CORRIGENDUM TO “CULLEN NUMBERS WITH THE LEHMER PROPERTY”

José María Grau Ribas and Florian Luca

(Communicated by Matthew A. Papanikolas)

Abstract. In this note, we correct an oversight in our paper “Cullen numbers with the Lehmer property”, Proc. Amer. Math. Soc. 140 (2012), 129–134.

There is an error on page 131 of paper [2] justifying that the expression $A$ is nonzero. After the sentence “Also, since $m_p$ divides $n_1$, it follows that $u \leq w$”, the argument continues in the following way. The case when $\rho = 1$ implies $n_1 = 1$, and this leads to the conclusion that all prime factors of $C_n$ are Fermat primes. This instance has been dealt with on page 131 in [2]. Thus, we may assume that $\rho \geq 3$. The relation $(2^{\alpha \rho^w} + \alpha)u = wn_p$ shows that $u \mid n_p$. Thus,

$$p = m_p2n_p + 1 = \rho^u 2n_p + 1 = X^u + 1,$$

where $X = \rho 2n_p/u$ is an integer. If $u > 1$, the above expression has $X + 1$ as a proper divisor $> 1$ (because $u$ is odd), which is impossible since $p$ is prime. Thus, $u = 1$. If $w = 1$, we first get that $m_p = n_1 = \rho$ and then that $n_p = \alpha + 2^\alpha \rho = \alpha + n$, so $p = C_n$, which is not allowed. Otherwise, $w \geq 3$, $n_1 = \rho^w$ and $p = \rho 2^{\alpha + n}/w + 1 = (n2^\alpha)^1/w + 1$. We now show that there is at most one prime $p$ with the above property. Indeed, assume that there are two of them, $p_1$ and $p_2$, corresponding to $w_1 < w_2$. Thus, $n_1 = \rho_1^{w_1} = \rho_2^{w_2}$, and both $w_1$ and $w_2$ divide $n + \alpha$. Let $W = \text{lcm}[w_1, w_2]$. Then $n_1 = \rho_0^W$ for some positive integer $\rho_0$. Furthermore, writing $W = \omega_1\lambda$, we have that $\lambda > 1$ and $\rho_0^\lambda = \rho_1$. Hence,

$$p_1 = \rho_1 2^{(\alpha + n)/w_1 + 1} = Y^{\lambda} + 1,$$

where $Y = \rho_0 2^{\alpha + n}/W$ is an integer. This is false since $\lambda > 1$ is odd. Therefore the above expression $Y^{\lambda} + 1$ has $Y + 1$ as a proper divisor $> 1$, contradicting the fact that $p_1$ is prime. Hence, if $A$ is zero for some $p$, then $p$ is unique. Further, in this case, $n_1 = \rho^w$ and $p = (n2^\alpha)^1/w + 1 \leq (n2^\alpha)^{1/3} + 1$. 

Received by the editors November 2, 2011.

2010 Mathematics Subject Classification. Primary 11A05; Secondary 11A07, 11N25.

©2013 American Mathematical Society

Reverts to public domain 28 years from publication.
The remainder of the argument from [2] shows that the expression $A$ is nonzero for all other primes $q$ of $C_n$, so all prime factors $q$ of $C_n$ satisfy inequality (5) in [2] with at most one exception, say $p$, which satisfies the inequality $p \leq (n2^n)^{1/3} + 1$. Hence, instead of the inequality from line 2 of page 132 in [2], we get that

$$C_n < ((n2^n)^{1/3} + 1)2^{6(k-1)(n \log n)^{1/2}},$$

giving

$$2^{6(k-1)(n \log n)^{1/2}} > \frac{n2^n}{(n2^n)^{1/3} + 1} > 2^{2n/3},$$

where the rightmost inequality above holds for all $n \geq 3$. This leads to a slightly worse inequality than inequality (6) in [2], namely,

(1)

$$k > 1 + \frac{n^{1/2}}{9(\log n)^{1/2}}.$$

Note that inequality (6) from [2] still holds whenever $A \neq 0$ for all primes $p$ dividing $n$, and in particular for all $n$ except maybe when $n_1 = \rho^w$ for some $\rho \geq 3$ and $w \geq 3$. So, from now on, we shall treat only the case when $n_1 = \rho^w$. Comparing estimate (3) in [2] with (1) leads to

(2)

$$\frac{n^{1/2}}{9(\log n)^{1/2}} < 2.4 \log n,$$

which implies that $n < 1.4 \times 10^6$. We now lower the bound in a way similar to the calculation on page 132 in [2]. Namely, first, if $2^{2^\gamma + 1}$ is a Fermat prime factor of $C_n$, then $\gamma \leq 20$, so $\gamma \in \{0, 1, 2, 3, 4\}$. Furthermore, $\log n / \log 3 \leq 12.9$; therefore $k \leq 5 + 12 = 17$. Now inequality (1) shows that

$$\frac{n^{1/2}}{9(\log n)^{1/2}} < 16,$$

giving $n < 260,000$. But then $\log n / \log 3 \leq 11.4$, giving $k \leq 16$. Also, if $n$ is not a multiple of 3, then the number of prime factors $p$ of $C_n$ with $m_p > 1$ is at most $\log 260,000 / \log 5 < 7.8$. Thus $C_n$ can have at most $5 + 7 = 12$ distinct prime factors, contradicting the result of Cohen and Hagis [1]. Hence, $3 \mid n$ shows that 3 does not divide $C_n$. Thus, $k \leq 15$, so

$$\frac{n^{1/2}}{9(\log n)^{1/2}} < 14,$$

giving $n < 200,000$. Also, $n$ cannot be divisible by a prime $q \geq 5$, for otherwise, since $n_1 = \rho^w$ for some $w \geq 3$, we would get that the number of prime factors $p$ of $C_n$ with $m_p > 1$ is at most $3 + \log(200,000/q^3) / \log 3 < 9.8$, so $k \leq 9 + 4 = 13$, again contradicting the result of Cohen and Harris. Hence $n = 2^\alpha \cdot 3^\beta$, and the proof finishes as in [2] after formula (7).
ACKNOWLEDGEMENT

The authors thank Dae Jun Kim for pointing out the oversight.

REFERENCES

[1] G. L. Cohen and P. Hagis, On the number of prime factors of \( n \) if \( \phi(n) \mid n - 1 \), *Nieuw Arch. Wisk.* 28 (1980), 177–185. MR582925 (81j:10002)


Departamento de Matemáticas, Universidad de Oviedo, Avda. Calvo Sotelo, s/n, 33007 Oviedo, Spain

E-mail address: grau@uniovi.es

Centro de Ciencias Matemáticas, Universidad Nacional Autónoma de México, C.P. 58089, Morelia, Michoacán, México

E-mail address: luca@matmor.unam.mx