The inverse Goldbach problem

by
Christian Elsholtz

Submission September 7, 2000
(this version includes galley corrections).
Appeared in Mathematika 2001.

Abstract

We improve the upper and lower bounds of the counting functions of the conceivable additive decomposition sets of the set of primes. Suppose that $\mathcal{A}+\mathcal{B}=\mathcal{P}'$, where $\mathcal{P}'$ differs from the set of primes in finitely many elements only and $|\mathcal{A}|,|\mathcal{B}|\geq 2$.

Here we prove the following bounds on the counting functions $A(x)$ and $B(x)$, for sufficiently large x:

$$x^{1/2}(\log x)^{-5} \ll A(x) \ll x^{1/2}(\log x)^4.$$

The same bounds hold for $B(x)$.

This immediately solves the ternary inverse Goldbach problem: there is no ternary additive decomposition $\mathcal{A}+\mathcal{B}+\mathcal{C}=\mathcal{P}'$, where $\mathcal{P}'$ is as above and $|\mathcal{A}|,|\mathcal{B}|,|\mathcal{C}|\geq 2$.

1 Introduction

The inverse Goldbach problem is the question of whether the set of primes has an additive decomposition in the following sense. Given subsets $\mathcal{A}$ and $\mathcal{B}$ of the positive integers, let

$$\mathcal{A}+\mathcal{B} := \{a+b:\ a\in\mathcal{A}, b\in\mathcal{B}\}$$

be the sum of these two sets. Let $\mathcal{P}$ denote the set of primes. Let $\mathcal{P}'$ denote a set of positive integers that differs from the set of primes $\mathcal{P}$ in only finitely many elements, i.e., for sufficiently large x_0, we have $\mathcal{P}\cap[x_0,\infty]=\mathcal{P}'\cap[x_0,\infty]$.

It is easy to see that $\mathcal{A}+\mathcal{B}=\mathcal{P}$ cannot hold with $|\mathcal{A}|,|\mathcal{B}|\geq 2$. But the following question of Ostmann (see page 13 of [9], or [2]) is still open: do there exist sets $\mathcal{A},\mathcal{B}$ and $\mathcal{P}'$ with $|\mathcal{A}|,|\mathcal{B}|\geq 2$ such that

$$\mathcal{A}+\mathcal{B}=\mathcal{P}'?$$

Even though it is generally believed that such a decomposition cannot exist, this might, according to Erdős (see [5]), be out of reach. The problem was posed again in the problem session at the 1998 Oberwolfach conference by Prof. Wirsing (see [14]).

Partial answers concentrated on bounds of the counting functions $A(x)=\sum_{a\in\mathcal{A},a\leq x}1$ and $B(x)$.

Note that such a decomposition would have far reaching consequences towards the prime k-tuple conjecture. It is easy to see that both $\mathcal{A}$ and $\mathcal{B}$ must contain infinitely many elements (see [4], [7], [9], [5]). If $b_1,b_2,\dots,b_k\in\mathcal{B}$, then there would be infinitely many integers n such that $n+b_1,\dots,n+b_k$ are simultaneously prime.

Here we prove the following bounds on the counting functions $A(x)$ and $B(x)$:

Theorem. *Suppose that there exist sets $\mathcal{P}',\mathcal{A},\mathcal{B}$ with $\mathcal{P}'=\mathcal{A}+\mathcal{B}$, where $|\mathcal{A}|,|\mathcal{B}|\geq 2$ and $\mathcal{P}'$ coincides with the set of primes for elements $p>x_0$. For sufficiently large $x\geq x_1$ the following bounds hold:*

$$\frac{x^{1/2}}{(\log x)^5} \ll A(x) \ll x^{1/2}(\log x)^4.$$

The same bounds hold for $B(x)$.

Our theorem immediately implies the following corollary.

Corollary (Solution of the inverse ternary Goldbach problem). *There do not exist sets of integers $\mathcal{A}, \mathcal{B}$, and $\mathcal{C}$ with $|\mathcal{A}|, |\mathcal{B}|, |\mathcal{C}| \geq 2$, and a set $\mathcal{P}'$ which coincides with the set of primes $\mathcal{P}$ for sufficiently large elements such that $\mathcal{A}+\mathcal{B}+\mathcal{C}=\mathcal{P}'$ holds.*

Our bounds in the binary case are close to best possible and should be compared with previous results on this subject. Hornfeck (see [4]) proved for arbitrary k that

$$(\log x)^k \ll A(x) \ll \frac{x}{(\log x)^k}$$

holds. Hofmann and Wolke (see [5]) improved this to

$$\exp\left(c\frac{\log x}{\log_2 x}\right) \ll A(x) \ll \frac{x}{\exp\left(c\frac{\log x}{\log_2 x}\right)}$$

and the present author (see [1]) refined their method to yield

$$\exp\left(c_r\frac{\log x}{\log_r x}\right) \ll A(x) \ll \frac{x}{\exp\left(c_r\frac{\log x}{\log_r x}\right)} \text{ for any } r.$$

Here $\log_r x$ denotes the r-th iterated logarithm. The same bounds hold for $B(x)$.
In the seventies, Wirsing proved (see [13]) that $A(x)B(x) = O(x)$, a result which was independently proved by Pomerance, Sárközy & Stewart (see [10]) and Hofmann & Wolke (see [5]).

Acknowledgements: the research on this paper was done while the author was working at the University of Stuttgart. He would like to thank J. Brüdern for encouraging remarks on earlier versions of this paper. Further thank goes to S. Daniel, C. List, L. Lucht, A. Schinzel, E. Wirsing, and D. Wolke for comments or further references.

2 Proof

Let us first prove that our theorem implies the corollary. We make use of the following result, which is a special case of a theorem of Pomerance, Sárközy, and Stewart, see theorem 3 of [10].

Lemma 1. *Let ε be a positive real number, let x be a positive integer, and let $\mathcal{A}, \mathcal{B}, \mathcal{C}$ denote nonempty subsets of $\{1, \cdots, x\}$. For sufficiently large x and for $\min(|\mathcal{A}|, |\mathcal{B}|, |\mathcal{C}|) > x^{1/3+2\varepsilon}$ there is a prime p with*

$$p < x^{1/3+\varepsilon}$$

such that $\mathcal{A}+\mathcal{B}+\mathcal{C}$ contains an element which is divisible by p.

Proof of the corollary. It follows from $(\mathcal{A}+\mathcal{B})+\mathcal{C} = (\mathcal{A}+\mathcal{C})+\mathcal{B} = \mathcal{A}+(\mathcal{B}+\mathcal{C}) = \mathcal{P}'$ and the lower bound found in the binary inverse Goldbach problem (which is our theorem) that $A(x), B(x), C(x) \gg x^{1/2-\varepsilon}$. For $x > (x_1)^{2.5}$ let $\mathcal{A}_1 = \mathcal{A} \cap [x^{0.4}, \infty]$. Then $A_1(x) \gg x^{1/2-\varepsilon}$ still holds. The lemma implies that $\mathcal{A}_1+\mathcal{B}+\mathcal{C}$ contains an element $a_1+b+c \geq x^{0.4}$ which is divisible by some prime $p \leq x^{1/3+\varepsilon}$. This proves the corollary. Of course, the same conclusion holds for more than three summands. $\square$

Before we turn to the proof of the theorem we have to recall some known results about the large sieve method and describe the new method. The large sieve method has been invented to deal with sieve problems where a large number of residue classes modulo primes can be sifted.

Suppose now we consider a sieve problem involving two sequences of integers. Then our new method allows to remove any given residue class either when sifting the first sequence by the first sieve method or when sifting the second sequence by the second sieve method. This means that *all* residue classes can be used in this combined sieve method.

Let us state MONTGOMERY's sieve (see [8]):

Lemma 2. *Let $\mathcal{P}$ denote the set of primes. Let p be a prime. Let $\mathcal{C}$ denote a set of integers which avoids $\omega(p)$ residue classes modulo p. Here $\omega : \mathcal{P} \to \mathbb{N}$ with $0 \leq \omega(p) \leq p-1$. Let $C(x)$ denote the counting function $C(x) = \sum_{c \leq x, c \in \mathcal{C}} 1$. Then the following upper bound on the counting function holds:*

$$C(x) \leq \frac{2x}{L}, \text{ where } L = \sum_{q \leq x^{1/2}} \mu^2(q) \prod_{p|q} \frac{\omega(p)}{p-\omega(p)}.$$

VAUGHAN (see [11]) has found a suitable evaluation of L if $\sum_{p \leq y} \dfrac{\omega(p)}{p}$ is known.

Lemma 3. *The following lower bound holds:*

$$L \geq \sum_m \exp\left(m \log \left(\frac{1}{m} \sum_{p \leq x^{1/(2m)}} \frac{\omega(p)}{p} \right) \right).$$

The size of this sum can be approximated by choosing a value of m which maximizes the summand. The parameter m denotes the number of prime factors of q in the definition of L. Hence $1 \leq m \leq \dfrac{\log(x^{1/2})}{\log 2}$.

In situations where the number of removed residue classes is close to p, so that only a small number of classes remain, it is better to use GALLAGHER's larger sieve (see [3]).

Lemma 4. *Let $\mathcal{S}$ denote a set of primes such that $\mathcal{A}$ lies modulo p (for $p \in \mathcal{S}$) in at most $\nu(p)$ residue classes. Then the following bound holds, provided the denominator is positive:*

$$A(x) \leq \frac{-\log x + \sum_{p \in \mathcal{S}} \log p}{-\log x + \sum_{p \in \mathcal{S}} \dfrac{\log p}{\nu(p)}}.$$

We intend to use MONTGOMERY's sieve to give an upper bound for $A(x)$. In view of $\pi(x) \ll A(x)B(x)$ this also implies lower bounds for $B(x)$. For $a \in \mathcal{A}, b \in \mathcal{B}, a + b = p_1 \in \mathcal{P}$ (for $p_1 > x_0$) we have $a \not\equiv -b \mod p$ for all primes $p < p_1$. A residue class that occurs in $\mathcal{B}$ induces a forbidden residue class in $\mathcal{A}$. This class will be used in the application of MONTGOMERY's sieve for an upper bound on $A(x)$. On the other hand, a class modulo p that does not occur in $\mathcal{B}$ can be sifted, when using GALLAGHER's sieve for bounds on $B(x)$. Even though we do not know how many residue classes modulo p are needed to cover the set $\mathcal{B}$ we do know that this number cannot be too small (on average). If the number of classes covering $\mathcal{B}$ is small, then many classes are excluded and an application of GALLAGHER's sieve

implies an upper bound on $B(x)$ that contradicts existing lower bounds. This combination of both types of the large sieve gives us new information which finally leads to much better bounds than were known before.
We now come to the details of the proof. We will first prove a slightly weaker result and then iterate the argument.

Proposition. *For any $\varepsilon > 0$ and for sufficiently large $x \geq x_2$, we have the following bounds:*

$$x^{1/2-\varepsilon} \ll A(x) \ll x^{1/2+\varepsilon}.$$

The same bounds hold for $B(x)$.

For sufficiently large $x > (x_0)^2$, we know that

$$\mathcal{P} \cap (x^{1/2}, \infty) = \mathcal{P}' \cap (x^{1/2}, \infty).$$

Put

$$\mathcal{A}_1 = \mathcal{A} \cap (x^{1/2}, x), \mathcal{B}_1 = \mathcal{B} \cap (0, x).$$

For any prime $x_0 < p \leq x^{1/2}$, let $\nu_{\mathcal{A}_1}(p)$ and $\nu_{\mathcal{B}_1}(p)$ denote the number of residue classes modulo p that contain elements of $\mathcal{A}_1$ and $\mathcal{B}_1$, respectively. Now $a_1 + b_1$ (with $a_1 \in \mathcal{A}_1, b_1 \in \mathcal{B}_1$) is a prime $p_1 > x^{1/2}$, i.e. $a_1 + b_1 \not\equiv 0 \bmod p$ for any prime $p \leq x^{1/2}$. Hence, for any prime $x_0 < p \leq x^{1/2}$, a_1 lies outside $\nu_{\mathcal{B}_1}(p)$ residue classes modulo p.
Let us sketch Hornfeck's bounds: With $|\mathcal{B}| \geq 2$ one can apply a two dimensional sieve which leads to $A(x) \ll \dfrac{x}{(\log x)^2}$. From $\pi(x) \ll A(x)B(x)$ we see that $B(x) \gg \log x$. In particular, $\mathcal{B}$ has infinitely many elements so that we can apply in a next step, for any fixed k, a $k+1$-dimensional sieve which proves $A(x) \ll \dfrac{x}{(\log x)^{k+1}}$ and $B(x) \gg (\log x)^k$.
At this stage, the argument of Hofmann and Wolke continues with sieving with $\omega(p) = c_k(\log p)^k$. This uses the fact that the elements of $\mathcal{B}$ which are less than p trivially lie in distinct classes modulo p. We take a completely different approach. We exploit the fact that $(\log x)^k$ can be considerably larger than $(\log p)^k$. Hence $\omega(p)$ can be chosen possibly much larger than assumed by Hofmann and Wolke.
In fact we shall make two iterations of essentially the same argument using different parameters.
Iteration A:
We shall use lemma 3 with the following choice of m:

$$m = m_A = \left[\frac{\varepsilon}{4} \frac{\log x}{\log \log x}\right].$$

Let $y = x^{1/(2m)}$. Hence $y \sim (\log x)^{2/\varepsilon}$. For the sieve process we use all primes in the interval $x_0 < p \leq y$. We split these primes into two sets,

$$\mathcal{P}_{A1} := \{x_0 < p \leq y \mid \nu_{\mathcal{B}_1}(p) < p^{1-\varepsilon}\} \text{ and } \mathcal{P}_{A2} := \{x_0 < p \leq y \mid \nu_{\mathcal{B}_1}(p) \geq p^{1-\varepsilon}\}.$$

One of these two sets must contain at least half of the primes of the interval $(x_0, y]$.
Let condition A1 denote the case in which $\mathcal{P}_{A1}$ contains at least half of these primes. Similarly, condition A2 is satisfied when $\mathcal{P}_{A2}$ contains at least half of these primes.

Lemma 5. *By the prime number theorem we have*

$$-\log x + \sum_{p\in\mathcal{P}_{A1}} \log p \le \sum_{p\le y} \log p \sim y.$$

Lemma 6. *Suppose that condition A1 holds. Then we have (for $y\to\infty$)*

$$\sum_{p\in\mathcal{P}_{A1}} \frac{\log p}{p^{1-\varepsilon}} \gg y^{\varepsilon}.$$

Because of the monotonicity of $\dfrac{\log p}{p^{1-\varepsilon}}$, the worst case occurs when all occurring primes are as large as possible.

$$\sum_{p\in\mathcal{P}_{A1}} \frac{\log p}{p^{1-\varepsilon}} \gg y^{\varepsilon} - (\frac{2y}{3})^{\varepsilon} \gg y^{\varepsilon}.$$

(Recall that both intervals, $(x_0, \frac{y}{2}]$ and $(\frac{y}{2}, y]$ contain asymptotically half of the primes of the interval $(x_0, y]$. Since $\mathcal{P}_{A1}$ contains by assumption half of these primes, the sum is -in this worst case- essentially over the interval $(\frac{y}{2}, y]$.)
Since $y \gg (\log x)^{2/\varepsilon}$, the last lemma implies:

Lemma 7. *Suppose that condition A1 holds. Then we have*

$$-\log x + \sum_{p\in\mathcal{P}_{A1}} \frac{\log p}{\nu_{\mathcal{B}_1}(p)} \gg y^{\varepsilon}.$$

Similarly we can state a lemma corresponding to condition A2.

Lemma 8. *Suppose that condition A2 holds. With $\omega(p) = \nu_{\mathcal{B}_1}(p) \ge p^{1-\varepsilon}$ for $p\in\mathcal{P}_{A2}$ and for $y\to\infty$ we have*

$$\sum_{p\in\mathcal{P}_{A2}} \frac{\omega(p)}{p} \gg \frac{y^{1-\varepsilon}}{\log y}.$$

Again, the worst case occurs when all of the primes in $\mathcal{P}_{A2}$ are as large as possible, whence

$$\sum_{p\in\mathcal{P}_{A2}} \frac{\omega(p)}{p} \ge \left(\pi(y) - \pi(\frac{2y}{3})\right)\frac{1}{y^{\varepsilon}} \gg \frac{y^{1-\varepsilon}}{\log y}.$$

After these preliminary remarks the proof of our proposition is very simple. In the case that condition A1 holds, we may apply GALLAGHER's sieve with $\nu_{\mathcal{B}_1}(p) < p^{1-\varepsilon}$ for $p\in\mathcal{P}_{A1}$. By lemmas 5 and 7

$$B(x) \le \frac{-\log x + \sum_{p\in\mathcal{P}_{A1}} \log p}{-\log x + \sum_{p\in\mathcal{P}_{A1}} \dfrac{\log p}{p^{1-\varepsilon}}} \ll \frac{y}{y^{\varepsilon}} = y^{1-\varepsilon} \ll (\log x)^{2(1-\varepsilon)/\varepsilon},$$

which contradicts previously known lower bounds on $B(x)$, even those due to HORNFECK. Hence condition A2 must hold. We use MONTGOMERY's sieve to give an upper bound on $A(x)$. Here we may sieve with $\omega(p) = \nu_{\mathcal{B}_1}(p) \ge p^{1-\varepsilon}$, for $p\in\mathcal{P}_{A2}$.

Lemma 3 and lemma 8 imply that (for some $c > 0$)

$$\begin{aligned}
L &\geq \exp\left(m \log\left(\frac{1}{m} \sum_{p\in\mathcal{P}_{A2}} \frac{\omega(p)}{p}\right)\right) \\
&\geq \exp\left(m \log\left(\frac{c}{m} \frac{\left(x^{1/(2m)}\right)^{1-\varepsilon}}{\log(x^{1/(2m)})}\right)\right) \\
&\geq \exp\left(m \log\left(\frac{c}{m} \frac{2mx^{(1-\varepsilon)/(2m)}}{\log x}\right)\right) \\
&\geq \exp\left(m\left(\log 2 + \log c - \log_2 x + \frac{1-\varepsilon}{2m} \log x\right)\right) \\
&\geq \exp\left(\left(\frac{1}{2} - \frac{\varepsilon}{2} - \frac{\varepsilon}{4}\right) \log x + m(\log 2 + \log c)\right) \\
&\gg x^{1/2-\varepsilon}.
\end{aligned}$$

By Montgomery's sieve method we have $A_1(x) \leq \frac{2x}{L} \ll x^{1/2+\varepsilon}$, for any $\varepsilon > 0$. This implies that

$$A(x) = A_1(x) + O(x^{1/2}) \ll x^{1/2+\varepsilon}.$$

The lower bound $B(x) \gg x^{1/2-\tilde{\varepsilon}}$, for any $\tilde{\varepsilon} > 0$, follows from $A(x)B(x) \gg \pi(x)$. This proves our proposition.
In this argument we assumed that $B(x) \gg (\log x)^{2(1-\varepsilon)/\varepsilon}$ is already known. Now, after having proved a much better lower bound, we can expect that the same idea brings us even further towards $x^{1/2}$.

Iteration B

The very same argument with differently chosen parameters works as follows: we choose $m = 2$ so that $y = x^{1/4}$, and $c = 20$. We split the primes $x_0 < p \leq y$ into two sets,

$$\mathcal{P}_{B1} := \{x_0 < p \leq y \mid \nu_{\mathcal{B}_1}(p) < \frac{p}{c \log p}\} \text{ and } \mathcal{P}_{B2} := \{x_0 < p \leq y \mid \nu_{\mathcal{B}_1}(p) \geq \frac{p}{c \log p}\}.$$

We say that condition B1 holds if $\mathcal{P}_{B1}$ contains at least half of the primes of the interval $(x_0, y]$; similarly condition B2 holds if $\mathcal{P}_{B2}$ contains at least half of these primes.
Let us assume that condition B1 holds. Then we see that for sufficiently large y

$$\begin{aligned}
\sum_{p\in\mathcal{P}_{B1}} \frac{\log p}{\nu_{\mathcal{B}_1}(p)} &\geq \sum_{p\in\mathcal{P}_{B1}} \frac{c(\log p)^2}{p} \geq \frac{c}{2}\left((\log y)^2 - (\log \frac{2y}{3})^2\right) = c(\log \frac{3}{2})(\log y) - \frac{c}{2}(\log \frac{2}{3})^2 \\
&\geq 2 \log x.
\end{aligned}$$

Gallagher's sieve yields

$$B(x) \leq \frac{-\log x + \sum_{p\in\mathcal{P}_{B1}} \log p}{-\log x + \sum_{p\in\mathcal{P}_{B1}} \frac{\log p}{\nu_{\mathcal{B}_1}(p)}} \leq \frac{y}{\log x} = \frac{x^{1/4}}{\log x},$$

which is a contradiction to our proposition.
This implies that condition B2 must hold. Therefore $\mathcal{P}_{B2}$ must contain at least half of the primes of the interval $(x_0, y]$. By Montgomery's sieve with $\omega(p) = \nu_{\mathcal{B}_1}(p)$ and suitable

constants c' and c'':

$$\begin{aligned} L &\geq \exp\left(m\log\left(\frac{1}{m}\sum_{p\in\mathcal{P}_{B2}}\frac{\omega(p)}{p}\right)\right)\\ &\geq \exp\left(m\log\left(\frac{1}{m}\sum_{p\in\mathcal{P}_{B2}}\frac{1}{c\log p}\right)\right)\\ &\geq \exp\left(m\log\left(\frac{c'}{m}\frac{y}{(\log y)^2}\right)\right)\\ &\geq \exp\left(2\frac{1}{4}\log x-4\log\log x+c''\right)\\ &\gg x^{1/2}(\log x)^{-4}. \end{aligned}$$

This implies $A_1(x) \ll x^{1/2}(\log x)^4$, i.e. $A(x) \ll A_1(x)+O(x^{1/2}) \ll x^{1/2}(\log x)^4$. Hence $B(x) \gg x^{1/2}(\log x)^{-5}$. By symmetry the same bounds hold for $A(x)$ and $B(x)$, which proves our theorem.

References

[1] Elsholtz, C., A remark on Hofmann and Wolke's Additive decompositions of the set of primes, Arch. Math. 76, 30–33, (2001).

[2] Erdős, P., Problems and results in number theory, Number Theory Day, New York, 1976, Springer, Lecture Notes in Math. 626, pp.43–72.

[3] Gallagher, P.X., A larger sieve, Acta Arith. 18, (1971), 77–81.

[4] Hornfeck, B., Ein Satz über die Primzahlmenge, Math. Z., 60, (1954), 271–273, see also the correction in vol. 62, (1955), page 502.

[5] Hofmann, A., Wolke, D., On additive decompositions of the set of primes, Arch. Math. 67, (1996), 379–382.

[6] Laffer, W.B., Mann, H.B., Decomposition of sets of group elements. Pacific J. Math. 14, 547–558, (1964).

[7] Mann, H., Addition theorems: The addition theorems of group theory and number theory, Wiley, Interscience, New York-London-Sydney, 1965.

[8] Montgomery, H.L., The Analytic Principle of the Large Sieve, Bull. Amer. Math. Soc., 84, (1978), 547–567.

[9] Ostmann, H.-H., Additive Zahlentheorie. 1. Teil: Allgemeine Untersuchungen, Springer-Verlag, Berlin-Heidelberg-New York, 1968.

[10] Pomerance, C., Sárközy, A., Stewart, C.L., On divisors of sums of integers. III, Pacific J. Math., 133, (1988), 363–381.

[11] Vaughan, R.C., Some Applications of Montgomery's Sieve, J. Number Theory, 5, (1973), 64–79.

[12] Wirsing, E., Ein metrischer Satz über Mengen ganzer Zahlen. Arch. Math. 4, (1953), 392–398.

[13] Wirsing, E., Über additive Zerlegungen der Primzahlmenge, unpublished manuscript, an abstract can be found in Tagungsbericht 28/1972, Oberwolfach.

[14] Wirsing, E., Problem at the problem session, Abstracts of the Oberwolfach Conference 10/1998.

Author's address:
Christian Elsholtz
Institut für Mathematik
TU Clausthal
Erzstrasse 1
D-38678 Clausthal-Zellerfeld
Germany
elsholtz@math.tu-clausthal.de

AMS Classification:
11P32 Goldbach type theorems; other additive questions involving primes
11N35 Sieves
11N36 Applications of sieve methods
11P70 Inverse problems of additive number theory