Available online at www.sciencedirect.com

ScienceDirect

Indagationes Mathematicae 26 (2015) 147–161

indagationes mathematicae

www.elsevier.com/locate/indag

On the counting function of irregular primes

Florian Luca[a,1], Amalia Pizarro-Madariaga[b,*], Carl Pomerance[c]

[a] *School of Mathematics, University of the Witwatersrand, P.O. Box Wits 2050, South Africa*
[b] *Instituto de Matemáticas, Universidad de Valparaíso, Chile*
[c] *Department of Mathematics, Dartmouth College, Hanover, NH 03755-3551, USA*

Received 9 July 2014; received in revised form 26 August 2014; accepted 2 September 2014

Communicated by R. Tijdeman

Abstract

It is well-known that there are infinitely many irregular primes. We prove a quantitative version of this statement, namely the number of such primes $p \leq x$ is at least $(1 + o(1)) \log\log x / \log\log\log x$ as $x \to \infty$. We show that the same conclusion holds for the irregular primes corresponding to the Euler numbers. Under some conditional results from Diophantine approximation, the above lower bounds can be improved to $\gg \log x/(\log\log x)^2$.

Keywords: Irregular primes; Sieve methods; Linear form in logarithms

1. Introduction

The Bernoulli numbers $\{B_m\}_{m\geq 0}$ are defined via their exponential generating function

$$\frac{t}{e^t - 1} = \sum_{m\geq 0} B_m \frac{t^m}{m!}. \tag{1}$$

* Corresponding author. Tel.: +56 0322508373.
E-mail addresses: fluca@matmor.unam.mx (F. Luca), amalia.pizarro@uv.cl, amalia.pizarro@gmail.com (A. Pizarro-Madariaga), carl.pomerance@dartmouth.edu (C. Pomerance).
1 Also at: Mathematical Institute, UNAM Juriquilla 76230 Santiago de Querétaro, Mexico.

http://dx.doi.org/10.1016/j.indag.2014.09.002
0019-3577/

The first few values are

$$B_0 = 1, \qquad B_1 = -1/2, \qquad B_2 = 1/6, \qquad B_3 = 0, \qquad B_4 = -1/30,$$
$$B_5 = 0, \qquad B_6 = 1/42.$$

Evaluating relation (1) at $-t$ and subtracting the resulting formula from (1), one gets that $B_m = 0$ for all odd $m \geq 3$. There are several explicit formulas for computing B_m as well as the recurrences among them such as

$$\sum_{k=0}^{m-1} \binom{m}{k} B_k = 0 \quad \text{for all } m \geq 2,$$

which can be used to compute B_{m-1} in terms of B_j for $j \in \{0, \ldots, m-2\}$.

A prime $p > 2$ is called regular if it divides the class number of the cyclotomic field $\mathbb{Q}(\zeta_p)$, where $\zeta_p = e^{2\pi i/p}$ is a nontrivial pth root of unity. In 1850, Kummer [8] showed that p is regular if and only if it does not divide the numerator of any of the numbers

$$B_2, B_4, \ldots, B_{p-3}.$$

The first few regular primes are

$$3,\ 5,\ 7,\ 11,\ 13,\ 17,\ 19,\ 23,\ 29,\ 31,\ 41, \ldots.$$

This is sequence A007703 in [17]. In 1964, Siegel [16] conjectured that the regular primes have relative density $1/\sqrt{e}$ as a subset of all the primes. However, it is not even known that there are infinitely many regular primes. An odd prime which is not regular is called irregular. The first few irregular primes are

$$37,\ 59,\ 67,\ 101,\ 103,\ 131,\ 149, \ldots. \tag{2}$$

This is sequence A000928 in [17]. Unlike with the regular primes, it is known that there are infinitely many irregular primes. The first proof of this fact was given in 1915 by Jensen in [7], who in fact showed that there are infinitely many irregular primes congruent to 3 modulo 4. Almost 40 years later, in 1954, Carlitz [1], gave a simple proof of the weaker result that there are infinitely many irregular primes. Jensen's result was extended to the existence of irregular primes in other congruence classes by Montgomery [14] and Metsänkylä [13].

Let

$$\mathcal{I}_B = \{p : p \text{ irregular}\}$$

and let $\mathcal{I}_B(x) = \mathcal{I}_B \cap [1, x]$. Our main result is the following.

Theorem 1. *The inequality*

$$\#\mathcal{I}_B(x) \geq (1 + o(1)) \frac{\log\log x}{\log\log\log x}$$

holds as $x \to \infty$.

Let $\{E_m\}_{m \geq 0}$ be the sequence of Euler numbers whose exponential generating function is given by

$$\sec t = \sum_{m \geq 0} E_m \frac{t^m}{m!}.$$