JOURNAL
de Théorie des Nombres
de BORDEAUX

anciennement Séminaire de Théorie des Nombres de Bordeaux

Eryk Tadeusz LIPKA

Corrigendum to "Automaticity of the sequence of last nonzero digits of factorial in a fixed base"

Tome 37, nº 2 (2025), p. 711-714.

https://doi.org/10.5802/jtnb.1338

CENTRE MERSENNE

Le Journal de Théorie des Nombres de Bordeaux *est membre du Centre Mersenne pour l'édition scientifique ouverte*
http://www.centre-mersenne.org/
e-ISSN : 2118-8572

Journal de Théorie des Nombres
de Bordeaux **37** (2025), 711–714

Corrigendum to "Automaticity of the sequence of last nonzero digits of factorial in a fixed base"

J. Théor. Nombres Bordeaux 31 (2019), no. 1, p. 283-291

par Eryk Tadeusz LIPKA

Résumé. Nous corrigeons notre preuve précédente du fait que la suite des derniers chiffres non nuls de $n!$ est automatique lorsque la base de numération est une puissance d'un nombre premier. L'erreur a été récemment remarquée par J.-M. Deshouillers.

Abstract. We correct our previous proof of the fact that the sequence of the last nonzero digits of a factorial is automatic when considered in a base being a power of a prime. The error was recently noticed by J.-M. Deshouillers.

Let $\ell_b(x)$ denote the last (least-significant) nonzero digit of x in a base b. In our previous paper we proposed a complete characterization of such bases b, that $(\ell_b(n!))_{n\in\mathbb{N}}$ is automatic. This was a continuation of previous work by Deshouillers and Ruzsa [2] who considered case $b = 12$. We used the following lemma to show that for some b, $(\ell_b(n!))_{n\in\mathbb{N}}$ is automatic.

Lemma 3.6. *If $b = p^a, p \in \mathbb{P}, a \in \mathbb{N}$ then the sequence $(\ell_b(n!))_{n\in\mathbb{N}}$ is b-automatic.*

We claimed that the above fact is true and was generally known before. Because we couldn't find a concrete proof of it, we decided to include one in our paper for the sake of completeness. Proofs of special cases of this fact could be found elsewhere [3]. The work on the topic was continued by Sobolewski [5], who generalized the problem by looking at sequences of k last nonzero digits of $n!$ for $k \geq 1$. It is worth noting that his results imply Lemma 3.6. The most significant difference is that Sobolewski's approach is using fixed points of morphisms, while we focused on an automata construction.

However, as recently pointed out by J.-M. Deshouillers in private communications, the proof we provided is actually wrong. We start the proof

Manuscrit reçu le 22 avril 2024, révisé le 19 mai 2024, accepté le 17 juillet 2024.
2010 *Mathematics Subject Classification.* 11B85, 11A63, 68Q45, 68R15.
Mots-clefs. Automatic sequence, factorial, the last nonzero digit.

with "notice that $\ell_b(xy) = \ell_b(\ell_b(x)\ell_b(y))$", which is false for $b = p^a, a \geq 2$. A simple counterexample is

$$3 = \ell_4(12) = \ell_4(6 \cdot 2) \neq \ell_4(\ell_4(6)\ell_4(2)) = \ell_4(2 \cdot 2) = \ell_4(4) = 1$$

and it is easy to construct similar counterexamples for other b. A few sentences later, we use Euler's totient theorem without ensuring that the base of exponentiation is coprime with the modulus. Both of those errors are the result of (obviously wrongly) assuming that $\ell_b(x)$ for a positive integer x is coprime with b. This makes our proof incorrect for cases where b is not a prime but a power of a prime. Below we present a corrected proof where l_b is, for the most part, replaced with another sequence that actually has the required properties. As this is only a correction, we assume the reader is familiar with basic definitions and facts regarding automatic sequences and the automata theory that we used in the original paper. For in-depth details, we recommend the book by Allouche and Shallit [1].

Proof. Fix a base $b = p^a$. Instead of directly constructing an automaton computing $l_b(n!)$, we will construct smaller automata, the output of which can be easily combined to obtain $l_b(n!)$.

Let $v(x) = \max\{k \in \mathbb{N} : p^k | x\}$, $f(x) = \frac{x}{p^{v(x)}} \bmod b$, i.e., the value of $f(x)$ is the number one obtains by writing x in the base p, removing the trailing zeros and taking last a of the remaining digits. We have

$$\frac{xy}{p^{v(xy)}} = \frac{xy}{p^{v(x)+v(y)}} = \frac{x}{p^{v(x)}} \cdot \frac{y}{p^{v(y)}},$$

$$f(xy) = \left(\frac{x}{p^{v(x)}} \cdot \frac{y}{p^{v(y)}}\right) \bmod b = (f(x)f(y)) \bmod b = f(f(x)f(y)).$$

For any positive integer x the value of $f(x)$ is coprime with b, so from Euler's totient theorem $f(x)^{\varphi(b)} \equiv 1 \bmod b$. Let $A_y(n) = \#\{i \in \mathbb{N} : 1 \leq i \leq n, f(i) = y\} \bmod \varphi(b)$. Value of $f(n!)$ can be computed if we know $A_y(n)$ for all $1 \leq y < b$ using the formula

$$\begin{aligned} f(n!) &= \prod_{1 \leq i \leq n} f(i) \bmod b \\ &= \prod_{1 \leq y < b} y^{\#\{i \in \mathbb{N}: 1 \leq i \leq n, f(i) = y\}} \bmod b \\ &= \prod_{1 \leq y < b} y^{A_y(n)} \bmod b. \end{aligned} \tag{0.1}$$

Now we will construct an automaton computing $A_y(n)$ for given $1 \leq y < b$. If $p | y$ then $A_y(n) = 0$, so from now on assume $p \nmid y$. The set $\{i \in \mathbb{N} : 1 \leq i \leq n, f(i) = y\}$ can be written as a disjoint sum $\bigsqcup_{0 \leq k} B_{y,k}(n)$ where $B_{y,k}(n) = \{i \in \mathbb{N} : 1 \leq i \leq n, f(i) = y, v(i) = k\}$. Because $p^{\log_p(n)+1} > n$, for $k > \log_p(n)$ we have $B_{y,k} = \emptyset$.

Notice, that $B_{y,k} = \{(0\cdot b+y)p^k, (1\cdot b+y)p^k, (2\cdot b+y)p^k, \ldots\} \cap \{1,\ldots,n\}$, so $B_{y,k}$ is an arithmetic progression with a difference of bp^k. The number of elements in $B_{y,k}$ is $\left\lfloor \frac{n}{bp^k} \right\rfloor$ when $\left\lfloor \frac{n}{bp^k} \right\rfloor bp^k + yp^k > n$ or $\left\lceil \frac{n}{bp^k} \right\rceil$ otherwise. That last condition can be rewritten as $yp^k \le (n \bmod (bp^k))$. If we look at the digits of $n = n_g n_{g-1} \ldots n_1 n_0$ then the condition is equivalent to checking whether $n_{k+a-1} \ldots n_{k+1} n_k \ge y$, and the number $\left\lfloor \frac{n}{bp^k} \right\rfloor$ is just $n_g \ldots n_{k+a+1} n_{k+a}$.

Our automaton will read a number from left to right and store internally three values. After reading the digits $n_g \ldots n_h$, the memory will consist of: $(n_g \ldots n_{h+a}) \bmod \varphi(b), (n_{h+a-1} \ldots n_h), (\sum_{k=h}^{\log_b n} B_{y,k}(n)) \bmod \varphi(b)$. Formally, we define an automaton $(Q, \Sigma, \rho, q_0, \Delta, \tau)$ by:

- the input alphabet $\Sigma = \{0, 1, 2, \ldots, p-1\}$;
- the output alphabet $\Delta = \{0, 1, \ldots \varphi(b) - 1\}$;
- the set of states $Q = \Delta \times \Sigma^a \times \Delta$;
- the initial state $q_0 = (0, (0 \ldots 0), 0)$;
- the output function $\tau(u, v, w) = w$;
- the transition function $\rho : Q \times \Sigma \mapsto Q$, which is defined as follows: for a given state $(u, (v_{a-1} \ldots v_0), w)$ and an input digit s the transition function returns the state with the following three components

$$pu + v_{a-1} \bmod \varphi(b),$$
$$(v_{a-2} \ldots v_0 s),$$
$$\left(w + pu + v_{a-1} + \begin{cases} 1 \text{ if } (v_{a-2} \ldots v_0 s) \ge y \\ 0 \text{ otherwise} \end{cases} \right) \bmod \varphi(b).$$

It is easy to check that after reading the digit n_{h-1} the internal state of the automaton is exactly as we stated: the transition function replaces $(n_g \ldots n_{h+a}) \bmod \varphi(b)$ by $(n_g \ldots n_{h+a} n_{h+a-1}) \bmod \varphi(b)$, $(n_{h+a-1} \ldots n_h)$ by $(n_{h+a-2} \ldots n_{h-1})$ and $(\sum_{k=h}^{\log_b n} B_{y,k}(n)) \bmod \varphi(b)$ by $(\sum_{k=h-1}^{\log_b n} B_{y,k}(n)) \bmod \varphi(b)$. The output of this automaton is $(\sum_{k=0}^{\log_b n} B_{y,k}(n)) \bmod \varphi(b) = A_y(n)$.

This construction can be repeated for all possible y, and by taking the product of those automata, we obtain an automaton that computes $A_y(n)$ for each $1 \le y < n, p \nmid y$. Change of the output function according to (0.1) yields an automaton that computes $f(n!)$.

To recover the last nonzero base-b digit we only need to know the "alignment", or what blocks of base-p digits correspond to a single base-b digit. We have $l_b(n!) = f(n!) p^{(v(n!) \bmod a)} \bmod b$. By Legendre's formula $v(n!) = \frac{n - s_p(n)}{p-1}$, where $s_p(n)$ is the sum of base p digits of n. As we need $v(n!) \bmod a$, we can compute it from $n \bmod (a\cdot(p-1))$ and $s_p(n) \bmod (a \cdot (p-1))$, both of which are classic examples of p-automatic sequences.

Combining the p-automata computing $f(n!), v(n!) \bmod a$ we obtain a p-automaton, and thus a b-automaton computing $l_b(n!)$. □

References

[1] J.-P. Allouche & J. Shallit, *Automatic Sequences. Theory, Applications, Generalizations*, Cambridge University Press, 2003, xvi+571 pages.

[2] J.-M. Deshouillers & I. Z. Ruzsa, "The least nonzero digit of $n!$ in base 12", *Publ. Math. Debr.* **79** (2011), no. 3-4, p. 395-400.

[3] G. P. Dresden, "Three transcendental numbers from the last non-zero digits of n^n, F_n, and $n!$", *Math. Mag.* **81** (2008), no. 2, p. 96-105.

[4] E. T. Lipka, "Automaticity of the sequence of last nonzero digits of factorial in a fixed base", *J. Théor. Nombres Bordeaux* **31** (2019), no. 1, p. 283-291.

[5] B. Sobolewski, "On the last nonzero digits of $n!$ in a given base", *Acta Arith.* **191** (2019), no. 2, p. 173-189.

Eryk Tadeusz Lipka
University of the National Education Comission
Podchorążych 2
30-084 Kraków, Poland
E-mail: eryklipka0@gmail.com