Correction to: Good Integers and some Applications in Coding Theory

Somphong Jitman

Abstract

In this note, the errors in the paper "Good integers and some applications in coding theory, *Cryptography and Communications* 10, 685–704 (2018)" by S. Jitman have been discussed as well as corrections that are practical with the remaining parts of the original paper.

Keywords: good integers

MSC2010: 11N25

1 Introduction

For fixed coprime nonzero integers a and b, a positive integer d is said to be *good (with respect to a and b)* if it is a divisor of $a^k + b^k$ for some integer $k \geq 1$. Denote by $G_{(a,b)}$ the set of good integers defined with respect to a and b. This concept has been introduced in [2]. A positive integer d is said to be *oddly-good (with respect to a and b)* if $d|(a^k + b^k)$ for some odd integer $k \geq 1$, and *evenly-good (with respect to a and b)* if $d|(a^k + b^k)$ for some even integer $k \geq 2$ (see [1]). Denote by $OG_{(a,b)}$ (resp., $EG_{(a,b)}$) the set of oddly-good (resp., evenly-good) integers defined with respect to a and b.

Properties of good integers have been studied in [1] and [2]. Note that some results on good integers determined in [1] are not correct. The errors have been pointed out with possible corrections in [3]. Precisely, [1, Proposition 2.1] and [1, Proposition 2.3] are erroneous caused by the following false expressions "$\mathrm{ord}_{2^\beta}(\frac{a}{b}) = 2 \Rightarrow ab^{-1} \equiv -1 \bmod 2^\beta$" and "$\mathrm{ord}_d(\frac{a}{b}) = 2k \Rightarrow (ab^{-1})^k \equiv -1 \bmod d$" used in their proofs, where a, b and $d \geq 1$ are pairwise coprime odd integers and $\beta \geq 1$ is an integer.

S. Jitman is with the Department of Mathematics, Faculty of Science, Silpakorn University, Nakhon Pathom 73000, Thailand (email: sjitman@gmail.com).

In this note, corrections of [1, Proposition 2.1] and [1, Proposition 2.3] that are closed to their original statements and practical with the remaining part of [1] are discussed.

2 Results

In this section, corrections of [1, Proposition 2.1] and [1, Proposition 2.3] are given as well as their consequences.

First we note that $\mathrm{ord}_2(x) = 1$ and $\mathrm{ord}_{2^\beta}(x) = 2$ for all odd integers x and $\beta \geq 2$ such that $x \equiv -1 \bmod 2^\beta$.

A correction of [1, Proposition 2.1] is given in the following proposition.

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.*

1) $2^\beta \in G_{(a,b)}$.

2) $2^\beta | (a+b)$.

3) $ab^{-1} \equiv -1 \bmod 2^\beta$.

Proof. To prove 1) implies 2), assume that $2^\beta \in G_{(a,b)}$. If $\beta = 1$, then $2^\beta | (a+b)$ since $a+b$ is even. Then $2^\beta | (a^k + b^k)$ for some integer $k \geq 1$. Assume that $\beta > 1$. Then $4 | (a^k + b^k)$. If k is even, then $a^k \equiv 1 \bmod 4$ and $b^k \equiv 1 \bmod 4$ which implies that $(a^k + b^k) \equiv 2 \bmod 4$, a contradiction. It follows that k is odd. Since $a^k + b^k = (a+b)\left(\sum\limits_{i=0}^{k-1}(-1)^i a^{k-1-i} b^i\right)$ and $\sum\limits_{i=0}^{k-1}(-1)^i a^{k-1-i} b^i$ is odd, we have that $2^\beta | (a+b)$.

The statement 2) $\Rightarrow$ 1) follows from the definition. The equivalent statement 2) $\Leftrightarrow$ 3) is obvious. $\square$

The next proposition is a correction of [1, Proposition 2.3].

Proposition 2.2. *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 $2 || \mathrm{ord}_d(\frac{a}{b})$. In this case, $\mathrm{ord}_{2^\beta}(\frac{a}{b}) = 2$ and $2 || \mathrm{ord}_{2^\beta d}(\frac{a}{b})$.*

Proof. Assume that $2^\beta d \in G_{(a,b)}$. Let k be the smallest positive integer such that $2^\beta d | (a^k + b^k)$. Then $d | (a^k + b^k)$ and $2^\beta | (a^k + b^k)$ which implies that $d \in G_{(a,b)}$ and $(ab^{-1})^{2k} \equiv 1 \bmod d$. Moreover, $2^\beta | (a+b)$ and k must be odd by Proposition 2.1 and its proof. Let k' be the smallest positive integer such that $d | (a^{k'} + b^{k'})$. Then

$\mathrm{ord}_d(\frac{a}{b}) = 2k'$. Since $(ab^{-1})^{2k} \equiv 1 \bmod d$, we have $k'|k$. Consequently, k' is odd and $(a+b)|(a^{k'}+b^{k'})$. Hence, $2^\beta d|(a^{k'}+b^{k'})$. By the minimality of k, we have $k = k'$ and $d|(a^k+b^k)$. Consequently, $\mathrm{ord}_d(\frac{a}{b}) = 2k' = 2k$. Since k is odd, $d \in G_{(a,b)}$ is such that $2||\mathrm{ord}_d(\frac{a}{b})$.

Conversely, assume that $2^\beta|(a+b)$ and $d \in G_{(a,b)}$ is such that $2||\mathrm{ord}_d(\frac{a}{b})$. Let k be the smallest positive integer such that $d|(a^k+b^k)$. Then $(ab^{-1})^k \equiv -1 \bmod d$ which implies that $\mathrm{ord}_d(\frac{a}{b}) = 2k$. Since $2||\mathrm{ord}_d(\frac{a}{b})$, k must be odd. It follows that $(ab^{-1})^k \equiv ab^{-1} \equiv -1 \bmod 2^\beta$. Since d is odd, $(ab^{-1})^k \equiv -1 \bmod 2^\beta d$. Hence, $2^\beta d|(a^k+b^k)$ which means $2^\beta d \in G_{(a,b)}$ as desired.

In this case, we have $2^\beta|(a+b)$ which implies that $\mathrm{ord}_{2^\beta}(\frac{a}{b}) = 2$. Moreover, $\mathrm{ord}_{2^\beta d}(\frac{a}{b}) = \mathrm{lcm}\left(\mathrm{ord}_{2^\beta}(\frac{a}{b}), \mathrm{ord}_d(\frac{a}{b})\right) = 2k$ and k is odd. Therefore, $2||\mathrm{ord}_{2^\beta d}(\frac{a}{b})$. $\square$

As a consequence of the above corrections, [1, Theorem 2.1] and [1, Theorem 3.1] should be rewritten as follows.

Theorem 2.3 ([1, Corrected version of Theorem 2.1])**.** *Let a and b be coprime nonzero integers and let $\ell = 2^\beta d$ be a positive integer such that d is odd and $\beta \geq 0$. Then one of the following statements holds.*

1) *If ab is odd, then $\ell = 2^\beta d \in G_{(a,b)}$ if and only if one of the following statements holds.*

   (*a*) *$\beta \in \{0, 1\}$ and $d = 1$.*

   (*b*) *$\beta \in \{0, 1\}$, $d \geq 3$ and there exists $s \geq 1$ such that $2^s||\mathrm{ord}_p(\frac{a}{b})$ for every prime p dividing d.*

   (*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 $2||\mathrm{ord}_d(\frac{a}{b})$.*

2) *If ab is even, then $\ell = 2^\beta d \in G_{(a,b)}$ if and only if one of the following statements holds.*

   (*a*) *$\beta = 0$ and $d = 1$.*

   (*b*) *$\beta = 0$, $d \geq 3$, and there exists $s \geq 1$ such that $2^s||\mathrm{ord}_p(\frac{a}{b})$ for every prime p dividing d.*

Theorem 2.4 ([1, Corrrected Version of Theorem 3.1])**.** *Let a and b be coprime nonzero integers and let $\ell = 2^\beta d$ be an integer such that d is odd and $\beta \geq 0$. Then one of the following statements holds.*

1) *If ab is odd, then $\ell = 2^\beta d \in OG_{(a,b)}$ if and only if one of the following statements holds.*

   (a) $\beta \in \{0,1\}$ *and* $d = 1$.

   (b) $\beta \in \{0,1\}$, $d \geq 3$, *and* $2||\mathrm{ord}_p(\frac{a}{b})$ *for every prime* p *dividing* d.

   (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* $2||\mathrm{ord}_d(\frac{a}{b})$.

2) *If ab is even, then $\ell = 2^\beta d \in OG_{(a,b)}$ if and only if one of the following statements holds.*

   (a) $\beta = 0$ *and* $d = 1$.

   (b) $\beta = 0$, $d \geq 3$, *and* $2||\mathrm{ord}_p(\frac{a}{b})$ *for every prime* p *dividing* d.

Later in [1], [1, Proposition 2.1] and [1, Proposition 2.3] have been applied in the proof of [1, Proposition 3.1]. We have checked and certified that [1, Proposition 3.1] is correct. However, in the proof of [1, Proposition 3.1], Proposition 2.1 and Proposition 2.2 in this note need to be applied instead.

Finally, we note that the above corrections do not affect any other result given in the paper [1] are still practical with the applications in [1, Section 4].

Acknowledgements

The author would like to thank Professor Madhu Raka [3] and an anonymous researcher for pointed out the errors.

References

[1] Jitman, S.: Good integers and some applications in coding theory, Cryptogr. Commun. **10**, 685–704 (2018).

[2] Moree, P.: On the divisors of $a^k + b^k$. Acta Arithmetica **LXXX**, 197–212 (1997).

[3] Raka, M.: Good integers : A note on results of Jitman and Prugsapitak, (2018) http://128.84.21.199/abs/1804.01916.