Functiones et Approximatio
XXXVII (2007), 7–21

REFINEMENTS OF GOLDBACH'S CONJECTURE, AND THE GENERALIZED RIEMANN HYPOTHESIS

Andrew Granville

To Jean-Marc Deshouillers
on the occasion of his sixtieth birthday

Abstract: We present three remarks on Goldbach's problem. First we suggest a refinement of Hardy and Littlewood's conjecture for the number of representations of $2n$ as the sum of two primes positing an estimate with a very small error term. Next we show that if a strong form of Goldbach's conjecture is true then every even integer is the sum of two primes from a rather sparse set of primes. Finally we show that an averaged strong form of Goldbach's conjecture is equivalent to the Generalized Riemann Hypothesis; as well as a similar equivalence to estimates for the number of ways of writing integers as the sum of k primes.
Keywords: Goldbach, additive number theory, Riemann zeta function.

1. Three remarks on Goldbach's conjecture

In 1740 Goldbach conjectured, in a letter to Euler, that every integer > 1 is the sum of at most three primes. Euler replied that it would suffice to prove

Every even integer > 2 is the sum of two primes

and this is now known as "Goldbach's conjecture". Recently a publisher, seeking publicity for a new novel, offered a million dollars for its resolution, but the conjecture remains as open today as it ever has been. In 1922 Hardy and Littlewood [5] guesstimated, via a heuristic based on the circle method, an asymptotic for the number of representations of an even integer as the sum of two primes: Define

$$g(2N) = \#\big\{p, q \,\text{prime} : p + q = 2N\big\}.$$

Their conjecture is equivalent to $g(2N) \sim I(2N)$ where

$$I(2N) = C_2 \prod_{\substack{p \mid N \\ p>2}} \left(\frac{p-1}{p-2}\right) \int_2^{2N-2} \frac{dt}{\log t \log(2N-t)}$$

2001 Mathematics Subject Classification: 11P32, 11M26.

and C_2, the "twin prime constant", is defined by

$$C_2 = 2\prod_{p>2}\left(1-\frac{1}{(p-1)^2}\right) = 1.320323\ldots$$

We believe that a better guesstimate for $g(2N)$ is given by

$$I^*(2N) := I(2N)\left(1-\frac{4}{\sqrt{2N}}\prod_{p\geqslant 3}\left(1-\frac{(2N/p)}{p-2}\right)\right), \tag{1.1}$$

as we will discuss in Section 2; indeed it could well be that

$$g(2N) = I^*(2N) + O\left(\frac{\sqrt{N}}{\log N}\log\log N\right).$$

In analytic number theory it is usual to study the function $\sum_{p^k\leqslant x}\log p$ in place of $\sum_{p\leqslant x}1$ since this lends itself more naturally to complex analysis; and then to recover results about $\sum_{p\leqslant x}1$ by partial summation. Thus we introduce the function

$$G(2N) = \sum_{\substack{p+q=2N\\ p,q \text{ prime}}}\log p\,\log q.$$

The analysis of Hardy and Littlewood suggests that $G(2N)$, plus some terms corresponding to solutions of $p^k+q^l=2N$, should be very "well-approximated" by

$$J(2N) := C_2\prod_{\substack{p\mid N\\ p>2}}\left(\frac{p-1}{p-2}\right)\cdot 2N,$$

and the approximation $g(2N)\sim I(2N)$ is then deduced by partial summation. (In fact we believe that $G(2N) = J(2N)+O(N^{1/2+o(1)})$.) However this was done ignoring the contribution of solutions to $p^k+q^l=2N$. So, by including a suitable correction term to account for this (much like Riemann's "correction term" in estimating $\pi(x)$ which takes account of the contribution of squares of primes in the explicit formula), we obtain the guesstimate $I^*(2N)$ above.

If we believe that $G(2N)$ is always very well approximated by $J(2N)$ then, although this is too hard to prove, it may well be that some averaged form of this assertion is provable. In our first theorem we study the average of this difference.

Theorem 1A. *The Riemann Hypothesis is equivalent to the estimate*

$$\sum_{2N\leqslant x}(G(2N)-J(2N)) \ll x^{3/2+o(1)}.$$

Attempting to generalize this to find an equivalent to the generalized Riemann Hypothesis is not quite so simple.

Theorem 1B. *The Riemann Hypothesis for Dirichlet L-functions $L(s,\chi)$, over all characters $\chi \bmod m$ which are odd squarefree divisors of q, is equivalent to the estimate*

$$\sum_{\substack{2N\leqslant x\\ 2N\equiv 2 \,(\mathrm{mod}\, q)}} (G(2N) - J(2N)) \ll x^{3/2+o(1)}.$$

A similar result holds when the sum is over $2N \equiv a \,(\mathrm{mod}\, q)$ with $(a,q)=1$. Thus we only get a result for characters of squarefree conductor when we consider these "usual" arithmetic progressions mod q. However we can get a result involving all Dirichlet characters when we consider the arithmetic progression $0 \,(\mathrm{mod}\, q)$.

Theorem 1C. *The Riemann Hypothesis for Dirichlet L-functions $L(s,\chi), \chi \bmod q$ is equivalent to the conjectured estimate*

$$\sum_{\substack{2N\leqslant x\\ q\mid 2N}} G(2N) = \frac{1}{\phi(q)} \sum_{2N\leqslant x} G(2N) + O\left(x^{1+o(1)}\right). \tag{1.2}$$

However notice here that the main term is of size $\asymp_q x^2$ so the error term involves an amazing saving (that is, more than the "usual" $x^{1/2+o(1)}$), which is unsatisfying.

It is worth noting that similar results hold when trying to write integers as the sum of k primes: Define

$$G_k(n) = \sum_{p_1+p_2+\ldots+p_k=n} \log p_1 \log p_2 \ldots \log p_k$$

so that $G(n) = G_2(n)$. After Vinogradov we know asymptotics for this sum for each sufficiently large n, when $k \geqslant 3$ is given. In fact $G_k(n) \sim J_k(n)$ for each $n \equiv k \bmod 2$, where J_k is defined in Section 6. We prove the following.

Theorem 1D. *The Riemann Hypothesis is equivalent to the estimate*

$$\sum_{\substack{n\leqslant x\\ n\equiv k \,(\mathrm{mod}\, 2)}} (G_k(n) - J_k(n)) \ll x^{k-1/2+o(1)}.$$

Theorems 1A and 1D are based on the estimate, obtained after summation on the explicit formula for the number of primes up to x:

$$\sum_{n\leqslant x} G_k(n) = \frac{x^k}{k!} - k \sum_{\substack{\rho:\ \zeta(\rho)=0\\ |\mathrm{Im}\,\rho|\leqslant x}} \frac{x^{\rho+k-1}}{\rho(\rho+1)(\rho+2)\ldots(\rho+k-1)} + O(x^{k-2+2B+o(1)}) \tag{1.3}$$

where $B = \sup\{\mathrm{Re}\ \rho :\ \zeta(\rho)=0\}$.

The prime number theorem states that there are $\sim x/\log x$ primes $\leqslant x$ implying that there are $\sim x^2/2\log^2 x$ sums $p+q \leqslant x$ with p,q prime. Thus "on average" an even integer $n \leqslant x$ has $\sim x/\log^2 x$ representations as $p+q$ with p,q

prime. This is a lot of representations so one might think that finding at least one such representation would not be so difficult. In fact $I(2N) \geqslant C_2(2N)/\log^2(2N)$ for all $N \geqslant 4$, so we might expect that

$$g(2N) \geqslant C_2(2N)/\log^2(2N) \text{ for all } N \geqslant 2674.$$

Musing on the expected large number of representations of each even integer n as the sum of two primes, it seems likely that there must exist a relatively "thin" subset P of the primes such that every even integer is the sum of two primes in P. Define $P(x)$ to be the number of elements of P up to x. There are $\leqslant \left(P(x)^2 + P(x)\right)/2$ distinct pairs $p+q \leqslant x$ with $p, q \in P(x)$, so if every even integer is the sum of two primes in $P(x)$ then

$$x/2 - 1 \leqslant \left(P(x)^2 + P(x)\right)/2,$$

and thus $P(x) \geqslant \sqrt{x} - 1$ for $x \geqslant 4$. Our goal, then, is to show that if the Goldbach conjecture is true then there is such a set P with $P(x)$ "close" to $\sqrt{x}$ (note that if we take P to be the set of all primes then $P(x) \sim x/\log x$, which is much bigger than $\sqrt{x}$).

The Central Limit Theorem tells us that large sets of random choices, taken together, tend to converge to a predictable distribution, the "Bell curve". This extraordinary tendency allows us to use randomness in all sorts of surprising ways to prove results in "non-random" problems — This viewpoint was championed by Paul Erdös and discussed in detail in [1]. We use this here to prove:

Theorem 2. *Suppose that there exists a constant $\gamma > 0$ such that every even integer $n > 2$ can be written in more than $\gamma n/\log^2 n$ ways as $p+q$ with p, q prime. Then there exists a constant $\eta > 0$ such that there is an infinite set of primes P, with no more than $\eta\sqrt{x \log x}$ elements $\leqslant x$, such that every even integer n can be written as $p + q$ with $p, q \in P$.*

We shall show that there is such a "thin" set of primes P with this property, via a fairly simple application of the Central Limit Theorem. We also indicate, via probabilistic considerations, why we believe that any such set P must have $\liminf P(x)/\sqrt{x \log x} > 0$ Note that, "on average", an even integer n has about $\log n$ representations as $p + q$ with $p, q \in P$, far fewer than before.

Wirsing [16] showed that for any integer $k \geqslant 3$, there is a set of primes P, with $\ll (x \log x)^{1/k}$ elements $\leqslant x$, such that every integer $n \equiv k \bmod 2$ can be written as $p_1 + p_2 + \ldots + p_k$ with $p_1, p_2, \ldots, p_k \in P$. In fact our Theorem 2 follows from Wirsing's Theorem 1 (though was not observed by him)[1]. We were inspired to prove the above result after reading [15] on a related question, and before seeing [16].

This result is conditional (on Goldbach's Conjecture) and it is desirable to prove something like this unconditionally: By very similar methods we will prove the following:

[1] The right side of the hypothesis (8) in [15] should be "$M(x)x^{-1/k}$", not "$M(x)^{-1/k}$".

Theorem 3. *For any $\varepsilon > 0$ there exists a constant $\kappa_\varepsilon > 0$ such that there exists a set of primes P_ε with*

$$P_\varepsilon(x) \leqslant \kappa_\varepsilon \sqrt{x} \text{ for } x \text{ sufficiently large,}$$

for which all but at most εx even integers up to x can be written as $p+q$ with $p, q \in P_\varepsilon(x)$.

Letting $\varepsilon \to 0$ we can deduce the following

Corollary. *Let $g(x)$ be any function that $\to \infty$ as $x \to \infty$. There exists a set of primes P such that $P(x) \leqslant \sqrt{x} g(x)$ for x sufficiently large for which all but $o(x)$ even integers up to x can be written as $p+q$ with $p, q \in P(x)$.*

We will also try to justify our belief later that this cannot be improved.

Let us now review what is known, and what we need to know about Goldbach's problem, and about the Central Limit Theorem.

2. A brief history of Goldbach's problem: A refined conjecture

Computers have verified that every even integer $2n \leqslant 4 \cdot 10^{14}$ is the sum of two primes [12]. Chudakov [2], Van der Corput [13] and Estermann [4] showed in 1937 that "almost all" integers are the sum of two primes (that is, all but $o(x)$ up to x): In 1976 Montgomery and Vaughan [9] showed that the number of exceptions is $O(x^{1-c})$ for some $c > 0$, and recently Pintz [10] announced that one can take $c = 1/3$. In 1937 Vinogradov [14] showed that every sufficiently large odd integer is the sum of three primes; and in 1995 Ramaré [11] showed that every integer > 1 can be written as the sum of at most seven primes

The modern heuristic to obtain the constant $C_2 \prod_{\substack{p|N \\ p>2}} \frac{p-1}{p-2}$ in $I(2N)$ runs as follows: For each prime l, if we take integer p "at random" then the probability that l does not divide p is $1 - 1/l$; and similarly for q. However if we pick p "at random" and $q = 2N - p$ then l divides p or q if $p \equiv 0 \bmod l$ or $p \equiv 2N \bmod l$, respectively. So the probability that l does not divide either p or q is $1 - 2/l$ if $l \not| 2N$, and is $1 - 1/l$ if l divides $2N$. Therefore "the ratio" of these probabilities is, 2 if $l = 2$, and is

$$\frac{1-2/l}{(1-1/l)^2} \text{ times } \begin{cases} 1 & \text{if } l \not| 2N \\ (l-1)/(l-2) & \text{if } l | 2N, l \geqslant 3. \end{cases}$$

We will modify this to justify the refinement I^* of I, when approximating g. Let

$$E(2N) = \sum_{\substack{p^k + q^l = 2N \\ k,l \geqslant 1 \\ k+l \geqslant 3}} \log p \log q.$$

First note that

$$\sum_{\substack{p^k+q^l=2N\\ k\geqslant 3}} \log p\,\log q \leqslant \log^2 N\cdot \sum_{\substack{p^k\leqslant 2N\\ k\geqslant 3}} 1 \ll N^{1/3}\log^2 N,$$

and a similar argument works for $l\geqslant 3$. Also it is well-known that there are $N^{o(1)}$ pairs of integer p,q with $p^2+q^2=2N$. Thus

$$E(2N)=2\sum_{p+q^2=2N}\log p\,\log q\,+\,O(N^{1/3}\log^2 N).$$

Now, when we study solutions to $p+q^2=2N$ we find that l divides p if and only if $2N\equiv q^2 \bmod l$. Thus if $(2N/l)=0$ or -1 then l divides pq if and only if $q\equiv 0 \bmod l$. If $(2N/l)=1$ then there are 2 non-zero values of $q \bmod l$ for which l divides p, and we also need to count when l divides q. Therefore our factor is 2 if $l=2$, and

$$\frac{\left(1-\frac{2+(2N/l)}{l}\right)}{(1-1/l)^2}\ \text{times}\ \begin{cases}1 & \text{if}\quad l\not| 2N\\ (l-1)/(l-2) & \text{if}\quad l|2N, l\geqslant 3.\end{cases}$$

Now $\#\{m,n>0:\ m+n^2=2N\}=\sqrt{2N}+O(1)$ so we predict that

$$\sum_{p+q^2=2N}\log p\log q\sim \prod_{l\geqslant 3}\left(1-\frac{(2N/l)}{l-2}\right)C_2\prod_{\substack{p|2N\\ p>2}}\left(\frac{p-1}{p-2}\right)\sqrt{2N}.$$

and thus, after partial summation, that

$$2\sum_{\substack{p+q^2=2N\\ p,q\ \text{prime}}}1\sim 4\prod_{l\geqslant 3}\left(1-\frac{(2N/l)}{l-2}\right)C_2\prod_{\substack{p|2N\\ p>2}}\left(\frac{p-1}{p-2}\right)\ \frac{\sqrt{2N}}{\log^2(2N)}.$$

Subtracting this from $I(2N)$, we obtain the prediction $I^*(2N)$, as in (1.1). We can give the more accurate prediction

$$C_2\prod_{\substack{p|N\\ p>2}}\left(\frac{p-1}{p-2}\right)\int_2^{2N-2}\frac{1}{\log t\log(2N-t)}\left(1-\prod_{p\geqslant 3}\left(1-\frac{(2N/p)}{p-2}\right)\left(\frac{1}{\sqrt{t}}+\frac{1}{\sqrt{2N-t}}\right)\right)dt$$

with this method, though this is also significantly trickier to calculate.

One might guess that the distribution of

$$\frac{g(2N)-I^*(2N)}{\sqrt{I^*(2N)}}$$

looks Normal; though computer experiments with small $2N$ by me, and for larger $2N$ by Richstein, do not seem to justify this guess. It would be good to understand why not.

3. The Central Limit Theorem and the proofs of the Theorems

Let $X_1, X_2, \dots X_k$, be independent random variables and let $Y = X_1 + \dots + X_k$. Evidently $\mathbb{E}(Y) = \sum_{i=1}^k \mathbb{E}(X_i)$ and a simple computation reveals that the variance

$$\mathbb{V}(Y) := \mathbb{E}\Big(\big(Y - \mathbb{E}(Y)\big)^2\Big) = \sum_{i=1}^k \mathbb{V}(X_i).$$

Now $\mathbb{V}(X_i) = \mathbb{E}(X_i^2) - \mathbb{E}(X_i)^2$, so if X_i only takes values 0 or 1 then $X_i^2 = X_i$ so that $\mathbb{V}(X_i) = \mathbb{E}(X_i) - \mathbb{E}(X_i)^2 \leqslant \mathbb{E}(X_i)$.

The central limit theorem tells us that if $\mathbb{E}(Y) \to \infty$ as $k \to \infty$ then the probability that $Y \leqslant \mathbb{E}(Y) + \tau\sqrt{\mathbb{V}(Y)}$ tends to

$$\frac{1}{\sqrt{2\pi}} \int_{-\infty}^{\tau} e^{-t^2/2}\, dt,$$

a remarkable result.

In this paper we need explicit results for "small" k in the case that the X_i's only take values 0 or 1. In this case Chernoff's Theorem [1] is particularly useful:

$$\text{Prob}\Big(\big|Y - \mathbb{E}(Y)\big| > \tau\mathbb{E}(Y)\Big) \leqslant 2\exp\Big(-\kappa_\tau \mathbb{E}(Y)\Big) \tag{3.1}$$

where $\kappa_\tau = \min\big\{\tau^2/2, (1+\tau)\log(1+\tau) - 1\big\}$. In fact $\kappa_1 = \log(4/e)$ so that

$$\text{Prob}\big(Y = 0\big) \leqslant 2\big(e/4\big)^{\mathbb{E}(Y)}. \tag{3.2}$$

Using these results from probability we will deduce the following unconditional theorem from which we deduce Theorem 2.

Proposition 3.1. *For given $\gamma > 0$ define $\mathcal{N} = \mathcal{N}_\gamma = \{2n : g(2n) > 4\gamma n/\log^2(2n)\}$. There exists a constant $\eta = \eta_\gamma > 0$ such that there is an infinite set of primes P, with no more than $\eta\sqrt{x\log x}$ elements $\leqslant x$, such that every integer $n \in \mathcal{N}$ can be written as $p + q$ with $p, q \in P$.*

Theorem 2 follows immediately from Proposition 3.1. From the proof below we find that we can take $\eta = 4/\sqrt{\gamma} + o(1)$. As we noted in the introduction we expect that all sufficiently large $n \in \mathcal{N}$ when $\gamma = C_2/2$; and Theorem 2 would follow with $\eta = 8/\sqrt{2C_2} \approx 4.923057346$. (In fact Proposition 3.1 follows, more-or-less, from Corollary 2 of [16].)

Note that, by a strong form of the result of Chudakov/Van der Corput/Estermann, we know that almost all integers n belong to $\mathcal{N}$ if γ is sufficiently small.

In this section we define $P_n = \{ \text{ primes } p < n/2 : \ p \text{ and } n-p \text{ is prime}\}$ and so $\#P_n > \gamma n/\log^2 n + O(1)$ if $n \in \mathcal{N}_\gamma$.

Let $\theta(x)$ be a positive real-valued function such that $\theta(x)/\sqrt{x}$ is decreasing for sufficiently large x, with limit 0.

Let $\{w_p,\ p \text{ prime}\}$ be independent random variables with each $w_p = 0$ or 1, and

$$\text{Prob}(w_p = 1) = \theta(p)/\sqrt{p}.$$

For each $p \in P_n$ define $v_{n,p} = w_p w_{n-p}$ and note that these are independent random variables. We have

$$\mathbb{E}(v_{n,p}) = \mathbb{E}(w_p)\mathbb{E}(w_{n-p}) = \frac{\theta(p)}{\sqrt{p}}\,\frac{\theta(n-p)}{\sqrt{n-p}} \geqslant \left(\frac{\theta(n)}{\sqrt{n}}\right)^2$$

if p is sufficiently large (independent of n). Therefore for

$$Y_n = \sum_{p \varepsilon P_n} v_{n,p},$$

and $n \in \mathcal{N}$, we have

$$\mathbb{E}(Y_n) = \sum_{p \in P_n} \mathbb{E}(v_{n,p}) \geqslant \left(\frac{\theta(n)}{\sqrt{n}}\right)^2 \cdot \frac{\gamma n}{\log^2 n} + O(1) = \gamma\left(\frac{\theta(n)}{\log n}\right)^2 + O(1).$$

Proof of Proposition 3.1. Taking $\theta(x) = 2\left((\log^3 x)/\gamma\right)^{1/2}$ we get $\mathbb{E}(Y_n) \geqslant 4\log n + O(1)$ and so, by (3.1),

$$\text{Prob}(Y_n = 0) \ll (e/4)^{4\log n} \ll 1/n^{3/2}. \tag{3.3}$$

Thus

$$E_\theta := \mathbb{E}\big(\#\{n \in \mathcal{N}: Y_n = 0\}\big) \leqslant \sum_{n \in \mathcal{N}} \text{Prob}(Y_n = 0) \ll \sum_{n \geqslant 1} \frac{1}{n^{3/2}} \ll 1.$$

Note that

$$\text{Prob}\big(\#\{n \in \mathcal{N} : \ Y_n = 0\} > 100E_\theta\big) \leqslant 1/100.$$

Thus if we choose a set of primes P "at random" (where "at random" is according to our probabilities above) then there is a $\geqslant 99\%$ chance that no more than $100E_\theta$ elements of $\mathcal{N}$ are not the sum of two elements of P (and so there certainly exists such a set P). For such $n \in \mathcal{N}$, add p and q to P for some primes

p, q with $p+q=n$. Thus our new set of primes P' has the desired property; and $P' \setminus P$ is finite.

Next we wish to examine $P(x) = \#\{p \in P : p \leqslant x\}$: Let $W_x = \sum_{p \leqslant x} w_p$ so that

$$\mathbb{E}(W_x) = \sum_{p \leqslant x} \frac{\theta(p)}{\sqrt{p}} = \frac{2}{\sqrt{\gamma}} \sum_{p \leqslant x} \frac{(\log p)^{3/2}}{p^{1/2}} \sim 4\sqrt{\frac{x}{\gamma} \log x}$$

by the prime number theorem. By (3.1) we see that

$$W_x \ll \sqrt{x \log x}$$

with probability $1 - o(1)$ and thus Proposition 3.1 follows. ∎

Proof of Theorem 3. By the result of Chudakov/Van der Corput/Estermann we know that $\#\{n \in \mathcal{N} : n \leqslant x\} \sim x/2$. Let $\vartheta(x) = A \log x$ for some very large $A > 0$, in the argument above, so that $\mathbb{E}(Y_n) = \gamma A^2 + o(1)$, and thus $\text{Prob}\,(Y_n = 0) \ll (e/4)^{\gamma A^2}$ for each $n \in \mathcal{N}$. Therefore

$$\begin{aligned}\mathbb{E}\Big(\#\{n \leqslant x : \ Y_n = 0\}\Big) &\leqslant \#\{n \leqslant x : n \notin \mathcal{N}\} + \sum_{\substack{n \leqslant x \\ n \in \mathcal{N}}} \text{Prob}\,(Y_n = 0) \\ &\leqslant o(x) + O\Big(x\,(e/4)^{\gamma A^2}\Big),\end{aligned}$$

and so there certainly exist such sets P with

$$\#\{n \leqslant x : Y_n = 0\} \ll x(e/4)^{\gamma A^2}.$$

At the same time we note that

$$\mathbb{E}(W_x) = A \sum_{p \leqslant x} \frac{\log p}{\sqrt{p}} \sim 2Ax^{1/2}.$$

Thus in Theorem 3 we may take $\varepsilon \asymp (e/4)^{\gamma A^2}$ so that $\kappa_\varepsilon = 3A \asymp \sqrt{\log(1/\varepsilon)}$. ∎

4. Heuristic

Let W_n be independent random variables with each $W_n = 0$ or 1 and $\text{Prob}\,(W_n = 1) = \theta(n)/\sqrt{n}$. Let $\mathbb{Z}_n = \sum_{a+b=n} W_a W_b$. Then

$$\begin{aligned}\text{Prob}(\mathbb{Z}_n = 0) &= \prod_{1 \leqslant a \leqslant n/2} \text{Prob}(W_a W_{n-a} = 0) \\ &= \prod_{1 \leqslant a \leqslant n/2} \left(1 - \frac{\theta(a)}{\sqrt{a}} \frac{\theta(n-a)}{\sqrt{n-a}}\right)\end{aligned}$$

Now

$$\sum_{a\leqslant n-1}\left(\frac{\theta(a)\theta(n-a)}{\sqrt{a}\sqrt{n-a}}\right)^2 \leqslant \left(\max_{a\leqslant n}\theta(a)\right)^4 \sum_{a\leqslant n-1}\frac{1}{a(n-a)}$$
$$\ll \frac{\log n}{n}\max_{a\leqslant n}\big(\theta(a)\big)^4.$$

So if $\theta(a)=a^{o(1)}$,

$$\text{Prob}\,(\mathbb{Z}_n=0)\sim \exp\left(-\sum_{1\leqslant a<n/2}\frac{\theta(a)\theta(n-a)}{\sqrt{a(n-a)}}\right).$$

Suppose θ is non-decreasing and $\theta\left(n^{1-o(1)}\right)\sim\theta(n)$. Then it can be shown that

$$\sum_{1\leqslant a<n/2}\frac{\theta(a)\theta(n-a)}{\sqrt{a(n-a)}}\sim\frac{\pi}{2}\theta(n)^2 \text{ since } \int_0^{1/2}\frac{dt}{\sqrt{t(1-t)}}=\frac{\pi}{2}.$$

On the other hand

$$\mathbb{E}\left(\sum_{a\leqslant n}W_a\right)=\sum_{a\leqslant n}\frac{\theta(a)}{\sqrt{a}}\sim 2\,\theta(n)\sqrt{n}.$$

Therefore if we have a random set S of $\sim\kappa\sqrt{x}$ integers up to x, then we expect that about $e^{-\pi\kappa^2/8}x$ of the integers $n\leqslant x$ are not the sum of two elements of S. In particular we don't believe that the corollary can be improved.

Moreover we expect all but finitely many integers to be the sum of two elements of S provided

$$\sum_n \exp\left(-\frac{\pi}{2}\,\theta(n)^2\right) \text{ converges.}$$

This happens for $\theta(n)>\sqrt{\left(\frac{2}{\pi}+\varepsilon\right)\log n}$. So we doubt the consequence of Theorem 2 can be improved (though this suggests we must have $\eta>\sqrt{8/\pi}\approx 1.595769122$, whereas above we suggested we could take $\eta<4.923057346\ldots$ so there is still some room for improvement).

5. Goldbach and the Generalized Riemann Hypothesis

The explicit version of the prime number theorem gives a formula of the form

$$\sum_{p\leqslant x}\log p = x-\sum_{\substack{\rho\\ |\text{Im }\rho|\leqslant x}}\frac{x^\rho}{\rho}+O(\log^2 x),$$

where the sum is over zeros ρ of $\zeta(\rho)=0$ with $\mathrm{Re}(\rho)>0$. In Littlewood's famous paper [7] he investigates the sign of $\pi(x)-\mathrm{Li}(x)$ by a careful examination of a sum of the form $\sum_{\rho:\ |\mathrm{Im}\,\rho|\leqslant T}\mathrm{Li}(x^\rho)$, showing that this gets bigger than $x^{1/2-\varepsilon}$ for certain values of x, and smaller than $-x^{1/2-\varepsilon}$ for other values of x. His method can easily be modified to show that the above implies that

$$\max_{y\leqslant x}\left|\sum_{p\leqslant y}\log p-y\right|=x^{B+o(1)}$$

where $B=\sup\{\mathrm{Re}\,\rho:\zeta(\rho)=0\}$ (note that $1\geqslant B\geqslant 1/2$). By partial summation it is not hard to show that

$$\sum_{2N\leqslant x}G(2N)=\sum_{p+q\leqslant x}\log p\log q=\frac{x^2}{2}-2\sum_{\substack{\rho\\ |\mathrm{Im}\,\rho|\leqslant x}}\frac{x^{1+\rho}}{\rho(1+\rho)}+O(x^{2B+o(1)}) \tag{5.1}$$

so that, by Littlewood's method,

$$\max_{y\leqslant x}\left|\sum_{2N\leqslant y}G(2N)-\frac{y^2}{2}\right|=x^{1+B+o(1)}.$$

Therefore the Riemann Hypothesis ($B=1/2$) is equivalent to the conjectured estimate

$$\sum_{2N\leqslant x}G(2N)=\frac{x^2}{2}+O\left(x^{3/2+o(1)}\right). \tag{5.2}$$

This implies Theorem 1A since

$$\begin{aligned}\sum_{2n\leqslant x}J(2n)&=C_2\sum_{2n\leqslant x}2n\sum_{\substack{d\mid n\\ d\ \text{odd}}}\frac{\mu^2(d)}{\prod_{p\mid d}(p-2)}\\ &=2C_2\sum_{\substack{d\leqslant x/2\\ d\ \text{odd}}}\frac{\mu^2(d)}{\prod_{p\mid d}(p-2)}\sum_{\substack{n\leqslant x/2\\ d\mid n}}n\\ &=2C_2\sum_{\substack{d\leqslant x/2\\ d\ \text{odd}}}\frac{\mu^2(d)}{\prod_{p\mid d}(p-2)}\left(\frac{x^2}{8d}+O(x)\right)\\ &=\frac{x^2}{2}+O(x\log x).\end{aligned} \tag{5.3}$$

Going further we note that for any coprime integers $a,q\geqslant 2$

$$\sum_{\substack{p\leqslant x\\ p\equiv a\ (\mathrm{mod}\ q)}}\log p=\frac{1}{\phi(q)}\left(x-\sum_{\chi\ (\mathrm{mod}\ q)}\overline{\chi}(a)\sum_{\substack{\rho:L(\rho,\chi)=0\\ |\mathrm{Im}\,\rho|\leqslant x}}\frac{x^\rho}{\rho}\right)+O(\log^2(qx));$$

and thus

$$\max_{y\leqslant x}\Big|\sum_{\substack{p\leqslant y\\ p\equiv a \pmod q}}\log p-\frac{y}{\phi(q)}\Big|=x^{B_q+o(1)}, \tag{5.4}$$

where $B_q=\sup\{\operatorname{Re}\rho:\ L(\rho,\chi)=0 \text{ for some } \chi \pmod q\}$. R.C. Vaughan noted, in an exchange of email, that by the same methods but now using the above formula, we get a remarkable cancellation which leads to the explicit formula

$$\sum_{\substack{2N\leqslant x\\ q|2N}}G(2N)-\frac{1}{\phi(q)}\sum_{2N\leqslant x}G(2N)$$
$$=\frac{1}{\phi(q)}\sum_{\substack{\chi \pmod q\\ \chi\neq\chi_0}}\chi(-1)\sum_{\substack{\rho:L(\rho,\chi)=0\\ \sigma:L(\sigma,\overline{\chi})=0\\ |\operatorname{Im}\rho|,|\operatorname{Im}\sigma|\leqslant x}}c_{\rho,\sigma}\,x^{\rho+\sigma}+O(x\log^2(qx))$$

where $c_{\rho,\sigma}=\int_0^1\frac{1}{\rho}(1-t)^\rho\,t^{\sigma-1}\ dt$ is a constant depending only on ρ and σ (and note that $c_{\rho,\sigma}=c_{\sigma,\rho}$, integrating by parts, when $\operatorname{Re}\rho,\operatorname{Re}\sigma>0$). Thus Theorem 1C follows since $c_{\rho,\sigma}\leqslant(1/\rho)\int_0^1 t^{\sigma-1}dt=1/\rho\sigma$ and as $\sum_{|\operatorname{Im}\sigma|\leqslant x}1/\rho\ll\log^2(qx)$.

As in the proof of (5.3) we have

$$\sum_{\substack{2n\leqslant x\\ q|2n}}J(2n)=\frac{x^2}{2\phi(q)}+O(x\log x). \tag{5.5}$$

Now, Hardy and Littlewood showed that Generalized Riemann Hypothesis implies that

$$\sum_{2n\leqslant x}\Big|G(2n)-J(2n)\Big|^2\ll x^{5/2+o(1)}. \tag{5.6}$$

We expect, as we saw in section 2, that $G(2n)-J(2n)\ll n^{1/2+o(1)}$ and so we believe that

$$\sum_{2n\leqslant x}\Big|G(2n)-J(2n)\Big|^2\ll x^{2+\delta+o(1)} \tag{5.7}$$

for $\delta=0$. This implies, by Cauchy's inequality, that

$$\sum_{2n\leqslant x}G(2n)=\sum_{2n\leqslant x}J(2n)+O\left(x^{\frac{3+\delta}{2}+o(1)}\right)$$
$$=x^2/2+O\left(x^{(3+\delta)/2+o(1)}\right)$$

by (5.3), which implies the Riemann Hypothesis if $\delta=0$ (as after (5.2) above); and implies that $\zeta(\rho)\neq0$ if $\operatorname{Re}\rho>3/4$ if $\delta=1/2$ (that is, assuming Hardy and Littlewood's (5.6))

We find that (1.2) is too delicate to obtain the Riemann Hypothesis for $L(s,\chi), \chi \pmod q$ from (5.7). Instead we note that

$$\sum_{\substack{2N\leqslant x\\ 2N\equiv 2 \,(\mathrm{mod}\, q)}} G(2N) = c_q \left(\frac{x^2}{2} - 2 \sum_{\substack{m\mid q\\ m \ \text{odd}}} \frac{\mu(m)}{\prod_{\substack{p\mid m\\ p>2}} (p-2)} \sum_{\substack{\chi \bmod m\\ \chi \text{ primitive}}} \overline{\chi}(2) \sum_{\substack{\rho: L(\rho,\chi)=0\\ |\mathrm{Im}\,\rho|\leqslant x}} \frac{x^{\rho+1}}{\rho(\rho+1)} \right)$$

plus an error term $O(x^{2B_q+o(1)})$, where $c_q = \frac{(2,q)}{q} \prod_{\substack{p\mid q\\ p \,\text{odd}}} \frac{p(p-2)}{(p-1)^2}$. As in (5.3) one can show that

$$\sum_{\substack{2N\leqslant x\\ 2N\equiv 2 \,(\mathrm{mod}\, q)}} J(2N) = c_q \frac{x^2}{2} + O(x \log x),$$

so that

$$\sum_{\substack{2N\leqslant x\\ 2N\equiv 2 \,(\mathrm{mod}\, q)}} (G(2N) - J(2N)) = O(x^{1+C_q+o(1)})$$

where $C_q = \sup\{\mathrm{Re}\,\rho : L(\rho,\chi) = 0 \text{ for some } \chi \bmod m, \text{ where } m|q \text{ and } m \text{ is odd and squarefree}\}$. This implies Theorem 1B. By the above we see that if (5.7) holds with $\delta = 0$ then $C_q = 1/2$ and thus the Riemann Hypothesis follows for L-functions with squarefree conductor (this was also proved in unpublished work of Montgomery and Vaughan [8] in 1971 by somewhat different means). Surely one can obtain the Riemann Hypothesis for L-functions with other conductors by this method, though I have, as yet, been unable to do so.

6. Multi-sums

By methods similar to the previous section one can easily show (1.3) so that

$$\max_{y\leqslant x} \left| \sum_{n\leqslant y} G(n) - \frac{y^k}{k!} \right| = x^{k-1+B+o(1)}. \tag{6.1}$$

Therefore the Riemann Hypothesis is equivalent to the conjectured estimate

$$\sum_{n\leqslant x} G_k(n) = \frac{x^k}{k!} + O\left(x^{k-1/2+o(1)}\right).$$

To use the heuristic of Section 2 we note that

$$\begin{aligned} &\#\{a_1,\dots,a_k \bmod p :\ p \not| a_1\dots a_k \text{ and } a_1+\dots+a_k \equiv n \bmod p\} \\ &= \frac{(p-1)^k - (-1)^k}{p} + (-1)^k \delta_{n,0}, \end{aligned}$$

where $\delta_{i,j} = 1$ if $i = j$, and $= 0$ otherwise. Now define

$$C_k = 2 \prod_{p>2} \frac{(p-1)^k - (-1)^k}{(p-1)^k}.$$

If $n \not\equiv k \bmod 2$ then define $J_k(n) = 0$. If $n \equiv k \bmod 2$ then define

$$J_k(n) = C_k \frac{n^{k-1}}{(k-1)!} \prod_{\substack{p|n \\ p>2}} \left(1 + \frac{p(-1)^k}{(p-1)^k - (-1)^k}\right).$$

Let ε_d be a multiplicative function with $\varepsilon_p := p(-1)^k/((p-1)^k - (-1)^k)$. Then

$$\begin{aligned}\sum_{n \leqslant x} J_k(n) &= C_k \sum_{\substack{n \leqslant x \\ n \equiv k \bmod 2}} \frac{n^{k-1}}{(k-1)!} \sum_{\substack{d|n \\ d \text{ odd}}} \mu^2(d)\varepsilon_d \\ &= C_k \sum_{\substack{d \leqslant x \\ d \text{ odd}}} \mu^2(d)\varepsilon_d \left(\frac{x^k}{2d(k!)} + O(x^{k-1})\right) \\ &= C_k \frac{x^k}{2(k!)} \prod_{p>2} \left(1 + \frac{\varepsilon_p}{p}\right) + O(x^{k-1}) = \frac{x^k}{k!} + O(x^{k-1})\end{aligned}$$

for $k \geqslant 3$. We deduce Theorem 1D.

7. Concluding remark

Evidently $0 \leqslant g(2N) \leqslant 2\pi(2N) - \pi(N) - \pi(N-1)$. Goldbach's conjecture asserts that this lower bound in not attained for any $N > 1$, that is $g(2N) \neq 0$ for $N \geqslant 2$. We might also ask how often the upper bound is attained? One finds that this upper bound is attained for $2N = 210$ and Deshouillers, Narkiewicz, Pomerance and I proved [3] that this is the largest even integer for which this upper bound is obtained. It is with this collaboration in mind that I am happy to dedicate this further article on the Goldbach problem to Jean-Marc.

Acknowledgements. I would like to thank Dan Goldston and Bob Vaughan for useful email discussion concerning section 6; Joerg Richstein for doing the requested calculations from section 2; and the referee for pointing out the references [2] and [4].

References

[1] Noga Alon and Joel H. Spencer, *The Probabilistic Method*, Wiley 1992.
[2] N. Chudakov, *On Goldbach's problem* (Russian), Dokl. Akad. Nauk SSSR **17** (1937), 331–334.

[3] Jean-Marc Deshouillers, Andrew Granville, Wladyslaw Narkiewicz and Carl Pomerance, *An upper bound in Goldbach's problem*, Math. Comp. **61** (1993), 209–213.

[4] T. Estermann, *On Goldbach's problem: Proof that almost all even positive integers are sums of two primes*, Proc. London Math. Soc **44** (1938), 307–314.

[5] G.H. Hardy and J.E. Littlewood, *Some problems of 'partitio numerorum'; V: A further contribution to the study of Goldbach's problem* Proc. London Math. Soc **22** (1924), 46–56.

[6] M. Kolountzakis, *On the additive complements of the primes and sets of similar growth*, Acta Arith **77** (1996), 1–8.

[7] J.E. Littlewood, *Distribution des nombres premiers*, C. R. Acad. Sci. Paris **158** (1914), 1869–1872.

[8] H.L. Montgomery and R.C. Vaughan, *Error terms in additive prime number theory and the GRH*, to appear.

[9] H.L. Montgomery and R.C. Vaughan, *The exceptional set in Goldbach's problem*, Acta. Arith **27** (1975), 353–370.

[10] J. Pintz, *Explicit formulas and the exceptional set in Goldbach's problem*, to appear.

[11] O. Ramaré, *On S'nirel'man's constant*, Ann. Sci. Norm. Super. Pisa **21** (1995), 645–705.

[12] J. Richstein, *Verifying the Goldbach conjecture up to* $4 \cdot 10^{14}$, Math. Comp **70** (2000), 1745–1749.

[13] J. G. Van der Corput, *Sur l'hypothèse de Goldbach*, Proc. Acad. Wet. Amsterdam **41** (1938), 76–80.

[14] I. M. Vinogradov, *Representation of an odd number as a sum of three primes*, Comptes Rendus (Doklady) de l'Académie des Sciences de l'URSS **15** (1937), 291–294.

[15] Van Vu, *High order complementary bases of primes*, Integers **2** (2002).

[16] E. Wirsing, *Thin subbases*, Analysis **6** (1986), 285–308.

Address: Département de Mathématiques et statistique, Université de Montral, CP 6128 succ. Centre-Ville, Montréal QC H3C 3J7, Canada
E-mail: andrew@dms.umontreal.ca
Received: 25 April 2006; **revised:** 7 June 2006