The ternary Goldbach problem

Harald Andrés Helfgott

October 2014

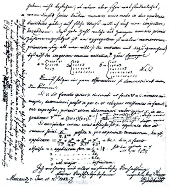
The ternary Goldbach problem: what is it? What was known?

From the letters of Leonhard Euler and Christian Goldbach:

Ternary, or weak, Goldbach conjecture (1742) ("three-prime problem"):
Every odd number $n > 5$ is the sum of three primes.

Binary, or strong, Goldbach conjecture (1742):
every even number $n > 2$ is the sum of two primes.

The strong conjecture implies the weak conjecture.



A little more history

Descartes (1630s? 1640s?) - Every integer $n \geq 1$ is the sum of one, two or three prime numbers (conjecture in a posthumously published manuscript).

XIXth century:
Goldbach's conjectures become widely known (sometimes under Waring's name).

The binary conjecture is checked at least until 10000.

This could have been used to check the ternary conjecture up to, say, 10^7: it is enough to construct a "ladder" of prime numbers $p_1, p_2, p_3, \ldots$ up to 10^7 with $p_{i+1} - p_i \leq 10000$.

The twentieth century, and now

Hardy-Littlewood (1922): There is a C such that every odd number $\geq C$ is the sum of three primes, if we assume the generalized Riemann hypothesis (GRH).
Vinogradov (1937): The same result, unconditionally.

News?

Theorem (Helfgott, May 2013)

Every odd number $n > 5$ is the sum of three primes.

Introduction
Fourier analysis
The circle method
The major arcs
The minor arcs
Conclusion

Bounds for more prime summands

We also know:
every $n > 1$ is the sum of $\leq K$ primes (**Schnirelmann, 1930**),
and after intermediate results by **Klimov (1969)** ($K = 6 \cdot 10^9$), **Klimov-Piltay-Sheptiskaya**, **Vaughan**, **Deshouillers (1973)**, **Riesel-Vaughan**…,
every even $n \geq 2$ is the sum of ≤ 6 primes (**Ramaré, 1995**)
every odd $n > 1$ is the sum of ≤ 5 primes (**Tao, 2012**).

Ternary Goldbach holds for all n conditionally on the generalized Riemann hypothesis (GRH) (**Deshouillers-Effinger-te Riele-Zinoviev, 1997**)

Ternary Goldbach: bounds for $n \geq C$

It is clear why computer bounds are for $n \leq c$, where c is a constant.

Why are analytic bounds for $n \geq C$, where C is a constant?

An analytic proof tells you that the number (or: weighted number) of ways to write n (here, an odd number) in a specified form (here, as the sum of 3 primes) is

$$\text{main term} + \text{error term},$$

where "main term" is some precise expression $f(n)$, and "error term" is something whose absolute value is at most $g(n)$. If $f(n) > g(n)$, we win.

Highly simplified example: say $f(n) = n^2$, $g(n) = 1000n^{3/2}$. Then we win for $n > C$, where $C = 10^6$.

To improve C, we must (a) make the error term $g(n)$ smaller, (b) rig the game (weights) so that $f(n)$ becomes larger.

Ternary Goldbach: improvements in C

Every odd $n \geq C$ is the sum of three primes (Vinogradov)

Bounds for C? $C = 3^{3^{15}}$ (Borozdkin, 1956), $C = 3.33 \cdot 10^{43000}$ (Wang-Chen, 1989), $C = 2 \cdot 10^{1346}$ (Liu-Wang, 2002).

Verification for small n:
every even $n \leq 4 \cdot 10^{18}$ is the sum of two primes (Oliveira e Silva, Herzog and Pardi, 2012);
together with a prime staircase, this implies every odd $5 < n \leq 8.875 \cdot 10^{30}$ is the sum of three primes (Helfgott-Platt, 2013).

We have a problem:
$8.875 \cdot 10^{30}$ is much smaller than $2 \cdot 10^{1346}$.
In fact, the number of protons and neutrons in the observable universe is just $\sim 10^{80}$.

We must bring C down from $2 \cdot 10^{1346}$ to $\sim 10^{30}$. I brought it down to 10^{27}.

Fourier series

A function $f : \mathbb{R} \to \mathbb{C}$ with $f(\alpha + 1) = f(\alpha)$ can be decomposed into a sum of sines and cosines:

$$f(\alpha) = \sum_n a_n e(\alpha n) = \sum_n a_n (\cos(2\pi\alpha n) + i \sin(2\pi\alpha n)),$$

where $e(t) = e^{2\pi i t}$.

Example: The sawtooth function

$$f(\alpha) = \begin{cases} \alpha - [\alpha] & \text{if } \{\alpha\} \in [0, 1/2], \\ [\alpha + 1] - \alpha & \text{if } \{\alpha\} \in [1/2, 1]. \end{cases}$$

can be written as

$$f(\alpha) = \sum_{n \text{ odd}} \frac{e(\alpha n)}{\pi^2 n^2} = \sum_{n \text{ odd}} \frac{1}{\pi^2 n^2} \cdot \cos(2\pi\alpha n).$$

How to determine a_n? Fourier inversion theorem:

$$a_n = \int_0^1 f(\alpha) e(\alpha n) d\alpha.$$

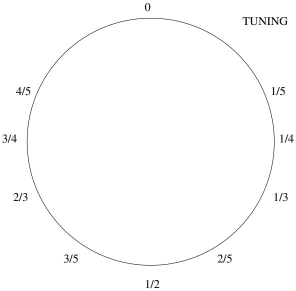
Fourier analysis: the other way around

What happens if we have a function $f : \mathbb{Z} \to \mathbb{C}$? We can then write it as an *integral*:

$$\int_0^1 \widehat{f}(\alpha) e(-\alpha n) d\alpha.$$

Here the coefficients $\widehat{f}(\alpha)$ are given by a Fourier inversion theorem:

$$\widehat{f}(\alpha) = \sum_n f(n) e(-\alpha n).$$



The circle method

The study of $f(n)$ through the study of $\widehat{f}(\alpha)$ is called the *circle method*, because $e(\alpha) = e^{2\pi i\alpha}$ goes around the circle when α goes from 0 to 1.

Why is this useful for additive problems? Convolution:

$$(f_1 * f_2)(n) = \sum_{\substack{m_1,m_2 \\ m_1+m_2=n}} f_1(m_1) f_2(m_2).$$

Easy to prove that

$$\widehat{f_1 * f_2}(n) = \widehat{f_1}(n)\widehat{f_2}(n).$$

We can have $(f_1 * f_2 * f_3)(n) \neq 0$ only if $n = m_1 + m_2 + m_3$ for some m_1, m_2, m_3 with $f_1(m_1), f_2(m_2), f_3(m_3) \neq 0$. So: define $f_i(m)$ so that it is $\neq 0$ only for m prime.

The circle method, continued

Hardy and Littlewood used $f_i(n) = f(n)$, where $f(n) = 0$ for n composite (or $n \leq 0$) and $f(n) = (\log n)e^{-n/N}$ (where N will be set later) for n prime. A factor such as $e^{-n/N}$ is needed for fast decay; choice of $e^{-n/N}$ very clever (though not best). Factor of $\log n$ useful for technical reasons (inverse of density of primes).

Our task is to show $(f * f * f)(n) \neq 0$ for $n > C$ ($C \sim 10^{30}$), since this implies that there are m_1, m_2, m_3 with $m_1 + m_2 + m_3 = n$ and $f(m_1), f(m_2), f(m_3) \neq 0$ (and thus m_1, m_2, m_3 prime).

$$(f{*}f{*}f)(n) = \int_0^1 \widehat{f * f * f}(\alpha) e(\alpha n) d\alpha = \int_0^1 (\widehat{f}(\alpha))^3 e(\alpha n) d\alpha.$$

Task: show this last integral is > 0.

Introduction
Fourier analysis
The circle method
The major arcs
The minor arcs
Conclusion

The basic strategy in the circle method

It will turn out that $\widehat{f}(\alpha)$ is large when α is close to a rational a/q with q small.

Idea: estimate $\widehat{f}(\alpha)$ for α in the union $\mathfrak{M}$ of intervals around rationals with small denominators (*major arcs*); bound $\widehat{f}(\alpha)$ for α outside the major arcs (here $\mathfrak{m} = [0,1] \setminus \mathfrak{M}$ is called the *minor arcs*); show that the bound on the integral over $\mathfrak{m}$ is smaller than a lower bound on the integral over $\mathfrak{M}$, thus showing that

$$\int_0^1 (\widehat{f}(\alpha))^3 e(\alpha n) d\alpha \geq \int_{\mathfrak{M}} (\widehat{f}(\alpha))^3 e(\alpha n) d\alpha - \int_{\mathfrak{m}} \left|\widehat{f}(\alpha)\right|^3 d\alpha > 0.$$

(This is what can't be done for binary Goldbach: the integral over $\mathfrak{m}$ is then bigger.)

The major arcs

To estimate $\int_{\mathfrak{M}} (\widehat{f}(\alpha))^3 e(-N\alpha)$, we need to estimate $\widehat{f}(\alpha)$ for α near a/q, q small ($q \leq m(x)$).

We do this by studying $L(s,\chi)$ for Dirichlet characters mod q, i.e., characters $\chi : (\mathbb{Z}/q\mathbb{Z})^* \to \mathbb{C}$.

$$L(s,\chi) := \sum_n \chi(n) n^{-s}$$

for $\Re(s) > 1$; this has an analytic continuation to all of $\mathbb{C}$ (with a pole at $s = 1$ if χ is trivial).
We express $\widehat{f}(\alpha)$, $\alpha = a/q + \delta/x$, as a sum of

$$S_{\eta,\chi}(\delta/x, x) = \sum_{n=1}^{\infty} \Lambda(n)\chi(n)e(\delta n/x)\eta(n/x)$$

for χ varying among all Dirichlet characters modulo q.

The explicit formula

"Explicit formula":

$$S_{\eta,\chi}(\delta/x, x) = [F_\delta(1)x] - \sum_\rho F_\delta(\rho)x^\rho + \text{small error},$$

(a) the term $F_\delta(1)x$ appears only for χ principal ($\sim$ trivial),
(b) ρ runs over the complex numbers ρ with $L(\rho, \chi) = 0$ and $0 < \Re(\rho) \leq 1$ (called "non-trivial zeroes"),
(c) F_δ is the Mellin transform of $\eta(t) \cdot e(\delta t)$.

Mellin transform of a function f:

$$\mathcal{M}f = \int_0^\infty f(x)x^{s-1}dx.$$

Analytic on a strip $x_0 < \Re(s) < x_1$ in $\mathbb{C}$.

It is a Laplace transform (or Fourier transform!) after a change of variables.

Where are the zeroes of $L(s,\chi)$?

Let $\rho = \sigma + it$ be any non-trivial zero of $L(s,\chi)$.

What we believe:
$\sigma = 1/2$ (Generalized Riemann Hypothesis (HRG))

What we know:
$\sigma \leq 1 - \frac{1}{C \log q|t|}$ (classical zero-free region (**de la Vallée Poussin**, 1899), C explicit (McCurley 1984, Kadiri 2005)

There are zero-free regions that are broader asymptotically (**Vinogradov-Korobov**, 1958) but narrower, i.e., worse, in practice.

What we can also know:
for a given χ, we can verify GRH for $L(s,\chi)$ "up to a height T_0". This means: verify that every zero ρ with $|\Im(\rho)| \leq T_0$ satisfies $\sigma = 1/2$.

Verifying GRH up to a given height

For the purpose of proving strong bounds that solve ternary Goldbach, zero-free regions are far too weak. We must rely on verifying GRH for several $L(s,\chi)$, $|t| \leq T_0$.

For χ trivial ($\chi(x) = 1$), $L(s,\chi) = \zeta(s)$. The Riemann hypothesis has been verified up to $|t| \leq 2.4 \cdot 10^{11}$ (**Wedeniwski** 2003), $|t| \leq 1.1 \cdot 10^{11}$ (**Platt** 2012, rigorous), $|t| \leq 2.4 \cdot 10^{12}$ (**Gourdon-Demichel** 2004, not duplicated to date).

For χ mod q, $q \leq 10^5$, GRH has been verified up to $|t| \leq 10^8/q$ (**Platt** 2011) rigorously (interval arithmetic).

This has been extended up to $q \leq 2 \cdot 10^5$, q odd, and $q \leq 4 \cdot 10^5$, q even ($|t| \leq 200 + 7.5 \cdot 10^7/q$) (**Platt** 2013).

How to use a GRH verification

We recall we must estimate $\sum_\rho F_\delta(\rho) x^\rho$, where F_δ is the Mellin transform of $\eta(t)e(\delta t)$.

If we checked GRH for $|t| \leq H$: the contribution of x^ρ, $\Im(\rho) \leq H$, is tiny ($|x^\rho| = \sqrt{x}$). For $|t| > H$, we need $F_\delta(\rho)$ to be tiny.

For $\eta(t) = e^{-t}$, the Mellin transform of $\eta(t)e(\delta t)$ is

$$F_\delta(s) = \frac{\Gamma(s)}{(1 - 2\pi i \delta)^s}.$$

Behaves like $|F_0(s)| \sim e^{-(\pi/2)|t|}$ for δ small and like $\eta(|t|/2\pi|\delta|) = e^{-|t|/2\pi|\delta|}$ for δ large. Problem: $e^{-|\tau|/2\pi\delta}$ does not decay very fast for δ large!

The Gaussian smoothing

Motivation for $\eta(t) = e^{-t}$ (Hardy-Littlewood)? The uncertainty principle tells us that η and its (Mellin) transform cannot both decay faster than exponentially. However, the Gaussian $\eta(t) = e^{-t^2/2}$ has faster than exponential decay, and its Mellin transform decays exponentially ($e^{-\pi|t|/4}$). We use this η.

The Mellin transform F_δ is then a parabolic cylinder function. Estimates in the literature weren't fully explicit (but: see Olver). Using the saddle-point method, I have given fully explicit upper bounds.

The main term in $F_\delta(\sigma + i\tau)$ behaves as

$$e^{-\frac{\pi}{4}|\tau|}$$

for δ small, $\tau \to \pm\infty$, and as

$$e^{-\frac{1}{2}\left(\frac{|\tau|}{2\pi\delta}\right)^2}$$

for δ large, $\tau \to \pm\infty$.

Major arcs: conclusions

Thus we obtain estimates for $S_{\eta,\chi}(\delta/x, x)$, where

$$\eta(t) = g(t)e^{-t^2/2},$$

and g is any "band-limited" function:

$$g(t) = \int_{-R}^{R} h(r)t^{-ir}\,dr$$

where $h : [-R, R] \to \mathbb{C}$. However: valid only for $|\delta|$ and q bounded!

All the rest of the circle must be minor arcs; $m(x)$ must be a constant M. (Writer for *Science*: "Muenster cheese" rather than "Swiss cheese".)
Thus, minor-arc bounds will have to be very strong.

The new bound for minor arcs

Theorem (Helfgott, May 2012 – March 2013)

Let $x \geq x_0$, $x_0 = 2.16 \cdot 10^{20}$. Let $2\alpha = a/q + \delta/x$, $\gcd(a,q) = 1$, $|\delta/x| \leq 1/qQ$, where $Q = (3/4)x^{2/3}$. Let $\eta_2(n) = 4(1_{[1/2,1]} * 1_{[1/2,1]})$. If $q \leq x^{1/3}/6$, then $|S_{\eta_2}(\alpha, x)|/x$ is less than

$$\frac{R_{x,\delta_0 q}(\log \delta_0 q + 0.002) + 0.5}{\sqrt{\delta_0 \phi(q)}} + \frac{2.491}{\sqrt{\delta_0 q}}$$

$$+ \frac{2}{\delta_0 \phi(q)} \left(\log \delta_0^{7/4} q^{13/4} + \frac{80}{9}\right)$$

$$+ \frac{2}{\delta_0 q} \left(\log q^{\frac{80}{9}} \delta_0^{\frac{16}{9}} + \frac{111}{5}\right) + 3.2 x^{-1/6},$$

where $\delta_0 = \max(2, |\delta|/4)$,

$$R_{x,t_1,t_2} = 0.4141 + 0.2713 \log \left(1 + \frac{\log 4t_1}{2 \log \frac{9x^{1/3}}{2.004 t_2}}\right).$$

Worst-case comparison

Let us compare the results here (2012-2013) with those of Tao (Feb 2012) for q highly composite, $|\delta| < 8$:

q_0	$\frac{\lvert S_\eta(a/q,x)\rvert}{x}$, HH	$\frac{\lvert S_\eta(a/q,x)\rvert}{x}$, Tao
10^5	0.04521	0.34475
$1.5 \cdot 10^5$	0.03820	0.28836
$2.5 \cdot 10^5$	0.03096	0.23194
$5 \cdot 10^5$	0.02335	0.17416
10^6	0.01767	0.13159
10^7	0.00716	0.05251

Table: Upper bounds on $x^{-1}|S_\eta(a/2q, x)|$ for $q \geq q_0$, $2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13|q$, $|\delta| \leq 8$, $x = 10^{25}$. The trivial bound is 1.

Need to do a little better than $1/2 \log q$ to win.
Meaning: GRH verification needed only for $q \leq 1.5 \cdot 10^5$, q odd, and $q \leq 3 \cdot 10^5$, q even. Yes, we have that.

The new bounds for minor arcs: ideas

Qualitative improvements:

- cancellation within Vaughan's identity
- $\delta/x = \alpha - a/q$ is a friend, not an enemy:
  In type I: (a) decrease of $\widehat{\eta}$,
  change in approximations;
  In type II: scattered input to the large sieve
- relation between the circle method and the large sieve – in its version for primes;
- the benefits of a continuous η (also in Tao, Ramaré),

Introduction
Fourier analysis
The circle method
The major arcs
The minor arcs
Conclusion

Cancellation within Vaughan's identity

Vaughan's identity:

$$\Lambda = \mu_{\leq U} * \log - \Lambda_{\leq V} * \mu_{\leq U} * 1 + 1 * \mu_{>U} * \Lambda_{>V} + \Lambda_{\leq V},$$

where $f_{\leq V}(n) = f(n)$ if $n \leq V$, $f_{\leq V}(n) = 0$ if $n > V$. (Four summands: type I, type I, type II, negligible.)
This is a gambit:

- Advantage: flexibility – we may choose U and V;
- Disadvantage: cost of two factors of log. (Two convolutions.)

We can recover at least one of the logs*.*
Alternative would have been: use a log-free formula (e.g. Daboussi-Rivat); proceeding as above seems better in practice.

How to recover factors of log

In type I sums:
We use cancellation in $\sum_{n \leq M : d|n} \mu(n)/n$.
This is allowed: we are using only ζ, not L.
This is explicit: **Granville-Ramaré**, **El Marraki**, **Ramaré**.

Vinogradov's basic lemmas on trigonometric sums get improved.

In type II sums:
Proof of cancellation in $\sum_{m \leq M} (\sum_{d > U : d|m} \mu(d))^2$, even for U almost as large as M.

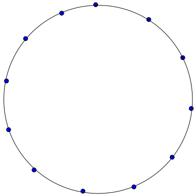
Application of the large sieve for primes.

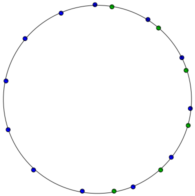
The "error" $\delta/x = \alpha - a/q$ is a friend

In type II:

- $\widehat{\eta}(\delta) \ll 1/\delta^2$ (so that $|\eta''|_1 < \infty$),
- if $\delta \neq 0$, there has to be another approximation a'/q' with $q' \sim x/\delta q$; use it.

In type II: the angles $m\alpha$ are separated by $\geq \delta/x$ (even when $m \geq q$). We can apply the large sieve to *all* $m\alpha$ in one go. We can even use prime support: double scattering, by δ and by **Montgomery**'s lemma.





Introduction

Fourier analysis

The circle method

The major arcs

The minor arcs

Conclusion

Final result

All goes well for $n \geq 10^{27}$ (or well beneath that). As we have seen, the case $n \leq 10^{27}$ (and in fact $n \leq 8.8 \cdot 10^{30}$) is already done (computation).

Theorem (Helfgott, May 2013)

Every odd number $n \geq 7$ is the sum of three prime numbers.