Period Math Hung (2018) 76:271–273
https://doi.org/10.1007/s10998-017-0227-7

CORRECTION

Correction to: The arithmetic of Carmichael quotients

Min Sha[1]

Published online: 30 November 2017

Abstract The statement of Proposition 4.3 in the published paper is not correct. Here we change the statement and give a complete proof.

Erratum to: Period Math Hung (2015) 71:11–23 https://doi.org/10.1007/s10998-014-0079-3

1 Replacement of [3, Proposition 4.3]

We first illustrate a counter-example for [3, Proposition 4.3]. Take $m = 273 = 3 \times 7 \times 13$. Using the notation in [3, Proposition 4.3], we have $d = 3$ and $d' = 1$. That is, the homomorphism ϕ_m defined there is surjective. However, for any positive integer a coprime to m, $C_m(a)$ is divisible by 3, because $6 \mid \lambda(m)$ and then $9 \mid a^{\lambda(m)} - 1$. This leads to a contradiction.

Proposition 4.3 and its proof in [3] should be replaced by Proposition 1.1 below. Fortunately, this does not affect other results and arguments in [3], although Proposition 4.3 in [3] was quoted several times there.

Assume that positive integer m has the prime factorization $m = p_1^{r_1} \cdots p_k^{r_k}$. In [1, Proposition 4.4], the Euler quotient has been used to define a homomorphism from $(\mathbb{Z}/m^2\mathbb{Z})^*$ to $(\mathbb{Z}/m\mathbb{Z}, +)$, whose image is $d\mathbb{Z}/m\mathbb{Z}$, where

$$d = \prod_{i=1}^{k} d_i \quad \text{and} \quad d_i = \begin{cases} \gcd(p_i^{r_i}, 2\varphi(m)/\varphi(p_i^{r_i})) & \text{if } p_i = 2 \text{ and } r_i \geq 2, \\ \gcd(p_i^{r_i}, \varphi(m)/\varphi(p_i^{r_i})) & \text{otherwise.} \end{cases} \tag{1.1}$$

In fact, the above d, d_i are equivalent to those d, d_i defined in [3], respectively.

The online version of the original article can be found under https://doi.org/10.1007/s10998-014-0079-3.

✉ Min Sha
shamin2010@gmail.com

1 Department of Computing, Macquarie University, Sydney, NSW 2109, Australia

By [3, Proposition 2.2 (2)], the Carmichael quotient $C_m(x)$ induces a homomorphism

$$\phi_m : (\mathbb{Z}/m^2\mathbb{Z})^* \to (\mathbb{Z}/m\mathbb{Z}, +), x \mapsto C_m(x),$$

where $C_m(x) = (x^{\lambda(m)} - 1)/m$ and $\lambda(m)$ is the Carmichael function.

Proposition 1.1 *Let $m = p_1^{r_1} \cdots p_k^{r_k}$ be the prime factorization of $m \geq 2$. For $1 \leq i \leq k$, put*

$$d_i' = \begin{cases} \gcd(p_i^{r_i}, 2\lambda(m)/\lambda(p_i^{r_i})) & \text{if } p_i = 2 \text{ and } r_i = 2, \\ \gcd(p_i^{r_i}, \lambda(m)/\lambda(p_i^{r_i})) & \text{otherwise.} \end{cases}$$

Let $d' = \prod_{i=1}^k d_i'$. Then the image of the homomorphism ϕ_m is $d'\mathbb{Z}/m\mathbb{Z}$.

Proof We show the desired result case by case.

(I) First we prove the result for the case $k = 1$, that is $m = p^r$, where p is a prime and r is a positive integer.

Suppose that $p = 2$. If $r = 2$, then $C_m(3) = 2$, and for any positive integer n we have $C_m(2n+1) = n(n+1)$, which is even, so the image of ϕ_m is $2\mathbb{Z}/m\mathbb{Z}$. On the other hand, if $r = 1$ or $r \geq 3$, since $C_2(3) = 1$ and $C_8(3) = 1$, by using [3, Proposition 2.8] we see that $C_m(3)$ is an odd integer, so the image of ϕ_m is $\mathbb{Z}/m\mathbb{Z}$.

Now, assume that $p > 2$. Note that $C_p(p+1) \equiv -1 \pmod p$, by [3, Proposition 2.8] we have $C_m(p+1) \equiv -1 \pmod p$, which implies that $p \nmid C_m(p+1)$. Thus, there exists a positive integer n such that $nC_m(p+1) \equiv 1 \pmod m$. Then, by [3, Proposition 2.2 (1)] we deduce that $C_m((p+1)^n) \equiv 1 \pmod m$. So, the image of ϕ_m is $\mathbb{Z}/m\mathbb{Z}$.

(II) To complete the proof, we prove the result when $k \geq 2$.

For simplicity, denote $m_i = m/p_i^{r_i}$ and $n_i = \lambda(m)/\lambda(p_i^{r_i})$ for each $1 \leq i \leq k$, and then let m_i' be an integer such that $m_i^2 m_i' \equiv 1 \pmod{p_i^{r_i}}$. By [3, Proposition 2.7], we have

$$C_m(a) \equiv \sum_{i=1}^k m_i m_i' n_i C_{p_i^{r_i}}(a) \pmod m. \tag{1.2}$$

So, for each $1 \leq i \leq k$, $C_m(a) \equiv m_i m_i' n_i C_{p_i^{r_i}}(a) \pmod{p_i^{r_i}}$. If $p_i = 2$ and $r_i = 2$, note that for any odd integer $a > 1$, $C_4(a)$ is even, then we see that $d_i' \mid n_i C_{p_i^{r_i}}(a)$, and thus $d_i' \mid C_m(a)$. Otherwise if $p_i > 2$ or $r_i \neq 2$, then $d_i' \mid n_i$, and so $d_i' \mid C_m(a)$. Hence, we have $d' \mid C_m(a)$ for any integer a coprime to m.

Let $b = \gcd(m, m_1 m_1' n_1, \ldots, m_k m_k' n_k)$. Then, there exist integers $X_1, \ldots, X_k$ such that

$$b \equiv \sum_{i=1}^k m_i m_i' n_i X_i \pmod m. \tag{1.3}$$

If we denote $b_i = \gcd(p_i^{r_i}, m_i m_i' n_i)$ for each $1 \leq i \leq k$, then $b = \prod_{i=1}^k b_i$; here, we remark that $b_i = \gcd(p_i^{r_i}, n_i)$. It is easy to see that for each $1 \leq i \leq k$, if $p_i > 2$ or $r_i \neq 2$, we have $d_i' = b_i$. Further, when $p_i = 2$ and $r_i = 2$, $d_i' = 2b_i$ if $8 \nmid \lambda(2p_1 \ldots p_k)$, and $d_i' = b_i$ otherwise.

We now have three cases for m:

(i) There exists $1 \leq j \leq k$ such that $p_j = 2, r_j = 2$ and

$$8 \nmid \lambda(2p_1 \ldots p_k).$$

(ii) There exists $1 \le j \le k$ such that $p_j = 2, r_j = 2$ and

$$8 \mid \lambda(2p_1 \dots p_k).$$

(iii) All the other cases.

Clearly, in Cases (ii) and (iii) we have $d' = b$, and in Case (i) $d' = 2b$.

According to (I), there exist integers a_i with $p_i \nmid a_i$ for $1 \le i \le k$ defined by

$$C_{p_i^{r_i}}(a_i) \equiv \begin{cases} 2X_i & \text{in Case (i),} \\ X_i & \text{in Case (iii),} \\ X_i & \text{in Case (ii) and } i \neq j, \\ 0 & \text{in Case (ii) and } i = j. \end{cases} \pmod{p_i^{r_i}}$$

By the Chinese Remainder Theorem, we can choose a positive integer a such that $a \equiv a_i \pmod{p_i^{2r_i}}$. So, by [3, Proposition 2.2 (2)] we have $C_{p_i^{r_i}}(a) \equiv C_{p_i^{r_i}}(a_i) \pmod{p_i^{r_i}}$. Then, combining with (1.3) and the relation between b and d', we obtain $m_i m_i' n_i C_{p_i^{r_i}}(a) \equiv d' \pmod{p_i^{r_i}}$ for each $1 \le i \le k$ in all the three cases. Finally, using (1.2) we have $C_m(a) \equiv d' \pmod{m}$, which completes the proof. □

Comparing (1.1) with Proposition 1.1, we have $d' \mid d$. Moreover, by [3, Proposition 2.1] we get

$$\frac{\varphi(m)}{\lambda(m)} d'\mathbb{Z}/m\mathbb{Z} = d\mathbb{Z}/m\mathbb{Z},$$

which implies that $\gcd(\frac{\varphi(m)}{\lambda(m)} d', m) = d$.

2 Another error

We take this opportunity to correct another error. In the proof of [3, Lemma 3.4], the last identity "$\equiv \ell n^{-1} 2^{r-2}$" may be not true, and it should be deleted. Because by using $n^{2^{r-2}} \equiv 1 \pmod{2^r}$, we only know that $(n^{2^{r-2}} + 1)/2$ is an odd integer, which may be not congruent to 1 modulo 2^r. Clearly, this error does not change the result there.

Acknowledgements The author wants to thank the anonymous referee of his joint paper [2] for pointing out the error in [3, Proposition 4.3] and giving the counter-example.

References

1. T. Agoh, K. Dilcher, L. Skula, Fermat quotients for composite moduli. J. Number Theory **66**, 29–50 (1997)
2. F. Luca, M. Sha, I.E. Shparlinski, On two functions arising in the study of the Euler and Carmichael quotients. Colloq. Math. **149**, 179–192 (2017)
3. M. Sha, The arithmetic of Carmichael quotients. Period. Math. Hung. **71**, 11–23 (2015)