Andrew Granville*
is the Canadian Research Chair in number theory at the Université de Montréal.

A good new millenium for the primes

Prime numbers, the building blocks from which integers are made, are central to much of mathematics. Understanding their distribution is one of the most natural, and hence oldest, problems in mathematics. Once the ancient Greeks had determined that there are infinitely many then it was natural to ask how many there are up to any given point, perhaps a very large point, how many there are in certain special subsequences (for example, primes of the form "a square plus one"), and how to identify primes quickly. If one examines tables of primes then they appear to be "randomly distributed" though, as Bob Vaughan once put it, "we do not yet know what random means". Answering these questions has thus proved to be difficult, each success requiring new, far reaching ideas and methods. During the last thirty years there had been few new results of this type but then, in the last decade, several surprises, some of which we will discuss here:

- Identifying primes;
- Primes values of some polynomials in two variables of degree > 2;
- Arithmetic progressions of primes;
- Short gaps between primes;
- Links between the distribution of primes and randomly selected matrices.

x	$\pi(x) = \#\{\text{primes} \leq x\}$	**Overcount: Li** $(x) - \pi(x)$
10^8	5761455	753
10^9	50847534	1700
10^{10}	455052511	3103
10^{11}	4118054813	11587
10^{12}	37607912018	38262
10^{13}	346065536839	108970
10^{14}	3204941750802	314889
10^{15}	29844570422669	1052618
10^{16}	279238341033925	3214631
10^{17}	2623557157654233	7956588
10^{18}	24739954287740860	21949554
10^{19}	234057667276344607	99877774
10^{20}	2220819602560918840	222744643
10^{21}	21127269486018731928	597394253
10^{22}	201467286689315906290	1932355207

Table 1: Primes up to various x, and the overcount in Gauss's prediction.

1. History

The first good guesses for an asymptotic estimate[1] for $\pi(x)$, the number of primes up to x, emerged at the beginning of the nineteenth century, none better than Gauss's observation, made at sixteen years of age when studying tables of primes up to 3 million, that "the density of primes at around x is about $1/\log x$." Interpreting this, we guess that $\pi(x)$ is about $\int_2^x \frac{dt}{\log t}$ which we denote by Li(x). Comparing this prediction (rounded to the nearest integer) with the latest data (Table 1) we see that Gauss's prediction is amazingly accurate. It does seem to always be an overcount, but since the width of the last column is about half that of the central one it appears that the difference is no bigger than something like $\sqrt{x}$.

Are there infinitely many primes in the arithmetic progression a mod q (that is, $a, a+q, a+2q, \ldots$)? Realizing that (a,q) divides all the numbers in the arithmetic progression a mod q we see that we must have $(a,q) = 1$. In 1837 Dirichlet showed that this is the only restriction, that each arithmetic progression a mod q with $(a,q) = 1$ does indeed contain infinitely many primes.

In the middle of the nineteenth century, Riemann defined what we now call the *Riemann zeta function* $\zeta(s) := \sum_{n\geq 1} 1/n^s$ when this converges absolutely, that is when $\Re(s) > 1$. In the rest of the complex plane, this function can be given a new but consistent definition, its meromorphic continuation (with its only pole being a simple pole at $s = 1$). Riemann showed how the zeros of this meromorphic continuation are intertwined with the distribution of prime numbers via the following *explicit formula*

$$\sum_{\substack{p \text{ prime}, m \geq 1 \\ p^m \leq x}} \log p = x - \frac{\zeta'(0)}{\zeta\ (0)} - \sum_{\rho:\, \zeta(\rho)=0} \frac{x^\rho}{\rho},$$

valid when $x \in \mathbb{Z} + ½$

Riemann conjectured that if $\zeta(\rho) = 0$ then $\mathrm{Re}(\rho) = 1/2$ or ρ is a negative even integer. If so then each $|x^\rho/\rho| = x^{\mathrm{Re}(\rho)}/|\rho| \leq x^{1/2}/|\rho|$, and so by getting a good estimate for the number of zeros up to height T one can deduce, from a slight variant of the explicit formula[2], that $|\pi(x)-\mathrm{Li}(x)| \leq \sqrt{x} \log 5x$, for all $x \geq 5$. Evidently if one can simply show that the zeros are sufficiently far to the left of the line $\mathrm{Re}\,(s) = 1$ then the same ideas can be used to prove that $\pi(x) \sim \mathrm{Li}(x) (\sim x/\log x)$, the *prime number theorem*, something which was accomplished by Hadamard and de la Vallée Poussin in 1896. By much the same methods, de la Vallée Poussin was also able to establish that there is roughly the same number of primes up to x in each arithmetic progression a mod q with $(a, q) = 1$, once x is sufficiently large.

2. Identifying whether a given integer is prime

"The problem of distinguishing prime numbers from composite numbers … is … one of the most important and useful in arithmetic … The dignity of the science itself seems to require that every possible means be explored for the solution of a problem so elegant and so celebrated." C. F. Gauss (1801).

The use of factoring and primality testing in applied mathematics (cryptography) has inspired a lot of research in the last twenty years. In practice we have long known how to determine whether large numbers are primes (up to 10,000 digits) but until recently all of our quick algorithms were either not *guaranteed* to always work, or were not unconditionally proved to be quick (though we expect them to be). In 2002, Manindra Agrawal, Neeraj Kayal and Nitin Saxena [1, 6], brilliantly developed a "polynomial time deterministic primality test" out of the ideas already in play. Their test can be stated as an elegant (and rapidly verifiable) characterization of prime numbers:

For given integer $n \geq 2$, let r be *a* positive integer $< n$, for which n has order $> (\log n)^2$ modulo r. Then n is prime if and only if n is not a perfect power, n does not have any prime factor $\leq r$, and $(x+a)^n - x^n - a$ is a $\mathbb{Z}[x]$-linear combination of n and $x^r - 1$, for each integer a, $1 \leq a \leq \sqrt{r} \log n$.

3. Primes values of polynomials

In any number field $K/\mathbb{Q}$, the number of prime ideals of norm $\leq x$ in a given ideal class is $\sim c\mathrm{Li}(x)$ for an appropriate constant $c > 0$. The easiest example of this is when $[K:\mathbb{Q}] = 2$ which, when taking norms, corresponds to the number of distinct prime values taken by a certain binary quadratic form. In fact all examples in the prime ideal theorem correspond to the prime values taken by certain homogenous polynomials of degree $d = [K:\mathbb{Q}]$ in d variables. This type of result was first proved by Landau using a (simple) variant of de la Vallée Poussin's method.

All sequences of values of polynomials that can be considered by such techniques have one thing in common – they are not sparse, containing more than $x^{1-\epsilon}$ elements up to x. It took a century from the proof of the prime number theorem until John Friedlander and Henryk Iwaniec [3] proved in 1998 that a certain more sparse sequence of polynomial values contain an infinite sequence of prime numbers; namely that there are infinitely many primes among numbers of the form $a^2 + b^4$, and even determining their frequency.

Getting hold of such a comparatively thin sequence (which contains $\sim cx^{3/4}$ elements up to x), involved a brilliant development of Enrico Bombieri's *asymptotic sieve*. This sieve allowed Friedlander and Iwaniec to break through the notorious "parity problem," which in the past had been a barrier against the use of sieve theory in questions about the distribution of primes. Inspired by their work, Heath-Brown and Moroz [8] in 2002 determined how often any given primitive binary cubic form (an even more sparse sequence of values with $\sim cx^{2/3}$ integers up to x), for example $a^3 + 2b^3$, is prime, an extraordinary achievement.

Length	Arithmetic Progression	Last Term
3	$3 + 2n$	7
4	$5 + 6n$	23
5	$5 + 6n$	29
6	$7 + 30n$	157
7	$7 + 150n$	907
8	$199 + 210n$	1669
9	$199 + 210n$	1879
10	$199 + 210n$	2089
11	$110437 + 13860n$	249037
12	$110437 + 13860n$	262897
13	$4943 + 60060n$	725663
14	$31385539 + 420420n$	36850999
15	$115453391 + 4144140n$	173471351
16	$53297929 + 9699690n$	198793279
17	$3430751869 + 87297210n$	4827507229
18	$4808316343 + 717777060n$	17010526363
19	$8297644387 + 4180566390n$	83547839407
20	$214861583621 + 18846497670n$	572945039351
21	$5749146449311 + 26004868890n$	6269243827111

Table 2: The k-term arithmetic progression of primes with smallest last term. (One might guess that the last term should be about $(ke^{1-\gamma}/2)^{k/2}$, which is a good fit with the data above.[3])

Perhaps the next goal is prime values of $4a^3+27b^2$, the discriminant of the omnipresent elliptic curve $y^2 = x^3+ax+b$; this sequence is less sparse ($x^{5/6+o(1)}$ integers up to x), but is more difficult to work with, since the form $4a^3 + 27b^2$ does not factor in $\mathbb{C}[a, b]$.

4. Arithmetic progressions of primes

There are no pairs of consecutive primes (which is easy to prove since one of the two must be even), but one finds many *prime twins*, that is pairs of primes that differ by exactly 2, for example 3 and 5, 5 and 7, 11 and 13, 17 and 19, … One is soon led to conjecture that there are infinitely many such pairs, and indeed that there are infinitely many prime pairs $n, n+d$ if (and only if) d is even. To generalize the above to triplets of primes or quadruplets we similarly have to be wary of divisibility by other small primes (for example, one of $n, n+2, n+4$ is always divisible by 3) but the general conjecture is that k polynomials with integer coefficients (perhaps in several variables) can be simultaneously prime for infinitely many sets of integer values for the variables as long as the polynomials are all irreducible with positive leading coefficients and there is no prime p which divides all of the values of the product of the polynomials. Thus we believe that there are infinitely many pairs of integers a and d such that $a, a+d, a + 2d, \dots, a + (k-1)d$ are all prime (Table 2 shows the smallest examples of such arithmetic progressions of primes, of lengths 3, 4, … , 21).

Until recently this had only been proved for $k = 3$ (indeed there were several different proofs in the literature), though in 1990 Antal Balog [2], gave a nice variation on the theme. He showed that there are infinitely many 3-by-3 squares of primes, where each row and each column has three primes in arithmetic progression, and infinitely many 3-by-3-by-3 such cubes of primes, and indeed in any dimension!

No one had worked on the seemingly impossible problem of primes in arithmetic progressions in such a long time that it came as an enormous shock when, in 2004, Ben Green and Terry Tao announced that they had indeed proven that, for each k, there are infinitely many pairs of integers a and d such that $a, a + d, a + 2d, \dots, a+(k-1)d$ are all prime, and could even give a (mammoth) upper bound on the smallest such pair.

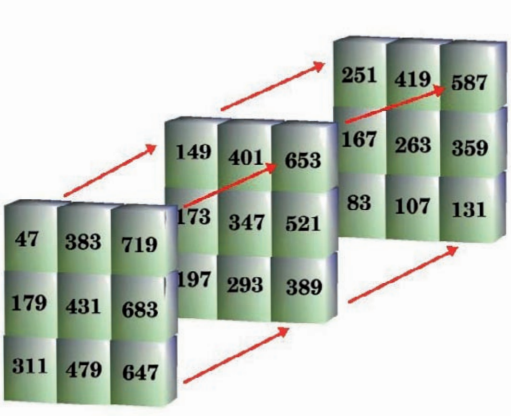

Table 3: A 3-by-3-by-3 "Balog cube" of primes.

The methods used are new to analytic number theory and are best described as *additive combinatorics*, an amalgam of harmonic analysis, combinatorics, ergodic theory, graph theory, combinatorial group theory and number theory, which is inspired by the innovative norms introduced by Tim Gowers [5]. In retrospect Gregori Freiman's theorem from the 1960s on the structure of set addition and various ideas of Imre Ruzsa developing this and tying it into harmonic analysis have been key to these new developments. Freiman's theorem states that if $A+A = \{a+b : a, b \in A\}$ is "small" for a given finite set of integers A, then the set A must be a "large" subset of a small dimensional arithmetic progression, that is a set of the form $\{a_0 + a_1m_1 + \dots a_dm_d$ where $0 \le m_j \le M_j$ for each $j\}$.

The startlingly new[4] technique of Green and Tao promises to revolutionize analytic number theory. It may yet answer many more questions about the distribution of prime tuples and they have made great efforts to re-develop the method so as to fit better with classical analytic number theory, as well as to better interpret what it means for a Gowers norm to be large.

One final detail of the proof of the k-primes in arithmetic progression theorem came in a majorization of the primes by certain sieve weights, originally constructed by Selberg, weights which also appear in the next breakthrough.

5. Sieves

Primes are integers that are not divisible by any "relatively small" primes. So to count primes in a sequence A we delete those elements divisible by 2, 3, … , indeed any of the small primes. If A is the set of integers up to x, then the number divisible by d is x/d with an error term of at most 1; and in typical sieve problems the number of elements divisible by d is $w(d)\ |A|/d$ (where $w(\cdot)$ is a multiplicative function[5]) with a small error term, at least on average. If one tries to estimate the primes in A directly from this information, for example by the inclusion-exclusion principle, one finds that the error terms accumulate to swamp the main term. Thus it pays to either come up with a suitable modification of inclusion-exclusion (*the combinatorial sieve*), or to try to get upper and lower bounds on the number of primes in A by treating each such question as an optimization problem subject to certain constraints (the bounds on the error terms). One can in principle "solve" such problems via Lagrangian multipliers but there are so many variables and such a solution is so complicated that one cannot work with it. Thus Atle Selberg refined the constraints of our optimization problem in such a way that he could elegantly find bounds which are frequently stronger than those obtained by the combinatorial sieve, and that are relatively easy to use in applications. As we have described them, sieve methods typically identify integers up to x without prime factors $\leq y$, where y is some fixed power[6] of x, though a significantly smaller power than ½. Jing-Run Chen used this *Selberg sieve* (amongst other things) to show that there are infinitely many primes p for which $p + 2$ has at most two prime factors. Selberg went on to note the parity principle, that his formulation of sieve problems could not easily distinguish between integers with an odd number of prime factors and integers with an even number of prime factors; so that some new ingredient is needed to prove that there are infinitely many twin primes.

6. Short gaps between primes

The prime number theorem tells us that there are $\sim x/\log x$ primes up to x, and so the average gap between primes up to x is $\sim \log x$. One might ask if there are gaps between consecutive primes that are significantly larger, or significantly smaller than the average? Writing $p_1 = 2, p_2 = 3, p_3 = 5, \ldots$ for the primes, we therefore ask whether

$$\limsup_{n \to \infty} \frac{p_{n+1} - p_n}{\log p_n} = \infty \qquad \text{and}$$

$$\liminf_{n \to \infty} \frac{p_{n+1} - p_n}{\log p_n} = 0\ ?$$

The first is quite easy to prove, simply by exhibiting long sequences of consecutive integers which have a small prime factor. The largest gaps known have size $c \log p_n \log\log p_n \log\log\log\log p_n / (\log\log\log p_n)^2$ for a certain constant $c > 0$; in the last 68 years only the value of c has been improved, and Paul Erdös offered $ 10,000 for a proof that one can let $c \to \infty$ in this result! It is conjectured that gaps get as large as $c'(\log p_n)^2$, for some $c' > 1$.

The second of the above questions, as to whether there are significantly smaller than average gaps between primes, resisted all attempts for much longer, indeed work on this question inspired the development of the *large sieve* (a tool which has had more success in giving estimates for the number of primes at the beginning of arithmetic progressions). Until recently the smallest gaps proved were little less than ¼ $\log p_n$, which seems rather pathetic given that we believe that there are infinitely many gaps of length 2! Even more, it has been almost forty years since Chen's result that there are infinitely many primes p for which $p + 2$ has at most two prime factors.

It therefore came as a surprise when in 2005, Dan Goldston, Janos Pintz and Cem Yıldırım [4] announced that they could finally show that there are small gaps between primes, indeed that $p_{n+1} - p_n \leq (\log p_n)^{1/2+\epsilon}$ infinitely often. As surprising as the result is, the proof is even more so, because it uses ideas that have been around sieve theory for fifty years, and because it seems to contradict the "parity principle" discussed above. Of course the methods are not *exactly* the sieve formulation of Selberg but close enough that this is completely unexpected.

These new methods do not seem to be quite strong enough to prove that there are infinitely many pairs of twin primes, though it is plausible that they might be developed to prove the slightly weaker statement that $p_{n+1} - p_n \leq B$ infinitely often, for some absolute constant B. (In fact this would follow from knowing that primes are well-distributed at the beginning of arithmetic progressions, in slightly shorter arithmetic progressions than those given by the large sieve.) An exciting possibility.

7. The distribution of primes and randomly selected matrices

Our table of the count of primes gives pretty good evidence that the expected number of primes up to x is about $\mathrm{Li}(x)$. So what is the variance? In other words, the average of $(\pi(x) - \mathrm{Li}(x))^2$. If we examine the appropriate modification of the explicit formula then we see that the terms here involve pairs of zeros of the Riemann zeta function, and when we average (i.e. integrate over a range of values of x) then the only terms that are significant are those in which the distance between the two zeros is small. Therefore, if we assume the Riemann Hypothesis and denote its zeros by $\frac{1}{2} \pm i\gamma_1$, $\frac{1}{2} \pm i\gamma_2$, $\frac{1}{2} \pm i\gamma_3, \ldots$ where $0 < \gamma_1 < \gamma_2 < \ldots$, then it is of interest to determine how frequently $\gamma_{n+k} - \gamma_n$ is small. In 1973 Montgomery [9] gave good evidence to suggest that this distribution function is something surprising – that the zeros are not spaced like the same number of randomly chosen points up to a given height, but rather according to a strikingly different function, one which suggests that the zeros of $\zeta(s)$ repel each other in comparison to randomly selected points: More concretely, the expected number of $m > n$ for which $\gamma_m - \gamma_n$ is no more than α times the average gap between zeros (up to this height) is

$$\int_0^\alpha \left\{1 - \left(\frac{\sin \pi t}{\pi t}\right)^2\right\} dt$$

Dyson was struck that Montgomery's distribution function for the $\gamma_{n+k} - \gamma_n$ is the same as that for the distribution of pairs of eigenvalues of randomly chosen matrices (something that one encounters studying energy levels in quantum chaos), and suggested that perhaps the statistics for zeros taken three or four (or more) at a time, indeed all the local spacing statistics, would be the same as for eigenvalues. Following wads of computational evidence by Odlyzko, good theoretical evidence was given for Dyson's suggestion in a landmark 1996 paper of Zeev Rudnick and Peter Sarnak [10].

Extrapolating, Sarnak guessed that perhaps the zeros of all zeta functions of interest satisfy the same local spacing statistics as randomly chosen matrices (of increasing dimension), where we "randomly choose" our matrices only from certain classical groups. Computer tests revealed a beguiling (highly conjectural) theory, and Nick Katz and Sarnak even proved a (weak) version of such a theory for finite field zeta functions.

Mathematical physicists led by Sir Michael Berry and Jon Keating have joined forced with experts on the zeta function to build a conjectural framework to better understand the many mysterious properties of $\zeta(s)$. It is perhaps fair to say that little has been proved unconditionally about $\zeta(s)$ as a consequence, but we do have a much better understanding now of many questions to do with zeros and the size of zeta functions.

8. Conclusion

It has been a wonderful new millenium for our understanding of the distribution of primes and better yet, we have seen exciting new methods (from additive combinatorics), prophetic new perspectives (from random matrices), and the development of a key method, sieves, well beyond where it appeared to be stuck (Friedlander and Iwaniec) and we have even seen that the parity problem, which had seemed to be a fundamental obstruction, is not and we have yet to really understand why not! There are surely further interesting times ahead, but we should always bear in mind that

"Mathematicians have tried in vain to discover some order in the sequence of prime numbers but we have every reason to believe that there are some mysteries which the human mind will never penetrate."
L. Euler (1770).

Acknowledgements:

I would like to thank John Friedlander, K. Soundararajan and the editors for their remarks on earlier drafts of this article.

Footnotes

[*] L'auteur est partiellement soutenu par une bourse de la Conseil de recherches en sciences naturelles et en génie du Canada.

[1] That is, an estimate which is correct up to a factor that → 1 as x → ∞.

[2] Where we truncate the sum to involve only those zeros with $|\mathrm{Im}(\rho)| \leq T$, at a cost of an error term $O(x(\log xT)^2/T)$.

[3] The Euler-Mascheroni constant γ is defined as $\lim_{n\to\infty} \{(1/1 + 1/2 + \ldots + 1/n) - \log n\}$.

[4] Though it has several features in common with the circle method.

[5] That is, $w(mn) = w(m)\,w(n)$ if $(m, n) = 1$

[6] Note that if all the prime factors of n are $> n^{1/3}$ then n has no more than two prime factors.

References

[1] Manindra Agrawal, Neeraj Kayal and Nitin Saxena, Primes in P, to appear in Ann. Math.

[2] Antal Balog, The prime k-tuplets conjecture on average., in "Analytic Number Theory" (eds. B.C. Berndt et. al), Birkhäuser, Boston. (1990), 165-204.

[3] John Friedlander and Henryk Iwaniec, The polynomial $X^2 + Y^4$ captures its primes., Ann. Math. 148 (1998), 945–1040.

[4] Dan Goldston, Janos Pintz and Cem Yıldırım, Primes in Tuples I, preprint: http://xxx.arxiv.org/math.NT/0508185

[5] Tim Gowers, A new proof of Szemerdi's Theorem for arithmetic progressions of length four, GAFA 8 (1998), 529 - 551.

[6] Andrew Granville, It is easy to determine whether a given integer is prime, Bull. Amer. Math. Soc 42 (2005), 3-38.

[7] Ben Green and Terence Tao, The primes contain arbitrarily long arithmetic progressions, preprint: http://xxx.arxiv.org/math.NT/0404188, to appear in Ann. Math.

[8] Roger Heath-Brown and Boris Moroz, Primes represented by binary cubic forms, Proc. London Math. Soc 84 (2002), 257-288.

[9] Hugh Montgomery, The Pair Correlation of Zeros of the Zeta Function, Proc. Symp. Pure Math. (Amer. Math. Soc., Providence) 24 (1973), 181-193.

[10] Zeev Rudnick and Peter Sarnak, Zeros of principal L-functions and random matrix theory, Duke Math. J. 81 (1996), 269-322.