Proof of Fermat's Last Theorem by means of Elementary Probability Theory

Andrea Prunotto*
Institute of Medical Biometry and Statistics
Albert-Ludwigs-Universität Freiburg
Freiburg im Breisgau, Germany

February 6, 2022

Abstract

In this work, we introduce the concept of Fermat's Urn, an urn containing three types of marbles, and such that it holds a peculiar constraint therein: The probability to get at least one marble of a given type (while performing multiple independent drawings) is equal to the probability not to get any marble of another type. Further, we discuss a list of implicit hypotheses related to Fermat's Equation, which would allow us to interpret this equation exactly as the mentioned constraint in Fermat's Urn. Then, we study the properties of this constraint in relation with the capability to distinguish the types of marbles within the urn, namely in case of the event "to get at least one marble of each type". Eventually, on the basis of a simple theorem related to this event, we prove that Fermat's Equation and Fermat's Urn may share those properties only if we perform at most two drawings from the urn. This result reflects then in the solution of Fermat's Equation.

Keywords: Number Theory; Fermat's Equation; Combinatorial probability

MSC: 60-03; 60C05; 11D41;

1 Fermat's Urn

Consider an urn C containing three distinct types of marbles, say type A, B and G, and such that each of the three types is represented in the urn by at least one marble. Let us denote with $\alpha, \beta, \gamma > 0$ the respective numbers of marbles and with $c = \alpha + \beta + \gamma$ the total number of marbles in the urn C. Let us perform n drawings with replacement of one marble at a time from the urn C (in the following, we will simply refer to this kind of drawings as to "trials").

Denoting with L_n^A the event "to get at least one marble of type A in n trials", the probability to obtain a success for this event is $P(L_n^A) = 1 - \left(\frac{\beta+\gamma}{c}\right)^n$. Similarly, denoting with L_n^B the event "to get at least one marble of type B in n trials", the probability to obtain a success for this event is $P(L_n^B) = 1 - \left(\frac{\alpha+\gamma}{c}\right)^n$. It is of historical interest to remark that Fermat was familiar with such sort of event, having discussed about it, around the year 1664, in a series of letters exchanged with B. Pascal in response to the famous challenge thrown down by A. Gombaud to Mersenne's Salon [1].

*Corresponding author: Email: prunotto@imbi.uni-freiburg.de – ORCID: 0000-0003-1235-1740

Let us suppose to have found some α, β, γ such that it exists a specific number of trials n for which $P(L_n^A) = P(\neg L_n^B)$. In this case, it must hold the following constraint:

$$1 - \left(\frac{\beta+\gamma}{c}\right)^n = \left(\frac{\alpha+\gamma}{c}\right)^n . \tag{1}$$

We will refer to such a peculiar urn as to a *Fermat's Urn*, since, denoting $a = \alpha + \gamma$, $b = \beta + \gamma$ (and recalling that $c = \alpha + \beta + \gamma$), the above constraint formally coincides with Fermat's Equation $a^n + b^n = c^n$ [2].

2 Some properties of Fermat's Equation

We hereby discuss some simple properties of the integers a, b, c defining Fermat's Equation.

(i) $a, b \in (0, c)$: If $a = 0$ or $b = 0$ Fermat's Equation reads $b = c$ or $a = c$. If $a \geq c$ or $b \geq c$, Fermat's Equation cannot hold. Therefore, in order to state a proper Fermat's Equation, avoiding trivial solutions, it must be $0 < a < c$ and $0 < b < c$. This allows to interpret the quantities a/c, b/c, $(a/c)^n$, $(b/c)^n$ as probabilities. This property will be useful, since in the following we will study those quantities in the context of a Fermat's Urn (and in the light of the Inclusion-exclusion principle).

(ii) $a, b > 1$: Let us suppose that $a = 1$ (a similar discussion will apply if $b = 1$). In this case, Fermat's Equation reads $1 + b^n = c^n$, i.e. $1 = c^n - b^n$. On the other hand, it is easy to prove [3] that $c^n - b^n = (c-b)(c^{n-1} + c^{n-2}b + \ldots + cb^{n-2} + b^{n-1})$. However, since $c - b > 1$ (discarding the trivial solution $b = c$), then, in case $c^n - b^n = 1$, we would have $1 = (c-b)(c^{n-1} + c^{n-2}b + \ldots + b^{n-1}) > 1$, which is a contradiction.

(iii) $a \neq b$: If $a = b$, then we would have $2a^n = c^n$ and therefore $\sqrt[n]{2} = c/a$, where the first member is irrational and the second one is rational. Therefore, Fermat's Equation may hold only if $a \neq b$.

(iv) $a + b > c$: In fact, $c^n = a^n + b^n < (a+b)^n \implies c^n < (a+b)^n$ and therefore $c < a + b$. This means that the integer a, b, c appearing in Fermat's Equation can always define an integer triangle with sides of lengths a, b, c, and whose longest side is of length c, because of Prop. (i). This property will be clarified below.

(v) a, b can be decomposed in the sum of two non-zero integers : We first observe that Prop. (ii) ensures that $a \geq 2$ and $b \geq 2$. Applying the notation $a = \alpha + \gamma$ and $b = \beta + \gamma$, and $c = \alpha + \beta + \gamma$, we can construct the integers α, β, γ (given the integers a, b, c appearing in Fermat's Equation) by the simple rules $\alpha = c - b$, $\beta = c - a$ and $\gamma = a + b - c$. We observe that none among the α, β, γ obtained from a Fermat's Equation by means of the previous construction can be equal to 0. Let us suppose that $\alpha = 0$ (a similar reasoning applies also for $\beta = 0$): In this case, we find $(0 + \gamma)^n + (\beta + \gamma)^n = (0 + \beta + \gamma)^n$, which is obviously false (unless also $\gamma = 0$, which yields to a trivial solution of Fermat's Equation). Similarly, if $\gamma = 0$, we have $(\alpha + 0)^n + (\beta + 0)^n = (\alpha + \beta + 0)^n$, which is again false, unless one or both among α and β are equal to 0, or unless $n = 1$. Finally, we observe that Prop. (iv) yields to an immediate geometric relationship between the integers a, b, c related to a Fermat's Equation and the integers α, β, γ, see Fig. (1).

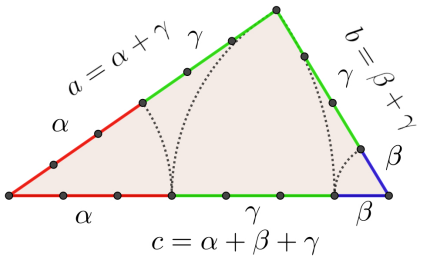

Figure 1: Given any non-isosceles triangle (iii) with integer sides a, b, c, where c is the longest side (i), by reporting the sides a and b onto c, we can always define a related triplet of non-null (v) integers α, β, γ such that $a = \alpha + \gamma$, $b = \beta + \gamma$ and $c = \alpha + \beta + \gamma$ (this procedure is always possible, since c is the longest side). If a, b, c satisfy a Fermat's Equation, α, β, γ define the respective Fermat's Urn.

The properties (i-v) allow us to state that, given a triplet of integers a, b, c which satisfies Fermat's Equation $a^n + b^n = c^n$, we can always find a triplet of integers α, β, γ by means of which we can build a respective Fermat's Urn. In other words, Fermat's Equation can be always interpreted as the constraint $P(L_n^A) = P(\neg L_n^B)$ within an urn C in such a way that the equivalence between (1) and Fermat's Equation is not only formal, but substantial.

We observe that α, β, γ, n are integers by construction, as required by Fermat's Equation. Otherwise, (1) does not represent the equivalence among the probabilities of the events L_n^A and $\neg L_n^B$. In fact, at each trial, we must be sure to get either one marble of type A, or one marble of type B, or one marble of type G, without ambiguity. In other words, the integer nature of the trials is reflected in the integer nature of the marbles, and vice versa.

3 Probability to get at least one marble of each type

Let us consider the events L_n^A, L_n^B, L_n^G, and let us apply the Inclusion–exclusion principle:

$$P(L_n^A \cup L_n^B \cup L_n^G) = P(L_n^A) + P(L_n^B) + P(L_n^G) - \\ - P(L_n^A \cap L_n^B) - P(L_n^A \cap L_n^G) - P(L_n^B \cap L_n^G) + P(L_n^A \cap L_n^B \cap L_n^G).$$

Observing that, since there is at least one marble of each type in the urn it must hold $P(L_n^A \cup L_n^B \cup L_n^G) = 1$, this expression can be written as

$$P(L_n^A \cap L_n^B \cap L_n^G) = 1 - P(L_n^A) - P(L_n^B) - P(L_n^G) + \\ + P(L_n^A \cap L_n^B) + P(L_n^A \cap L_n^G) + P(L_n^B \cap L_n^G), \quad (2)$$

which gives us the probability to get at least one marble of each type in n trials.

Let us explicit the above expression in terms of the numbers of marbles α, β, γ. Observing that

$$P(L_n^A \cap L_n^B) = P(L_n^A|L_n^B)P(L_n^B) = [1 - P(\neg L_n^A|L_n^B)]P(L_n^B) = \\ = P(L_n^B) - P(\neg L_n^A|L_n^B)P(L_n^B) = P(L_n^B) - P(L_n^B|\neg L_n^A)P(\neg L_n^A),$$

we find

$$P(L_n^A \cap L_n^B) = 1 - \left(\frac{\alpha+\gamma}{c}\right)^n - \left[1 - \left(\frac{\gamma}{\beta+\gamma}\right)^n\right]\left(\frac{\beta+\gamma}{c}\right)^n = \\ = 1 - \left(\frac{\alpha+\gamma}{c}\right)^n - \left(\frac{\beta+\gamma}{c}\right)^n + \left(\frac{\gamma}{c}\right)^n.$$

With the same reasoning used to get the explicit form of $P(L_n^A \cap L_n^B)$, we find

$$P(L_n^A \cap L_n^G) = 1 - \left(\frac{\alpha+\beta}{c}\right)^n - \left(\frac{\beta+\gamma}{c}\right)^n + \left(\frac{\beta}{c}\right)^n$$

and

$$P(L_n^B \cap L_n^G) = 1 - \left(\frac{\alpha+\beta}{c}\right)^n - \left(\frac{\alpha+\gamma}{c}\right)^n + \left(\frac{\alpha}{c}\right)^n.$$

With these results, it is easy to verify that Eq. (2) can be written as

$$P(L_n^A \cap L_n^B \cap L_n^G) = 1 - \left(\frac{\alpha+\gamma}{c}\right)^n - \left(\frac{\beta+\gamma}{c}\right)^n - \left(\frac{\alpha+\beta}{c}\right)^n + \\ + \left(\frac{\alpha}{c}\right)^n + \left(\frac{\beta}{c}\right)^n + \left(\frac{\gamma}{c}\right)^n. \quad (3)$$

A trivial theorem related to this probability reads

$$P(L_n^A \cap L_n^B \cap L_n^G) = 0 \iff n \leq 2. \quad (4)$$

In fact, since there is at least one marble of each of the three types in the urn C, the only scenario in which it results absolutely impossible to get at least one marble of each type in n trials is when we perform less trials than the number of distinct types of marbles in the urn. We remark that this is also the only case in which $P(L_n^A \cap L_n^B \cap L_n^G)$ does not depend on the exact values of the integers α, β, γ.

In case of Fermat's Urn, applying the constraint (1) in Eq. (3), we find

$$P(L_n^A \cap L_n^B \cap L_n^G) = -\left(\frac{\alpha+\beta}{c}\right)^n + \left(\frac{\alpha}{c}\right)^n + \left(\frac{\beta}{c}\right)^n + \left(\frac{\gamma}{c}\right)^n. \quad (5)$$

The above equation represents a fully equivalent way to express the constraint $P(L_n^A) = P(\neg L_n^B)$ defining a Fermat's Urn, as in (1), through the Inclusion-exclusion principle.

4 Discussion

In the previous sections, we proved that assessing a Fermat's Equation is totally equivalent to impose a constraint among the probability of L_n^A and $\neg L_n^B$ in an urn containing three distinct types of marbles (Fermat's Urn).

A synoptic comparison between the two ways in which we can formulate such constraint, i.e. as in (1) and as in (5),

$$1 - \left(\frac{\alpha+\gamma}{c}\right)^n - \left(\frac{\beta+\gamma}{c}\right)^n = 0, \quad P(L_n^A \cap L_n^B \cap L_n^G) = \frac{\alpha^n + \beta^n + \gamma^n - (\alpha+\beta)^n}{c^n},$$

highlights how the first expression does not explicitly refer to α, β, γ (but only to the sums $a = \alpha + \gamma$, $b = \beta + \gamma$), whereas the second one does.

This means that, if Fermat's Equation holds, the constraint $P(L_n^A) = P(\neg L_n^B)$ as in (1) can be imposed in the urn C without being able to distinguish all the three types of marbles. In fact, in order to assess (1), it is sufficient to have the capability to distinguish, among the c marbles in the urn, the ones of type A from the ones of type $B \cup G$ – to define $P(L_n^A)$ – *or* the ones of type B from the ones of type $A \cup G$ –

to define $P(L_n^B)$. We said *or* because the relation (1) allows us to know one of the two probabilities, given the other one.

On the contrary, since the integers α, β, γ appear explicitly in (5), the capability to distinguish all the three types of marbles among them is instead required in order to state the constraint in this manner.

One may argue that, even if we are not able to distinguish all the three types of marbles, we can anyway infer the values of the integers α, β, γ, namely by means of the construction rules given in Prop. (v). However, Eq. (5) requires that the ratio therein must represent a probability. Its denominator c^n, indeed, evaluates all the possible cases in which we can extract c marbles in n trials. In turn, the numerator $\alpha^n + \beta^n + \gamma^n - (\alpha + \beta)^n$ must account for a number of favorable cases related to a distinguishable characteristic of the drawn marbles. But, again, if we are not able to distinguish all the three types of marbles to one another, this number (no matter how we calculate it) does not represent the size of any subset of identifiable cases among the c^n ones, and therefore the ratio in (5) does not represent an actual probability.

5 Conclusions

We found that, applying to the letter the relationship between a, b, c, n imposed by Fermat's Equation into an urn C, the constraint $P(L_n^A) = P(\neg L_n^B)$ can be expressed in such a way that the capability to distinguish all the three types of marbles is not required, as in (1). Conversely, we observed that this constraint, written in the equivalent form (5), actually requires this capability. But the fact that Fermat's Equation hold can not depend on the capability to distinguish the types of marbles within the urn C. Therefore, if we require *a priori* that Fermat's Equation holds, then the constraint $P(L_n^A) = P(\neg L_n^B)$, although expressed in the form (5), must not depend, as well as (1), on the capability to distinguish all the types of marbles.

Due to the explicit dependence of (5) on α, β, γ, the only way to satisfy such requirement, is to assess that $P(L_n^A \cap L_n^B \cap L_n^G)$ does not depend on the exact values of α, β, γ or, in other words, to admit that, given any Fermat's Equation, the probability $P(L_n^A \cap L_n^B \cap L_n^G)$ takes always the same value. But, as we have seen in (4), this can be attained only if $P(L_n^A \cap L_n^B \cap L_n^G) = 0$, i.e. only if $n \leq 2$.

Now, to declare that Fermat's Equation has solutions coincides to state the hypotheses of Fermat's Last Theorem. Since we have already proved the equivalence between Fermat's Equation and the constraint defining the respective Fermat's Urn, the resulting condition $n \leq 2$ related to the latter must reflect in the solutions of the former, giving an elementary proof the well-known Theorem.

6 References

[1] O. Ore, *Pascal and the Invention of Probability Theory*, The American Mathematical Monthly, 67 (5): 409-419, (1960).

[2] S. Singh, *Fermat's Last Theorem*, (1997).

[3] G. E. Andrews, *Number Theory*, (1971).