An inequality for 3-factor Carmichael numbers due to J.M. Chick

We refer to Carmichael numbers with three prime factors as "C_3-numbers". Let $n = pqr$ be such a number, with $p < q < r$. Let g be the gcd of $p-1$, $q-1$ and $r-1$, and

$$p = ag + 1, \quad q = bg + 1, \quad r = cg + 1.$$

Then g is an even integer, a, b, c are pairwise coprime, and there is an integer k such that $E = kabc$, where

$$E = (bc + ca + ab)g + a + b + c \tag{1}$$

[e.g. Jam, 2.6]. So

$$k = \frac{E}{abc} = \left(\frac{1}{a} + \frac{1}{b} + \frac{1}{c}\right) g + \frac{1}{bc} + \frac{1}{ca} + \frac{1}{ab}. \tag{2}$$

LEMMA 1. *We have* $ka \leq 3g - 1$.

Proof. This follows from

$$\begin{aligned} ka &= \left(1 + \frac{a}{b} + \frac{a}{c}\right) g + \left(\frac{1}{b} + \frac{1}{c} + \frac{a}{bc}\right) \\ &< 3g - g\left(\frac{1}{b} + \frac{2}{c}\right) + \frac{1}{b} + \frac{2}{c} < 3g. \end{aligned} \tag{3}$$

In particular, $a \leq 3g - 1$. The following stronger inequality was established by J.M. Chick [Ch, Theorem 4.1].

THEOREM 1. *For all C_3-numbers, we have* $a < 3g - (g/2)^{1/2}$.

Here we present a slightly simplified version of Chick's proof. In fact, we will show that except in one very special type of case (which possibly may never occur), we have the stronger inequality $a < 3g - g^{1/2} + 1$. We then show how to extend the theorem to ka instead of a

First, another general inequality for C_3-numbers:

LEMMA 2. *We have* $k(a + b + c) > 9g$.

Proof. Let $(abc)^{1/3} = G$ and $\frac{1}{3}(a+b+c) = A$, so that $A = 3g + \frac{1}{3}S_1$. By the inequality of the means, $A \geq G$. Also, $\frac{1}{3}(bc + ca + ab) \geq (bc.ca.ab)^{1/3} = G^2$. Now $(bc + ca + ab)g < E = abc = kG^3$, so $3G^2g < kG^3$, hence $kA \geq kG > 3g$. □

Next, we dispose of the case $g = 2$. We only have to show that $a \neq 5$. This follows from the well-known fact that there are no C_3-numbers with $p = 11$. (In fact, it is easily shown that the only C_3-numbers with $g = 2$ are $3 \times 11 \times 17$ and $7 \times 23 \times 41$.)

Note now that if $k \geq 2$, then $a < \frac{3}{2}g$, so we assume that $k = 1$, hence $abc = E$. Write

$$a = 3g + \alpha, \quad b = 3g + \beta, \quad c = 3g + \gamma. \tag{4}$$

Then $\alpha < \beta < \gamma$, and since $1 \leq a < 3g$, we have $-3g < \alpha < 0$. Write

$$S_1 = \alpha + \beta + \gamma, \qquad S_2 = \beta\gamma + \gamma\alpha + \alpha\beta.$$

By Lemma 2, $S_1 > 0$.

Call a triple of integers (α, β, γ) *admissible* if $\alpha < 0$, $\alpha \leq \beta < \gamma$ and $S_1 > 0$. Given such a triple, we show that there is at most one possible value for g, and that this value satisfies $g < 2\alpha^2$. To do this, we now regard g as a continuous variable and define $a = a(g)$, $b = b(g)$ and $c = c(g)$ by (4), $E = E(g)$ by (1) and $k(g)$ by (2). We will just write a, b, c instead of $a(g)$, etc. Clearly, $a > 0$ for $g > -\alpha/3$. Also, $k(g) = 1 - m(g)/(abc)$, where $m(g) = abc - E(g)$, so that $k(g) = 1$ iff $m(g) = 0$.

LEMMA 3. *We have*

$$m(g) = 3S_1 g^2 + (2S_2 - 9)g + \alpha\beta\gamma - S_1. \tag{5}$$

Proof. This follows from the identities

$$abc = 27g^3 + 9S_1 g^2 + 3S_2 g + \alpha\beta\gamma,$$

$$E(g) = (27g^2 + 6S_1 g + S_2)g + 9g + S_1.$$

For (a, b, c, g) to generate a Carmichael number with $k = 1$, we require g to be an even positive integer satisfying $g > -\alpha/3$ and $m(g) = 0$. Also, a, b and c must be pairwise coprime.

LEMMA 4. *If (α, β, γ) is admissible, then $m(-\alpha/3) < 0$.*

Proof. If $g = -\alpha/3$, then $a = 0$ and $c > b > 0$. Hence $m(g) = abc - E(g) = -bcg - b - c < 0$. □

Since $m(g)$ is a quadratic with positive leading coefficient, it follows that there is a unique $g^* = g^*(\alpha, \beta, \gamma) > -\alpha/3$ with $m(g^*) = 0$. Further, $m(g) < 0$ for $-\alpha/3 < g < g^*$ and $m(g) > 0$ for $g > g^*$, so if $g_0 > -\alpha/3$ and $m(g_0) > 0$, then $g^* < g_0$. This g^* is the only value of g that can combine with (α, β, γ) to generate a C_3-number with $k = 1$. Of course, it can only do so if it is also an even integer (which in many cases it is not).

LEMMA 5. *Suppose that* $(\alpha_1, \beta_1, \gamma_1)$ *and* $(\alpha_2, \beta_2, \gamma_2)$ *are admissible and* $\alpha_1 = \alpha_2 = \alpha$, $\beta_1 < \beta_2$ *and* $\beta_1 + \gamma_1 = \beta_2 + \gamma_2$. *Let* $m_j(g)$ *be derived from* $(\alpha_j, \beta_j, \gamma_j)$ *for* $j = 1, 2$. *Suppose that* $g > -\alpha/3$ *and* $m_1(g) > 0$. *Then* $m_2(g) > 0$.

Proof. Then (with obvious notation), $a_2 = a_1 > 0$, $b_2 > b_1$ and $b_2 + c_2 = b_1 + c_1$, also $b_2 \le c_2$. We have

$$k(g) = \frac{g}{a} + \left(g + \frac{1}{a}\right)\left(\frac{1}{b} + \frac{1}{c}\right) + \frac{1}{bc} = \frac{g}{a} + \left(g + \frac{1}{a}\right)\frac{b+c}{bc} + \frac{1}{bc}.$$

Now $b_2c_2 - b_1c_1 = (b_2 - b_1)c_2 + b_1(c_2 - c_1) = (b_2 - b_1)(c_2 - b_1) > 0$, so $k_2(g) < k_1(g)$, hence $m_2(g)/(a_2b_2c_2) > m_1(g)/(a_1b_1c_1) > 0$. □

Conclusion of proof of the Theorem. Write $\rho = -\alpha$.

Case 1: $S_1 \ge 2$. We show that in this case, $\rho > g^{1/2} - 1$. So we have to show that $g^* < (\rho + 1)^2$, where g^* is defined by $m(g^*) = 0$. This will follow if we can show that $m[(\rho + 1)^2] > 0$. By Lemma 5, it is enough to prove this for triples of the form (α, α, γ), since it then follows for all (α, β, γ) with the same value of S_1 (this simplifies the algebra slightly, though of course we are only interested in triples with $\beta \ge \alpha + 1$). Write $S_1 = S$, and take $\alpha = \beta = -\rho$ and $\gamma = S + 2\rho$. Then $S_2 = \rho^2 - 2\rho\gamma = -2\rho S - 3\rho^2$, so

$$m(g) = 3Sg^2 - (4S\rho + 6\rho^2 + 9)g + \rho^2(S + 2\rho) - S.$$

Since $\rho \ge 1$, we have $\rho^2(S + 2\rho) \ge S$ and hence

$$m[(\rho + 1)^2] > (\rho + 1)^2 f(S, \rho),$$

where (since $S \ge 2$)

$$\begin{aligned} f(S, \rho) &= 3S(\rho + 1)^2 - (4S\rho + 6\rho^2 + 9) \\ &= (3S - 6)\rho^2 + 2S\rho + 3S - 9 \\ &> 4\rho - 3 > 0. \end{aligned}$$

Case 2: $S_1 = 1$. In this case, we show that $\rho > (g/2)^{1/2}$, or $g < 2\rho^2$, which will follow if we can show that $m(2\rho^2) > 0$. For integer solutions (which are the only ones that matter), the condition $S_1 = 1$ implies that $a + b + c = 9g + 1$, so $a + b + c$ is odd. Since a, b and c are pairwise coprime, they are all odd, so α, β and γ are odd, and $\beta \ge \alpha + 2$. The case $\alpha = -1$ does not occur, since then $\beta \ge 1$ and $\gamma \ge 3$, so $S_1 \ge 3$ (so in fact by Case 1, $\alpha = -1$ never occurs for a C_3-number). Hence $\rho \ge 3$. By Lemma 5, it is sufficient to prove the result for the case $\beta = \alpha + 2$, so we take $\alpha = -\rho$, $\beta = 2 - \rho$ and $\gamma = 2\rho - 1$. Then

$$S_2 = \rho(\rho - 2) + (2 - 2\rho)(2\rho - 1) = -3\rho^2 + 4\rho - 2,$$

and $\alpha\beta\gamma \geq 3$, so

$$m(g) > 3g^2 - (6\rho^2 - 8\rho + 13)g,$$

hence $m(2\rho^2) > 2\rho^2 g(S, \rho)$, where

$$g(S, \rho) = 6\rho^2 - (6\rho^2 - 8\rho + 13) = 8\rho - 13 > 0.$$

To reconcile the two cases, note that $g^{1/2} - 1 > (g/2)^{1/2}$ when $g \geq 6$. When $g = 4$, given that ρ has to be an integer, both statements equate to $\rho \geq 2$. So in all cases, we can state that $\rho > (g/2)^{1/2}$. □

Note on the case $S_1 = 1$. Similar reasoning shows that $\rho > g^{1/2} - 1$ when $S_1 = 1$ and $\beta \geq -1$. However, it is clear from Case 2 that with $S_1 = 1$ and $\beta = \alpha + 2$, we will have $m[(\rho+1)^2] < 0$ for sufficiently large ρ, since the leading term is $-3\rho^4$. But we do not know an actual example in which $\rho < g^{1/2} - 1$ with g taking an even integer value. An example with integer g and $\rho < g^{1/2}$ is $(\alpha, \beta, \gamma) = (-3, -1, 5)$, which has the solution $g = 14$. (However, this combination fails to generate a Carmichael number, because $41 \times 14 + 1$ is the composite number 575; in Chick's terminology, it generates a "K_3-number".)

Further note. In practice, there are very few C_3-numbers with $a > 2g$. Computations reported by Chick [Ch, p. 15] have found that there are just eleven such numbers up to 10^{24}. The first one is defined by $(a, b, c, g) = (1049, 1841, 2304, 518)$, and the largest value of a/g (≈ 2.683) is attained by $(a, b, c, g) = (1497, 1601, 2002, 558)$. All these numbers have S_1 much greater than 1, and ρ much greater than $g^{1/2}$.

A generalisation

As Lemma 1 shows, the real comparison is between ka and $3g$. We now extend the reasoning to prove:

THEOREM 2. *For all C_3-numbers, we have $ka < 3g - (g/2)^{1/2}$.*

In the notation of [Jam], $ka - g$ is the number j, which plays an important part in the algebra of C_3-numbers. So Theorem 2 gives $j \leq 2g - (g/2)^{1/2}$.

The previous remark on the case $g = 2$ still applies, since $ka = 5$ could only occur with $k = 1$ and $a = 5$. So we may assume that $g \geq 4$.

We show first that when $a < 3g^{1/2} - 2$, the stated inequality is an easy consequence of the trivial fact that $b \geq a + 1$ and $c \geq a + 2$. Write $3g - ka = \rho$.

LEMMA 6. *For any C_3-number, we have*

$$\rho > \frac{3(g-1)}{a+2}.$$

Proof. Recall that

$$ka = \left(1 + \frac{a}{b} + \frac{a}{c}\right) g + \left(\frac{1}{b} + \frac{1}{c} + \frac{a}{bc}\right).$$

Since $b \geq a+1$ and $c \geq a+2$,

$$\frac{a}{b} + \frac{a}{c} \leq \frac{a}{a+1} + \frac{a}{a+2} = 2 - \frac{1}{a+1} - \frac{2}{a+2} < 2 - \frac{3}{a+2},$$

$$\frac{1}{b} + \frac{1}{c} + \frac{a}{bc} \leq \frac{1}{a+1} + \frac{1}{a+2} + \frac{a}{(a+1)(a+2)} = \frac{3a+3}{(a+1)(a+2)} = \frac{3}{a+2}.$$

The stated inequality follows. □

COROLLARY 6.1. *If $g \geq 4$ and $a \leq 3g^{1/2} - 2$, then $\rho > g^{1/2} - \frac{1}{2}$.*

Proof. Then

$$\rho > \frac{g-1}{g^{1/2}} = g^{1/2} - \frac{1}{g^{1/2}} \geq g^{1/2} - \frac{1}{2}. \qquad \square$$

We will need the following further consequence of Lemma 6.

LEMMA 7. *We have $\rho \geq \min(k, a-2)$.*

Proof. By Lemma 6, $(a+2)\rho > 3g - 3 = ka + \rho - 3$, hence $(k-\rho)a < \rho + 3$. If $\rho < k$ (so that $\rho \leq k-1$), this implies that $a < \rho + 3$, so $a - 2 \leq \rho$. □

LEMMA 8. *If $g \geq 4$ and $a > 3g^{1/2} - 2$, then $\rho \geq k$.*

Proof. By Lemma 7, this follows if we can show that $k \leq a - 2$. If not, we have $k \geq a - 1 > 3g^{1/2} - 3$, hence

$$ka - 3g > 6g - 15g^{1/2} + 6 = 2(g^{1/2} - 2)(2g^{1/2} - 1) > 0,$$

contradicting the fact that $ka < 3g$. □

We now follow the steps used to prove Theorem 1, with suitable modifications. Fix a positive integer k_0. We shall prove our statement for C_3-numbers with $k = k_0$. Given (α, β, γ), define a, b, c by

$$k_0 a = 3g + \alpha, \quad k_0 b = 3g + \beta, \quad k_0 c = 3g + \gamma, \tag{6}$$

and define S_1, S_2 as before. When these numbers generate a C_3-number, $\beta-\alpha$ and $\gamma-\beta$ will be multiples of k_0, and by Lemma 2, $S_1 > 0$. Also, define $E(g)$ by (1) and $k(g) = E(g)/(abc)$. Then

$$k(g) = k_0 - \frac{m(g)}{k_0^2 abc},$$

where $m(g) = k_0^3 abc - k_0^2 E(g)$, so $k(g) = k_0$ iff $m(g) = 0$.

LEMMA 9. *We have*

$$m(g) = 3S_1 g^2 + (2S_2 - 9k_0)g + \alpha\beta\gamma - k_0 S_1. \tag{7}$$

Proof. This follows from the identities

$$k_0^3 abc = 27g^3 + 9S_1 g^2 + 3S_2 g + \alpha\beta\gamma,$$

$$k_0^2 E(g) = (27g^2 + 6S_1 g + S_2)g + k_0(9g + S_1). \qquad \square$$

Lemmas 4 and 5 apply unchanged.

Proof of Theorem 2. The following includes the case $k_0 = 1$, hence Theorem 1.

Case 1: $S_1 \geq 2$. We show again that $\rho > g^{1/2} - 1$. By Lemmas 6 and 8, we only have to prove this when $\rho \geq k_0$. Write $S_1 = S$. By Lemma 5, it is enough to show that $m[(\rho+1)^2] > 0$ for triples (α, β, γ) with $\beta = 1 - \rho$, hence $\gamma = S + 2\rho - 1$ (though in fact $\beta \geq k_0 - \rho$ in cases of interest). Then

$$S_2 = \rho(\rho - 1) + (1 - 2\rho)(S + 2\rho - 1) = -3\rho^2 + 3\rho - 1 - S(2\rho - 1),$$

and $\alpha\beta\gamma \geq 0$, so

$$m(g) > 3Sg^2 - (4S\rho - 2S + 6\rho^2 - 6\rho + 2 + 9k_0)g - k_0 S,$$

so $m[(\rho+1)^2] > (\rho+1)^2 f(S,\rho) - k_0 S$, where (since $\rho \geq k_0$)

$$\begin{aligned} f(S,\rho) &= 3S(\rho+1)^2 - (4S\rho - 2S + 6\rho^2 - 6\rho + 9k_0 + 2) \\ &\geq (3S - 6)\rho^2 + 2S\rho + 5S - 3\rho - 2 \\ &> \rho + 5S - 2 > S, \end{aligned}$$

hence $m[(\rho+1)^2] > 0$.

Case 2: $S_1 = 1$. As before, we show that $\rho > (g/2)^{1/2}$. For integer solutions, we have $k_0(a+b+c) = 9g+1$, so k_0, a, b, c are all odd. So $\beta - \alpha$ is even and a multiple of k_0, hence of $2k_0$. Similarly for $\gamma - \beta$, so $\beta \geq 2k_0 - \rho$ and $\gamma \geq 4k_0 - \rho$. Hence $1 = S_1 \geq 6k_0 - 3\rho$, so

$\rho \geq 2k_0$. Now consider $m(g)$ with $\beta = 2 - \rho$ and $\gamma = 2\rho - 1$, as in case 2 of Theorem 1. Then $\alpha\beta\gamma \geq \rho > k_0$, so from the expression for S_2,

$$m(g) > 3g^2 - (6\rho^2 - 8\rho + 4 + 9k_0)g,$$

hence $m(2\rho^2) > 2\rho^2 g(S, \rho)$, where

$$g(S, \rho) = 6\rho^2 - (6\rho^2 - 8\rho + 4 + 9k_0) = 8\rho - 4 - 9k_0 \geq 7k_0 - 4 > 0.$$

References

[Ch] J.M. Chick, Carmichael number variable relations: three-prime Carmichael numbers up to 10^{24}, arXiv:0711.2915v2[math.NT].

[Jam] G.J.O. Jameson, Carmichael numbers with three prime factors, at `www.maths.lancs.ac.uk/~jameson`.

G.J.O. Jameson

January 2012