On a property of the minimal universal exponent, $\lambda(x)$

By Hans Riesel

The purpose of this note is to answer the following question: For which numbers $x$ does $\lambda(x)$ divide the given number $k$? The answer is: For all divisors $x$ of a certain number $X$, which will be constructed in the note.

In constructing $X$ one uses the following

Theorem. All "quadratfrei" solutions $q$ of the equation

$$\lambda(q) \mid k \quad (\lambda(q) \text{ divides } k),$$

are the divisors of the denominator $Q$ of the Bernoullian number $B_k$, given in its lowest terms.

The first step will be to prove the theorem. To begin with, the definition of $\lambda(n)$ and of the Bernoullian numbers $B_k$ will be recalled, $\lambda(n)$ being the so-called minimal universal exponent, i.e. the least positive exponent $\lambda$, for which the congruence $a^{\lambda} \equiv 1 \pmod{n}$ holds for all $a$ for which the g.c.d. $(a, n)$ of $a$ and $n$ equals 1. As is well known, $\lambda(n)$ is calculated in the following manner: Let $\varphi(n)$ denote Euler's $\varphi$-function

$$\varphi(n) = n \prod_{p \mid n} \left(1 - \frac{1}{p}\right) \quad \text{if} \quad n = \prod p_i^{r_i},$$

where all $p_i$ are different primes. Furthermore, let $\lambda(p_i^{r_i}) = r_i \varphi(p_i^{r_i})$. Here, $r_i = \frac{1}{2}$, if $p_i = 2$ and $\alpha_i \geq 3$, otherwise $r_i = 1$. Then

$$\lambda(n) = [\lambda(p_i^{r_i})],$$

(the l.c.m. of all numbers $\lambda(p_i^{r_i})$), which may be written

$$\lambda(n) = [r_i \varphi(p_i^{r_i})] = [r_i p_i^{r_i - 1} (p_i - 1)].$$

From (2), it immediately follows that

$$\lambda(d) \mid \lambda(n) \quad \text{if} \quad d \mid n.$$  (3)

The Bernoullian numbers $B_k$ are defined by the equation

$$\frac{x}{e^x - 1} = \sum_{m=0}^{\infty} \frac{x^m}{m!} B_m,$$

which gives

$$27: 5 \quad 401$$
HANS RIESEL, On a property of the minimal universal exponent, $\lambda(x)$

$$
B_0 = 1, \quad B_1 = -\frac{1}{2}, \quad B_2 = \frac{1}{6}, \quad B_4 = -\frac{1}{30}, \\
B_6 = \frac{1}{42}, \quad B_8 = -\frac{1}{30}, \quad B_{10} = \frac{5}{66}, \quad B_{12} = -\frac{691}{2730}, \ldots \\
B_3 = B_5 = B_7 = \ldots = 0.
$$

The proof of the theorem proceeds as follows: If $q$ is "quadratfrei" $q = \prod p_i$, and

$$
\lambda(q) = [p_i - 1],
$$

which divides $k$ if and only if $(p_i - 1)|k$ for all $i$. The greatest "quadratfrei" solution $Q$ is thus obtained as the product of all primes $p_i$ for which $(p_i - 1)|k$. According to (3) and because of the fact that every factor of a "quadratfrei" number $Q$ is a "quadratfrei" number, it is clear that all "quadratfrei" solutions of (1) are the divisors of $Q$.

Now from the theorem by von Staudt and Clausen:

$$
B_k \equiv -\sum_i \frac{1}{p_i} \pmod{1},
$$

where the summation is extended over all primes $p_i$ such that $(p_i - 1)|k$, it follows that the denominator of $B_k$, given in its lowest terms, is the above number $Q$. This proves the theorem.

Example. $k = 10$ gives $(p_i - 1)|k$, if $p_i = 2, 3$ or $11$. $Q = \prod p_i = 2 \cdot 3 \cdot 11 = 66$. $B_{10} = \frac{5}{66}$. The "quadratfrei" solutions of $\lambda(q)|10$ are the 8 divisors of 66, for which one has

$$
\begin{align*}
\lambda(1) &= 1, \quad \lambda(2) = 1, \quad \lambda(3) = 2, \quad \lambda(6) = 2, \\
\lambda(11) &= 10, \quad \lambda(22) = 10, \quad \lambda(33) = 10, \quad \lambda(66) = 10.
\end{align*}
$$

For odd numbers $k$, $(p_i - 1)|k$ if and only if $p_i = 2$. In this case $Q = 2$, and the solutions $q = 1$ and $q = 2$ alone exist. Thus in this connection all Bernoullian numbers with odd indices $> 1$, $B_3 = B_5 = \ldots = 0$ should be provided with the denominator 2, as is already the case with $B_1 = -\frac{1}{2}$. However, because of the simple nature of this special case we do not want to introduce such a convention.

It is, however, possible to get not only all "quadratfrei" solutions $q$ to (1), but all solutions $x$. One must first determine the number $Q$ and then examine for each prime $p_i$ in $Q$ which is the greatest exponent $a_i$, such that

$$
\lambda(p_i^{a_i})|k.
$$

The number $X$ will be obtained as $\prod p_i^{a_i}$. According to (3), as before, all divisors $x$ of $X$ will be the solutions of

$$
\lambda(x)|k.
$$

Example. $k = 2 \cdot 3^3 \cdot 19$, $Q = 2 \cdot 3 \cdot 7 \cdot 19$
\[ \lambda(2^k) | k \text{ gives } \alpha \leq 3, \]
\[ \lambda(3^k) | k \text{ gives } \alpha \leq 4, \]
\[ \lambda(7^k) | k \text{ gives } \alpha \leq 1, \]
\[ \lambda(19^k) | k \text{ gives } \alpha \leq 2, \]

which gives \( X = 2^3 \cdot 3^4 \cdot 7 \cdot 19^2. \)

The formula for constructing \( X \) might also be written

\[ X = 2 Q \cdot \max_n (Q^n, k). \]