

An Equivalent Problem To The Twin Prime Conjecture

Francesca Balestrieri*

July 1, 2011

Abstract

In this short paper we will show, via elementary arguments, the equivalence of the Twin Prime Conjecture to a problem which might be simpler to prove. Some conclusions are drawn, and it is shown that proving the Twin Prime Conjecture is equivalent to proving that there cannot be an infinite string of consecutive natural numbers satisfying some specified equations.

1 Main Theorem

The main theorem of this paper is the following.

Theorem 1.1 (Main Theorem). *The Twin Prime Conjecture is true if, and only if, there exist infinitely many $n \in \mathbb{N}$ such that $n \neq 6xy + x - y$ and $n \neq 6xy + x + y$ and $n \neq 6xy - x - y$, for all $x, y \in \mathbb{N}$.*

In other words, the Conjecture is true iff $\exists N \in \mathbb{N}$ such that $\forall n \geq N$, n is of one of the forms $n = 6xy + x - y$ or $n = 6xy + x + y$ or $n = 6xy - x - y$, for some $x, y \in \mathbb{N}$.

In order to prove the Main Theorem, we will need to prove some preliminary results; two thirds of this paper are devoted to this aim.

2 Preliminary Results

Consider the two sequences:

$$a_n = 6n + 1 \tag{1}$$

$$b_n = 6n - 1 \tag{2}$$

A simple argument shows that these two sequences generate all the prime numbers (and some other non-prime numbers). The following Lemma is a useful criterion which tells us for which n the terms a_n and b_n are non-prime, and hence, by complement, for which n the terms a_n and b_n are prime.

*fb340@cam.ac.uk

Lemma 2.1. *Let a_n and b_n be the two sequences specified before. Then*

$$a_n \text{ non - prime} \iff n = 6xy + x - y$$

$$b_n \text{ non - prime} \iff n = 6xy + x + y \text{ or } n = 6xy + x - y$$

for all $x, y \in \mathbb{N}$.

To prove this Lemma, we need to prove some minor lemmata first.

2.1 Some proofs

Let $A = \{a_n : n \in \mathbb{N}\}$ and let $B = \{b_n : n \in \mathbb{N}\}$, where a_n and b_n are the sequences (1) and (2) respectively.

Lemma 2.2. *It is not possible to express any term a_k of the sequence a_n as the product $a_x \cdot a_y$ for any $(a_x, a_y) \in A \times A$, nor to express it as the product $b_x \cdot b_y$ for any $(b_x, b_y) \in B \times B$. It is possible to express a term a_k of the sequence a_n as the product $a_t \cdot b_r$ of a couple of numbers $(a_t, b_r) \in A \times B$ if, and only if, $k = 6tr + t - r$. In other words, $a_k = a_t \cdot b_r$ if, and only if, $k = 6tr + t - r$.*

Proof. Let $a_k = 6k - 1$, $a_t = 6t - 1$, $a_x = 6x - 1$, $a_y = 6y - 1$ and $b_r = 6r + 1$.

The last part of the theorem is almost trivial. In fact,

$$\begin{aligned} a_t \cdot b_r &= (6t - 1) \cdot (6r + 1) \\ &= 36tr - 6r + 6t - 1 \\ &= 6(6tr - r + t) - 1 \end{aligned}$$

and hence $a_k = a_t \cdot b_r$ if, and only if, $k = 6tr + t - r$.

For the first part, consider

$$\begin{aligned} a_x \cdot a_y &= (6x - 1) \cdot (6y - 1) \\ &= 36xy - 6x - 6y + 1 \\ &= 36xy - 6x - 6y + 2 - 1 \\ &= 2(18xy - 3x - 3y + 1) - 1. \end{aligned}$$

Hence, we must show that $18xy - 3x - 3y + 1$ is not divisible by 3. This is easy, since

$$18xy - 3x - 3y + 1 = 3(9xy - x - y) + 1 \equiv 1 \pmod{3}.$$

Therefore, there are no $x, y \in \mathbb{N}$ such that $a_x \cdot a_y = a_k$.

Similarly, consider

$$\begin{aligned} b_x \cdot b_y &= (6x + 1) \cdot (6y + 1) \end{aligned}$$

$$\begin{aligned}
&= 36xy + 6x + 6y + 1 \\
&= 36xy + 6x + 6y + 2 - 1 \\
&= 2(18xy + 3x + 3y + 1) - 1.
\end{aligned}$$

Hence, we must show that $18xy+3x+3y+1$ is not divisible by 3. Again, this is straightforward since

$$18xy + 3x + 3y + 1 = 3(9xy + x + y) + 1 \equiv 1 \pmod{3}.$$

Therefore, there are no $x, y \in \mathbb{N}$ such that $b_x \cdot b_y = a_k$. \square

A similar lemma can be proved for the terms of the sequence b_n .

Lemma 2.3. *It is not possible to express any term b_k of the sequence b_n as the product $a_x \cdot d_y$ for any $(a_x, d_y) \in A \times B$. It is possible to express a term b_k of the sequence b_n as the product $a_t \cdot a_r$ of a couple of numbers $(a_t, a_r) \in A \times A$ if, and only if, $k = 6tr - t - r$, and as the product $b_t \cdot b_r$ of a couple of numbers $(b_t, b_r) \in B \times B$ if, and only if, $k = 6tr + t + r$. In other words, $b_k = a_t \cdot a_r$ if, and only if, $k = 6tr - t - r$ and $b_k = b_t \cdot b_r$ if, and only if, $k = 6tr + t + r$.*

Proof. Let $b_k = 6k + 1$, $a_t = 6t - 1$, $a_r = 6r - 1$, $a_x = 6x - 1$, $b_t = 6t + 1$, $b_r = 6r + 1$ and $b_y = 6y + 1$.

The last part of the theorem is almost trivial. In fact,

$$\begin{aligned}
&a_t \cdot a_r \\
&= (6t - 1) \cdot (6r - 1) \\
&= 36tr - 6r - 6t + 1 \\
&= 6(6tr - r - t) + 1
\end{aligned}$$

and hence $b_k = a_t \cdot a_r$ if, and only if, $k = 6tr - t - r$.

Also,

$$\begin{aligned}
&b_t \cdot b_r \\
&= (6t + 1) \cdot (6r + 1) \\
&= 36tr + 6r + 6t + 1 \\
&= 6(6tr + r + t) + 1
\end{aligned}$$

and hence $b_k = b_t \cdot b_r$ if, and only if, $k = 6tr + t + r$.

For the first part, consider

$$\begin{aligned}
&a_x \cdot b_y \\
&= (6x - 1) \cdot (6y + 1) \\
&= 36xy + 6x - 6y - 1 \\
&= 36xy + 6x - 6y - 2 + 1 \\
&= 2(18xy + 3x - 3y - 1) + 1.
\end{aligned}$$

Hence, we must show that $18xy + 3x - 3y - 1$ is not divisible by 3. This is easy, since

$$18xy + 3x - 3y - 1 = 3(9xy + x - y) - 1 \equiv -1 \pmod{3}.$$

Therefore, there are no $x, y \in \mathbb{N}$ such that $a_x \cdot b_y = b_k$. \square

The following is an obvious result.

Lemma 2.4. *Given any term a_k of the sequence a_n , all the primes smaller than a_k have already been generated by the sequences a_n and b_n for $n < k$. Similarly, given any term b_k of the sequence b_n , all the primes smaller than b_k have already been generated by the sequences a_n and b_n for $n \leq k$.*

Proof. Consider the sequence $p_n = (a_1, b_1, a_2, b_2, a_3, b_3, \dots, a_k, b_k, \dots)$. Evidently, p_n is a strictly increasing sequence. Furthermore, p_n contains all the prime numbers. Suppose that one prime number p smaller than a_k is not generated before the term a_k ; then, since all the prime numbers are generated by the sequence p_n , p must be generated after a_k . But the sequence p_n is strictly increasing, and therefore p is greater than a_k . This is a contradiction, and hence all the primes smaller than a_k are generated before a_k .

The second half of the Lemma can be proved in a similar way. □

2.2 More proofs

A few remarks and observations are now necessary.

2.2.1

Given a term a_k , we have shown that

$$a_k = a_t \cdot b_r \iff k = 6tr + t - r;$$

otherwise, a_k cannot be expressed as the product of any other pair of terms in $A \times A$, $B \times B$ or $A \times B$.

This can be generalised.

Note: An improper but self-evident use of notation will be made in the next paragraph.

Let a_k be a non-prime term of the sequence a_n . Using Lemma 2.4, all the factors of a_k will be terms a_i, b_j for some $i, j < k$. Let say that α factors of a_k belong to the set A , and β factors of a_k belong to the set B . Since a_k is non-prime, $\alpha + \beta > 1$. In short form,

$$a_k = A^\alpha \cdot B^\beta \quad (\text{with } \alpha + \beta > 1),$$

where A (improperly) denotes an element of A and B (improperly) denotes an element of B .

There are a few cases to consider, depending on the values of α and β . Notice that in each case we will repetively use Lemma 2.2 and Lemma 2.3.

1. If $\alpha = 0$, then for any natural value of $\beta (> 1)$, we will have that $a_k = B^\beta$. But B^β is an element of the set B . Hence, we have an equation with an element of the set A in the LHS and an element of the set B in the RHS, and $A \cap B = \emptyset$. This is nonsense, and hence it cannot be that $\alpha = 0$.

2. If α is even, then for any $\beta \in \mathbb{N} \cup \{0\}$, we can write a_k as

$$a_k = A^\alpha \cdot B^\beta = (A \cdot A) \cdot (A \cdot A) \cdot \dots \cdot (A \cdot A) \cdot B^\beta = B^{\alpha/2} \cdot B^\beta = B^{(\alpha/2)+\beta}$$

and we have a situation analogous to the one in case 1. Hence, α cannot be even.

3. If α is odd, then $\alpha - 1$ is positive even or zero) and, for any $\beta \in \mathbb{N} \cup \{0\}$, we can write a_k as

$$a_k = A^\alpha \cdot B^\beta = A \cdot A^{\alpha-1} \cdot B^\beta = A \cdot B^{(\alpha-1)/2} \cdot B^\beta = A \cdot B^{(\alpha-1)/2+\beta}$$

and this is consistent with what we have already proved, since A denotes an element a_t of the set A and $B^{(\alpha-1)/2+\beta}$ is an element b_r of B , that is, $A \cdot B^{(\alpha-1)/2+\beta} = a_t \cdot b_r$ for some $t, r \in \mathbb{N}$.

So, if a_k is non-prime, it is necessarily of the form $a_k = A^\alpha \cdot B^\beta$, where α is odd, β is any number in $\mathbb{N} \cup \{0\}$, and $(\alpha + \beta) > 1$. Of course, the converse is also true.

Hence, a_k is non-prime $\iff a_k = A^\alpha \cdot B^\beta$ where α is odd, β is any number in $\mathbb{N} \cup \{0\}$, and $(\alpha + \beta) > 1 \iff a_k = a_t \cdot b_r$ for some $t, r \in \mathbb{N} \iff k = 6tr + t - r$.

By Lemma 2.4, in all the other cases a_k is prime.

2.2.2

Given a term b_k , we have shown that

$$b_k = a_t \cdot a_r \iff k = 6tr - t - r;$$

$$b_k = b_t \cdot b_r \iff k = 6tr + t + r;$$

otherwise, b_k cannot be expressed as the product of any other pair of terms in $A \times A$, $B \times B$ or $A \times B$.

This, again, can be generalised.

Note: An improper but self-evident use of notation will be made in the next paragraph.

Let b_k be a non-prime term of the sequence b_n . Using Lemma 2.4, all the factors of b_k will be terms a_i , b_j for some $i \leq k$ and some $j < k$. Let say that α factors of b_k belong to the set A , and β factors of b_k belong to the set B . Since b_k is non-prime, $\alpha + \beta > 1$. In short form,

$$b_k = A^\alpha \cdot B^\beta \quad (\text{with } \alpha + \beta > 1),$$

where A (improperly) denotes an element of A and B (improperly) denotes an element of B .

There are a few cases to consider, depending on the values of α and β . Notice that in each case we will repetively use Lemma 2.2 and Lemma 2.3.

1. If $\alpha = 0$, then for any natural value of $\beta (> 1)$, we will have that $b_k = B^\beta$, and this is consistent with what we have already proved, since B denotes an element b_t of the set B and $B^{\beta-1}$ is an element b_r of B , that is, $B \cdot B^{\beta-1} = b_t \cdot b_r$ for some $t, r \in \mathbb{N}$.
2. If α is even, then for any $\beta \in \mathbb{N} \cup \{0\}$, we can write b_k as

$$b_k = A^\alpha \cdot B^\beta = (A \cdot A) \cdot (A \cdot A) \cdot \dots \cdot (A \cdot A) \cdot B^\beta = B^{\alpha/2} \cdot B^\beta = B^{(\alpha/2)+\beta}$$

and we have a situation analogous to the one in case 1, which is consistent. Furthermore, if α is even, then $\alpha - 2$ is positive even or zero. Then for any $\beta \in \mathbb{N} \cup \{0\}$, we can write b_k as

$$b_k = A^\alpha \cdot B^\beta = A \cdot A \cdot A^{\alpha-2} \cdot B^\beta = A \cdot A \cdot B^{(\alpha-2)/2} \cdot B^\beta = (A \cdot B^{(\alpha-2)/2}) \cdot (A \cdot B^\beta)$$

and this is consistent with what we have already proved, since $(A \cdot B^{(\alpha-2)/2})$ is an element a_t of the set A and $(A \cdot B^\beta)$ is an element a_r of the set A , that is, $(A \cdot B^{(\alpha-2)/2}) \cdot (A \cdot B^\beta) = a_t \cdot a_r$ for some $t, r \in \mathbb{N}$.

3. If α is odd, then $\alpha - 1$ is positive even or zero and, for any $\beta \in \mathbb{N} \cup \{0\}$, we can write b_k as

$$b_k = A^\alpha \cdot B^\beta = A \cdot A^{\alpha-1} \cdot B^\beta = A \cdot B^{(\alpha-1)/2} \cdot B^\beta = A \cdot B^{(\alpha-1)/2+\beta}.$$

But $A \cdot B^{(\alpha-1)/2+\beta}$ is an element of the set A , and hence we have an equation with an element of the set B in the LHS and an element of the set A in the RHS. Since, $A \cap B = \emptyset$, this is nonsense, and therefore it cannot be that α is odd.

So, if b_k is non-prime, it is necessarily of the form $b_k = A^\alpha \cdot B^\beta$, where α is positive even or zero, β is any number in $\mathbb{N} \cup \{0\}$, and $(\alpha + \beta) > 1$. Of course, the converse is also true.

Hence, b_k is non-prime $\iff a_k = A^\alpha \cdot B^\beta$ where α is even positive or zero, β is any number in $\mathbb{N} \cup \{0\}$, and $(\alpha + \beta) > 1 \iff b_k = b_t \cdot b_r$ or $b_k = a_t \cdot a_r$ for some $t, r \in \mathbb{N} \iff k = 6tr + t + r$ or $k = 6tr - t - r$.

By Lemma 2.4, in all the other cases b_k is prime.

3 Proof of the Main Theorem

We are now ready to give a proof of the Main Theorem.

Theorem 3.1 (Main Theorem). *The Twin Prime Conjecture is true if, and only if, there exist infinitely many $n \in \mathbb{N}$ such that $n \neq 6xy + x - y$ and $n \neq 6xy + x + y$ and $n \neq 6xy - x - y$, for all $x, y \in \mathbb{N}$.*

Proof. Let p be prime, with $p \geq 5$. Clearly if $(p, p + 2)$ is a twin primes couple, then we must have that p belongs to the sequence a_n and $p + 2$ belongs to the sequence b_n . That is, $p = a_n = 6n - 1$ and $p + 2 = b_n = 6n + 1$, for a same $n \in \mathbb{N}$. But by Lemma 2.1, (a_n, b_n) is a twin primes couple if, and only if, $n \neq 6xy + x - y$ and $n \neq 6xy + x + y$ and $n \neq 6xy - x - y$ for all $x, y \in \mathbb{N}$. Hence, there are infinitely many twin primes couples (a_n, b_n) (and thus infinitely many twin primes) if, and only if, there exist infinitely many $n \in \mathbb{N}$ such that $n \neq 6xy + x - y$ and $n \neq 6xy + x + y$ and $n \neq 6xy - x - y$ for all $x, y \in \mathbb{N}$. This completes the proof. \square

4 Considerations

In this new form, the Twin Prime Conjecture seems to suggest a natural way of proving it which a *reductio ad absurdum* type of argument.

Note that the Lemma 2.1 proves that, for p prime such that $p \geq 5$, the twin primes couples $(p, p + 2)$ are exactly those $(a_n, b_n) = (6n - 1, 6n + 1)$ for which $n \neq 6xy + x - y$ and $n \neq 6xy + x + y$ and $n \neq 6xy - x - y$ for all $x, y \in \mathbb{N}$. Thus, Lemma 2.1 gives a way to find twin primes: it is sufficient to find an n satisfying the above conditions to get a twin primes couple $(6n - 1, 6n + 1)$.

Assuming the negation of the Conjecture would mean assuming the existence of an infinite string of consecutive natural numbers such that, for any n in this string, $n = 6xy + x - y$ or $n = 6xy + x + y$ or $n = 6xy - x - y$ for some $x, y \in \mathbb{N}$; if this could lead to a contradiction, then the Conjecture would prove to be true. (Nevertheless, a direct proof of the impossibility of constructing such an infinite string would be equally effective - if we want to prove the truth of the Conjecture, of course.)

5 References

[1] Hardy, G.H. and Wright, E.M.; (1988) *An Introduction to the Theory of Numbers*, Clarendon Press, Oxford, 5th ed.