ELECTRONIC RESEARCH ANNOUNCEMENTS
OF THE AMERICAN MATHEMATICAL SOCIETY
Volume 3, Pages 99–104 (September 17, 1997)
S 1079-6762(97)00031-0

A COMPLETE VINOGRADOV 3-PRIMES THEOREM UNDER THE RIEMANN HYPOTHESIS

J.-M. DESHOUILLERS, G. EFFINGER, H. TE RIELE, AND D. ZINOVIEV

(Communicated by Hugh Montgomery)

Abstract. We outline a proof that if the Generalized Riemann Hypothesis holds, then every odd number above 5 is a sum of three prime numbers. The proof involves an asymptotic theorem covering all but a finite number of cases, an intermediate lemma, and an extensive computation.

1. Introduction

By "The 3-Primes Problem," we mean: *can every odd number greater than* 5 *be written as a sum of three prime numbers?* This problem was first successfully attacked by Hardy and Littlewood in their seminal 1923 paper [6]; using their *Circle Method* and assuming a "Weak Generalized Riemann Hypothesis," they proved that every sufficiently large odd number could be so written. The second author has calculated [4] directly from that paper that "sufficiently large," assuming the "full" Generalized Riemann Hypothesis (GRH below, i.e., that all non-trivial zeros of all Dirichlet L-functions have real part equal to $1/2$), is approximately 10^{50}. In 1926 Lucke [11], in an unpublished doctoral thesis under Edmund Landau, had already shown that with some refinements the figure could be taken as 10^{32}.

In 1937 Vinogradov [15] used his ingenious methods for estimating exponential sums to establish the desired asymptotic result while avoiding the GRH entirely. However, the numerical implications of avoiding the GRH are substantial: in 1956 Borodzkin [1] showed that sufficiently large in Vinogradov's proof meant numbers greater than $3^{3^{15}} \approx 10^{7000000}$. This figure has since been improved significantly, most recently by Chen and Wang [2], who have established a bound of 10^{43000}, but in any case this figure is far beyond hope of "checking the remaining cases by computer."

If, however, we return to the original stance of Hardy and Littlewood by assuming the truth of the GRH while at the same time using some of the refined techniques of primarily Vinogradov and Linnik [10], and using an extensive computer search, we do indeed arrive at the following:

Theorem. *Assuming the GRH, every odd number greater than* 5 *can be expressed as a sum of three prime numbers.*

Received by the editors February 26, 1997.
1991 *Mathematics Subject Classification.* Primary 11P32.
Key words and phrases. Goldbach, Vinogradov, 3-primes problem, Riemann hypothesis.

The proof of this result falls naturally into three parts: an asymptotic theorem handling all but a finite number of cases, a lemma assuring the existence of primes relatively near unchecked odd numbers, and a computer search for 2-*primes* representations of the remaining differences. We now outline each of these parts.

2. The asymptotic theorem

Theorem (Zinoviev)**.** *Assuming the GRH, every odd number greater than* 10^{20} *is a sum of three prime numbers.*

We discuss here briefly the main ideas behind this result; for complete details see [16].

Fix $N \geq 9$. We are interested in the number of triples (p_1, p_2, p_3) of prime numbers which satisfy the equation

$$N = p_1 + p_2 + p_3. \tag{1}$$

Following [10] we introduce the function

$$J(N) = \sum_{p_1+p_2+p_3=N} \log(p_1)\log(p_2)\log(p_3),$$

where the sum ranges over all triples of primes (≥ 2). If $J(N) > 0$ then there is at least one solution of (1). Here by $\Lambda(n)$ (n is always a natural number) we denote von Mangoldt's function: $\Lambda(n) = \log(p)$ if $n = p^k$ (p is prime), and $\Lambda(n) = 0$ otherwise. For any real number α set

$$S(\alpha) = \sum_{n>1} \Lambda(n) e^{-2\pi i \alpha n} e^{-n/N}.$$

Then we have

$$S(\alpha) = \sum_{p>1} \log(p) e^{-2\pi i \alpha p} e^{-p/N} + \theta N^{0.5} \log^2(N),$$

where $|\theta| \leq 1$. Clearly, for any integer m

$$\int_0^1 e^{2\pi i \alpha m} d\alpha = \begin{cases} 1 & \text{if } m = 0, \\ 0 & \text{if } m \neq 0. \end{cases}$$

Changing the order of summation and integration (see [10]), for some new real θ ($|\theta| \leq 1$) we obtain

$$J(N) = e \int_{-w}^{1-w} S^3(\alpha) e^{2\pi i \alpha N} d\alpha + \theta N^{1.5} \log^3(N),$$

where $w = w(N)$ is a small number defined later. We will express $J(N)$ as a sum of the leading term and the remainder. Estimating the remainder from above, we will show that it is less than the leading term when $N \geq 10^{20}$. We then conclude that $J(N) > 0$.

Following Linnik and Vinogradov, we subdivide the interval $[-w, 1-w]$ into the disjoint union of subsets E_1', E_1'', E_2. Our main idea is to refine this subdivision. In particular we change the set of "major arcs", which in our case is E_1', making the intervals from this set smaller. We do it as follows.

Let $Q = [1.1 \log^2(N)]$, $\tau = 4900 \log^4(N)$, $w = 1/\tau$.

Denote by $E(a,q)$ (where if $q>1$, then $(a,q)=1$, $0<a<q$, and if $q=1$, then $a=0$) the interval

$$\left[\frac{a}{q}-\frac{1}{q\tau},\ \frac{a}{q}+\frac{1}{q\tau}\right].$$

Then

$$[-w,1-w]=\bigcup_{0<q\le\tau}\ \bigcup_{\substack{0\le a<q\\(q,a)=1}}\left[\frac{a}{q}-\frac{1}{q\tau},\ \frac{a}{q}+\frac{1}{q\tau}\right].$$

Let $E_1=\{E(a,q),\ q\le Q\}$ and $E_2=[-w,1-w]-E_1$.

Finally, denote by E_1' the set of intervals E_1 with smaller length

$$\left[\frac{a}{q}-\frac{2\log(N)}{\phi(q)N},\ \frac{a}{q}+\frac{2\log(N)}{\phi(q)N}\right],$$

and set $E_1''=E_1-E_1'$.

We split the integral $J(N)$ into two integrals: over E_1' (the leading term) and $E_1''\cup E_2$ (the remainder). The following lemma is used to estimate the remainder term.

Lemma. *For any $\alpha\in E_1''\cup E_2$, and for any $N>10^{20}$ (not necessarily odd), GRH implies that*

$$|S(\alpha)|<0.18\,\frac{N}{\log(N)}.$$

The proof of this lemma uses the Riemann-Hadamard method which involves summation over the zeroes of L-functions.

The leading term is treated using the circle method of Hardy and Littlewood, as used by Vinogradov and Linnik.

3. An intermediate lemma

Now, by the asymptotic theorem, our problem is reduced to considering odd numbers which are $\le 10^{20}$. For these, we need the following:

Lemma. *If the GRH holds and if $6\le n\le 10^{20}$, then there exists a prime number p such that $4\le n-p\le 1.615\times 10^{12}$.*

Proof. The conclusion of the lemma obviously holds for $n<10^{12}$, say. For larger n, we apply Schoenfeld [13], equation (6.1). Let $\Theta(n)=\sum_{p\le n}\log p$; if the GRH holds, and if $n\ge 23\times 10^8$, we have

$$|\Theta(n)-n|<\frac{1}{8\pi}\sqrt{n}(\log n-2)\log n.$$

Just suppose that there is no prime in the interval $(n-h,n]$ except possibly for two of the six consecutive numbers from $n-5$ through n; then we have

$$2\log n>\Theta(n)-\Theta(n-h)=(\Theta(n)-n)-(\Theta(n-h)-(n-h))+h,$$

whence by the above,

$$h<\frac{1}{4\pi}\sqrt{n}(\log n-2)\log n+2\log n.$$

Since $n\le 10^{20}$, we get $h<1.615\times 10^{12}$. We conclude then that there must be a prime p such that $4\le n-p\le 1.615\times 10^{12}$. $\square$

We note here that the GRH actually implies an estimate on $|\Theta(n)-n|$ which has a *single* log factor; see Ivic [7] for example. However, the second author, in working through the details of such an estimate, found that the constant obtained was large enough so that, at the level $n = 10^{20}$, Schoenfeld's estimate gives a slightly better numerical result.

4. The computer search for 2-primes representations

Finally, then, if n is an odd number $\leq 10^{20}$ and p is as in the previous lemma, then $m = n - p$ is even and $\leq 1.615 \times 10^{12}$. But for m we have the following:

Theorem (Deshouillers and te Riele). *Every even number $4 \leq m \leq 10^{13}$ is a sum of two prime numbers.*

For a complete exposition of this and related results, see [3].

Let p_i be the ith odd prime number.

The usual approach [5], [14] to verify the Goldbach conjecture on a given interval $[a, b]$ is to find, for every even $e \in [a, b]$, the smallest odd prime p_i such that $e - p_i$ is a prime. An efficient way to do this is to generate the set of primes

$$\mathcal{Q}(a, b) = \{q \mid q \text{ prime and } a - \epsilon_a \leq q \leq b\},$$

where ϵ_a is chosen in a suitable way, and to generate the sets of even numbers $\mathcal{E}_0 \subset \mathcal{E}_1 \subseteq \mathcal{E}_2 \subseteq \cdots$, defined by $\mathcal{E}_0 = \emptyset$,

$$\mathcal{E}_{i+1} = \mathcal{E}_i \cup (\mathcal{Q}(a, b) + p_{i+1}), \ i = 0, 1, \ldots,$$ [1]

until $\mathcal{E}_j$ covers *all* the even numbers in the interval $[a, b]$ for some j. The set $\mathcal{Q}(a, b)$ is generated with the sieve of Eratosthenes: this is the most time-consuming part of the computation. For the choice of ϵ_a it is sufficient that ϵ_a exceeds the largest odd prime used in the generation of the sets $\mathcal{E}_j$. In the computations checking the Goldbach conjecture up to 4×10^{11} [14], the largest *small* odd prime needed was $p_{446} = 3163$ (this is the smallest prime p for which $244885595672 - p$ is prime).

A more efficient idea, which we have implemented, is to find, for every even $e \in [a, b]$, a prime q, close to a, for which $e - q$ is a prime. To do that efficiently, a set of k consecutive primes $q_1, q_2, \ldots, q_k$ close to a is generated, for suitably chosen k, and a large set $\mathcal{P}$ of all the odd primes up to about $b - a$ is precomputed (with the sieve of Eratosthenes) in order to check the numbers $e - q$ for primality. For the actual check of the interval $[a, b]$, we generate the sets of even numbers $\mathcal{F}_0 \subset \mathcal{F}_1 \subseteq \mathcal{F}_2 \subseteq \cdots$, defined by $\mathcal{F}_0 = \emptyset$,

$$\mathcal{F}_{i+1} = \mathcal{F}_i \cup (\mathcal{P} + q_{i+1}), \ i = 0, 1, \ldots,$$

until $\mathcal{F}_j$ covers *all* the even numbers in the interval $[a, b]$ for some j. In our experiments, we have chosen the intervals $[a, b]$ to have a fixed length of 10^8. The largest possible prime we may need in the set $\mathcal{P}$ lies close to $b - q_1$. By the prime number theorem, $q_1 \approx a - k \log a$, so that $b - q_1 \approx 10^8 + k \log a$. For the choice of k we notice that the density of the odd primes among the odd numbers up to 10^8 is about 0.115 (there are 5761454 odd primes below 10^8). This means that a proportion of about 0.885 of the even numbers in $[a, b]$ is *not* covered by the set $\mathcal{F}_1 = \mathcal{P} + q_1$; *if* the primes up to 10^8 were uniformly distributed, which they are *not*, a proportion of about 0.885^2 of the even numbers would not be covered by $\mathcal{F}_2$. After 151 steps, this proportion is reduced to below 10^{-8}. It turned out that $k = 360$ was sufficient

[1] By $\mathcal{Q}(a, b) + p_{i+1}$ we mean the set: $\{q + p_{i+1} | q \in \mathcal{Q}(a, b)\}$.

for our experiments. For $a \approx 10^{13}$ this implies that the largest prime in the set $\mathcal{P}$ must have a size close to $10^8 + 10^4$.

In the first approach, a *small* set of small primes up to 5000, say, has to be available, and for each interval $[a, b]$ to be treated, *all* the primes in $[a, b]$ have to be generated. In the second approach, a *large* set of small primes up to about 10^8+10^4 has to be generated (only once), and for each interval $[a, b]$ to be treated, one has to find the largest k primes $\leq a$. Of course, this is much cheaper than to find *all* the primes in the interval $[a, b]$. The price to pay is that for each $e \in [a, b]$ *some* prime p is found for which $e - p$ is prime, but in general this p is neither the smallest nor the largest such prime.

For the actual generation of k primes close to a we have used Jaeschke's computational results [8], stating that if a positive integer $n < 2152302898747$ is a strong pseudoprime with respect to the first five primes $2, 3, 5, 7, 11$, then n is prime; corresponding bounds for the first six and seven primes are 3474749660383 and 341550071728321, respectively.

We have implemented the second approach on a Cray C98 vector computer and verified the Goldbach conjecture for all even numbers $> 4 \times 10^{11}$ and $\leq 10^{13}$. After the generation of k primes near a, the actual verification was carried out by sieving with a long array of 64-bit integers called ODD, where each bit represents an odd number $< 10^8 + 10^4$, the bit being 1 if the corresponding odd number is prime, and 0 if it is composite. Generating $\mathcal{F}_{i+1}$ from $\mathcal{F}_i$ amounts to doing an "or" operation between one long array of integers and a shifted version of the array ODD. This can be carried out very efficiently on the Cray C98. In one typical run, we handled 5000 consecutive intervals of length 10^8. Close to 10^{13} the time to generate 5000×360 large primes was about 2600 CPU-seconds, and the total sieving time was about 5040 seconds. The total time used to cover the interval $[4 \times 10^{11}, 10^{13}]$ was approximately 53 (low priority) CPU-hours. The largest number of large primes which we needed was 328: for $e = 7379095622422$ and first prime $q_1 = 7378999992031$ it turned out that $e - q_i$ is composite for $i = 1, \ldots, 327$, and prime for $i = 328$ ($q_{328} = 7379000002739$ and $e - q_{328} = 95619683$).

Acknowledgment

The second author wishes to thank Paul T. Bateman and Marshall Ash for helpful correspondences on this topic.

References

1. K. G. Borodzkin, *On I. M. Vinogradov's constant*, Proc. 3rd All-Union Math. Conf., vol. 1, Izdat. Akad. Nauk SSSR, Moscow, 1956. (Russian) MR **20:**6973a
2. Jingrun Chen and Tianze Wang, *On the odd Goldbach problem*, Acta Math. Sinica **32** (1989), 702–718. MR **91e:**11108
3. Jean-Marc Deshouillers, Herman te Riele, and Yannick Saouter, *New experimental results concerning the Goldbach conjecture*, to appear.
4. Gove Effinger, *Some numerical implication of the Hardy and Littlewood analysis of the 3-primes problem*, submitted for publication.
5. A. Granville, J. van de Lune, and H. te Riele, *Checking the Goldbach conjecture on a vector computer*, Number Theory and Applications (R.A. Mollin, ed.), Kluwer Academic Publishers, 1989, 423–433. MR **93c:**11085
6. G. H. Hardy and L. E. Littlewood, *Some problems of 'Partitio Numerorum'. III: On the expression of a number as a sum of primes*, Acta Mathematica **44** (1922), 1–70.
7. A. Ivic, *The Riemann zeta-function*, J. Wiley and Sons, 1985. MR **87d:**11062

8. Gerhard Jaeschke, *On strong pseudoprimes to several bases*, Math. Comp. **61** (1993), 915–926. MR **94d:**11004
9. A. A. Karatsuba, *Basic analytic number theory*, Springer-Verlag, 1993. MR **94a:**11001
10. U. V. Linnik, *The new proof of Goldbach-Vinogradov's theorem*, Mat. Sb. **19** (1946), 3–8. MR **8:**317c
11. Bruno Lucke, *Zur Hardy-Littlewoodschen Behandlung des Goldbachschen Problems*, Doctoral Dissertation, Göttingen, 1926.
12. Paulo Ribenboim, *The book of prime number records*, Springer-Verlag, 1988. MR **89e:**11052
13. Lowell Schoenfeld, *Sharper bounds for the Chebyshev functions* $\Theta(x)$ *and* $\Psi(x)$, Mathematics of Computation **30** (1976), 337–360. MR **56:**15581b
14. Matti K. Sinisalo, *Checking the Goldbach conjecture up to* 4×10^{11}, Mathematics of Computation **61** (1993), 931–934. MR **94a:**11157
15. I. M. Vinogradov, *Representation of an odd number as a sum of three primes*, Comptes Rendues (Doklady) de l'Academy des Sciences de l'USSR **15** (1937), 191–294.
16. Dmitrii Zinoviev, *On Vinogradov's constant in Goldbach's ternary problem*, Journal of Number Theory, **65** (1997), 334–358.

Mathematiques Stochastiques, UMR 9936 CNRS-U.Bordeaux 1, U.Victor Segalen Bordeaux 2, F33076 Bordeaux Cedex, France
E-mail address: `dezou@u-bordeaux2.fr`

Department of Mathematics and Computer Science, Skidmore College, Saratoga Springs, NY 12866
E-mail address: `effinger@skidmore.edu`

Centre for Mathematics and Computer Science, P.O. Box 4079, 1009 AB Amsterdam, The Netherlands
E-mail address: `herman.te.riele@cwi.nl`

Memotec Communications, Inc., 600 Rue McCaffrey, Montreal, QC, H4T1N1, Canada
E-mail address: `zinovid@memotec.com`