# A combinatorial approach to the Last Theorem of Fermat

Andrea Prunotto

Haslacherstraße 119, 79115 Freiburg im Breisgau, Germany

andrea.prunotto@gmail.com

February 22, 2018

**Abstract**

The condition of equiprobability among two events involving independent extractions of elements from a finite set is shown to coincide with Fermat's Diophantine equation. The problem of the division of the stakes, related to the events, is also discussed.

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

A set $C$ contains a finite number $c$ of 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 perform $n > 0$ independent extractions (i.e. with replacement) of one element at a time from the set $C$.

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 $P(\mathscr{E}_n^G) = \left(\frac{\gamma}{c}\right)^n$.

We define 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 $P(\mathscr{L}_n^{AB}) = 1 - \left(\frac{\alpha+\gamma}{c}\right)^n - \left(\frac{\beta+\gamma}{c}\right)^n + \left(\frac{\gamma}{c}\right)^n$.

To prove that this is the actual expression of $P(\mathscr{L}_n^{AB})$, we can first 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 $P(\mathscr{L}_n^B) = 1 - \left(\frac{c-\beta}{c}\right)^n$. Then, we define the event-intersection $\mathscr{L}_n^{AB} \equiv \mathscr{L}_n^A \cap \mathscr{L}_n^B$ 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[1], 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 $b \equiv \beta + \gamma$.

[1] This sort of problems was familiar to Pierre de Fermat. See for instance J. V. Uspensky, *Introduction to Mathematical Probability*, 1937, McGraw-Hill, p. 21-22.

## 2 Equiprobability of $\mathscr{E}_n^G$ and $\mathscr{L}_n^{AB}$

An appropriate choice of $\alpha, \beta > 0$ and $\gamma \geq 0$ allows the naturals $a = \alpha + \gamma$ and $b = \beta + \gamma$ to assume any value greater than 1. Similarly, given any $c \geq 2$, 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 the 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 $a + b \geq c$. We exclude the cases $\alpha = 0$, $\beta = 0$ and $\alpha = \beta = 0$ because they imply the degenerate case of $C = \emptyset$.

On the basis of our definitions, the request of equiprobability $P(\mathscr{E}_n^G) = P(\mathscr{L}_n^{AB})$, given the same $\alpha, \beta, \gamma$, 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. In other words, we have shown that, given any $a, b, c, n \in \mathbb{N}$ such that $a, b < c$, $a + b \geq c$ and $n > 0$, it holds $a^n + b^n = c^n \iff P(\mathscr{E}_n^G) = P(\mathscr{L}_n^{AB})$.

## 3 Division of the stakes

Let us consider the events $\mathscr{E}_n^G$ and $\mathscr{L}_n^{AB}$ as the mathematical descriptions of two games. Fermat's hypothesis requires that the two games have, at the end of the $n$ trials, the same probability to be won. Therefore, it implies that betting the same amount of money in case of victory of each game is a fair gambling.

However, the first game can be won only in correpondence of the last trial, whereas the second game can be won at each trial after the first one (in the extreme case, already at the second trial). If two players put at stake a certain amount of money in case of victory of each game, how do they share it among them, in case the games are interrupted?

The situation recalls the *division of the stakes*, or *problem of points*, appearing in the letters exchanged between Fermat and Pascal around the year 1664[2], although, in our case, the probability of winning is not the same at each round for both the players.

In fact, interrupting the games in correspondence of any trial $k \in \{1, 2 \dots n-1\}$, would penalize in any case the player of the $\mathscr{E}_n^G$ game, since the player of the game $\mathscr{L}_n^{AB}$ could have already regularly won, with probability $P(\mathscr{L}_k^{AB})$.

To keep the fairness of the gambling, considering the problem of interrupting the games discussed by the French mathematicians, we must perform only $n = 2$ trials, in such a way that the last trial represents the only possibility to win also for the player of the game $\mathscr{L}_n^{AB}$.

Alternatively, it is possible to perform $n = 1$ trial, and remove all the elements of kind $G$ from the set $C$, in such a way that the probability to win is zero for both the players.

[2]Pascal, letter to Fermat, quoted in F. N. David, *Games, Gods, and Gambling*, 1962, Griffin Press, p. 239.