Goldbach's Conjecture — Towards the Inconsistency of Arithmetic

Ralf Wüsthofen

Abstract. This paper proves, using methods from elementary number theory, that there is an inconsistency in Peano arithmetic (PA), where the centerpiece is a strengthened form of the strong Goldbach conjecture. We express this form of the conjecture in terms of an infinite set and show that the conjunction of two properties of this set leads to a contradiction. An essential point here is the constructive role of the prime numbers within the natural numbers.

Notations. Let $\mathbb{N}$ denote the natural numbers starting from 1, let $\mathbb{N}_a$ denote the natural numbers starting from a > 1 and let $\mathbb{P}_3$ denote the prime numbers starting from 3.

The expression "we have a proof that P", where P is a statement, means that there is a proof in this paper that P.

Strengthened strong Goldbach conjecture (SSGB): *Every even number greater than 6 is the sum of two distinct odd primes.*

Theorem. *Peano arithmetic (PA) is inconsistent.*

Proof. Assuming PA is consistent, we will show that the statement FALSE can be deduced.

We define the set $S_g := \{ (pk, mk, qk) \mid k, m \in \mathbb{N};\ p, q \in \mathbb{P}_3,\ p < q;\ m = (p + q) / 2 \}$.

The term S_g is not a standard part of PA, but it can easily be defined within PA.

SSGB is equivalent to saying that every integer n ≥ 4 is the arithmetic mean of two distinct odd primes and so it is equivalent to saying that all integers n ≥ 4 appear as m in a middle component mk of S_g. So, by the definition of S_g we have

$$\text{SSGB} \iff \forall n \in \mathbb{N}_4 \ \exists (pk, mk, qk) \in S_g \quad n = m$$

$$\neg\text{SSGB} \iff \exists n \in \mathbb{N}_4 \ \forall (pk, mk, qk) \in S_g \quad n \neq m.$$

The set S_g has the following two properties.

First, the whole range of $\mathbb{N}_3$ can be expressed by the triple components of S_g ("*covering*"). We prove this by dividing it into the following three cases.

(i) $x \in \mathbb{N}_3$ is prime. Then, $x = pk$ with $p \in \mathbb{P}_3$, $k = 1$.

(ii) $x \in \mathbb{N}_3$ is composite and not a power of 2. Then, $x = pk$ with $p \in \mathbb{P}_3$, $k \neq 1$.

(iii) $x \in \mathbb{N}_3$ is a power of 2. Then, $x = (p + q)k / 2$ with $p = 3$, $q = 5$, $k =$ (a power of 2).

So we have

(C) $\forall x \in \mathbb{N}_3 \quad \exists (pk, mk, qk) \in S_g \quad x = pk \quad \vee \quad x = mk.$

A few examples of the covering:

x = 19: (**19·1**, 21·1, 23·1), (**19·1**, 60·1, 101·1)

x = 27: (**3·9**, 7·9, 11·9)

x = 42: (**3·14**, 5·14, 7·14), (**7·6**, 9·6, 11·6)

x = 4096: (3·1024, **4·1024**, 5·1024)

x = 10000: (**5·2000**, 6·2000, 7·2000).

Second, all pairs (p, q) of distinct odd primes are used in the definition of the set S_g ("*maximality*"). So we have

(M) $\forall p, q \in \mathbb{P}_3, p < q \quad \forall k \in \mathbb{N} \qquad (pk, mk, qk) \in S_g$, where $m = (p + q) / 2$.

From $\neg$(C) it would immediately follow that $\neg$SSGB holds, since an $x \geq 4$ that is different from all S_g triple components pk and mk is in particular different from all m in S_g. So the property (C) excludes this possibility.

The property (M) excludes the possibility that if there is an $n \geq 4$ different from all m in S_g (i.e. $\neg$SSGB), then n is the arithmetic mean of a pair of distinct odd primes not used in S_g.

So (M) rules out the possibility that the question of whether SSGB holds or not depends on whether (M) holds or not. (The proof would no longer be possible if we left out any pair of distinct odd primes in the formulation of SSGB and S_g.)

We will now show that ((C) $\wedge$ (M)) leads to a contradiction. The basic idea is the following.

Since, due to (C), an $n \in \mathbb{N}_4$ different from all m equals a component of some S_g triple that exists by definition and since, due to (M), this n cannot be the arithmetic mean of a pair of primes not used in S_g, we can prove that under the assumption that n exists (i.e. $\neg$SSGB), the S_g triples are the same as under the assumption that n does not exist (i.e. SSGB). This causes a contradiction because under the assumption SSGB the numbers m defined in S_g take all integer values $x \geq 4$ whereas under the assumption $\neg$SSGB they don't.

The following steps are independent of the choice of n if, in the case of $\neg$SSGB, there is more than one that is different from all m. For example, the minimal such n works.

We split S_g into two complementary subsets in the following way. For any $y \in \mathbb{N}_3$, we write

$S_g = S_g{+}(y) \cup S_g{-}(y)$, with

$S_g{+}(y) := \{ (pk, mk, qk) \in S_g \mid \exists\, k' \in \mathbb{N} \quad pk = yk' \ \vee\ mk = yk' \ \vee\ qk = yk' \}$

$S_g{-}(y) := \{ (pk, mk, qk) \in S_g \mid \forall\, k' \in \mathbb{N} \quad pk \neq yk' \ \wedge\ mk \neq yk' \ \wedge\ qk \neq yk' \}$.

We define $S_1 := \{ (pk, mk, qk) \in S_g \mid \text{SSGB} \}$ and $S_2 := \{ (pk, mk, qk) \in S_g \mid \neg\text{SSGB} \}$. I.e.,

$S_1 = S_g$ if SSGB is true, and $S_1 = \{ \}$ if SSGB is false
and
$S_2 = S_g$ if $\neg$SSGB is true, and $S_2 = \{ \}$ if $\neg$SSGB is false.

Under the assumption $\neg$SSGB there is an $n \in \mathbb{N}_4$ as described above and under the assumption SSGB there is no such n. Then, since under both assumptions SSGB and $\neg$SSGB the properties (C) and (M) hold, we obtain

(1.1) we have a proof that $(\forall y \in \mathbb{N}_3 \quad SSGB \Rightarrow S_1 = S_g+(y) \cup S_g-(y))$

$\wedge$

(1.2) we have a proof that $(\neg SSGB \Rightarrow S_2 = S_g+(n) \cup S_g-(n))$.

So, since $S_g+(n) \cup S_g-(n)$ is independent of n,

we have a proof that

$$((\forall y \in \mathbb{N}_3 \quad SSGB \Rightarrow S_1 = S_g+(y) \cup S_g-(y))$$

(1) $$\wedge$$

$$(\forall y \in \mathbb{N}_3 \quad \neg SSGB \Rightarrow S_2 = S_g+(y) \cup S_g-(y))).$$

Now, we will make use of the following principle.

If two sets of (possibly infinitely many) z-tuples are equal, then the sets of their corresponding i-th components are equal; $1 \le i \le z$.

To this end, for each $k \in \mathbb{N}$ we define

$M_1(k) := \{ mk \mid (pk, mk, qk) \in S_1 \}$ and $M_2(k) := \{ mk \mid (pk, mk, qk) \in S_2 \}$.

Then, applying the principle above to the middle component of the triples (pk, mk, qk), the fact that both conjuncts in (1) are proved implies, by transitivity, that

we have a proof that

$$((\forall k \in \mathbb{N} \quad \forall y \in \mathbb{N}_3 \quad SSGB \Rightarrow M_1(k) = \{ mk \mid (pk, mk, qk) \in S_g+(y) \cup S_g-(y) \})$$

(2) $$\wedge$$

$$(\forall k \in \mathbb{N} \quad \forall y \in \mathbb{N}_3 \quad \neg SSGB \Rightarrow M_2(k) = \{ mk \mid (pk, mk, qk) \in S_g+(y) \cup S_g-(y) \})).$$

Setting $M_1 := M_1(1)$ and $M_2 := M_2(1)$,

we have a proof that

$$((\forall y \in \mathbb{N}_3 \quad SSGB \Rightarrow M_1 = \{ m \mid (p, m, q) \in S_g+(y) \cup S_g-(y) \})$$

(2') $\wedge$

$$(\forall y \in \mathbb{N}_3 \quad \neg SSGB \Rightarrow M_2 = \{ m \mid (p, m, q) \in S_g+(y) \cup S_g-(y) \})).$$

We define $M := \{ m \mid (p, m, q) \in S_g \}$. Then, since for every $y \in \mathbb{N}_3$ $S_g+(y) \cup S_g-(y)$ equals S_g by definition, for every $y \in \mathbb{N}_3$ $\{ m \mid (p, m, q) \in S_g+(y) \cup S_g-(y) \}$ equals M by definition. If SSGB is true, M is equal to $\mathbb{N}_4$, and if SSGB is false, M is equal to some non-empty proper subset U of $\mathbb{N}_4$.

Therefore, defining X to be a variable that ranges either over the singleton set $\{ \mathbb{N}_4 \}$ or over the singleton set { U }, from (2') we obtain that

we have a proof that

(3) $((SSGB \Rightarrow M_1 = X) \quad \wedge \quad (\neg SSGB \Rightarrow M_2 = X)).$

A variable that ranges either over the set { B1 } or over the set { B2 } is either a variable that ranges over the set { B1 } or a variable that ranges over the set { B2 }.

Thus, X is either a variable in (3) that ranges over the set $\{ \mathbb{N}_4 \}$ or a variable in (3) that ranges over the set { U }. Therefore, we can make use of the following rule.

Let P = P(A) be a proposition that depends on a variable A, where A stands for a set. Then, for any set B,

(we have a proof that P(A) $\wedge$ we have a proof that A = B) => we have a proof that P(B).

If A is a variable in P that ranges over the set { B }, the above conjunct (we have a proof that A = B) is true, so that we get

(we have a proof that P(A)) => (we have a proof that P(B)).

So, if A is either a variable in P that ranges over the set { B1 } or a variable in P that ranges over the set { B2 }, we get

(we have a proof that P(A)) => (we have a proof that P(B1) $\vee$ we have a proof that P(B2)).

We apply the above rule with

P(A) = ((SSGB => M_1 = A) $\wedge$ ($\neg$SSGB => M_2 = A))

A = X

B1 = $\mathbb{N}_4$

B2 = U.

Then, since we have proved (3), we obtain

(3.1) we have a proof that ((SSGB => $M_1 = \mathbb{N}_4$) $\wedge$ ($\neg$SSGB => $M_2 = \mathbb{N}_4$))

$\vee$

(3.2) we have a proof that ((SSGB => $M_1 = U \neq \mathbb{N}_4$) $\wedge$ ($\neg$SSGB => $M_2 = U \neq \mathbb{N}_4$)).

This is equivalent to

(3.1') (we have a proof that (SSGB => $M_1 = \mathbb{N}_4$)
$\wedge$
we have a proof that ($\neg$SSGB => $M_2 = \mathbb{N}_4$))

$\vee$

(3.2') (we have a proof that (SSGB => $M_1 = U \neq \mathbb{N}_4$)
$\wedge$
we have a proof that ($\neg$SSGB => $M_2 = U \neq \mathbb{N}_4$)).

This implies

(4.1) we have a proof that ($\neg$SSGB => $M_2 = \mathbb{N}_4$)

$\vee$

(4.2) we have a proof that (SSGB => $M_1 = U \neq \mathbb{N}_4$).

Now, we will establish a contradiction to ((4.1) $\vee$ (4.2)).

We have a proof that (SSGB => $M = \mathbb{N}_4$) and we have a proof that ($\neg$SSGB => $M = U \neq \mathbb{N}_4$). Therefore, since SSGB => $M_1 = M$ and $\neg$SSGB => $M_2 = M$ by definition, we get

(5.1) we have a proof that (SSGB => $M_1 = \mathbb{N}_4$)

$\wedge$

(5.2) we have a proof that ($\neg$SSGB => $M_2 = U \neq \mathbb{N}_4$).

Because of ((5.1) $\wedge$ (5.2)) and because

we have a proof that (SSGB => $M_2 = \{ \} \neq \mathbb{N}_4$)

and

we have a proof that ($\neg$SSGB => $M_1 = \{ \} \neq U$),

we have a proof that ($M_2 = \mathbb{N}_4$) is false and we have a proof that ($M_1 = U \neq \mathbb{N}_4$) is false.

Therefore, ((4.1) $\vee$ (4.2)) yields

(6.1) we have a proof that ($\neg$SSGB => FALSE)

$\vee$

(6.2) we have a proof that (SSGB => FALSE).

And this yields

(7.1) we have a proof that SSGB

$\vee$

(7.2) we have a proof that $\neg$SSGB.

Since we have neither a proof of SSGB nor of $\neg$SSGB, both (7.1) and (7.2) are false.

So, we obtain (FALSE $\vee$ FALSE) and thus FALSE.

Hence, the assumption that PA is consistent was false.

□