Cryptogr. Commun. (2018) 10:1203
https://doi.org/10.1007/s12095-018-0314-5

CORRECTION

Correction to: Good integers and some applications in coding theory

Somphong Jitman[1]

Received: 8 May 2018 / Accepted: 8 May 2018 / Published online: 18 May 2018

Correction to: Cryptogr. Commun. (2018) 10:685–704
https://doi.org/10.1007/s12095-017-0255-4

Proposition 2.1 and Proposition 2.3 in the original publication are incorrectly worded and they should be as follows.

Proposition 2.1 *Let a and b be coprime odd integers and let $\beta \geq 1$ be an integer. Then the following statements are equivalents.*

$i)$ $2^\beta \in G_{(a,b)}$.
$ii)$ $2^\beta | (a+b)$.
$iii)$ $ab^{-1} \equiv -1 \ mod\ 2^\beta$.

Proposition 2.3 *Let a, b and $d > 1$ be pairwise coprime odd positive integers and let $\beta \geq 2$ be an integer. Then $2^\beta d \in G_{(a,b)}$ if and only if $2^\beta | (a+b)$ and $d \in G_{(a,b)}$ is such that $2||ord_d(\frac{a}{b})$. In this case, $ord_{2^\beta}(\frac{a}{b}) = 2$ and $2||ord_{2^\beta d}(\frac{a}{b})$.*

As a consequence of the above corrections, the bullets (c) and (d) of Theorem 2.1 and Theorem 3.1 in the original paper should be rewritten as follows.

(c) $\beta \geq 2, d = 1$ and $2^\beta | (a+b)$.
(d) $\beta \geq 2, d \geq 3, 2^\beta | (a+b)$ and $d \in G_{(a,b)}$ is such that $2||\mathrm{ord}_d(\frac{a}{b})$.

The above rewordings do not affect any other result given in the paper.

The readers may refer to http://www.math.sc.su.ac.th/web3/files/somphong/J-Correction-GoodIntegers.pdf for a full discussion.

The online version of the original article can be found under https://doi.org/10.1007/s12095-017-0255-4

✉ Somphong Jitman
sjitman@gmail.com

[1] Department of Mathematics, Faculty of Science, Silpakorn University, Nakhon Pathom 73000, Thailand