Goldbach's Conjecture — A Route to the Inconsistency of Arithmetic

Ralf Wüsthofen

Abstract. This paper proves an inconsistency in Peano arithmetic (PA). The contradiction we derive is based on two properties of a specific set which we use to reformulate a strengthened form of the strong Goldbach conjecture. We show that the conjecture and its negation, if we express them as assumptions using that set, on the one hand make no difference, but on the other hand they do.

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

Strengthened strong Goldbach conjecture (SSGB): *Every even integer greater than 6 can be expressed as the sum of two different primes.*

Theorem. *PA is contradictory, i.e. the statement FALSE can be derived*.

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

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

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

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

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*”), because every integer x ≥ 3 can be written as some pk with k = 1 when x is prime, as some pk with k ≠ 1 when x is composite and not a power of 2, or as (3 + 5)k / 2 when x is a power of 2; p $\in \mathbb{P}_3$, k $\in \mathbb{N}$. So we have

(C) $\forall x \in \mathbb{N}_3 \quad \exists\, (pk, mk, qk) \in S_g \quad x = pk \;\vee\; x = mk = 4k.$

A few examples of the covering:

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

x = 36: (**3·12**, 7·12, 11·12)

x = 38: (**19·2**, 21·2, 23·2)

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

x = 64: (3·16, **4·16**, 5·16)

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

Second, according to the statement SSGB, 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 $\in \mathbb{N}$ $\quad$ (pk, mk, qk) $\in S_g$, where m = (p + q) / 2.

The proof is motivated by the following view.

There are two possibilities for S_g, exactly one of which must occur: Either there is an $n \in \mathbb{N}_4$ in addition to all the numbers m defined in S_g or there is not. The latter is equivalent to SSGB and the former is equivalent to ¬SSGB.

Since, due to (C), every n given by ¬SSGB as well as every multiple nk, $k \in \mathbb{N}$, equals a component of some S_g triple that exists by definition, the covering of $\mathbb{N}_3$ by the S_g triples if n exists (¬SSGB) is equal to that if n does not exist (SSGB). This causes a contradiction because in the case SSGB the numbers m defined in S_g take all integer values x ≥ 4 whereas in the case ¬SSGB they don't.

First of all, we note that each of the two properties (C) and (M) is a condition sine qua non for the proof, for the following reasons.

¬(C) immediately implies ¬SSGB, since an n ≥ 4 different from all S_g triple components pk, mk, qk is in particular different from all m in S_g.

The proof would no longer be possible if, for example, we omitted the factor k in the definition of S_g, because then the corresponding (C) could no longer be guaranteed.

Similarly, the property (M) rules out the possibility that there is an $n \geq 4$ different from all m (i.e. $\neg$SSGB) and n is the arithmetic mean of a pair of primes not used in S_g. Thus (M) excludes the possibility that $\neg$SSGB applies due to a missing prime number pair. This means that the proof would no longer be possible here either if we left out any prime number pair in the formulation of SSGB and S_g.

We will now show that ((C) $\wedge$ (M)) is sufficient to derive a contradiction.

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

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

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

Then, after defining

$S_1 := \{ (pk, mk, qk) \in S_g \mid$ SSGB holds $\}$

$S_2 := \{ (pk, mk, qk) \in S_g \mid \neg$SSGB holds $\}$,

we have

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

and

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

Now, we will make use of the following principle.

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

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

$M(k) := \{ mk \mid (pk, mk, qk) \in S_g \}$

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

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

Then, applying the principle above to the middle component of the triples (pk, mk, qk), (1) and (2) imply

(3) $\forall k \in \mathbb{N} \quad \forall y \in \mathbb{N}_3$

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

$\wedge$

(4) $\forall k \in \mathbb{N} \quad \forall y \in \mathbb{N}_3$

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

We set $M := M(1)$, $M_1 := M_1(1)$ and $M_2 := M_2(1)$. Since

$SSGB \Rightarrow M_1 = M$ and $\neg SSGB \Rightarrow M_1 = \{ \} \neq M$

and

$\neg SSGB \Rightarrow M_2 = M$ and $SSGB \Rightarrow M_2 = \{ \} \neq M$,

the implications in (3) and (4) are in fact equivalences.

So we get

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

$\wedge$

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

Since for every $y \in \mathbb{N}_3$ $S_g+(y) \cup S_g-(y)$ equals S_g, there is a set X such that for every $y \in \mathbb{N}_3$ $\{ m \mid (p, m, q) \in S_g+(y) \cup S_g-(y) \}$ equals X. So, from (3') and (4') we obtain

(5) $(SSGB \iff M_1 = M = X) \quad \wedge \quad (\neg SSGB \iff M_2 = M = X)$.

The set X is a free variable in (5) that is either equal to $\mathbb{N}_4$ or to some non-empty proper subset Y of $\mathbb{N}_4$. Therefore, (5) splits as follows.

(5.1) $((SSGB \iff M_1 = M = \mathbb{N}_4) \quad \wedge \quad (\neg SSGB \iff M_2 = M = \mathbb{N}_4))$

$\vee$

(5.2) $((SSGB \iff M_1 = M = Y \neq \mathbb{N}_4) \quad \wedge \quad (\neg SSGB \iff M_2 = M = Y \neq \mathbb{N}_4))$.

On the other hand, under the assumption SSGB the numbers m defined in S_g take all integer values $x \geq 4$ whereas under $\neg$SSGB they don't. Therefore, we have

(6.1) $SSGB \iff M_1 = M = \mathbb{N}_4$

(6.2) $\neg SSGB \iff M_2 = M \neq \mathbb{N}_4$.

The first conjunct in (5.1) is identical to (6.1) which is a tautology. So we can omit that conjunct in (5.1). And since (6.2) is another tautology, we can add it to (5.1). Thus, (5.1) implies

(7.1) $((\neg SSGB \iff M_2 = M = \mathbb{N}_4) \quad \wedge \quad (\neg SSGB \iff M_2 = M \neq \mathbb{N}_4))$.

Similarly, (5.2) implies

(7.2) $((SSGB \iff M_1 = M = \mathbb{N}_4) \quad \wedge \quad (SSGB \iff M_1 = M \neq \mathbb{N}_4))$.

Now we make use of this rule: Let P, Q, P', Q' be propositions. Suppose we have (P $\vee$ Q), (P => P') and (Q => Q'). Then, we can conclude that (P' $\vee$ Q').

We apply the rule with

P := (5.1)
Q := (5.2)
P' := (7.1)
Q' := (7.2)

and obtain

(7.1) $((\neg SSGB \iff M_2 = M = \mathbb{N}_4) \quad \wedge \quad (\neg SSGB \iff M_2 = M \neq \mathbb{N}_4))$

(7) $\vee$

(7.2) $((\quad SSGB \iff M_1 = M = \mathbb{N}_4) \quad \wedge \quad (\quad SSGB \iff M_1 = M \neq \mathbb{N}_4))$.

By transitivity of equivalence, from (7.1) we get that $M_2 = M = \mathbb{N}_4$ is equivalent to $M_2 = M \neq \mathbb{N}_4$, which is false. Similarly, from (7.2) we get that $M_1 = M = \mathbb{N}_4$ is equivalent to $M_1 = M \neq \mathbb{N}_4$, which is false too.

Therefore, we obtain

(7.1) => FALSE

and

(7.2) => FALSE.

So, (7) implies (FALSE $\vee$ FALSE), which is equivalent to FALSE.

□

Remark 1. The above proof uses the definition of a set under an assumption. By generalizing part of the proof argument, we will now show that this kind of set definition leads to another inconsistency in ZFC.

Let P be a proposition and let A and B be non-empty sets. We define

$A_1 := \{ a \in A \mid P \text{ holds} \}$ and $A_2 := \{ a \in A \mid \neg P \text{ holds} \}$.

We consider the statement

(F1) $((\ P \ \Rightarrow \ A_1 = A = B) \ \wedge \ (\ P \ \Rightarrow \ A_1 = A \neq B))$

(F) $\vee$

(F2) $((\neg P \ \Rightarrow \ A_2 = A = B) \ \wedge \ (\neg P \ \Rightarrow \ A_2 = A \neq B))$.

Then, the contradiction $((F) \wedge \neg(F))$ can be derived.

Proof. Since either P or ¬P is false, either (F1) or (F2) is trivially true. So, (F) is true.

On the other hand, since

$P \Rightarrow A_1 = A$ and $\neg P \Rightarrow A_1 = \{ \} \neq A$

and

$\neg P \Rightarrow A_2 = A$ and $P \Rightarrow A_2 = \{ \} \neq A$,

the implications in (F1) and (F2) are in fact equivalences.

Then, by transitivity of equivalence, from (F1) we get that $A_1 = A = B$ is equivalent to $A_1 = A \neq B$, which is false. Similarly, from (F2) we get that $A_2 = A = B$ is equivalent to $A_2 = A \neq B$, which is false too.

Therefore, we obtain

(F1) => FALSE

and

(F2) => FALSE.

So, (F) implies (FALSE $\vee$ FALSE), which is equivalent to FALSE. And so, (F) is false.

□

Remark 2. In the event that in the future the definition of a set under an assumption is ruled out by the axiom system, we now sketch an alternative for the proof of the number-theoretic contradiction that does not require such a set definition.

We express the set S_g by an infinite matrix where each k-th row, k ≥ 1, is formed by all triple components pk, mk, qk. It starts as follows.

$3{\cdot}1$ $4{\cdot}1$ $5{\cdot}1$ $3{\cdot}1$ $5{\cdot}1$ $7{\cdot}1$ ... $5{\cdot}1$ $6{\cdot}1$ $7{\cdot}1$ $5{\cdot}1$ $8{\cdot}1$ $11{\cdot}1$ ...
$3{\cdot}2$ $4{\cdot}2$ $5{\cdot}2$ $3{\cdot}2$ $5{\cdot}2$ $7{\cdot}2$ ... $5{\cdot}2$ $6{\cdot}2$ $7{\cdot}2$ $5{\cdot}2$ $8{\cdot}2$ $11{\cdot}2$ ...
...
...
...

By property (C) described in the main proof, the complete matrix represents all elements of $\mathbb{N}_3$ in a structured form. We imagine the matrix twice, one on the left and another identical on the right.

Now we consider the case ¬SSGB for the left matrix and the case SSGB for the right matrix, i.e. on the left there is an n ≥ 4 in addition to all m, and on the right there is no additional n. Then, due to (C), the assumed n as well as every multiple nk, k ≥ 1, is equal to some matrix element that exists in both matrices. Therefore, the matrices are the same in both cases.

On the other hand, there is a column mk = nk, k ≥ 1, in the right matrix that does not exist in the left matrix. So the matrices are different in the two cases. This is a contradiction.