. Nombres Bordeaux **2** (1990), 114–141.
[103] A. Odlyzko and A. Schönhage, *Fast algorithms for multiple evaluations of the Riemann zeta function*, Trans. Amer. Math. Soc. **309** (1988), 797–809.
[104] The PARI Group, `PARI/GP` *version 2.13.4*, Univ. Bordeaux (2022), `http://pari.math.u-bordeaux.fr/`.
[105] W. Plesken and B. Souvignier, *Computing isometries of lattices*, J. Symbolic Comp. **24** (1997), 327–334.
[106] M. Pohst and H. Zassenhaus, *Algorithmic algebraic number theory (3rd ed.)*, Cambridge Univ. Press (1993).
[107] R. Pollack and G. Stevens, *Overconvergent modular symbols and p-adic L-functions*, Ann. Sci. ENS **44** (2011), 1–42.
[108] C. Pomerance, *The quadratic sieve factoring algorithm*, Lecture Notes in Comp. Science **209**, Springer-Verlag (1985), 169–182.
[109] A. Pethö, M. Pohst, H. Williams, and H. Zimmer (eds), *Computational number theory*, Walter de Gruyter (1991).
[110] B. Poonen, *Heuristics for the arithmetic of elliptic curves*, arXiv:1711.10112v2 (2017).
[111] B. Poonen and E. Rains, *Random maximal isotropic subspaces and Selmer groups*, J. Amer. Math. Soc. **25** (2012), 245–269.
[112] C. Poor and D. Yuen, *Paramodular cusp forms*, Math. Comp. **84** (2015), 1401–1438.
[113] D. Roberts and F. Rodriguez-Villegas, *Hypergeometric motives*, arXiv:2109.00027 (2021).
[114] The Sage Developers, *SageMath, the Sage Mathematics Software System version 9.5*, (2022), `https://www.sagemath.org`.
[115] T. Satoh, *The canonical lift of an ordinary elliptic curve over a finite field and its point counting*, J. Ramanujan Math. Soc. **15** (2000), 247–270.
[116] R. Schoof, *Elliptic curves over finite fields and the computation of square roots mod p*, Math. Comp. **44** (1985), 483–494.
[117] D. Shanks, *Class number, a theory of factorization, and genera*, Proc. Sympos. Pure Math. **20**, American Math. Soc. (1971), 415–440.
[118] P. Shor, *Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer*, arXiv:quant-ph/9508027v2 (1996).
[119] C.-L. Siegel, *Contributions to the theory of the Dirichlet L-series and the Epstein zeta-functions*, Ann. of Math. (2) **44** (1943), 143–172.
[120] A. Silvester, M. Jacobson, and H. Williams, *Shorter compact representations in real quadratic fields*, Lecture Notes in Computer Science **8260** (2013), 50–72.
[121] N. Smart, *The algorithmic resolution of Diophantine equations*, London Math. Soc. student texts **41** (1998).
[122] A. Smith, 2^∞*-Selmer groups,* 2^∞*-class groups, and Goldfeld's conjecture*, arXiv:1702.02325v2 (2017).
[123] C. Smyth, *The Mahler measure of algebraic numbers: a survey*, in J. McKee and C. Smyth (eds.), Number theory and polynomials, Cambridge Univ. Press (2008), 322–349.
[124] H. Stark, *L-functions at* $s = 1$ *I, II, III, IV*, Adv. Math. **7** (1971), 301–343, **17** (1975), 60–92, **22** (1976), 64–84, **35** (1980), 197–235.
[125] H. Stark, *Fourier coefficients of Maass waveforms*, in "Modular forms", R. Rankin ed., Ellis Horwood (1984), 263–269.
[126] W. Stein, *Modular forms, a computational approach*, Graduate Studies in Math. **79**, American Math. Soc. (2007).
[127] M. Stoll, *Documentation for the ratpoints program*, arXiv:0803.3165v5 (2022).

[128] A. Sutherland, *Computing Hilbert class polynomials with the Chinese remainder theorem*, Math. Comp. **80** (2011), 501–538.
[129] A. Sutherland, *On the evaluation of modular polynomials*, Proceedings ANTS X, Open Book Series **1** (2013), 531–555.
[130] A. Sutherland, *Sato–Tate distributions*, Contemp. Math. **740** (2019), 197–248.
[131] A. Sutherland, *Counting points on superelliptic curves in average polynomial time*, Proceedings ANTS XIV, Open Book Series **4** (2020), 403–422, or arXiv:2004.10189v4.
[132] D. Tingley, *Elliptic curves uniformized by modular functions*, Ph.D. thesis, Univ. of Oxford, 1975.
[133] A. Turing, *Some calculations of the Riemann zeta-function*, Proc. London Math. Soc. **3** (1953), 99–117.
[134] W. Wang and M. Matchett Wood, *Moments and interpretations of the Cohen–Lenstra–Martinet heuristics*, arXiv:1907.11201v2 (2020).
[135] M. Watkins, *Some remarks on Heegner point computations*, Panoramas et synthèses **36**, Soc. Math. de France (2012), 81–97.
[136] M. Watkins, *A discursus on* 21 *as a bound for ranks of elliptic curves over* $\mathbb{Q}$*, and sundry related topics*, `http://magma.maths.usyd.edu.au/~watkins/papers/DISCURSUS.pdf` (2015).
[137] M. Watkins, *Class numbers of imaginary quadratic fields*, Math. Comp. **73** (2004), 907–938.
[138] A.-E. Wilke, thesis, in preparation.
[139] S. Wong, *Densities of quartic fields with even Galois groups*, Proc. Amer. Math. Soc. **133** (2005), 2873–2881.
[140] H. Zimmer, *Computational problems, methods, and results in algebraic number theory*, Lecture Notes in Math. **262**, Springer–Verlag (1972).

Univ. Bordeaux, CNRS, INRIA, Bordeaux INP, IMB, UMR 5251, F-33400 TALENCE