TOKYO J. MATH.
VOL. 43, NO. 2, 2020
DOI: 10.3836/tjm/1502179333

Erratum to Geometric Aspects of Lucas Sequences, I

Noriyuki SUWA

Chuo University

There are mistakes in the statements of Corollary 3.13 and Corollary 3.14 in ⟨Geometric Aspects of Lucas sequences, I⟩. The author has forgotten to specify the assumption $(p, Q) = 1$ in Corollary 3.13 and Corollary 3.14. Besides, he has left out the assumption needed in Corollary 3.14 (3): $L_{k(p)+1} \equiv 1 \mod p^{\nu}$.

Here are corrected statements and an adapted proof. Concerning Corollary 3.14, we add a new assertion as (3) and modify the assertion (3) in the previous version as (4).

COROLLARY 3.13. *Let p be an odd prime with $(p, Q) = 1$. Then $k(p)/r(p)$ divides $p - 1$.*

COROLLARY 3.14. *Let p be an odd prime with $(p, Q) = 1$ and n a positive integer, and put $\nu = \mathrm{ord}_p L_{r(p)}$. Moreover, let ν' denote the greatest positive integer such that $L_{k(p)} \equiv 0 \mod p^{\nu'}$ and $L_{k(p)+1} \equiv 1 \mod p^{\nu'}$. Then we have:*
(1) $\nu = \mathrm{ord}_p L_{k(p)}$;
(2) $r(p^n) = \begin{cases} r(p) & (n \leq \nu) \\ p^{n-\nu} r(p) & (n > \nu) \end{cases}$;
(3) $k(p^n) = \begin{cases} k(p) & (n \leq \nu') \\ p^{n-\nu'} k(p) & (n > \nu') \end{cases}$;
(4) *Assume $L_{k(p)+1} \equiv 1 \mod p^{\nu}$. Then we have $\nu' = \nu$.*

PROOF. First we prove the assertion (1). It follows from the definition of ν that $\beta(\theta)^{r(p)} = 1$ in $G_{(D)}(\mathbb{Z}/p^{\nu}\mathbb{Z})$ but $\beta(\theta)^{r(p)} \neq 1$ in $G_{(D)}(\mathbb{Z}/p^{\nu+1}\mathbb{Z})$. Therefore, we obtain $\beta(\theta)^{k(p)} = 1$ in $G_{(D)}(\mathbb{Z}/p^{\nu}\mathbb{Z})$ since $k(p)$ is divisible by $r(p)$. On the other hand, we obtain $\beta(\theta)^{k(p)} \neq 1$ in $G_{(D)}(\mathbb{Z}/p^{\nu+1}\mathbb{Z})$, combining the facts: (a) $\beta(\theta)^{r(p)} \in \mathrm{Ker}[G_{(D)}(\mathbb{Z}/p^{\nu+1}\mathbb{Z}) \to G_{(D)}(\mathbb{Z}/p^{\nu}\mathbb{Z})]$, (b) $\mathrm{Ker}[G_{(D)}(\mathbb{Z}/p^{\nu+1}\mathbb{Z}) \to G_{(D)}(\mathbb{Z}/p^{\nu}\mathbb{Z})]$ is of order p (cf. Corollary 2.21) and (c) $k(p)/r(p)$ divides $p - 1$ (Corollary 3.13).

Received January 17, 2020; revised February 1, 2020
Mathematics Subject Classification: 11B27
Key words and phrases: Lucas sequence, affine group scheme, Laxton group