Entropy and Natural Numbers
(A Short Proof of Fermat's Last Theorem)

Marko V. Jankovic

Institute of Electrical Engineering “Nikola Tesla”, Belgrade, Serbia,
Swiss Rockets Serbia, Belgrade,Serbia

Abstract In this paper, entropy of natrual numbers is going to be introduced. It will be shown that every natural number can be associated with a family of discrete probablity distributions and their entropies. After an introduction of a new Tesla's entropy measure, a usefulness of the concept is going to be demonstrated by a short proof of Fermat's Last Theorem, based on a simplified ABC theorem for prime numbers.

1 Introduction

In this paper it is going to be shown that every natural number can be related to different entropy measures. A relation between natural numbers and standard entropy measures is going to be presented, first. After that, a new entropy measure named Tesla's entropy is going to be introduced. That entropy measure is used to create a short proof of the Fermat's Last Theorem (FLT) [1] (first stated in a copy of *Arithmetica* by Pierre de Fermat in 1637) . The proof follows from the proof of the vaguely simplfied version of ABC conjecture for prime numbers (proposed by David Masser [2]). Once the simplfied version of ABC conjecture (ŠABAC Theorem) is proved, the proof of FLT follows the line of the proof presented by professor Jeff Valler in his Youtube's video about *ABC* conjecture. It is interesting to notice that the method used here cannot be used to produce a short proof of the Mihälescu's theorem [3].

2 Natural numbers and entropy

Fundamental theorem of arithemtic [4] states that every integer grater than 1 either is prime number itself or can be represented as the product of powers of prime numbers, and that this representation is unique up to the order of factors. So, every natural number n can be represented as

$$n=\prod_{i=1}^{I} p_i^{k_i}$$

where p_i are some prime numbers and k_i and I are natural numbers.

Every number in the form

$$p_i^{k_i}$$

can be represented by the following expression

$$p_i^{k_i}=x_i^{x_i} \quad ,$$

where

$$x_i=e^{W_0(\ln(p_i^{k_i}))}$$

and W_0 represents the principal branch of Lambert W function. Having in mind derivation of Shannon's entropy proposed in [5], it is not difficult to conclude that any natural number n can be related to the following discrete probabilistic distribution $q = \{q_i\}$ (of anti-Boltzman type)

$$q_i=\frac{e^{W_0(k_i \ln(p_i))}}{\sum e^{W_0(k_i \ln(p_i))}} \quad .$$

Now, it is clear that we can use any known entropy measure (like Shannon's, Tsallis', Rényi's and so on) for this probabilistic distribution, and which one is used will depend

on the problem that is analysed. It can be also noticed that we actually can connect the number n with a whole family of probabilistic distributions if we consider the fact that n can be wirtten as

$$n=\prod_{i=1}^{I} p_i^{k_i} \prod_{j=1}^{J} 1^1 \quad ,$$

where J is a whole number and $J \geq 0$. Different choices for J will result in different probabilistic distribution and each of those distributions could be related to the family of different entropy measures.

Here we are going to introduce/define a new entropy measure that is going to be named Tesla's entropy (it is clear that it would be possible to define many similar entropy measures, but that is out of the scope of this paper). This entropy definition is not related to the probabilistic distribution but rather to the natural number charcteristic values. For every individual power of the prime factor of the number n, given by

$$p_i^{k_i}$$

we are going to define Tesla's entropy as

$$E_T(p_i^{k_i})=\frac{k_i}{2\cdot p_i^2}+\ln(p_i^2) \quad .$$

Then, entropy of a number n can be defined as (having in mind that $p_{i\text{-}}$ have no common factors)

$$E_T(n)=\sum_i \frac{k_i}{2\cdot p_i^2}+\ln(p_i^2) \quad .$$

Since the multiplication by 1 does not change the number, the following is assumed

$$E_T(1)=0 \quad .$$

3 PIN Conjecture

In this section we are going to state the major result of this paper as a conjecture – a proof is going to be provided in another paper.

Let A, B and C be natural numbers such that

1. $A + B = C$,
2. A, B and C are each nonzero
3. A, B and C have no common prime factor, or in other words the greatest common divisor (gcd) of A and B is 1, or $\gcd(A, B) = 1$.

Define

$$Z = \{ p : p|ABC\}$$

to be primes that divide A, B or C.

Based on Fundamental theorem of arithemtic A, B and C can be represented as:

$$A=\prod_{i=1}^{I} a_i^{\alpha_i} \qquad B=\prod_{j=1}^{J} b_j^{\beta_j} \qquad C=\prod_{k=1}^{K} c_k^{\gamma_k}$$

where a_i, b_j and c_k represent prime numbers and I, J, K, α_i, β_j, and γ_k are natural numbers.

Now we can understand that p represent elements of the set Z that is created as union of sets $\{a_i\}$, $\{b_j\}$ and $\{c_k\}$.

Lets mark the least common multiplier (lcm) of numbers A, B and C as S, or:

$$S=lcm(A,B,C)=\prod_{i=1}^{I} a_i^{\alpha_i}\prod_{j=1}^{J} b_j^{\beta_j}\prod_{k=1}^{L} c_k^{\gamma_k} \quad .$$

Now we can state a PIN conjecture.

PIN conjecture: If natural numbers A, B and C fulfil the conditions 1-3, then the following holds:

$$E_T(S) > \ln(C) \quad .$$

Note: In the case gcd(A, B) = M > 1, the following holds

$$E_T(S) > \ln\left(\frac{C}{M}\right) \quad .$$

4 Proof of the ŠABAC Theorem

In this section the ŠABAC Theorem is going to be formulated and proved.

Theorem 1 (ŠABAC Theorem):

Let A, B and C be natural numbers such that

4. $A + B = C$,
5. A, B and C are each nonzero,
6. A, B and C have no common prime factor.

Define

$$Z = \{ p : p|ABC\}$$

to be primes that divide A, B or C.

Based on Fundamental theorem of arithemtic A, B and C can be represented as:

$$A = \prod_{i=1}^{I} a_i^{\alpha_i} \qquad B = \prod_{j=1}^{J} b_j^{\beta_j} \qquad C = \prod_{k=1}^{K} c_k^{\gamma_k}$$

where a_i, b_j and c_k represent prime numbers and α_i, β_j and γ_k are natural numbers (I, J, and K are natural numbers, too). If we asume that PIN Conjecture holds, then the following inequality must hold

$$max\{A, B, C\} < \left(\prod_{p \in Z} p\right)^3 \quad .$$

Proof:

If we define S as

$$S = \mathrm{lcm}(A, B, C),$$

from the definition of Tesla's entropy we have,

$$E_T(S) = \sum_i \frac{\alpha_i}{2 \cdot a_i^2} + \ln(a_i^2) + \sum_j \frac{\beta_j}{2 \cdot b_j^2} + \ln(b_j^2) + \sum_k \frac{\gamma_k}{2 \cdot c_k^2} + \ln(c_k^2) \quad .$$

After a few simple algebraic manipulations it is simple to understand that

$$E_T(S) = \sum_i \frac{\alpha_i}{2 \cdot a_i^2} + \sum_j \frac{\beta_j}{2 \cdot b_j^2} + \sum_k \frac{\gamma_k}{2 \cdot c_k^2} + \ln\left(\left(\prod_{p \in Z} p\right)^2\right) \quad . \tag{1}$$

Also, it is not difficult to conclude that the following holds

$$\sum_i \frac{\alpha_i}{2 \cdot a_i^2} + \sum_j \frac{\beta_j}{2 \cdot b_j^2} + \sum_k \frac{\gamma_k}{2 \cdot c_k^2} < \frac{\ln(C)}{\ln(2)} \cdot \frac{1}{2 \cdot 2^2} + \frac{\ln(C)}{\ln(3)} \cdot \frac{1}{2 \cdot 3^2} < \frac{\ln(C)}{4} < \frac{\ln(C)}{3} \quad . \tag{2}$$

It is obvious that (2) does not give the tight upper bound for the expression on the most left side of inequality. However, that will not impact the subsequent line of the reasoning (but will simplify the equations that follow).

From PIN Conjecture we know that the following holds:

$$E_T(S) > \ln(C) \quad ,$$

so, having in mind (1) and (2), we have

$$\ln(C) < E_T(S) < \frac{\ln(C)}{3} + \ln\left(\left(\prod_{p \in Z} p\right)^2\right) \quad .$$

After a simple algebraic manipulation we obtain the following

$$\ln(C) < \ln\left(\left(\prod_{p \in Z} p\right)^3\right) \quad .$$

Having in mind that natural logarithm is a monotonically increasing function we can conclude that the following holds

$$C < \left(\prod_{p \in Z} p\right)^3 \quad ,$$

and that completes the proof of ŠABAC Theorem, since it is simple to understand that

$$C = \max(A, B, C).$$

5 A short proof of the Fermat's Last Theorem

Fermat's Last Theorem states that there are no three positive natural numbers a, b and c that satisfy the equation

$$a^n + b^n = c^n,$$

for any natural number n greater than 2.

If we denote $a^n = A$, $b^n = B$ and $c^n = C$, assume that gcd(a, b) =1, and define

$$Z = \{ p : p|ABC\}$$

to be primes that divide A, B or C, we can apply ŠABAC Theorem, and the folowing must hold

$$max\{A, B, C\} = C < \left(\prod_{p \in Z} p\right)^3 .$$

That leads toward (having in mind that not a single prime factor of numbers A, B and C can be bigger than c)

$$C = c^n < (c)^9 .$$

(See Jeff Vaaler's video about ABC conjecture for more detailed explanation.)

From the previous inequality we can conclude that the following holds:

$$n < 9.$$

It means that FLT holds for any number greater than 8 and it has been known for almost 200 years, that FLT holds for all numbers up to 8, and that completes the proof.

6 Conclusion

In this paper it was shown that every natural number can be related to many entropy measures, or, in a sense, every natural number represents a family of discrete distributions and their entropy measures. A new entropy measure is defined and used to state the PIN conjecture. Based on the PIN conjecture, a new simplified version of ABC conjecture for prime numbers has been proved and used to create a short proof of Fermat's Last Theorem.

References

1. A. Wiles (1995). "Modular eliptic curves and Fermat's Last Theorem", Annals of Mathematics, 141(3): 443-551.
2. D.W Masser (1985). "Open problems". In Chen, W. W. L. *ed). Proceeedings of the Symposium on Analytic Number Theory. London, Imperial College.
3. P. Mihälescu (2004). "Primary Cyclotomic Units and a Proof of Catalan's Conjecture", J. Reine Angew. Math., 2004(572), 167-195.
4. Euclid (1956). Heath, Thomas Little (ed.). "The Thirteen Books of the Elements", Vol. 2 (Books III-IX), Translated by Heath Thomas Little (2nd unabridged reprint ed.). New York: Dover Publications.
5. M.V. Jankovic (2009). "Geometrical Interpretation of Shannon's Entropy Based on the Born Rule", *arXiv preprint, arXiv*:*0909.4995*.