

Goldbach's Conjecture — Towards the Inconsistency of Arithmetic

Ralf Wüsthofen

Abstract. This paper proves that ZFC and Peano arithmetic (PA) are inconsistent, the latter result being a corollary of the former. We introduce a strengthened form of the strong Goldbach conjecture and, assuming consistency, establish the following contradiction. Based on two properties of an infinite set, which we use to reformulate the conjecture, we either prove that the conjecture leads to FALSE, or that its negation leads to FALSE. This is equivalent to saying that we either have a proof of the conjecture or a proof of its negation. However, this is false, as we actually have no proof for either statement. We apply elementary number theory, where the constructive role of prime numbers within the natural numbers is a key point.

In a further corollary, we show that even if ZFC and PA were sound (which they are not due to the inconsistency), the conjecture would be independent of ZFC and PA, i.e., ZFC (PA) could neither prove nor disprove the conjecture. We also show that this is true for the original strong Goldbach conjecture. The consequence of this is that both the original and the strengthened conjecture are true.

Introduction. [A comprehensive introduction will be added later. It will refer, among other things, to this motivational article [1] and this expository article [2].]

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

We use the syntactic entailment symbol \vdash to make statements of the form $\vdash P$ for some statement P , which means that there exists a proof of P .

Let $\vdash_w P$ be the notation for the statement "we have a proof of P ", which means that, within a proof, there is a proof of P from the preceding steps, that is, up to this point we have constructed a proof of P .

Let SSGB denote the following strengthened form of the strong Goldbach conjecture: *Every even number greater than 6 is the sum of two distinct odd primes.*

Theorem. *ZFC is inconsistent.*

Proof. Let us assume that ZFC is consistent. We will show that this leads to a contradiction.

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

S_g has the following two properties.

First, every element of \mathbb{N}_3 can be expressed by a S_g triple component (" \mathbb{N}_3 covering"). We prove this by dividing it into the following three cases.

- (i) $a \in \mathbb{N}_3$ is prime. Then, $a = pk$ with $p \in \mathbb{P}_3, k = 1$.
- (ii) $a \in \mathbb{N}_3$ is composite and not a power of 2. Then, $a = pk$ with $p \in \mathbb{P}_3, k \neq 1$.
- (iii) $a \in \mathbb{N}_3$ is a power of 2. Then, $a = (p + q)k / 2$ with $p = 3, q = 5, k = (a \text{ power of } 2)$.

So we have

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

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

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

There is the following relationship between SSGB and S_g .

Since SSGB is equivalent to saying that every integer $n \geq 4$ is the arithmetic mean of two distinct odd primes, we have

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

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

So, under the assumption $\neg \text{SSGB}$ there is an $n \in \mathbb{N}_4$ that is different from all m defined in S_g , whereas under the assumption SSGB there is no such n .

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

Property (C) implies that if $\neg \text{SSGB}$ holds, n equals a component of some S_g triple. Also, (C) implies that if SSGB holds, instead of n , any $a \in \mathbb{N}_3$ equals a component of some S_g triple.

Property (M) excludes the possibility that if $\neg\text{SSGB}$ holds, n is the arithmetic mean of a pair of distinct odd primes not used in S_g . So, (M) excludes the possibility that the question of whether SSGB holds or not depends on whether (M) holds or not.

The outline of the proof is now as follows.

Based on the properties (C) and (M), we prove that, assuming $\neg\text{SSGB}$, the set S_g can be written as the union of the following triples.

- (a) S_g triples of the form $(pk = n, mk, qk)$ with $k = 1$, if n is prime, due to (C)
- (b) S_g triples of the form $(pk = n, mk, qk)$ with $k \neq 1$, if n is composite and not a power of 2, due to (C)
- (c) S_g triples of the form $(3k, 4k = n, 5k)$ with $k = (\text{a power of } 2)$, if n is a power of 2, due to (C)
- (d) all other S_g triples of the form $(pk = n, mk, qk)$ or $(pk, mk = n, qk)$ or $(pk, mk, qk = n)$
- (e) S_g triples of the form $(pk \neq n, mk \neq n, qk \neq n)$.

Since under the assumption SSGB there is no n as above, again based on (C) and (M), we prove that, assuming SSGB, the set S_g can be written as the above union of triples, where n is replaced by any $a \in \mathbb{N}_3$.

This means that S_g , and therefore the set of numbers m defined in S_g , is always the same set, regardless of whether SSGB or $\neg\text{SSGB}$ is assumed. This conflicts with the fact that under the assumption SSGB the numbers m take all integer values ≥ 4 whereas under the assumption $\neg\text{SSGB}$ they don't. We show that the consequence of this is that we either have a proof that the assumption SSGB leads to FALSE, or that we have a proof that the assumption $\neg\text{SSGB}$ leads to FALSE, which is equivalent to stating that we either have a proof of SSGB or a proof of $\neg\text{SSGB}$. However, this is false, as we actually have no proof for either of them and as we assume ZFC to be consistent.

To formalize this, we make the following definitions.

For each $a \in \mathbb{N}_3$, we define

$$S_{g+}(a) := \{ (pk, mk, qk) \in S_g \mid pk = a \vee mk = a \vee qk = a \}$$

$$S_{g-}(a) := \{ (pk, mk, qk) \in S_g \mid pk \neq a \wedge mk \neq a \wedge qk \neq a \}.$$

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

Then, based on (G) and (NG), we obtain, due to (C) and (M),

$$(1.1) \quad \forall a \in \mathbb{N}_3 \quad \vdash (SSGB \Rightarrow S_1 = S_{g^+}(a) \cup S_{g^-}(a))$$

\wedge

$$(1.2) \quad \vdash (\neg SSGB \Rightarrow S_2 = S_{g^+}(n) \cup S_{g^-}(n)).$$

So, since $S_{g^+}(n) \cup S_{g^-}(n)$ is independent of n ,

$$(1.1') \quad \forall a \in \mathbb{N}_3 \quad \vdash (SSGB \Rightarrow S_1 = S_{g^+}(a) \cup S_{g^-}(a))$$

\wedge

$$(1.2') \quad \forall a \in \mathbb{N}_3 \quad \vdash (\neg SSGB \Rightarrow S_2 = S_{g^+}(a) \cup S_{g^-}(a)).$$

Now we use 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; $1 \leq i \leq z$.

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

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

Then, applying the principle above to the middle component of the triples (pk, mk, qk) , we obtain from $((1.1') \wedge (1.2'))$ by transitivity

$$(2.1) \quad \forall k \in \mathbb{N} \quad \forall a \in \mathbb{N}_3 \quad \vdash (\text{SSGB} \Rightarrow M_1(k) = \{ mk \mid (pk, mk, qk) \in S_{g^+}(a) \cup S_{g^-}(a) \})$$

$$\wedge$$

$$(2.2) \quad \forall k \in \mathbb{N} \quad \forall a \in \mathbb{N}_3 \quad \vdash (\neg \text{SSGB} \Rightarrow M_2(k) = \{ mk \mid (pk, mk, qk) \in S_{g^+}(a) \cup S_{g^-}(a) \}).$$

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

$$(2.1') \quad \forall a \in \mathbb{N}_3 \quad \vdash (\text{SSGB} \Rightarrow M_1 = \{ m \mid (p, m, q) \in S_{g^+}(a) \cup S_{g^-}(a) \})$$

$$\wedge$$

$$(2.2') \quad \forall a \in \mathbb{N}_3 \quad \vdash (\neg \text{SSGB} \Rightarrow M_2 = \{ m \mid (p, m, q) \in S_{g^+}(a) \cup S_{g^-}(a) \}).$$

Since $a \in \mathbb{N}_3$ is an arbitrary constant in (2.1') and (2.2'), we can apply the \forall -introduction rule of sequent calculus and get

$$(2.1'') \quad \vdash \forall x \in \mathbb{N}_3 \quad (\text{SSGB} \Rightarrow M_1 = \{ m \mid (p, m, q) \in S_{g^+}(x) \cup S_{g^-}(x) \})$$

$$\wedge$$

$$(2.2'') \quad \vdash \forall x \in \mathbb{N}_3 \quad (\neg \text{SSGB} \Rightarrow M_2 = \{ m \mid (p, m, q) \in S_{g^+}(x) \cup S_{g^-}(x) \}).$$

Now we make use of the following metamathematical analogue of the first-order logic rule $\forall y (P(y) \wedge Q(y)) \Leftrightarrow (\forall y P(y)) \wedge (\forall y Q(y))$.

Lemma. (Distribution of Universal Quantifier over Conjunction in Proofs)

Let T be a formal theory, and let $P(y)$ and $Q(y)$ be formulas. Then,

$$T \vdash \forall y (P(y) \wedge Q(y)) \iff (T \vdash \forall y P(y)) \wedge (T \vdash \forall y Q(y)).$$

(The lemma holds in standard proof systems for first-order logic; see standard textbooks, e.g. [3]).

Applying the lemma to ZFC, we obtain that $((2.1'') \wedge (2.2''))$ is equivalent to

$$(2) \vdash \forall x \in \mathbb{N}_3$$

$$((\text{SSGB} \Rightarrow M_1 = \{ m \mid (p, m, q) \in S_{g^+}(x) \cup S_{g^-}(x) \})$$

\wedge

$$(\neg \text{SSGB} \Rightarrow M_2 = \{ m \mid (p, m, q) \in S_{g^+}(x) \cup S_{g^-}(x) \})).$$

Now, for each $k \in \mathbb{N}$ we define $M(k) := \{ mk \mid (pk, mk, qk) \in S_g \}$. Then, since $\forall a \in \mathbb{N}_3 \vdash S_{g^+}(a) \cup S_{g^-}(a) = S_g$, by applying again the above principle of triples (pk, mk, qk) and their middle component, we get

$$\forall k \in \mathbb{N} \quad \forall a \in \mathbb{N}_3 \quad \vdash \{ mk \mid (pk, mk, qk) \in S_{g^+}(a) \cup S_{g^-}(a) \} = M(k).$$

Setting $M := M(1)$,

$$\forall a \in \mathbb{N}_3 \quad \vdash \{ m \mid (p, m, q) \in S_{g^+}(a) \cup S_{g^-}(a) \} = M.$$

Applying the above \forall -introduction rule,

$$\vdash \forall x \in \mathbb{N}_3 \quad \{ m \mid (p, m, q) \in S_{g^+}(x) \cup S_{g^-}(x) \} = M.$$

Since M is either equal to \mathbb{N}_4 or equal to some non-empty proper subset U of \mathbb{N}_4 ,

$$\exists! X \in \{ \mathbb{N}_4, U \} \quad \vdash \quad \forall x \in \mathbb{N}_3 \quad \{ m \mid (p, m, q) \in S_{g^+}(x) \cup S_{g^-}(x) \} = X.$$

Since (2) is not within the scope of the existential quantifier,

$$\exists! X \in \{ \mathbb{N}_4, U \} \quad ((\vdash \forall x \in \mathbb{N}_3 \quad \{ m \mid (p, m, q) \in S_{g^+}(x) \cup S_{g^-}(x) \} = X) \quad \wedge \quad (2)).$$

Using the above lemma again,

$$\begin{aligned} \exists! X \in \{ \mathbb{N}_4, U \} \quad \vdash \quad \forall x \in \mathbb{N}_3 \\ ((\text{SSGB} \Rightarrow M_1 = \{ m \mid (p, m, q) \in S_{g^+}(x) \cup S_{g^-}(x) \}) \\ \wedge \\ (\neg \text{SSGB} \Rightarrow M_2 = \{ m \mid (p, m, q) \in S_{g^+}(x) \cup S_{g^-}(x) \}) \\ \wedge \\ (\{ m \mid (p, m, q) \in S_{g^+}(x) \cup S_{g^-}(x) \} = X)). \end{aligned}$$

This yields

$$\begin{aligned} \exists! X \in \{ \mathbb{N}_4, U \} \quad \vdash \quad \forall x \in \mathbb{N}_3 \\ ((\text{SSGB} \Rightarrow (M_1 = \{ m \mid (p, m, q) \in S_{g^+}(x) \cup S_{g^-}(x) \} \\ \wedge \\ \{ m \mid (p, m, q) \in S_{g^+}(x) \cup S_{g^-}(x) \} = X)) \\ \wedge \\ (\neg \text{SSGB} \Rightarrow (M_2 = \{ m \mid (p, m, q) \in S_{g^+}(x) \cup S_{g^-}(x) \} \\ \wedge \\ \{ m \mid (p, m, q) \in S_{g^+}(x) \cup S_{g^-}(x) \} = X))). \end{aligned}$$

Again using the lemma,

$$\exists! X \in \{ \mathbb{N}_4, U \}$$

$$(\vdash \forall x \in \mathbb{N}_3 \quad (\text{SSGB} \Rightarrow (M_1 = \{ m \mid (p, m, q) \in S_{g^+}(x) \cup S_{g^-}(x) \} \\ \wedge \{ m \mid (p, m, q) \in S_{g^+}(x) \cup S_{g^-}(x) \} = X)))$$

\wedge

$$(\vdash \forall x \in \mathbb{N}_3 \quad (\neg \text{SSGB} \Rightarrow (M_2 = \{ m \mid (p, m, q) \in S_{g^+}(x) \cup S_{g^-}(x) \} \\ \wedge \{ m \mid (p, m, q) \in S_{g^+}(x) \cup S_{g^-}(x) \} = X))).$$

By the transitivity of "=" and the transitivity of "=>", we obtain

$$(3) \exists! X \in \{ \mathbb{N}_4, U \} \quad (\vdash (\text{SSGB} \Rightarrow M_1 = X) \quad \wedge \quad \vdash (\neg \text{SSGB} \Rightarrow M_2 = X)).$$

Since the statements $(\text{SSGB} \Rightarrow M_1 = X)$ and $(\neg \text{SSGB} \Rightarrow M_2 = X)$ depend on X and since X is the unique element of $\{ \mathbb{N}_4, U \}$ such that these statements hold, we will make use of the following rule.

Let $P_1(A)$ and $P_2(A)$ be statements that depend on a set A , and let A be the unique element of $\{ B_1, B_2, \dots, B_z \}$ such that $P_1(A)$ and $P_2(A)$ hold, where each B_i , $1 \leq i \leq z$, is a non-empty subset of \mathbb{N} .

Then,

$$(\exists! A \in \{ B_1, B_2, \dots, B_z \} \quad (\vdash P_1(A) \wedge \vdash P_2(A))) \Rightarrow ((\vdash P_1(B_1) \wedge \vdash P_2(B_1)) \vee \\ (\vdash P_1(B_2) \wedge \vdash P_2(B_2)) \vee \dots \vee (\vdash P_1(B_z) \wedge \vdash P_2(B_z))).$$

We apply the rule with

$$P_1(A) = (\text{SSGB} \Rightarrow M_1 = A), P_2(A) = (\neg \text{SSGB} \Rightarrow M_2 = A)$$

$$z = 2, B_1 = \mathbb{N}_4, B_2 = U.$$

Then, since the left-hand side of the rule is true, we obtain

$$(3.1) \quad (\vdash (\text{SSGB} \Rightarrow M_1 = \mathbb{N}_4) \quad \wedge \quad \vdash (\neg \text{SSGB} \Rightarrow M_2 = \mathbb{N}_4))$$

\vee

$$(3.2) \quad (\vdash (\text{SSGB} \Rightarrow M_1 = U) \quad \wedge \quad \vdash (\neg \text{SSGB} \Rightarrow M_2 = U)).$$

This implies

$$(4.1) \quad \vdash (\neg \text{SSGB} \Rightarrow M_2 = \mathbb{N}_4)$$

\vee

$$(4.2) \quad \vdash (\text{SSGB} \Rightarrow M_1 = U).$$

On the other hand, we have $\vdash (\text{SSGB} \Rightarrow M = \mathbb{N}_4)$ and $\vdash (\neg \text{SSGB} \Rightarrow M = U)$. Therefore, since $\vdash (\text{SSGB} \Rightarrow M_1 = M)$, $\vdash (\neg \text{SSGB} \Rightarrow M_2 = M)$, $\vdash (\neg \text{SSGB} \Rightarrow M_1 = \{ \})$ and $\vdash (\text{SSGB} \Rightarrow M_2 = \{ \})$, we get

$$(5.1) \quad \vdash (\text{SSGB} \Leftrightarrow M_1 = \mathbb{N}_4)$$

\wedge

$$(5.2) \quad \vdash (\neg \text{SSGB} \Leftrightarrow M_2 = U).$$

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

$$\vdash (\text{SSGB} \Rightarrow M_2 = \{ \} \neq \mathbb{N}_4)$$

and

$\vdash (\neg \text{SSGB} \Rightarrow M_1 = \{\} \neq U),$

we have

(6.1) $\vdash M_1 \neq U$

\wedge

(6.2) $\vdash M_2 \neq \mathbb{N}_4.$

Using $((6.1) \wedge (6.2)), ((4.1) \vee (4.2))$ yields

(7.1) $\vdash (\neg \text{SSGB} \Rightarrow \text{FALSE})$

\vee

(7.2) $\vdash (\text{SSGB} \Rightarrow \text{FALSE}).$

And this yields

(8.1) $\vdash \text{SSGB}$

\vee

(8.2) $\vdash \neg \text{SSGB}.$

Now, all the above derived statements of the form $\vdash P$ can be replaced by $\vdash_w P$, since each of these statements follows from the preceding steps and thus P is proved by the preceding steps.

In particular, the three \vdash -related rules, i.e., the \forall -introduction rule, the lemma, and the rule for splitting (3) into $((3.1) \vee (3.2))$, also apply to the operator \vdash_w . The reason is that the rules depend only on structural properties of proofs, and \vdash_w does not alter those structures. \vdash_w does not introduce new inference rules or change what counts as a proof; it just allows us to refer to a completed derivation.

Then, with this replacement, we finally obtain

(8.1') $\vdash_w \text{SSGB}$

\vee

(8.2') $\vdash_w \neg \text{SSGB}$.

On the other hand, since this paper contains neither a proof of SSGB nor of $\neg \text{SSGB}$ and since we assumed that ZFC is consistent (inconsistency would make any statement provable), (8.1') and (8.2') are both false. So we have $\neg ((8.1') \vee (8.2'))$, which is a contradiction.

□

Corollary 1. *Peano arithmetic (PA) is inconsistent.*

Proof. The term S_g from the above inconsistency proof is not a standard part of PA, but it can easily be defined within PA. This also applies to all other sets used in that proof, since they are all based on S_g or on \mathbb{N} . Therefore, the corollary is proved in the same way by using the operators \vdash and \vdash_w in the system PA.

□

Corollary 2. *If ZFC and PA are sound, then SSGB is independent of ZFC and PA, i.e., ZFC (PA) can neither prove nor disprove SSGB.*

Proof. Let us assume that ZFC (PA) is sound, i.e., all provable statements in ZFC (PA) are true. Then we apply the \forall -introduction rule to $((1.1') \wedge (1.2'))$ of the proof above and obtain

$$(1.1'') \vdash \forall x \in \mathbb{N}_3 \quad (\text{SSGB} \Rightarrow S_1 = S_{g^+}(x) \cup S_{g^-}(x))$$

\wedge

$$(1.2'') \vdash \forall x \in \mathbb{N}_3 \quad (\neg \text{SSGB} \Rightarrow S_2 = S_{g^+}(x) \cup S_{g^-}(x)).$$

Suppose now that SSGB is provable in ZFC (PA), i.e., $\vdash \text{SSGB}$.

Then, using the “ \vdash ” version of modus ponens, which is

$$(\vdash P \wedge \vdash (P \Rightarrow Q)) \Rightarrow \vdash Q,$$

from (1.1'') we get

$$(S1) \vdash \forall x \in \mathbb{N}_3 \quad S_1 = S_{g^+}(x) \cup S_{g^-}(x).$$

Using the lemma of the above proof, (S1) is equivalent to

$$(S1.1) \vdash \forall x \in \mathbb{N}_3 \quad (\text{SSGB} \Rightarrow S_1 = S_{g^+}(x) \cup S_{g^-}(x))$$

\wedge

$$(S1.2) \vdash \forall x \in \mathbb{N}_3 \quad (\neg \text{SSGB} \Rightarrow S_1 = S_{g^+}(x) \cup S_{g^-}(x)).$$

Since under the assumption $\neg \text{SSGB}$ $S_1 = \{ \}$ and $S_{g^+}(x) \cup S_{g^-}(x) \neq \{ \}$, and since we assumed that ZFC (PA) is sound, (S1.2) is false.

To see this, let us assume (S1.2) is true. Then, due to the soundness of ZFC (PA), $(\neg \text{SSGB} \Rightarrow S_1 = S_{g^+}(x) \cup S_{g^-}(x))$ must be true in every model of ZFC (PA). But in any model with $\neg \text{SSGB}$ true and $S_1 = \{ \}$, the antecedent is true and the consequent is false, so the implication is false. Hence the assumption was false.

Since (S1.2) is false, (S1) is false, and so the assumption that SSGB is provable in ZFC (PA) was false.

Similarly for the assumption $\vdash \neg \text{SSGB}$, for which we use (1.2").

□

Remark. The result from Corollary 2 also applies to the original strong Goldbach conjecture:

$\text{SGB} := \text{Every even number greater than 2 is the sum of two primes.}$

Because in the above proof of the Theorem, SSGB can be replaced by

$\text{SGB}' := \text{Every even number greater than 4 is the sum of two odd primes,}$

and S_g by

$S_{g'} := \{ (pk, mk, qk) \mid k, m \in \mathbb{N}; p, q \in \mathbb{P}_3, p \leq q; m = (p + q) / 2 \}.$

(M), (G) and (NG) must then be adjusted accordingly. This adapted proof then works in the same way and in particular yields $((1.1') \wedge (1.2'))$.

Note. The consequence of Corollary 2 and the above remark is that both SGB and SSGB are true, because $\neg \text{SGB} \Rightarrow \vdash \neg \text{SGB}$ and $\neg \text{SSGB} \Rightarrow \vdash \neg \text{SSGB}$.

References

- [1] *Warning Signs of a Possible Collapse of Contemporary Mathematics*, by Edward Nelson (2006). <https://web.math.princeton.edu/~nelson/papers/warn.pdf>
- [2] *The Consistency of Arithmetic*, by Timothy Y. Chow (2018). <https://arxiv.org/pdf/1807.05641>
- [3] *Introduction to Metamathematics*, by Stephen Cole Kleene (North-Holland, 1952).