The role of reproducibility in number theory, from my perspective

Michael Rubinstein

University of Waterloo

ICERM, Dec 13, 2012

Computation in number theory can:

- contribute to rigorous mathematical proof.
- help verify conjectures experimentally.
- stimulate mathematical discovery, theorems, relationships, conjectures, and uncover phenomena.
- motivate work on algorithms and complexity (exs: factoring, primality testing, Ghaith Hiary's algorithm for computing the zeta function).
- involve automated theorem proving and proof verification.

What does it mean for a computation to be rigorous? Even assuming that the algorithms/methods are correct in principle, how does one certify, potentially, thousands of lines of code as being correct when there are many places where things can go wrong:

- mathematical coding errors (ex: signs, branches of log).
- programming errors (ex: wrong loop or array bounds, memory issues, confusing types),
- loss of precision (accumulated round-off, cancellation), wrong error analysis/inequalities.
- reliance on black boxes: computer chips (Intel division bug), compilers and optimizers (constantly releasing new versions with bug fixes), computer memory (can get corrupted), closed source software (Mathematica), other people's packages, and using them in ways that were not originally intended or foreseen.

At present we usually declare a program to be bug free once it produces output that is consistent with our expectations. We tend to give more trust to computational results that are reproducible using separate code and hardware, or for which there is more than method that gives the same output, or for which the correctness of the result can be easily tested (examples: factorization of an integer, explicit formula for zeros of an L-function).

Excerpt from Tao's paper:

To prove Theorem 1.4, we will also need to rely on two numerically verified results in addition to Theorem 1.3:

Theorem 1.5 (Numerical verification of Riemann hypothesis). *Let* $T_0 := 3.29 \times 10^9$. *Then all the zeroes of the Riemann zeta function* ζ *in the strip* $\{s : 0 < \Re(s) < 1; 0 \leqslant \Im(s) \leqslant T_0\}$ *lie on the line* $\Re(s) = 1/2$. *Furthermore, there are at most* 10^{10} *zeroes in this strip.*

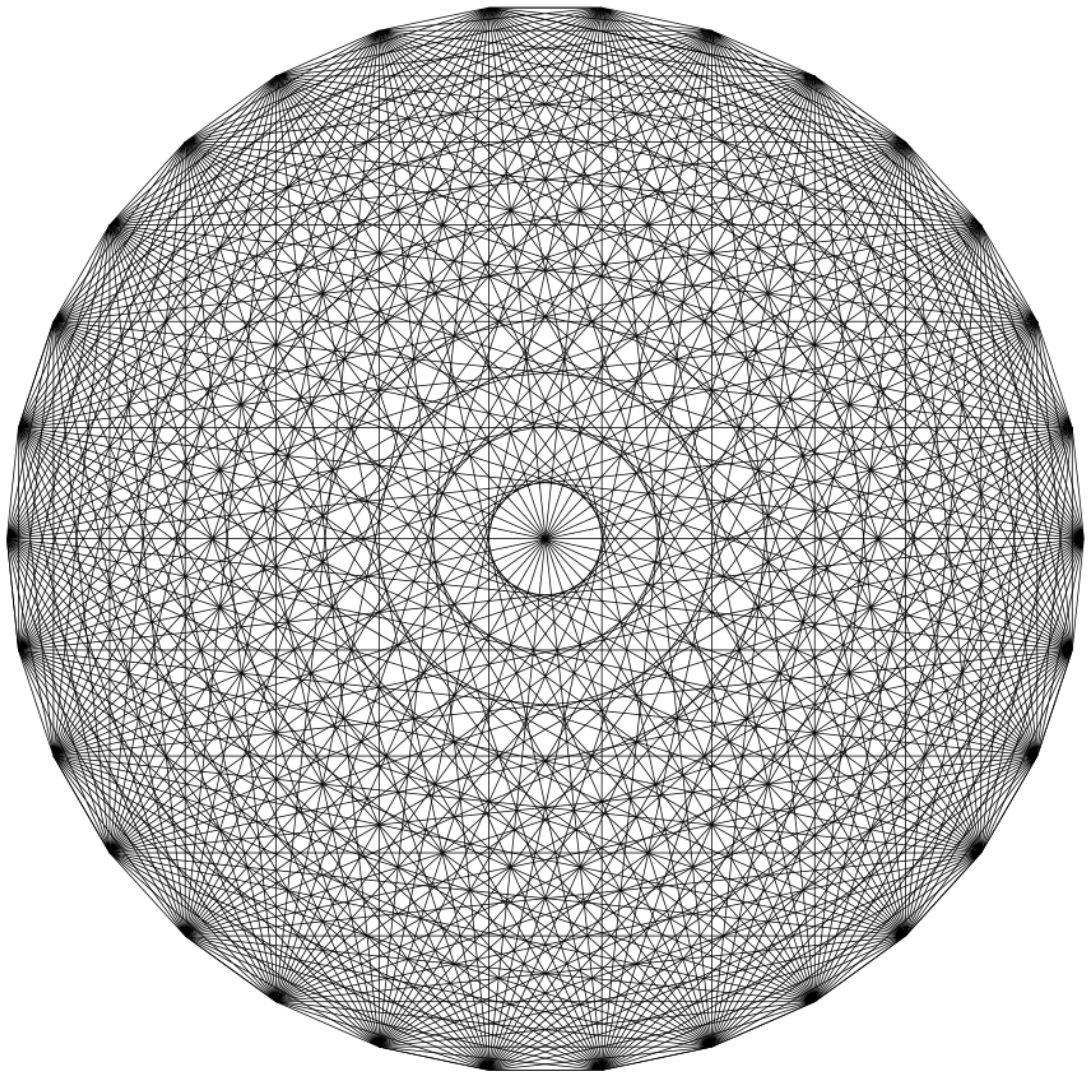
Proof. This was achieved independently by van de Lune (unpublished), by Wedeniwski [50], by Gourdon [14], and by Platt [34]. Indeed, the results of Wedeniwski allow one to take T_0 as large as 5.72×10^{10}, and the results of Gourdon allow one to take T_0 as large as 2.44×10^{12}; using interval arithmetic, Platt also obtained this result with T_0 as large as 3.06×10^{10}. (Of course, in these latter results there will be more than 10^{10} zeroes.) However, we will use the more conservative value of $T_0 = 3.29 \times 10^9$ in this paper as it suffices for our purposes, and has been verified by four independent numerical computations. □

Theorem 1.6 (Numerical verification of even Goldbach conjecture). *Let* $N_0 := 4 \times 10^{14}$. *Then every even number between* 4 *and* N_0 *is the sum of two primes.*

Proof. This is the main result of Richstein [41]. A subsequent (unpublished) verification of this conjecture by the distributed computing project of Oliveira e Silva [32] allows one to take N_0 as large as 2.6×10^{18} (with the value $N_0 = 10^{17}$ being double-checked), but again we shall use the more conservative value of $N_0 = 4 \times 10^{14}$ in this paper as it suffices for our purposes, and has been verified by three independent numerical computations. □

Rigour and bugs in computation

Once upon a time I had a very frustrating bug that took me 3 days to find. It had to do with my project, in 1994 (published 1998), with Bjorn Poonen on determining the number of intersection points formed by the diagonals of a regular n-gon.



(Poonen, R. 1994)

Theorem

For $n \geq 3$, the number of interior intersection points formed by the diagonals of a regular n-gon, $I(n)$, is given by

$$\begin{aligned} I(n) &= \binom{n}{4} + (-5n^3 + 45n^2 - 70n + 24)/24 \cdot \delta_2(n) - (3n/2) \cdot \delta_4(n) \\ &\quad + (-45n^2 + 262n)/6 \cdot \delta_6(n) + 42n \cdot \delta_{12}(n) + 60n \cdot \delta_{18}(n) \\ &\quad + 35n \cdot \delta_{24}(n) - 38n \cdot \delta_{30}(n) - 82n \cdot \delta_{42}(n) - 330n \cdot \delta_{60}(n) \\ &\quad - 144n \cdot \delta_{84}(n) - 96n \cdot \delta_{90}(n) - 144n \cdot \delta_{120}(n) - 96n \cdot \delta_{210}(n). \end{aligned}$$

The form of $I(n)$ was obtained by studying an equation involving a dozen roots of unity. The specific coefficients were found by fitting $I(n)$ to actual intersection counts for various $n \leq 420$. Our derivation was, thus, reduced to a finite computation.

n	$\frac{a_2(n)}{n}$	$\frac{a_3(n)}{n}$	$\frac{a_4(n)}{n}$	$\frac{a_5(n)}{n}$	$\frac{a_6(n)}{n}$	$\frac{a_7(n)}{n}$	$\frac{I(n)-1}{n}$	n	$\frac{a_2(n)}{n}$	$\frac{a_3(n)}{n}$	$\frac{a_4(n)}{n}$	$\frac{a_5(n)}{n}$	$\frac{a_6(n)}{n}$	$\frac{a_7(n)}{n}$	$\frac{I(n)-1}{n}$
6	2						2	216	392564	4848	119	49			397580
12	19	5	1				25	222	426836	5166	126	54			432182
18	84	12	3	3			102	228	463303	5441	127	54			468925
24	256	36	11	1			304	234	501762	5718	129	57			507666
30	460	75	14	6	4	1	560	240	541612	6121	165	61		5	547964
36	1179	109	11	6			1305	246	584782	6340	140	60			591322
42	1786	194	27	13			2020	252	629399	6693	137	70			636299
48	3168	220	25	7			3420	258	676580	6972	147	63			683762
54	4722	288	24	12			5046	264	725976	7276	151	61			733464
60	6251	422	63	12		5	6753	270	777420	7643	150	66	4	1	785284
66	9172	460	35	15			9682	276	831575	7969	155	66			839765
72	12428	504	35	13			12980	282	887986	8326	161	69			896542
78	15920	642	42	18			16622	288	947132	8640	161	67			956000
84	20007	805	43	28			20883	294	1008358	9056	174	76			1017664
90	25230	863	45	21	4	1	26164	300	1072171	9462	203	72		5	1081913
96	31240	948	53	19			32260	306	1139436	9780	171	75			1149462
102	37786	1096	56	24			38962	312	1208944	10164	179	73			1219360
108	45447	1201	53	24			46725	318	1281100	10582	182	78			1291942
114	53768	1368	63	27			55226	324	1356315	10957	179	78			1367529
120	62652	1601	95	31		5	64384	330	1434110	11375	189	81	4	1	1445760
126	73676	1658	72	34			75440	336	1514816	11856	193	89			1526954
132	85319	1825	71	30			87245	342	1598970	12216	192	84			1611462
138	97990	2002	77	33			100102	348	1685843	12661	197	84			1698785
144	112100	2136	77	31			114344	354	1775788	13108	203	87			1789186
150	127070	2345	84	36	4	1	129540	360	1868312	13669	231	91		5	1882308
156	143635	2549	85	36			146305	366	1965272	14010	210	90			1979582
162	161520	2736	87	39			164382	372	2064919	14465	211	90			2079685
168	180504	3008	95	47			183654	378	2167754	14930	219	97			2183000
174	201448	3178	98	42			204766	384	2274136	15396	221	91			2289844
180	223251	3470	129	42		5	226897	390	2383690	15885	224	96	4	1	2399900
186	247562	3630	105	45			251342	396	2496999	16369	221	96			2513685
192	273144	3844	109	43			277140	402	2613536	16896	231	99			2630762
198	300294	4092	108	48			304542	408	2733888	17380	235	97			2751600
204	329171	4357	113	48			333689	414	2857752	17898	234	102			2875986
210	359556	4661	125	55	4	1	364402	420	2984383	18598	273	112		5	3003371

Initially we formed this table by computing floating point approximations to the intersection points and, experimentally, declaring points equal if they agreed to 12, and then 40 decimal places.
The patterns in our table broke down around $n \approx 150$, when we first ran our computation. It took me 3 days to track down the bug to the value of

$$\pi = 3.1415926538979323846264338327950288419 7 \ldots$$

Later, we redid the computation rigorously, by also checking that the intersection points of multiplicity > 1 fell into our classification of possible intersection points (Theorem 4 of our paper). That boiled down to comparing integers and we could do it exactly. Not only did it provide a rigorous count of the intersection points, but it also served as an extra check that our classification was complete.

Another anecdote

Using number theoretic heuristics, and guided by techniques and results from random matrix theory, Conrey, Farmer, Keating, R., and Snaith conjectured:

For positive integer k, and any $\epsilon > 0$,

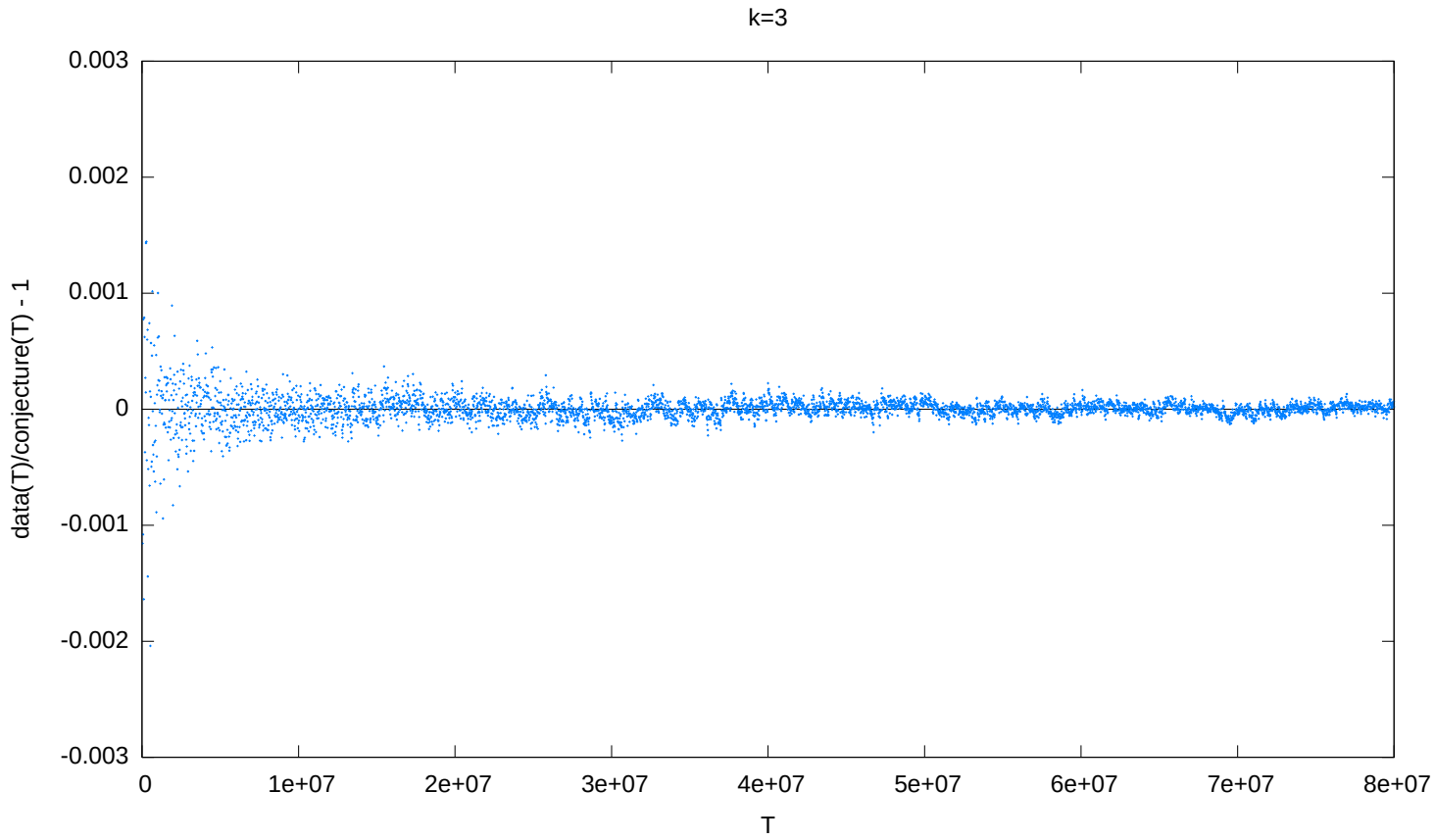
$$\int_0^T |\zeta(1/2 + it)|^{2k} dt \sim \int_0^T P_k \left(\log \tfrac{t}{2\pi}\right) dt,$$

where P_k is the polynomial of degree k^2 given implicitly by a complicated $2k$-fold residue.

From the residue, we developed elaborate formulas for the coefficients of $P_k(x)$ and found, for example, (coefficients are rounded):

$$
\begin{aligned}
P_3(x) = \quad & 0.000005708527034652788398376841445252313\, x^9 \\
+ \quad & 0.000405021330884114403312153320259 84\, x^8 \\
+ \quad & 0.011072455215246998350410400826667\, x^7 \\
+ \quad & 0.148400730801502726808514015187 74\, x^6 \\
+ \quad & 1.045925177905488343938532379805 9\, x^5 \\
+ \quad & 3.984385094823534724747964073429\, x^4 \\
+ \quad & 8.607319145781206756148347636 29\, x^3 \\
+ \quad & 10.27433083070344613418300952 2\, x^2 \\
+ \quad & 6.593913020649758104657133 92\, x \\
+ \quad & 0.916515507637893059017854 3.
\end{aligned}
$$

A completely different method was then developed, using another approach/formula and very high precision (thousands of digits) to see our way through high order poles that cancelled, to obtain the same coefficients to about 20-25 digits.



Graph of: $\frac{\int_0^T |\zeta(1/2+it)|^6 dt}{\int_0^T P_3(\log(t)/(2\pi))dt} - 1$, for $0 < T < 8 \times 10^7$.
(R.-Yamagishi) Agreement is to about 4-5 decimal places out of 15.