Snapshots of modern mathematics
from Oberwolfach

№ 7/2013

The ternary Goldbach problem

Harald Helfgott

Leonhard Euler (1707–1783) – one of the greatest mathematicians of the eighteenth century and of all times – often corresponded with a friend of his, Christian Goldbach (1690–1764), an amateur and polymath who lived and worked in Russia, just like Euler himself. In a letter written in June 1742, Goldbach made a conjecture – that is, an educated guess – on prime numbers:

> *Es scheinet wenigstens, dass eine jede Zahl, die größer ist als* 2, *ein aggregatum trium numerorum primorum sey.*
>
> It seems [...] that every positive integer greater than 2 can be written as the sum of three prime numbers.

In this snapshot, we will describe to what extent the mathematical community has resolved Goldbach's conjecture, with some emphasis on recent progress.

1 Weak and strong Goldbach conjecture

In the time since Goldbach's original statement of his conjecture, its wording has changed to say "greater than 5" instead of "greater than 2", since we no longer consider 1 to be a prime number. It has long been customary to split this conjecture into two halves:

- The weak (or ternary) Goldbach conjecture, which states that every odd integer n greater than 5 can be written as the sum of three primes; for example: $11 = 3 + 3 + 5,\ 21 = 2 + 2 + 17$
- The strong (or binary) Goldbach conjecture, which states that every even integer n greater than 2 can be written as the sum of two primes. for example: $10 = 5 + 5,\ 36 = 13 + 23$

As their names suggest, the strong conjecture implies the weak one. (In order to express an odd number $n \geq 5$ as the sum of three primes, subtract 3 and obtain an even number $n - 3 \geq 2$. If the strong conjecture is true, we can express $n - 3$ as a sum of two primes p_1, p_2; thus, $n = (n - 3) + 3$ is the sum of the primes p_1, p_2 and 3. As Euler himself pointed out to Goldbach, the strong conjecture also implies (and is implied by) Goldbach's original statement.

The history of the problem can be looked up in [1, Ch. XVIII].

A brief summary: in the first half of the seventeenth century, René Descartes (1596-1650) made a statement similar to Goldbach's in a manuscript that would be published only posthumously (in 1901!). During the nineteenth century, there was some computational work (checking the conjecture for small integers by hand), but little real progress.

The strong conjecture is still out of reach. In 2013, I finished the proof of the weak Goldbach conjecture. I had worked on it for several years.

2 Proof of the weak Goldbach conjecture

The proof builds on the foundations laid at the beginning of the twentieth century by Hardy, Littlewood and Vinogradov. In 1937, Vinogradov proved [10] that the conjecture holds for all odd numbers larger than some constant C. (Hardy and Littlewood had already shown the same, under the assumption that the Generalized Riemann Hypothesis[1] (GRH) is true. The GRH is a long-standing standard conjecture that is still unproved.) Since then, the constant C has been specified and gradually improved, but the best (i.e., smallest) available

[1] More information on the Generalized Riemann Hypothesis can be found in the Snapshot "Dirichlet Series" (No. 6/2014).

 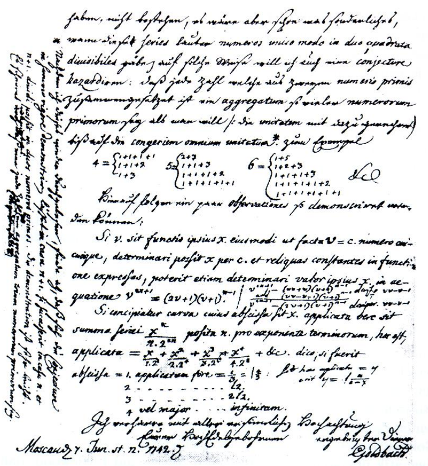

Figure 1: Euler and Goldbach's letter. It seems non-trivial to find a genuine portrait of Goldbach.

value of C was

$$C = e^{3100} \approx 2 \cdot 10^{1346}$$

(Liu-Wang [8]), which was way too large. We simply cannot hope to check the first 10^{1346} cases by computer – in fact, it is highly doubtful that any earthly or alien civilization that will ever exist could ever check, say, 10^{120} cases of any conceivable statement one by one: the number of picoseconds since the beginning of the universe is less than 10^{30}, whereas the number of protons in the observable universe is currently estimated at $\sim 10^{80}$, meaning that even parallel computing and galactic dictatorship wouldn't be enough.

I managed to bring C down to 10^{27}. The binary Goldbach conjecture had already been checked by computers up to $4 \cdot 10^{18}$ [9]; using that fact, one can check the ternary Goldbach conjecture up to 10^{27} in a few hours on a modern desktop computer. (In fact, D. Platt and I [6] had already checked it up to $8.8 \cdot 10^{30}$ on parallel computers.) This means the ternary (that is, weak) Goldbach conjecture is now proven for all (odd) integers.

It is clear why a brute-force computation can check a conjecture such as Goldbach's only for n smaller than some constant C: a computation has to be finite. But why would a mathematical proof ever give a bound valid only for n *larger* than a constant C?

3 Methods used to prove the theorem

This is in fact typical of *analytical* proofs, i.e., proofs using tools such as Calculus, Fourier analysis, etc. Such a proof usually tells you more than just the fact that an integer can be written in a certain way (here: as a sum of three primes). It actually gives you an estimate for the number of ways in which this is possible. The estimate takes the following form: the number of ways to write an integer n in a certain way is equal to a "main term" – some function $f(n)$ – and an "error term" – something that may be positive or negative, but whose absolute value is shown to be smaller than another function $g(n)$. If $f(n) > g(n)$, this shows that there is at least one way to write n as the sum of three primes.

Here is a highly simplified example: say you were able to prove an estimate with $f(n) = n^2$, $g(n) = 1000n^{3/2}$. Then we succeed when $f(n) > g(n)$, and this happens for all $n > C$, where $C = 10^6$.

This is what usually happens: one manages to show that $f(n)$ **is** larger than $g(n)$, but only once n gets large enough. The case of small n needs to be checked by hand (that is, by computer). The aim is thus to make the error term $g(n)$ as small as possible; this will make C smaller. (We can also "rig the game" (say, by giving a greater weight to some primes) so that the main term becomes larger relative to the error term; such "rigging" also presents other advantages, especially if the weights are continuous.)

What are the main analytical tools used? Some readers are familiar with Fourier analysis, i.e., the practice of decomposing a function f of time into sine waves of different frequencies. In fact, we do that every day, when we tune an analog radio, or when our brain picks up a musical note from several notes being played at the same time.

In fact, Fourier analysis is more general than that: f need not be a function of a continuous variable such as time. In particular, even if f is defined just on the integers, we can still decompose it into frequencies. It turns out to be natural to draw these frequencies on a circle and label them with real numbers from 0 to 1, just like, in the usual case, we put frequencies on a line and give them labels such as "88 Mhz" or "A = 440Hz". (This is why the general stategy we are describing is called the *circle method*.)

In our case, we can define f to be the function such that $f(n) = 1$ when n is a prime, and $f(n) = 0$ when n is not a prime. (In practice, we actually use a slightly more complicated version of this: we want $f(n)$ to decay continuously when n grows, for one thing.) Why would it be helpful to decompose such a function into functions of the form $n \mapsto \sin(2\pi\alpha n)$ or $n \mapsto \cos(2\pi\alpha n)$?

An additive problem, such as Goldbach's, can be restated in terms of *convolutions*. The (additive) convolution $g * h$ of two functions g, h is a new function constructed from g and h. At a number n, it is defined to be the sum of $g(m_1)h(m_2)$ over all pairs of integers m_1, m_2, such that $m_1 + m_2 = n$. In

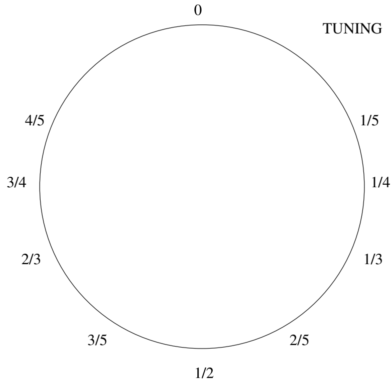

Figure 2: The dial in a true number theorist's radio.

formulas, this reads

$$(g * h)(n) = \sum_{m_1+m_2=n} g(m_1)h(m_2).$$

Thus, for the function f we just defined, if we showed that $(f * f)(n) > 0$, then this would imply that n can be written as the sum of two primes in at least one way, whereas if we show that $(f * f * f)(n) > 0$, this will imply that n can be written as the sum of three primes in at least one way[2].

One of the basic properties of a decomposition into frequencies is that a convolution behaves very nicely under such a decomposition: the *Fourier transform* of $g * h$ (that is, its decomposition into frequencies) is just the product of the Fourier transform of g and the Fourier transform of h. (A Fourier transform $\widehat{f}$ is a function from the space of frequencies (in our case, the circle) to the complex numbers; it tells you "how much" of $n \mapsto \sin(2\pi\alpha n)$ or $n \mapsto \cos(2\pi\alpha n)$ is present in f, i.e., the strength of what you hear when you set your radio's dial to α.)

It turns out that $\widehat{f}(\alpha)$ is particularly large when α is close to a rational number with small denominator (such as the numbers drawn in Figure 2). (This is, if you wish, analogous to how a radio signal gets strong when you move the dial close to the frequency of a radio station.) The bits of the circle close to such rational numbers are called *major arcs*; the rest is called *minor arcs*. Ever since Vinogradov, the basic idea has been to estimate $\widehat{f}(\alpha)$ as accurately as possible for α on the major arcs, and to show that it is small outside them. This then allows you to estimate an integral that you know is equal to $(f * f * f)(n)$.

[2] Can you figure out why that is?

This, incidentally, is the point at which the basic approach breaks down for the binary problem. Major arcs are called "major" not because they are large (they aren't) but because they make the major contribution to the integral of $\widehat{f}(\alpha)^3$ over the circle. If, instead, you are integrating $\widehat{f}(\alpha)^2$ (as you have to do when you are summing 2, rather than 3, primes), the contribution of the "major" arcs isn't major any longer – it gets overwhelmed by the integral of $|\widehat{f}(\alpha)|^2$ over the minor arcs: squaring amplifies peaks, but not nearly as much as cubing does. In order to go further, we would actually have to be able to estimate $\widehat{f}(\alpha)$ rather precisely on the minor arcs, and nobody yet knows how to do that.

4 Conclusion

This is the basic framework. What is new in my work? I had to redo the proof from scratch and find improvements in every part: the estimates for $\widehat{f}(\alpha)$ on the major arcs, the upper bounds on the minor arcs (the hardest part, from my perspective), and also the way in which the two are put together. Several of the techniques I had to improve or develop should be useful elsewhere in number theory or even in applied mathematics.

Some of this can be found in a longer, more detailed exposition I wrote a couple of months ago. The present text is partly based on that, with the difference that the mentioned text focuses on the novelties within the proof. The first version of that other exposition appeared in my blog (http://valuevar.wordpress.com); later versions were published (in Spanish and French) in [7] and [2]. The same exposition served as a basis for a more detailed article that will appear in the Proceedings of the International Conference of Mathematicians, in connection with my talk in Korea in August 2014. Go read any of these versions. Whoever wishes to get the full picture can read my papers [4], [3], [5], which I have tried to make as clear and readable as I could.

Image credits

Fig. 1 left image "Euclid". Licensed under Public domain via Wikimedia Commons,http://commons.wikimedia.org/wiki/File:Euclid.jpg, [Online; accessed 06-August-2014]

Fig. 1 right image "Christian Goldbach: Correspondance mathématique et physique de quelques célèbres géomètres du XVIIIème siècle (Vol. 1), St.-Pétersbourg 1843, p. 125âĂŞ129". Licensed under Public domain via Wikimedia Commons,http://commons.wikimedia.org/wiki/File:Letter_Goldbaxh-Euler.jpg, [Online; accessed 06-August-2014]

References

[1] L. E. Dickson, *History of the theory of numbers. Vol. I: Divisibility and primality.*, Chelsea Publishing Co., New York, 1966. MR 0245499 (39 #6807a)

[2] H. A. Helfgott, *La conjecture de Goldbach ternaire*, Preprint. To appear in *Gaz. Math.*

[3] ———, *Major arcs for Goldbach's problem*, Preprint. Available as http://arxiv.org/abs/1305.2897.

[4] ———, *Minor arcs for Goldbach's problem*, Preprint. Available as http://arxiv.org/abs/1205.5252.

[5] ———, *The Ternary Goldbach Conjecture is true*, Preprint. Available as http://arxiv.org/abs/1312.7748.

[6] H. A. Helfgott and D. Platt, *Numerical verification of ternary Goldbach*, To appear in *Exp. Maths.* Available as `arXiv:1305.3062`.

[7] H.A. Helfgott, *La conjetura débil de Goldbach*, Gac. R. Soc. Mat. Esp. **16** (2013), no. 4.

[8] M.-Ch. Liu and T. Wang, *On the Vinogradov bound in the three primes Goldbach conjecture*, Acta Arith. **105** (2002), no. 2, 133–175. MR 1932763 (2003i:11147)

[9] T. Oliveira e Silva, S. Herzog, and S. Pardi, *Empirical verification of the even goldbach conjecture, and computation of prime gaps, up to* $4 \cdot 10^{18}$, Accepted for publication in Math. Comp., 2013.

[10] I. M. Vinogradov, *Representation of an odd number as a sum of three primes*, Dokl. Akad. Nauk. SSR **15** (1937), 291–294.

Harald Helfgott *is a researcher at the École Normale Supérieur in Paris, France.*
helfgott@dma.ens.fr

Communicated by
Jörg Brüdern

Mathematical subjects
Algebra and Number Theory

Connections to other fields
Computer Science

DOI
10.14760/SNAP-2013-007-EN

Snapshots of modern mathematics from Oberwolfach are written by participants in the scientific program of the Mathematisches Forschungsinstitut Oberwolfach (MFO). The snapshot project is designed to promote the understanding and appreciation of modern mathematics and mathematical research in the general public world-wide. It is part of the mathematics communication project "Oberwolfach meets IMAGINARY" funded by the Klaus Tschira Foundation and the Oberwolfach Foundation. All snapshots can be found on www.imaginary.org.

Junior Editor
Lea Renner
junior-editors@mfo.de

Senior Editor
Dr. Carla Cederbaum
cederbaum@mfo.de

Mathematisches Forschungsinstitut
Oberwolfach gGmbH
Schwarzwaldstr. 9 – 11
77709 Oberwolfach
Germany

Director
Prof. Dr. Gerhard Huisken

Mathematisches Forschungsinstitut Oberwolfach
Member of the Leibniz Association
Klaus Tschira Stiftung gemeinnützige GmbH
KTS
oberwolfach FOUNDATION
IMAGINARY open mathematics