

# Sketch Proof of the Erdős-Straus Conjecture

Christiaan Brand

December 13, 2021

The Erdős-Straus conjecture states that, for every positive integer  $n \geq 2$ , there exists a solution in positive integers  $a, b, c$  to the equation

$$\frac{4}{n} = \frac{1}{a} + \frac{1}{b} + \frac{1}{c}.$$

We provide a simple proof. First, we show that proving the general case of  $n$  is equivalent to proving the case of prime  $n$ . We rewrite the initial equation above and use this to derive the basis of our proof. We show that, in general, for each prime  $n$  there is an  $a$  from which the values of  $b, c$  can be recovered, provided that either:

1. one of the divisors  $a^2$  is congruent to 2 modulo 3, or
2. the sum of  $a$  and one of the divisors of  $a^2$  is divisible by 3, which is true in general.

---

To begin, each positive non-prime integer  $n > 1$  can be written as  $n = pq$  where  $p$  is prime and  $q > 1$  is a positive integer. Therefore, if we possess a solution in  $a, b, c$  for  $p$ , then we have an equivalent solution for  $n$ , since

$$\begin{aligned}\frac{4}{p} &= \frac{1}{a} + \frac{1}{b} + \frac{1}{c} \\ \frac{4}{n} \Rightarrow \frac{4}{pq} &= \frac{1}{aq} + \frac{1}{bq} + \frac{1}{cq}.\end{aligned}$$

We consider only the case of prime  $n$ . It is clear that each of  $a, b, c$  is either divisible by  $n$  or not, and at least one must be, as opposed to collectively sharing divisors of which the product is  $n$ . We rewrite the initial equation as

$$\begin{aligned}\frac{4}{p} &= \frac{1}{a} + \frac{1}{bp} + \frac{1}{c} \\ pb \cdot (a + c) &= ac \cdot (4b - 1) \\ \frac{bp}{4b - 1} &= \frac{ac}{a + c}.\end{aligned}\tag{1}$$

It is important to know when  $\frac{pb}{4b-1}$  will be in its lowest terms. We note that  $b$  is necessarily coprime to  $4b-1$ , so it is only when  $p$  divides  $4b-1$  that the fraction may be simplified any further.

Thus,

$$k \cdot b = ac, \quad k \cdot \frac{4b-1}{p} = a+c, \text{ if } p \mid (4b-1) \quad (2)$$

$$k \cdot bp = ac, \quad k \cdot (4b-1) = a+c, \text{ if } p \nmid (4b-1). \quad (3)$$

We introduce the  $k$  because the expansion of the left hand-sides into  $ac$  and  $a+c$  may require multiplication by a constant (i.e. multiplying the fraction by  $k/k$ ).

We rearrange the equations to solve for  $c$ , and equate them to one another such that in (2)

$$a^2 = k \cdot \frac{(a \cdot (4b-1) - bp)}{p}, \quad (4)$$

and in (3)

$$a^2 = k \cdot (a \cdot (4b-1) - bp). \quad (5)$$

We consider the above in terms of the function  $f(a)$ , a line of the form  $f(x) = Ax + B$ , such that  $a^2 = k \cdot f(a)$ . It is clear that for a given  $p$ , the line will have a “fix-point” at  $f\left(\frac{p}{4}\right) = -\frac{1}{4}$  for (4) and at  $f\left(\frac{p}{4}\right) = -\frac{p}{4}$  for (5), irrespective of the parameter  $b$ , which determines its slope.

Since we wish to know whether for a given  $p$  there exists some positive integer  $a$  such that either of (4) or (5) is satisfied, it is sufficient to know whether the line to  $f(a)$  from the fix-point has a positive integer slope. We use this fix-point to show in the case of (2) that

$$\frac{\frac{a^2}{k} + \frac{1}{4}}{a - \frac{p}{4}} = \frac{4a^2 + k}{k \cdot (4a - p)},$$

and in the case of (3) that

$$\frac{\frac{a^2}{k} + \frac{p}{4}}{a - \frac{p}{4}} = \frac{4a^2 + kp}{k \cdot (4a - p)}.$$

We set  $a^2 = k \cdot d$ , which leaves  $\frac{4d+1}{4a-p}$  and  $\frac{4d+p}{4a-p}$ , respectively.

Given the above, we consider the general case for positive integer  $Q$  such that  $4a - Q$  divides either  $4d + 1$  or  $4d + Q$ , where  $Q < 4a$ .

We call the result of either fraction  $m$  and solve for  $Q$ , then

$$\begin{aligned} \frac{4d+1}{4a-Q} &= m \\ Q &= \frac{4(am-d)-1}{m} \end{aligned} \tag{6}$$

and

$$\begin{aligned} \frac{4d+Q}{4a-Q} &= m \\ Q &= \frac{4(am-d)}{m+1}. \end{aligned} \tag{7}$$

In the case of (6) we see that  $4(am - d) - 1$  is odd, so  $m$  must be odd to divide it; i.e. for  $Q$  to be an integer, which also is odd. In the case of (7), however,  $m$  might be odd or even depending on whether  $m + 1$  is a divisor of the even number  $4(am - d)$ .

We restrict  $m$  such that  $am > d$  for the appropriate values of  $a, d$ .

Suppose that  $a$  is fixed. We enumerate the values of  $d$ , and the corresponding  $m$  and  $Q$  for both (6) and (7), where  $a = 1, 2, \dots, 5$ . The largest values of  $m$  and  $Q$  for each  $d$  are emphasized.

For  $a = 1$ , in the case of (6) and (7), respectively:

$d$	1	$d$	1
$m$	<b>5</b>	$m$	<b>3</b>
$Q$	<b>3</b>	$Q$	<b>3</b>

For  $a = 2$ :

$d$	1	2	4	$d$	1	2	4
$m$	1	<b>5</b>	3	<b>9</b>	<b>17</b>	<b>15</b>	3, 5, 7, 11
$Q$	3	<b>7</b>	5	<b>7</b>	<b>7</b>	<b>7</b>	2, 4, 5, 6

For  $a = 3$ :

$d$	1	3	9	$d$	1	3	9
$m$	1	<b>5</b>	<b>13</b>	<b>37</b>	<b>15</b>	2, 3, 5, 7, 11	<b>23</b>
$Q$	7	<b>11</b>	<b>11</b>	<b>11</b>	<b>11</b>	4, 6, 8, 9, 10	<b>11</b>

For  $a = 4$ :

$d$	1	2	4	8	16
$m$	1	<b>5</b>	1, 3	<b>9</b>	<b>17</b>
$Q$	11	<b>15</b>	7, 13	<b>15</b>	<b>15</b>

  

$d$	1	2	4	8	16
$m$	3, 4, 9	<b>19</b>	2, 5, 7, 11	<b>23</b>	3, 7, 15
$Q$	11, 12, 14	<b>15</b>	8, 12, 13, 14	<b>15</b>	8, 12, 14

For  $a = 5$ :

$d$	1	5	25
$m$	1	<b>5</b>	<b>21</b>
$Q$	15	<b>19</b>	13, 17

  

$d$	1	5	25
$m$	2, 3, 7, 11	<b>23</b>	4, 9, 19
$Q$	12, 14, 17, 18	<b>19</b>	12, 16, 18

In the case of (6), for each  $a$  and  $d = 1$  we see that the largest  $m = 5$ . The difference between consecutive largest  $m$  is  $4(d_{i+1} - d_i)$ .

In the case of (7), for each  $a$  and  $d = 1$  we see that the largest  $m = 3 + 4a$ . The difference between consecutive largest  $m$  is also  $4(d_{i+1} - d_i)$ .

The largest  $Q = 4a - 1$ , in either case.

We write the largest  $m$  for each  $d_i$  as  $M_{1,i}$  in the case of (6), and, as  $M_{2,i}$  in the case of (7). We wish to characterize the smaller values of  $m$  for each  $d_i$  in terms of these “maxima”, such that

$$Q - R = \frac{4(a \cdot (M_{1,i} - r) - d_i) - 1}{M_{1,i} - r}$$

in the case of (6), and

$$Q - R = \frac{4(a \cdot (M_{2,i} - r) - d_i)}{M_{2,i} - r + 1}$$

in the case of (7) where the smaller values of  $m$  are  $M_{1/2,i} - r$ .

These maxima can be computed with our observations above as

$$\begin{aligned} M_{1,i} &= 1 + 4 \left( 1 + \sum_{1 \leq j \leq i-1}^{i-1} (d_{j+1} - d_j) \right) \\ &= 1 + 4d_i \end{aligned} \tag{8}$$

and

$$\begin{aligned} M_{2,i} &= 3 + 4 \left( a + \sum_{1 \leq j \leq i-1}^{i-1} (d_{j+1} - d_j) \right) \\ &= 3 + 4(a + d_i - 1). \end{aligned} \tag{9}$$

We show that this is indeed the case by substituting (8) into (6), such that

$$\begin{aligned} Q &= \frac{4(a \cdot (1 + 4d_i) - d_i) - 1}{1 + 4d_i} \\ &= 4a - 1 \end{aligned}$$

and by substituting (9) into (7), such that

$$\begin{aligned} Q &= \frac{4(a \cdot (3 + 4(a + d_i - 1)) - d_i)}{3 + 4(a + d_i - 1) + 1} \\ &= 4a - 1 \end{aligned}$$

which is what we expect.

We ignore, for the moment, the maximal case of  $m$ , and consider the general case:

For the first case, we substitute (6) for  $Q$  and solve for  $r$ , which yields

$$\begin{aligned} Q - R &= \frac{4(a \cdot (m - r) - d) - 1}{m - r} \\ r &= \frac{m^2 R}{4d + mR + 1}. \end{aligned} \tag{10}$$

For the second case, we substitute (7) for  $Q$  and solve for  $r$ , which yields

$$\begin{aligned} Q - R &= \frac{4(a \cdot (m - r) - d)}{m - r + 1} \\ r &= \frac{(m + 1)^2 \cdot R}{4(a + d) + (m + 1) \cdot R}. \end{aligned} \tag{11}$$

We recall that the largest  $Q$  for each  $a$ , irrespective of the divisor  $d$ , is  $4a - 1$ . Thus, we have a clear case in which there is a solution to (1) for each  $a \geq 1$ , which accounts for the positive integers  $Q \equiv 3 \pmod{4}$  and therefore the primes  $p \equiv 3 \pmod{4}$ .

In general, the corresponding values in (1) for  $b, c$  can be recovered by considering (4) and (5), which we restate here:

$$a^2 = k \cdot \frac{(a \cdot (4b - 1) - pb)}{p},$$

$$a^2 = k \cdot (a \cdot (4b - 1) - pb).$$

This can be rewritten to facilitate recovery, such that

$$\begin{aligned} a \cdot (4b - 1) - pb &= 4ab - a - pb \\ &= b \cdot (4a - p) - a. \end{aligned}$$

In the context of (4) and (6), we see that  $d = \frac{b \cdot (4a - Q) - a}{Q}$ .

In the context of (5) and (7), we see that  $d = b \cdot (4a - Q) - a$ .

Thus, given some  $a, d, Q = p$ , we can recover  $b$  by

$$b = \frac{dp + a}{4a - p}$$

in the case of (6), and

$$b = \frac{d + a}{4a - p}$$

in the case of (7). We recover  $k = \frac{a^2}{dp}$  or  $k = \frac{a^2}{d}$ , from the restatements above, and  $c = \frac{k \cdot bp}{a}$ , from (2) and (3).

We wish to show that there exists also at least one  $Q \equiv 1 \pmod{4}$  for each  $a$  and therefore for each prime  $p \equiv 1 \pmod{4}$ . In fact, we wish to show that at least one of either

$$4a - 3 = \frac{4(a \cdot (M_{1,i} - r) - d_i) - 1}{M_{1,i} - r}$$

or

$$4a - 3 = \frac{4(a \cdot (M_{2,i} - r) - d_i)}{M_{2,i} - r + 1}$$

is satisfied for a positive integer  $r$ . We know how to express  $r$  in terms of  $a, d, m, R$ , and therefore, want to find a solution to either (10) or (11) for some  $a, d = d_i, m = M_{1/2,i}, R = 2$ .

In the case of (10), then

$$r = \frac{2M_{1,i}^2}{4d_i + 2M_{1,i} + 1}.$$

We substitute (8) for  $M_{1,i}$  such that

$$\begin{aligned} r &= \frac{2(1 + 4d_i)^2}{4d_i + 2(1 + 4d_i) + 1} \\ &= \frac{2(1 + 4d_i)}{3}. \end{aligned} \tag{12}$$

In the case of (11), then

$$r = \frac{2(M_{2,i} + 1)^2}{4(a + d_i) + 2(M_{2,i} + 1)}.$$

We substitute (9) for  $M_{2,i}$  such that

$$\begin{aligned} r &= \frac{2(3 + 4(a + d_i - 1) + 1)^2}{4(a + d_i) + 2(3 + 4(a + d_i - 1) + 1)} \\ &= \frac{8(a + d_i)}{3}. \end{aligned} \tag{13}$$

We consider the two possible cases:

1. For (12) we have that  $Q = 4a - 3$  when at least one of the divisors of  $a^2$  is congruent to 2 modulo 3, since  $4(3x - 1) + 1 = 3(4x - 1)$  for any  $x$ .
2. For (13) the sum of  $a$  and one of the divisors of  $a^2$  is divisible by 3.  
If  $a \equiv 1 \pmod{3}$ , then  $a^2 \equiv 2 \pmod{3}$ , since  $(3x - 2)^2 = 3(3x^2 - 4x - 1) - 1$  for any  $x$ .  
If  $a \equiv 2 \pmod{3}$ , then  $a^2 \equiv 1 \pmod{3}$ , since  $(3x - 1)^2 = 3(3x^2 - 2x + 1) - 2$  for any  $x$ .  
If  $a \equiv 0 \pmod{3}$ , then  $a^2 \equiv 0 \pmod{3}$ , for any  $a$ .

With these two cases, the second in particular, we can now account for each  $Q \equiv 1 \pmod{4}$ , and therefore we prove the Erdős-Straus conjecture.

QED.