A probabilistic interpretation of the Last Theorem of Fermat

Andrea Prunotto
Haslacherstraße 119, 79115 Freiburg im Breisgau, Germany
andrea.prunotto@gmail.com

March 14, 2018

Abstract

The equiprobability among two events involving independent extractions of elements from a finite set is shown to be related to the solutions of Fermat's Diophantine equation.

1 Definitions of the events $\mathscr{E}_n^G$ and $\mathscr{L}_n^{AB}$

A set C contains $c \in \mathbb{N}$ indexed elements of three different kinds: there are $\alpha > 0$ elements of kind A, $\beta > 0$ elements of kind B and $\gamma \geq 0$ elements of kind G, and $|C| = c = \alpha + \beta + \gamma$. We assume c finite.

We perform $n > 0$ independent extractions (i.e. with replacement) of one element at a time from the set C and we define the event $\mathscr{E}_n^G$ as "to get, in n independent trials, exactly n times one element of kind G", so that $P(\mathscr{E}_n^G) = \left(\frac{\gamma}{c}\right)^n$ (the order of the trials matters).

We define also the event $\mathscr{L}_n^{AB}$ as "to get, in n independent trials, at least one element of kind A and at least one element of kind B", so that $P(\mathscr{L}_n^{AB}) = 1 - \left(\frac{\alpha+\gamma}{c}\right)^n - \left(\frac{\beta+\gamma}{c}\right)^n + \left(\frac{\gamma}{c}\right)^n$ (see Appendix).

We observe that the event $\mathscr{E}_n^G$ can occur only in correspondence of the last trial, whereas the event $\mathscr{L}_n^{AB}$ can occur in correspondence of each trial, except the first one.

2 Equiprobability as a Diophantine equation

An appropriate choice of $\alpha, \beta > 0$ and $\gamma \geq 0$ allows the naturals $a \equiv \alpha + \gamma$ and $b \equiv \beta + \gamma$ to assume any value greater than 1. Similarly, given $c = \alpha + \beta + \gamma \geq 2$, we can build any a, b such that $a, b < c$ and $a + b \geq c$ (e.g. by means of the sides of a triangle whose hypotenuse is of lenght c).

We notice that these two conditions are implicit in Fermat's Diophantine equation $a^n + b^n = c^n$. In fact, if either $a \geq c$ or $b \geq c$, the equation cannot be

verified. Moreover, by means of the triangular inequality, we have $(a+b)^n \geq a^n + b^n = c^n$, which implies $a + b \geq c$.

Interestingly, the request of equiprobability $P(\mathscr{E}_n^G) = P(\mathscr{L}_n^{AB})$, given the same α, β, γ, can be written as $\left(\frac{\gamma}{c}\right)^n = 1 - \left(\frac{\alpha+\gamma}{c}\right)^n - \left(\frac{\beta+\gamma}{c}\right)^n + \left(\frac{\gamma}{c}\right)^n$, and also as $0 = 1 - \left(\frac{a}{c}\right)^n - \left(\frac{b}{c}\right)^n$, which coincides with Fermat's equation.

3 Distributions of successes for $\mathscr{E}_n^G$ and $\mathscr{L}_n^{AB}$

Given the n trials $k \in \{1, 2 \dots n\}$, we can define the n events $\mathscr{E}_{n,k}^G$ as "to verify the event $\mathscr{E}_n^G$ in correspondence of the trial k" and the n events $\mathscr{L}_{n,k}^{AB}$ as "to verify the event $\mathscr{L}_n^{AB}$ in correspondence of the trial k", so that $P(\mathscr{E}_{n,k}^G) = \left(\frac{\gamma}{c}\right)^n \delta_{n,k}$ and $P(\mathscr{L}_{n,k}^{AB}) = 1 - \left(\frac{\alpha+\gamma}{c}\right)^k - \left(\frac{\beta+\gamma}{c}\right)^k + \left(\frac{\gamma}{c}\right)^k$ (see Appendix). We will refer to $P(\mathscr{E}_{n,k}^G)$ and $P(\mathscr{L}_{n,k}^{AB})$ as to the "distributions of successes" for the events $\mathscr{E}_n^G$ and $\mathscr{L}_n^{AB}$. Clearly, $P(\mathscr{E}_{n,n}^G) = P(\mathscr{E}_n^G)$ and $P(\mathscr{L}_{n,n}^{AB}) = P(\mathscr{L}_n^{AB})$.

Finally, we observe that, given the same values of α, β, γ, each value of $P(\mathscr{E}_{n,k}^G)$ and $P(\mathscr{L}_{n,k}^{AB})$ can be represented by the area of a target, and each ordered trial k can be interpreted as a single shot, aiming the target related to that specific trial (see Fig. 1).

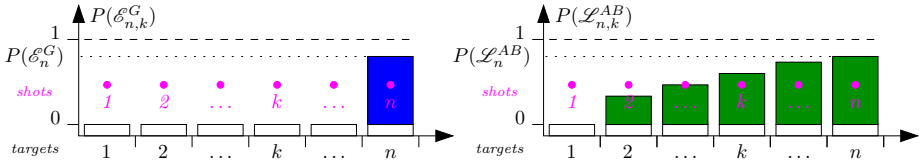

Figure 1: Distributions of successes for the events $\mathscr{E}_n^G$ (right) and $\mathscr{L}_n^{AB}$ (left), related to the same α, β, γ, as a function of the ordered number of trial k. The target areas associated to $P(\mathscr{E}_{n,k}^G)$ are colored in blue, whereas the ones associated to $P(\mathscr{L}_{n,k}^{AB})$ are colored in green. Each target has the same width, therefore the probabilities to hit the targets are fully described by the targets heights. The n magenta dots, together with the n colored areas, illustrate the interpretation of the n trials as n shots, aiming the respective n targets (one shot for each target). In this example we assumed $P(\mathscr{E}_n^G) = P(\mathscr{L}_n^{AB})$.

4 Equiprobability and number of trials

Given the same α, β, γ, we study for which n it applies the condition $P(\mathscr{E}_n^G) = P(\mathscr{L}_n^{AB})$ or, equivalently, the condition $P(\mathscr{E}_{n,n}^G) = P(\mathscr{L}_{n,n}^{AB})$.

If $P(\mathscr{E}_{n,n}^G) = P(\mathscr{L}_{n,n}^{AB})$ and $n > 2$, the probability to hit targets related to the event $\mathscr{E}_n^G$ by means of the n shots at our disposal (one for each target) is less than the probability to hit targets related to the event $\mathscr{L}_n^{AB}$ (in identical conditions), because the last target has the same height in both cases, but there are $n-2$ more shots aiming targets with non-zero height in the case of $\mathscr{L}_n^{AB}$, but not in the case of $\mathscr{E}_n^G$ (see Fig. 1).

Therefore, there are only two possibilities to keep the equiprobability of verifying the events $\mathscr{E}_n^G$ and $\mathscr{L}_n^{AB}$ with the same values of α, β, γ: Either to reduce the number of targets/shots related to the distribution of successes of $\mathscr{L}_n^{AB}$ to a single one as well – which, thus, must be of height $P(\mathscr{E}_{n,n}^G)$ – or to remove all the targets. In details,

- If $\alpha, \beta, \gamma > 0$, the distribution $P(\mathscr{L}_{n,k}^{AB})$ is a strictly monotonically increasing function of k. Therefore, $\mathscr{L}_n^{AB}$ is associated to a unique target (of non-zero height) if and only if $n = 2$.
- If we remove all the targets, we impose $P(\mathscr{E}_n^G) = P(\mathscr{L}_n^{AB}) = 0$, which implies $\gamma = 0$ (no elements of kind G) and $n = 1$ (the event $\mathscr{L}_n^{AB}$ cannot occur at the first trial).

In conclusion, the equiprobability between the events $\mathscr{E}_n^G$ and $\mathscr{L}_n^{AB}$, related to the same set C (i.e. to the same values of α, β, γ), can be achieved only if $n \leq 2$.

Since we have already shown that the condition of equiprobability between the events $\mathscr{E}_n^G$ and $\mathscr{L}_n^{AB}$ corresponds to the Diophantine equation of the type $a^n + b^n = c^n$, this result must apply also to its solutions.

The cases $\alpha = 0$, $\beta = 0$ and $\alpha = \beta = 0$ are excluded because they imply the degenerate case of $C = \emptyset$.

5 Appendix

5.1 Expression of $P(\mathscr{L}_n^{AB})$

We define the event $\mathscr{L}_n^A$ as "to get, in n independent trials, at least one element of kind A", and the event $\mathscr{L}_n^B$ as "to get, in n independent trials, at least one element of kind B", so that $P(\mathscr{L}_n^A) = 1 - \left(\frac{c-\alpha}{c}\right)^n$ and $P(\mathscr{L}_n^B) = 1 - \left(\frac{c-\beta}{c}\right)^n$.

Eventually, we define the event $\mathscr{L}_n^{AB} \equiv \mathscr{L}_n^A \cap \mathscr{L}_n^B$ as "to get, in n independent trials, at least one element of kind A and at least one element of kind B". By means of Bayes' theorem and the concept of opposite event, we find

$$P(\mathscr{L}_n^{AB}) = P(\mathscr{L}_n^A \cap \mathscr{L}_n^B) = P(\mathscr{L}_n^A|\mathscr{L}_n^B)P(\mathscr{L}_n^B) = [1 - P(\overline{\mathscr{L}_n^A}|\mathscr{L}_n^B)]P(\mathscr{L}_n^B) =$$

$$= P(\mathscr{L}_n^B) - P(\mathscr{L}_n^B|\overline{\mathscr{L}_n^A})P(\overline{\mathscr{L}_n^A}) = 1 - \left(\frac{c-\beta}{c}\right)^n - \left[1 - \left(\frac{\gamma}{\beta+\gamma}\right)^n\right]\left(\frac{\beta+\gamma}{c}\right)^n =$$

$$= 1 - \left(\frac{\alpha+\gamma}{c}\right)^n - \left(\frac{\beta+\gamma}{c}\right)^n + \left(\frac{\gamma}{c}\right)^n = 1 - \left(\frac{a}{c}\right)^n - \left(\frac{b}{c}\right)^n + \left(\frac{\gamma}{c}\right)^n,$$

where $a \equiv \alpha + \gamma = c - \beta$ and $b \equiv \beta + \gamma$.

5.2 Expressions of $P(\mathscr{E}_{n,k}^G)$ and $P(\mathscr{L}_{n,k}^{AB})$

Analyzing the tree diagram in Fig. 2 (related to $n = 3$ trials), we find that the probability to get a success for the event $\mathscr{E}_3^G$ is zero at any trial, except the last one, therefore $P(\mathscr{E}_{3,k}^G) = P(\mathscr{E}_3^G)\delta_{3,k} = \left(\frac{\gamma}{c}\right)^3 \delta_{3,k}$. The term $P(\mathscr{E}_{3,3}^G)$ corresponds to the height of the unique blue target represented in Fig. 1 (left graph). This result can be easily generalized to $P(\mathscr{E}_{n,k}^G) = P(\mathscr{E}_n^G)\delta_{n,k} = \left(\frac{\gamma}{c}\right)^n \delta_{n,k}$.

Similarly, by means of the tree diagram, we can compute the probabilities to verify the event $\mathscr{L}_3^{AB}$ in correspondence of $k \in \{1,2,3\}$:

$$P(\mathscr{L}_{3,1}^{AB}) = 0 = 1 - \left(\frac{\alpha+\gamma}{c}\right) - \left(\frac{\beta+\gamma}{c}\right) + \left(\frac{\gamma}{c}\right),$$

$$P(\mathscr{L}_{3,2}^{AB}) = 2\frac{\alpha\beta}{c^2} = 1 - \left(\frac{\alpha+\gamma}{c}\right)^2 - \left(\frac{\beta+\gamma}{c}\right)^2 + \left(\frac{\gamma}{c}\right)^2,$$

$$P(\mathscr{L}_{3,3}^{AB}) = 3\frac{\alpha^2\beta}{c^3} + 6\frac{\alpha\beta\gamma}{c^3} + 3\frac{\alpha\beta^2}{c^3} = 1 - \left(\frac{\alpha+\gamma}{c}\right)^3 - \left(\frac{\beta+\gamma}{c}\right)^3 + \left(\frac{\gamma}{c}\right)^3.$$

These values are obtained summing all the probabilities to select an ordered sequence of k trials (highlighted with a green node on the k-th magenta circle in Fig. 2) in which the event $\mathscr{L}_n^{AB}$ occurs. The sum is justified by the fact that these possible sequences are all mutually exclusive. The three terms correspond to the heights of the first three green targets illustrated in Fig. 1 (right graph). We can easily generalize this result to $P(\mathscr{L}_{n,k}^{AB}) = 1 - \left(\frac{a}{c}\right)^k - \left(\frac{b}{c}\right)^k + \left(\frac{\gamma}{c}\right)^k$. The distribution $P(\mathscr{L}_{n,k}^{AB})$ is therefore a strictly monotonically increasing function of k, since $a, b < c$ and $a, b > \gamma$.

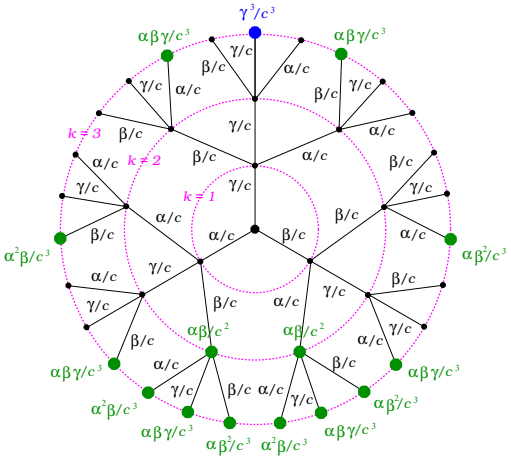

Figure 2: Tree diagram illustrating the distributions $P(\mathscr{E}_{3,k}^G)$ and $P(\mathscr{L}_{3,k}^{AB})$, with $k \in \{1,2,3\}$. The root-node is located at the center of the picture, and each trial is indicated with a dashed circle (in magenta). The probability to get a success for the event $\mathscr{E}_3^G$ is zero at any trial, except the third one (where the unique blue node is located). The sum of the probabilities in each green node related to each trial, gives the terms $P(\mathscr{L}_{3,1}^{AB}) = 0$ (no green nodes related to $k = 1$), $P(\mathscr{L}_{3,2}^{AB}) = 2\frac{\alpha\beta}{c^2}$ (2 green nodes related to $k = 2$), and $P(\mathscr{L}_{3,3}^{AB}) = 3\frac{\alpha^2\beta}{c^3} + 6\frac{\alpha\beta\gamma}{c^3} + 3\frac{\alpha\beta^2}{c^3}$ (12 green nodes related to $k = 3$).