Improvement of an estimate of H. Müller involving the order of 2(mod u) II

Pieter Moree

Abstract

Let $m \geq 1$ be an arbitrary fixed integer and let $N_m(x)$ count the number of odd integers $u \leq x$ such that the order of 2 modulo u is not divisible by m. In case m is prime estimates for $N_m(x)$ were given by Müller that were subsequently sharpened into an asymptotic estimate by the present author. Müller on his turn extended the author's result to the case where m is a prime power and gave bounds in the case m is not a prime power. Here an asymptotic for $N_m(x)$ is derived that is valid for all integers m. This asymptotic would easily have followed from Müller's approach were it not for the fact that a certain Diophantine equation has non-trivial solutions. All solutions of this equation are determined. We also generalize to other base numbers than 2. For a very sparse set of these numbers Müller's approach does work.

1 Introduction

Let u be odd. Denote by $l(u)$ the smallest natural number such that

$$2^{l(u)} \equiv 1 (\text{mod } u).$$

The number $l(u)$ is called the *order* of the congruence class 2(mod u). Let $N_m(x)$ denote the number of odd integers $u \leq x$ such that $m \nmid l(u)$. It was shown by Franco and Pomerance [1, Theorem 5] in the context of a generalization of the celebrated "$3x+1$"-problem, that almost all integers u have the property that $m|l(u)$, i.e. they established that, as x tends to infinity,

$$N_m(x) = o(x).$$

The object of this note is to derive an asymptotic formula for $N_m(x)$. Partial progress towards this goal was made by H. Müller in his papers [6, 7]. Let $q > 2$ be a prime. Müller [6] showed that

$$\frac{x}{\log^{1/(q-1)} x} \ll N_q(x) \ll \frac{x}{\log^{1/q} x}.$$

This was improved by the present author in [3], where he showed that

$$N_q(x) = c_q \frac{x}{\log^{q/(q^2-1)} x}\left(1 + O\left(\frac{(\log\log x)^5}{\log x}\right)\right), \tag{1}$$

with $c_q > 0$ a positive real constant. On his turn Müller [7] improved on this, by establishing the following generalization of the asymptotic estimate (1).

Theorem 1 (H. Müller). *Let $q > 2$ be a prime and $n \geq 1$ fixed. Then*

$$N_{q^n}(x) = c_{q^n} \frac{x}{\log^{q^{2-n}/(q^2-1)} x} \left(1 + O\left(\frac{(\log\log x)^5}{\log x}\right)\right),$$

with c_{q^n} a positive real constant.

Müller did not obtain an asymptotic result in case m is not a prime power. If $m = p_1^{e_1} \cdots p_r^{e_r}$, he notes that

$$N_{p_1^{e_1}}(x) \leq N_m(x) \leq N_{p_1^{e_1}}(x) + \cdots + N_{p_r^{e_r}}(x) \tag{2}$$

and from this infers, in case m is odd, that

$$\frac{x}{\log^{\alpha} x} \ll N_m(x) \ll \frac{x}{\log^{\beta} x},$$

where $\alpha := \max\{C(p_j, e_j) | 1 \leq j \leq r\}$, resp. $\beta := \min\{C(p_j, e_j) | 1 \leq j \leq r\}$, where for any prime q and integer $n \geq 1$ we define $C(q, n) := q^{2-n}/(q^2 - 1)$. (In fact, Müller erroneously swaps 'min' and 'max' in his definitions of α and β.)

Note that the stronger result, in case m is odd, that $x \log^{-\beta} x \ll N_m(x) \ll x \log^{-\beta} x$ actually follows from (2). More can be said however:

Lemma 1 *Let $m \geq 1$ be odd. Suppose that there is only one integer j such that $C(p_j, e_j) = \beta$, then we have that $N_m(x) \sim N_{p_j^{e_j}}(x)$ as x tends to infinity and the asymptotic behaviour of $N_m(x)$ is given by Theorem 1.*

Proof. W.l.o.g. we can assume that $C(p_1, e_1) = \beta$. Now if there is no further j such that that $C(p_j, e_j) = \beta$, then by Theorem 1 each of the terms $N_{p_k^{e_k}}(x)$ with $k \geq 2$ is asymptotically of smaller growth than $N_{p_1^{e_1}}(x)$ and so the lemma is proved. □

Note that if there is more than one integer j such that $C(p_j, e_j) = \beta$, then from (2) together with Theorem 1 the asymptotic behaviour of $N_m(x)$ cannot be determined. We are thus led to the problem of determining pairs of integers j and k and primes p_j and p_k such that $C(p_j, e_j) = C(p_k, e_k)$. The proof of the following result uses some arguments kindly provided by J.-H. Evertse and Y. Bilu. It follows that $C(2, 5) = C(5, 2) = C(3, 3) = 1/24$, $C(2, 6) = C(7, 2) = 1/48$ and $C(5, 3) = C(11, 2) = 1/120$.

Proposition 1 *There are only finitely many solutions (p, α, q, β) to*

$$p^{\alpha-2}(p^2 - 1) = q^{\beta-2}(q^2 - 1) \tag{3}$$

with α and β integers and p and q primes with $p < q$. These solutions are: $(2, 5, 3, 3)$, $(2, 5, 5, 2)$, $(2, 6, 7, 2)$, $(3, 3, 5, 2)$ and $(5, 3, 11, 2)$.

Proof. It is easy to see that if there is to be a solution, we must have $\alpha \geq 2$ and $\beta \geq 2$. Assume w.l.o.g. that $q > p$. If $\beta \geq 3$, then q must divide either $p-1$ or $p+1$. Since $q > p$ it follows that $q = p+1$ and so $p = 2$ and $q = 3$. This gives rise to precisely one solution: $(2,5,3,3)$. So we may assume that $\beta = 2$ and we are reduced to finding the solutions of

$$p^b(p^2-1) = q^2-1, \tag{4}$$

with $b \geq 0$.

First assume that $p = 2$. Then we have to solve the equation $q^2 - 1 = 3 \cdot 2^b$. As one of $q \pm 1$ cannot be divisible by 4, it follows that either $q-1 \in \{1,2,3,6\}$ or $q+1 \in \{1,2,3,6\}$. This gives rise to the solutions $(2,5,5,2)$ and $(2,6,7,2)$ (and no more). Thus we may assume that $p > 2$. There are two cases to be considered:
1) $p^b|q+1$. Then we can write $q+1 = p^b r$, $q-1 = s$ (say) and so $rs = p^2-1$. Thus $p^b r - s = 2$ and hence $r(p^b r - 2) = p^2 - 1$. Note that if $b > 1$, then we must have $r > 1$ and this gives rise to a contradiction. So $b = 1$ and hence we must have $r(pr-2) = p^2-1$. From this we infer that $0 < r < p$ and, furthermore that $-2r \equiv -1 (\mathrm{mod}\ p)$. It follows that $r = (p+1)/2$. Substituting this back we obtain $p^2 - 2p - 3 = 0$ which only gives rise to the solution $(3,3,5,2)$.
2) $p^b|q-1$. Now we have that $q+1$ divides p^2-1 and we obtain $p^b \leq q-1 < q+1 \leq p^2-1$, which is impossible when $b > 1$. We can write $q-1 = pr$, $q+1 = s$ (say) and so $rs = p^2-1$. Thus $s - pr = 2$ and hence $r(pr+2) = p^2-1$. From this we infer that $0 < r < p$ and, furthermore that $-2r \equiv 1 (\mathrm{mod}\ p)$. It follows that $r = (p-1)/2$. Substituting this back we see that $p^2 - 6p + 5 = 0$ which only gives rise to the solution $(5,3,11,2)$.

On collecting all solutions found along the way, the proof is completed. □

Since the Diophantine equation (3) has non-trivial solutions we are blocked for certain integers m (for example for $m = 2^5 \cdot 5^2 = 800$), in proving an asymptotic for $N_m(x)$ by using (2). We will provide an alternative to (2), Lemma 3, and use this to obtain a more precise estimate for $N_m(x)$ than can be provided by Müller's method, and works for every integer m. At the same time we generalize to other base numbers than 2.

2 Generalization to other base numbers

First we will generalize the main result mentioned sofar, Theorem 1, to the case where the base number g is rational and not in $\{-1,0,1\}$ (an assumption on g maintained throughout this paper). We let $\omega(n)$ denote the number of distinct prime divisors of n and by $\nu_p(n)$ denote the exponent of p in the prime factorization of n. Let $S(g)$ be the set of integers composed only of primes p that do not occur in the prime factorization of g (i.e. of primes p such that $\nu_p(g) = 0$). For each integer u in this set the order of g modulo u, $\mathrm{ord}_g(u)$, is well-defined. We let $P_g(d)(x)$ denote the number of primes $p \leq x$ with $p \in S(g)$ such that $d|\mathrm{ord}_g(p)$. It turns out that the set $P_g(d)$ of primes $p \in S(g)$ such that $d|\mathrm{ord}_g(p)$ has a natural density, which will be denoted by $\delta_g(d)$. This density was first determined by

Wiertelak [9], who derived a rather complicated explicit formula for it, a formula which was subsequently simplified by Pappalardi [8] and streamlined further by Moree [4]. It turns out that $\delta_g(d)$ is always a positive rational number. Part 1 of the following result is due to Wiertelak [9], part 2 to Moree [4]. As usual the logarithmic integral is denoted by $\mathrm{Li}(x)$.

Theorem 2 (Wiertelak [9], Moree [4]).
1) *We have* $P_g(d)(x) = \delta_g(d)\mathrm{Li}(x) + O\left(\frac{x}{\log^3 x}(\log\log x)^{\omega(d)+3}\right)$.
2) *Under GRH we have* $P_g(d)(x) = \delta_g(d)\mathrm{Li}(x) + O(\sqrt{x}\log^{\omega(d)+1} x)$.

In order to explicitly evaluate $\delta_g(d)$, some further notation is needed. Write $g = \pm g_0^h$, where g_0 is positive and not an exact power of a rational and h as large as possible. Let $D(g_0)$ denote the discriminant of the field $\mathbb{Q}(\sqrt{g_0})$. (This notation will reappear several times in the sequel.) Given an integer d, we denote by d^∞ the supernatural number (sometimes called Steinitz number), $\prod_{p|d} p^\infty$. Note that $\gcd(v, d^\infty) = \prod_{p|d} p^{\nu_p(v)}$.

`Definition`. Let d be even and let $\epsilon_g(d)$ be defined as in Table 1 with $\gamma = \max\{0, \nu_2(D(g_0)/dh)\}$.

Table 1: $\epsilon_g(d)$

$g\backslash\gamma$	$\gamma = 0$	$\gamma = 1$	$\gamma = 2$
$g > 0$	$-1/2$	$1/4$	$1/16$
$g < 0$	$1/4$	$-1/2$	$1/16$

Note that $\gamma \le 2$. Also note that $\epsilon_g(d) = (-1/2)^{2^\gamma}$ if $g > 0$.

Theorem 3 (Explicit evaluation of $\delta_g(d)$). *We have*

$$\delta_g(d) = \frac{\epsilon_1'(d)}{d\,\gcd(h, d^\infty)}\prod_{p|d}\frac{p^2}{p^2-1},\ \text{with}$$

$$\epsilon_1'(d) = \begin{cases} 1 & \text{if } 2 \nmid d; \\ 1 + 3(1-\mathrm{sgn}(g))(2^{\nu_2(h)}-1)/4 & \text{if } 2||d \text{ and } D(g_0) \nmid 4d; \\ 1 + 3(1-\mathrm{sgn}(g))(2^{\nu_2(h)}-1)/4 + \epsilon_g(d) & \text{if } 2||d \text{ and } D(g_0)|4d; \\ 1 & \text{if } 4|d,\ D(g_0) \nmid 4d; \\ 1 + \epsilon_{|g|}(d) & \text{if } 4|d,\ D(g_0)|4d. \end{cases}$$

By $N(x; g, m)$ we denote the number of integers $u \le x$ such that $u \in S(g)$ and $m \nmid \mathrm{ord}_g(u)$. Note that $N(x; 2, m) = N_m(x)$. A straightforward generalization of Theorem 1 yields the following result.

Theorem 4 *Let $n \ge 1$ be fixed. Then*

$$N(x; g, q^n) = c_{q^n}(g)\frac{x}{\log^{\delta_g(q^n)} x}\left(1 + O\left(\frac{(\log\log x)^5}{\log x}\right)\right).$$

It is an easy consequence of Theorem 3 that $\delta_g(q^n) = C(q,n)$ for almost all integers g. Furthermore, by Theorem 3 we find that

$$\delta_2(q^n) = \begin{cases} 17/24 & \text{if } q = 2 \text{ and } n = 1; \\ 5/12 & \text{if } q = 2 \text{ and } n = 2; \\ 2^{1-n}/3 & \text{if } q = 2 \text{ and } n \geq 3; \\ C(q,n) & \text{otherwise.} \end{cases}$$

This evaluation allows us to formulate Theorem 1 for every prime power (and thus also for every power of two). It then follows from (2) that $x \log^{-\gamma_2(m)} x \ll N_m(x) \ll x \log^{-\gamma_2(m)} x$, where

$$\gamma_g(m) := \min\{\delta_g(p_j^{e_j}) \mid 1 \leq j \leq r\}.$$

Lemma 1 can then be extended to all natural numbers m as follows:

Lemma 2 *Suppose that there is only one integer j such that $\delta_2(p_j^{e_j}) = \gamma_2(m)$, then we have that $N_m(x) \sim N_{p_j^{e_j}}(x)$ as $x \to \infty$ and the asymptotic behaviour of $N_m(x)$ follows from Theorem 4.*

We leave it as an exercise to the reader to show that the density of integers m satisfying such that $\delta_2(p_j^{e_j}) = \gamma_2(m)$ for only one integer j exists and equals

$$\frac{147497571941}{147916692000} \approx 0.9971665\cdots$$

An integer g such that there is only one integer j such that $\delta_g(p_j^{e_j}) = \gamma_g(m)$ for every natural number m, we define to be a *Müller number*. Müller's inequality (2) generalizes of course to

$$N(x; g, p_1^{e_1}) \leq N(x; g, m) \leq N(x; g, p_1^{e_1}) + \cdots + N(x; g, p_r^{e_r}). \tag{5}$$

The usefulness of Müller numbers is apparent from the following result.

Proposition 2 *If g is a Müller number and $\delta_g(p_j^{e_j}) = \gamma_g(m)$, then we have $N_m(x) \sim N_{p_j^{e_j}}(x)$ as $x \to \infty$ and the asymptotic behaviour of $N_m(x)$ is given by* Theorem 4.

In the next section it will be seen that, unfortunately, Müller numbers are very sparse.

3 Some further Diophantine considerations

The above discussion shows that if for $g = 2$ we want to cover odd integers m as well, rather than asking for the solutions of $C(p_i, e_i) = C(p_j, e_j)$, we should be asking for solutions of $\delta_2(p_i^{e_i}) = \delta_2(p_j^{e_j})$, and indeed, more generally, for the non-trivial solutions (p_1, e_1, p_2, e_2) with $p_1 \neq p_2$ primes and $e_1, e_2 \geq 1$ of

$$\delta_g(p_1^{e_1}) = \delta_g(p_2^{e_2}). \tag{6}$$

A variation of the proof of Proposition 1 gives that in case $g = 2$ we only have the non-trivial equalities $\delta_2(2^4) = \delta_2(3^3) = \delta_2(5^2)$, $\delta_2(2^5) = \delta_2(7^2)$ and $\delta_2(5^3) = \delta_2(11^2)$. The more general situation is described by the following result.

Theorem 5 *There are only finitely many quadruples* (p_1, e_1, p_2, e_2) *with* $p_1 < p_2$ *primes and* $e_1, e_2 \geq 1$ *such that* $\delta_g(p_1^{e_1}) = \delta_g(p_2^{e_2})$. *These quadruples are given as follows (and there are no further ones):*

$$\begin{cases} (2, 5-\tau_1-\nu_2(h), 3, 3-\nu_3(h)) & \text{if } 2^{5-\tau_2} \nmid h \text{ and } 3^3 \nmid h; \\ (2, 5-\tau_1-\nu_2(h), 5, 2-\nu_5(h)) & \text{if } 2^{5-\tau_2} \nmid h \text{ and } 5^2 \nmid h; \\ (2, 6-\tau_1-\nu_2(h), 7, 2-\nu_7(h)) & \text{if } 2^{6-\tau_2} \nmid h \text{ and } 7^2 \nmid h; \\ (3, 3-\nu_3(h), 5, 2-\nu_5(h)) & \text{if } 3^3 \nmid h \text{ and } 5^2 \nmid h; \\ (5, 3-\nu_3(h), 11, 2-\nu_{11}(h)) & \text{if } 5^3 \nmid h \text{ and } 11^2 \nmid h, \end{cases}$$

where

$$\tau_1(g) = \begin{cases} 1 & \text{if } D(g_0) = 8; \\ 0 & \text{otherwise,} \end{cases} \quad \text{and } \tau_2(g) = \tau_1(g) + \frac{1-\operatorname{sgn}(g)}{2}.$$

The associated values of δ_g *are* $1/24, 1/24, 1/48, 1/24$, *respectively* $1/120$.

Corollary 1 *Let*

$$S_1 = \{8000, 165373, 193600, 196000, 209088, 4002075, 4743200, 5122656\}.$$

Let S_2, *respectively* S_4 *be* S_1, *but with all even numbers in this set divided by* 2, *respectively* 4. *For a given number* g *equation* (6) *has only trivial solutions, that is* g *is a Müller number, if and only if* h *is divisible by a number from* $S_{2^{\tau_2(g)}}$.

`Example`. The numbers $-2^{2000}, 2^{4000}$ and 3^{8000} are examples of small Müller numbers. The number $g = 3^{4000}$ is not a Müller number, since $\delta_g(2^1) = \delta_g(7^2)$ by Theorem 5.

For the convenience of the reader we include a table where $\tau_1 = \tau_1(g)$ and $\tau_2 = \tau_2(g)$ are given.

Table 2: $\tau_1(g)$ and $\tau_2(g)$

	$D(g_0) \neq 8$		$D(g_0) = 8$	
	τ_1	τ_2	τ_1	τ_2
$g > 0$	0	0	1	1
$g < 0$	0	1	1	2

Clearly Müller numbers are very sparse. Indeed it is not difficult to quantify this: there are positive constants c_+ and c_- such that the number of positive Müller numbers up to x grows as $c_+ x^{1/8000}$ and the number of negative Müller numbers with absolute value not exceeding x as $c_- x^{1/4000}$ as $x \to \infty$.

The proof of Theorem 5 is unfortunately not very instructive as many cases have to be distinguished. As its level of difficulty is comparable to that of the proof of Proposition 1, we leave it to the interested reader.

In order to derive Corollary 1 we notice that the set of those integers h such that none of the 5 solutions in Theorem 5 occur, are the natural numbers of the form $(h_1) \cup \cdots \cup (h_s)$, where (h_i) denotes the ideal generated by h_i and $h_1, \ldots, h_s$ are certain integers. A priori the 5 solutions yield $2^5 = 32$ potential generators (for example $\operatorname{lcm}(3^3, 5^2, 7^2, 5^2, 11^2) = 4002075$), of which some turn out to be divisors of others (the latter ones can thus be left out from $S_{2^{\tau_2(g)}}$).

4 A more refined estimate for $N(x;g,m)$

We sharpen Müller's estimate (5) to an equality (given in Lemma 3) and use this to obtain a more refined estimate for $N(x;g,m)$ (and thus $N_m(x)$). As before we let $m={p_1}^{e_1}\cdots {p_r}^{e_r}$ denote the factorization of m. By $\kappa(m)=p_1\cdots p_r$ we denote the squarefree kernel of m. A divisor d of m is said to be *unitary* if $\gcd(d,m/d)=1$. Note that the non-trivial unitary divisors of m come out as 'blocks' from its factorization. Let $N'(x;g,m)$ denote the number of integers $u\le x$ from $S(g)$ such that $p_j^{e_j}\nmid \mathrm{ord}_g(u)$ for $1\le j\le r$. We let $P'(x;g,m)$ be similarly defined, but with the phrase 'integers $u\le x$' replaced by 'primes $p\le x$'. Note that $N'(x;g,p_j^{e_j})=N(x;g,p_j^{e_j})$.

Lemma 3 *We have*

$$N(x;g,m)=-\sum_{\substack{d\#m\\ d>1}}\mu(\kappa(d))N'(x;g,d),$$

where by $d\#m$ we indicate that the sum is over the unitary divisors d of m.

Proof. If $u\notin S(g)$, the integer u is not counted on either side of the purported identity. If $u\le x$ is in $S(g)$ we will show that it is counted with multiplicity one on both sides of the purported identity. If $m|\mathrm{ord}_g(u)$, then u is counted neither on the left nor on the right hand side. If $m\nmid \mathrm{ord}_g(u)$, we can assume w.l.o.g. that ${p_j}^{e_j}\nmid \mathrm{ord}_g(u)$ for $1\le j\le k$ and that $p_s^{e_s}|\mathrm{ord}_g(u)$ for $s>k$. By definition u is counted with multiplicity one on the left hand side. The contribution of u to the right hand side is

$$-\sum_{\substack{d\#{p_1}^{e_1}\cdots {p_k}^{e_k}\\ d>1}}\mu(\kappa(d))=-\sum_{\substack{d|p_1\cdots p_k\\ d>1}}\mu(d)=\mu(1)=1,$$

where we used the well-known identity $\sum_{d|n}\mu(d)=0$, which holds for every integer $n>1$. □

`Example`. We have $N(x;2,12)=N_{12}(x)=N_3(x)+N_4(x)-N'(x;2,12)$.

Put $\delta_g'(d)=\sum_{j\#m}\mu(\kappa(j))\delta_g(j)$.

Lemma 4 *We have*
1) *We have* $P'(x;g,d)=\delta_g'(d)\mathrm{Li}(x)+O\left(\frac{x}{\log^3 x}(\log\log x)^{\omega(d)+3}\right)$.
2) *Under GRH we have* $P'(x;g,d)=\delta_g'(d)\mathrm{Li}(x)+O(\sqrt{x}\log^{\omega(d)+1}x)$.

Proof. By inclusion and exclusion (or an argument as in the proof of Lemma 3) we see that $P'(x;g,d)=\sum_{j\#d}\mu(\kappa(j))P_g(j)(x)$. Then use Theorem 2. □

`Remark`. Wiertelak [9] studied $P'(x;g,d)$ in depth in case d is squarefree. Note (as did Wiertelak) that if d is squarefree, then $P'(x;g,d)$ counts the number of primes $p\le x$ with $\nu_p(g)=0$ such that the congruence $g^{dy}\equiv g(\mathrm{mod}\ p)$ has a solution y. In general $P'(x;g,d)$ counts the number of primes $p\le x$ with $\nu_p(g)=0$

such that the congruence $g^{dy} \equiv g^r (\text{mod } p)$ has a solution (r, y) with r dividing $d/\kappa(d)$.

The following result gives some insight in the properties of $\delta'_g(d)$.

Proposition 3 *Suppose that $d \geq 1$ and $d_1 > 1$ are natural numbers.*
1) *We have $\delta_g(dd_1) < \delta_g(d)$. If $g > 0$, then we have $\delta_g(dd_1) \leq \frac{5}{6}\delta_g(d)$.*
2) *We have*

$$\sup\{\frac{\delta_g(dd_1)}{\delta_g(d)}|d_1 > 1\} = 1 \text{ and } \sup\{\frac{\delta_g(dd_1)}{\delta_g(d)}|g > 0,\ d_1 > 1\} = \frac{5}{6}.$$

3) *We have $\delta'_g(p_1^{e_1}p_2^{e_2}) < \delta'_g(p_1^{e_1})$, with p_1 and p_2 primes.*
4) *We have $\delta'_g(p_1^{e_1}\cdots p_r^{e_r}) = (1-\delta_g(p_1^{e_1}))\cdots(1-\delta_g(p_r^{e_r}))$, with $p_1,\ldots,p_r$ distinct odd prime numbers.*
5) *We have* $\min\{1-\delta'_g(j)|j\#d,\ d > 1\} = \gamma_g(d)$.

Proof. 1) If $g > 0$, then one checks that $\epsilon'_1(dd_1) \leq \frac{5}{4}\epsilon'_1(d)$ and from this one easily infers that $\delta_g(dd_1) \leq \frac{5}{6}\delta_g(d)$. The general case requires some case distinctions and is left to the interested reader.
2) We have, e.g., $\lim_{e\to\infty} \delta_{-5^{2^e}}(6)/\delta_{-5^{2^e}}(3) = 1$ and $\delta_3(6) = 5\delta_3(3)/6$. Now invoke part 1.
3) On invoking part 1 we find that $\delta'_g(p_1^{e_1}p_2^{e_2}) - \delta'_g(p_1^{e_1}) = \delta_g(p_1^{e_1}p_2^{e_2}) - \delta_g(p_2^{e_2}) < 0$.
4) Considered as a function of d, $\delta_g(d)$ is a multiplicative function on the odd integers by Theorem 3. From this and the expression of δ'_g in terms of δ_g, the result then follows.
5) On noting that $\delta'_g(dd_1) \leq \delta'_g(d)$ and using part 3 we see that

$$\min\{1-\delta'_g(j)|j\#d,\ j > 1\} = \min\{1-\delta'_g(p_i^{e_i})|1 \leq j \leq r\} = \gamma_g(d),$$

where we used that $1 - \delta'_g(p_i^{e_i}) = \delta_g(p_i^{e_i})$. □

Next we will compute $N'(x; g, d)$ from $P'(x; g, d)$. To this end we will make use of the fact that the integers counted by $N'(x; g, d)$ as $x \to \infty$ can be related to completely multiplicative sets. Recall that a set S of natural numbers is said to be *completely multiplicative* if its characteristic function χ is completely multiplicative, that is satisfies $\chi(xy) = \chi(x)\chi(y)$ for all natural numbers x and y. Thus S is completely multiplicative when $x \cdot y \in S$ iff $x \in S$ and $y \in S$. The following result is a simple generalization of Lemma 1 of Müller [7] and easily follows from the observation that $\text{ord}_g(u_1u_2)|\gcd(u_1,u_2)\text{lcm}(\text{ord}_g(u_1),\text{ord}_g(u_2))$, cf. [7].

Lemma 5 *Let $m = {p_1}^{e_1}\cdots{p_r}^{e_r}$. The set of integers u from $S(g)$ such that $gcd(u,m) = 1$ and $p_j^{e_j} \nmid \text{ord}_g(u)$ for $1 \leq j \leq r$ is a completely multiplicative set.*

Let $N''(x; g, m)$ denote the number of integers $u \leq x$ from $S(g)$ such that $\gcd(u, m) = 1$ and $p_j^{e_j} \nmid \text{ord}_g(u)$ for $1 \leq j \leq r$. The integers thus counted (as $x \to \infty$) form a completely multiplicative set by Lemma 5 and can be counted using the following proposition.

Proposition 4 1) *Let S be a completely multiplicative set of natural numbers such that for $x \to \infty$ we have*

$$\sum_{\substack{p \le x \\ p \in S}} 1 = \tau \mathrm{Li}(x) + O\left(\frac{x(\log\log x)^\gamma}{\log^3 x}\right) \tag{7}$$

holds, where $\tau > 0$ and $\gamma \ge 0$, with τ real and γ an integer. Then we have for $x \to \infty$ that

$$S(x) := \sum_{\substack{n \le x \\ n \in S}} 1 = c_S x \log^{\tau-1} x + O(x(\log\log x)^{\gamma+1} \log^{\tau-2} x),$$

where c_S denotes a positive constant which only depends on the set S.
2) *If* (7) *holds with error term $O(x \log^{-2-\gamma_1} x)$ for some $\gamma_1 > 0$, then*

$$S(x) = x \sum_{0 \le \nu < \gamma_1} b_\nu \log^{\tau-1-\nu} x + O(x \log^{\tau-1-\gamma_1+\epsilon} x),$$

where $b_0 (= c_S), b_1, \ldots$ are constants.

Proof. The first part is proved in Moree [2]. The second part is a special case of Theorem 6 of [5]. □

Let $m \ge 1$ be fixed. Then, by the latter proposition and Lemmas 4 and 5,

$$N''(x; g, m) = c'_m(g) \frac{x}{\log^{1-\delta'_g(m)} x}\left(1 + O\left(\frac{(\log\log x)^{\omega(m)+4}}{\log x}\right)\right), \tag{8}$$

where $c'_m(g)$ is a positive constant.

As in [7] we conclude that there exists a finite set of numbers (actually prime powers) $n_1, \ldots, n_s$ (depending on g and m) such that

$$N'(x; g, m) = \sum_{j=1}^{s} N''(\frac{x}{n_j}; g, m). \tag{9}$$

It thus follows on invoking the estimates (8) and (9) that

$$N'(x; g, m) = c_m(g) \frac{x}{\log^{1-\delta'_g(m)} x}\left(1 + O\left(\frac{(\log\log x)^{\omega(m)+4}}{\log x}\right)\right). \tag{10}$$

On noting that $N'(x; g, p_j^{e_j}) = N(x; g, p_j^{e_j})$ and that $\delta'_g(p_j^{e_j}) = 1 - \delta_g(p_j^{e_j})$, we see that the estimate (10) generalizes Theorem 4.

Using (10) we can now generalize Proposition 2.

Proposition 5 *Assume that $m = p_1^{e_1} \cdots p_r^{e_r}$ with $\delta_g(p_1^{e_1}) \le \cdots \le \delta_g(p_r^{e_r})$. Then we have $N(x; g, m) \sim \sum_{j=1}^{\min\{r,3\}} N(x; g, p_i^{e_i})$. It follows that in particular we have $N(x; g, m) \sim c x \log^{-\delta_g(p_1^{e_1})} x$ for some $c > 0$ as $x \to \infty$.*

Proof. By Lemma 3, (10) and part 5 of Proposition 3, we have $N(x;g,m) \sim \sum_{j=1}^{r} N(x;g,p_i^{e_i})$. Since by Theorem 5 we cannot have that $\delta_g(p_1^{e_1}) = \delta_g(p_2^{e_2}) = \delta_g(p_3^{e_3}) = \delta_g(p_4^{e_4})$, the result follows on invoking (10) again. □

The main result of this paper makes the latter result more precise:

Theorem 6 *Let* $\{1-\delta_g'(j) \mid j\#m,\ j>1\} = \{\delta_1,\ldots,\delta_s\}$ *with* $\delta_1 < \delta_2 < \cdots < \delta_s$.
1) *Then* $\delta_1 = \gamma_g(m)$ *and*

$$N(x;g,m) = \sum_{j=1}^{s} c_j \frac{x}{\log^{\delta_j} x} + O\left(\frac{x(\log\log x)^5}{\log^{1+\gamma_g(m)} x}\right),$$

where the leading (asymptotically dominating) term is the one with $j=1$ *and* $c_1,\ldots,c_s$ *are constants with* $c_1 > 0$.
2) *Under GRH it is true that for each integer* $t \geq 0$ *we have*

$$N(x;g,m) = \sum_{j=1}^{s}\sum_{k=0}^{t} c_{j,k} \frac{x}{\log^{k+\delta_j} x} + O(\frac{x}{\log^{t+1} x}).$$

The constants c_j *and* $c_{j,k}$ *will depend on* g *and* m *in general and so do the implied constants in the error terms.*

Proof. 1) Follows on combining Lemma 3, (10) and part 5 of Proposition 3.
2) The proof is similar to that of part 1, except that instead of part 1 of Lemma 4 we use part 2 and that instead of part 1 of Proposition 4 we use part 2. □

`Acknowledgement`. The author thanks Yuri Bilu and Jan-Hendrik Evertse for their assistance in solving the Diophantine equation (4). The proof given is a compilation of their arguments. Moreover, he thanks Igor Shparlinski for pointing out the existence of [7] to him.

References

[1] Z. Franco and C. Pomerance, On a conjecture of Crandall concerning the $qx+1$ problem, *Math. Comp.* **64** (1995), 1333-1336.

[2] P. Moree, On the divisors of $a^k + b^k$, *Acta Arith.* **80** (1997), 197–212.

[3] P. Moree, Improvement of an estimate of H. Müller involving the order of 2(mod u), *Arch. Math.* **71** (1998), 197–200.

[4] P. Moree, On primes p for which d divides $\mathrm{ord}_p(g)$, *Funct. Approx. Comment. Math.* **33** (2005), 85–95.

[5] P. Moree and J. Cazaran, On a claim of Ramanujan in his first letter to Hardy, *Expo. Math.* **17** (1999), 289–312.

[6] H. Müller, Eine Bemerkung über die Ordnungen von 2(mod U) bei ungeradem U, *Arch. Math.* **69** (1997), 217–220.

[7] H. Müller, On the distribution of the orders of 2(mod u) for odd u, *Arch. Math.* **84** (2005), 412–420.

[8] F. Pappalardi, Square free values of the order function, *New York J. Math.* **9** (2003), 331–344.

[9] K. Wiertelak, On the density of some sets of primes. IV, *Acta Arith.* **43** (1984), 177–190.

Max-Planck-Institut für Mathematik
Vivatsgasse 7
D-53111 Bonn
Deutschland
E-mail: moree@mpim-bonn.mpg.de