Rend. Sem. Mat. Univ. Padova, Vol. 129 (2013)
DOI 10.4171/RSMUP/129-2

Perfect Numbers and Finite Groups

Tom De Medts (*) - Attila Maróti (**)

Abstract - A number is perfect if it is the sum of its proper divisors. We extend this notion to finite groups by calling a finite group a Leinster group if its order is equal to the sum of the orders of all proper normal subgroups of the group. We provide some general theory, we present examples of Leinster groups, and we prove some related results.

Mathematics Subject Classification (2010). 20D60.

Keywords. Perfect number, finite group.

1. Introduction

A number is perfect if it is the sum of its proper[1] divisors (e.g. 6 and 28 are perfect numbers). Perfect numbers are an ancient object of study. Euclid proved that the numbers $2^{t-1}(2^t-1)$ are perfect where t is a positive integer and 2^t-1 is a Mersenne prime. Euler showed the converse of this statement, namely that every even perfect number has the form $2^{t-1}(2^t-1)$ where 2^t-1 is a Mersenne prime. It is not known whether there are infinitely many Mersenne primes; neither is it known whether there exist odd perfect numbers.

(*) Indirizzo dell'A.: Department of Mathematics, Ghent University, Krijgslaan 281 – S22, 9000 Ghent, Belgium.

E-mail: tdemedts@java.ugent.be

(**) Indirizzo dell'A.: Alfréd Rényi Institute of Mathematics, Reáltanoda utca 13-15, H-1053, Budapest, Hungary.

E-mail: maroti.attila@renyi.mta.hu

The research of the second author was supported by a Marie Curie International Reintegration Grant within the 7th European Community Framework Programme, by the János Bolyai Research Scholarship of the Hungarian Academy of Sciences, and by OTKA K84233.

([1]) As usual, a divisor of a number n is called proper if it is not equal to n; in particular, 1 is a proper divisor of every natural number $n > 1$. Similarly, a subgroup is called proper if it is not equal to the whole group; in particular, the trivial subgroup is a proper subgroup of every non-trivial group.

Leinster [5] extended the notion of perfect numbers to finite groups. He called a finite group *perfect* if its order is equal to the sum of the orders of all proper normal subgroups of the group. We will call such a group a *Leinster group* [2] instead, since the term "perfect group" is customary for a group equal to its own derived subgroup. Note that a finite cyclic group is a Leinster group if and only if its order is a perfect number.

The motivation for studying Leinster groups is twofold. First, it is our hope that studying this class of groups is equally interesting as studying the class of perfect numbers, and in particular, the problem whether or not there exist odd perfect numbers has an obvious analogue for Leinster groups. We are aware of only a single odd order Leinster group, and the question whether there are others seems quite challenging.

Second, it seems that expressing that the sum $D(G)$ of the orders of the normal subgroups of a group G is not too large, is an interesting way of saying that G has relatively few normal subgroups, and we can indeed deduce structural properties if $D(G)$ is relatively small; this is precisely what we will do in Section 3.

In Section 4, we will focus on constructing examples. In [5] a method was introduced to generate examples of Leinster groups in the form of direct products where one component is a cyclic group. We will push this method further to find many other examples of this form.

Many of the Leinster groups that we will encounter, are so-called Zassenhaus metacyclic groups (finite groups with the property that all Sylow subgroups are cyclic). In Section 5 we perform a thorough investigation of Zassenhaus metacyclic groups, and in particular we combine our theoretical results with the cyclic extension method of Section 4 to obtain many more examples of Leinster groups which are Zassenhaus metacyclic.

Our hope was to find infinite families of Leinster groups, but so far we have only been able to find about 400 examples (not including the 48 cyclic examples that correspond to the 48 known perfect numbers).

A related, but slightly less natural problem (especially in view of Proposition 4.2 below) is obtained by replacing "normal subgroups" by "subgroups" or by "cyclic subgroups". If the order of a finite group is equal to the sum of the orders of all of its proper subgroups, then the group is cyclic. On the other hand, there are many finite groups the order of which is equal to the sum of the orders of all of its cyclic proper subgroups. We refer to [3] for more details.

([2]) In a recent discussion on Mathoverflow [6], Tom Leinster called these groups *immaculate groups*.

2. Perfect numbers and certain Leinster groups

DEFINITION 2.1. (i) If n is a positive integer, we let $D(n)$ be the sum of all (positive) divisors of n, and we define $\delta(n) := D(n)/n$.

(ii) If G is a finite group, we let $D(G)$ be the sum of the orders of all normal subgroups of G, and we define $\delta(G) := D(G)/|G|$.

(iii) A positive integer n is *perfect* precisely when $\delta(n) = 2$. If $\delta(n) > 2$, it is called *abundant*, and if $\delta(n) < 2$, it is called *deficient*. The value $\delta(n)$ is sometimes called the *abundancy index* of n.

(iv) Similarly, a finite group G is a *Leinster group* if and only if $\delta(G) = 2$. We will also occasionally talk about abundant groups and deficient groups, when $\delta(G) > 2$ or $\delta(G) < 2$, respectively.

As a first example, let n be an odd positive integer and t a positive integer, and let $M_{n,t}$ be the group

$$\langle x, y \mid x^n = y^{2^t} = 1, y^{-1}xy = x^{-1} \rangle = C_n : C_{2^t}.$$

The following proposition shows that the description of all pairs (n, t) for which $M_{n,t}$ is a Leinster group is equivalent to the problem of classifying all perfect numbers.

PROPOSITION 2.2. *The group $M_{n,t}$ is a Leinster group if and only if $t = 1$ and n is an odd perfect number, or $n = 2^t - 1$ is a Mersenne prime.*

PROOF. The center of $M_{n,t}$ is cyclic of order 2^{t-1}. From this it is easy to see that

$$D(M_{n,t}) = 2^t n + (1 + 2 + \ldots + 2^{t-1})D(n) = 2^t n + (2^t - 1)D(n).$$

Now $D(M_{n,t}) = 2^{t+1}n$ if and only if $(2^t - 1)D(n) = 2^t n$, and this is equivalent to $(2^t - 1)(D(n) - n) = n$. If $t = 1$ this occurs if and only if n is an odd perfect number. So assume that $t > 1$. Now $D(n) - n$ is a proper divisor of n. But $D(n) - n$ is the sum of all proper divisors of n. Thus $D(n) - n$ is the unique proper divisor of n, which means that n is prime and equal to $2^t - 1$. □

Note that in the proof above we used an idea of Leinster [5, Section 1.2]; the groups $M_{n,1}$ are precisely the dihedral groups.

If n is the largest known perfect number then $n = 2^{t-1}(2^t - 1)$ where $2^t - 1$ is the largest known Mersenne prime. In this case, the group $M_{n,t}$ has order precisely equal to $2n$.

In Section 5 below, we will see that these groups belong to the larger class of so-called Zassenhaus metacyclic groups. More precisely, the group

$M_{n,t}$ is $\mathsf{ZM}(n, 2^t, -1)$ in the notation of Section 5, and Theorem 5.7 implies Proposition 2.2.

3. Restrictions on $\delta(G)$

The goal of this section is to perform a theoretical study of the invariants $D(G)$ and $\delta(G)$ before we try to construct more examples.

Let us start by making three observations about the invariant $\delta(G)$.

OBSERVATION 3.1. (i) *For any finite group $G \neq 1$ we have $\delta(G) > 1$.*

(ii) *For any normal subgroup N of any finite group G we have $\delta(G/N) \leq \delta(G)$.*

(iii) *The function δ is multiplicative in the sense that whenever $G = G_1 \times G_2$ with $\gcd(|G_1|, |G_2|) = 1$, then $\delta(G) = \delta(G_1)\delta(G_2)$.*

Note that a stronger version of Observation 3.1(iii) holds; see Proposition 4.2 below.

The following proposition and its Corollary 3.3 below turn out to be very useful.

PROPOSITION 3.2. *If G is a finite nilpotent group with $\delta(G) \leq 2$ then G is cyclic and $|G|$ is a perfect or a deficient number.*

PROOF. Let G be a finite nilpotent group with $\delta(G) \leq 2$ and let P be an arbitrary Sylow p-subgroup of G for some prime divisor p of $|G|$; in particular P is a direct factor of G. By Observation 3.1(i and iii), or alternatively by Observation 3.1(ii), it follows that $\delta(P) \leq 2$.

Now let F denote the Frattini subgroup of P; then P/F is an elementary abelian p-group whose rank, say r, is the minimal number of generators of P. By Observation 3.1(ii), we have $\delta(P/F) \leq 2$. On the other hand, if $r > 1$, then $1 + (p+1)/p \leq \delta(P/F)$ since P/F contains at least $p + 1$ subgroups of order p^{r-1}. This forces $r = 1$; hence P is cyclic. Then every Sylow subgroup of G is cyclic. Since G is nilpotent, this implies that G itself must be cyclic. Therefore $\delta(G) = \delta(|G|)$, and we conclude that $|G|$ must be a perfect or a deficient number. □

The example $\delta(C_p \times C_p) = 2 + 1/p + 1/p^2$ shows that $\delta(G)$ can be arbitrarily close to 2 for a non-cyclic finite nilpotent group G.

An immediate corollary to Proposition 3.2 is the following.

COROLLARY 3.3. *Every nilpotent quotient of a Leinster group is cyclic.*

We now proceed to show that for certain classes of groups, the additional information that $\delta(G)$ is relatively small forces the group to be of a very specific type.

PROPOSITION 3.4. *Let G be a supersolvable group with $\delta(G) \leq 1 + |G|^{-1/3}$. Then $G \cong C_p$, C_{pq}, or $C_p : C_q$ for some not necessarily distinct primes p and q.*

PROOF. First we show that every minimal normal subgroup N of a finite supersolvable group G is cyclic. For a proof let $G = N_1 > \ldots > N_k = 1$ be a series of normal subgroups of G such that every factor group is cyclic. Then there exists an index i such that $N_i \geq N$ and $N_{i+1} \cap N = 1$. Then $N_i/N_{i+1} \geq NN_{i+1}/N_{i+1} \cong N/(N_{i+1} \cap N) \cong N$. Hence N is cyclic.

Let G be a minimal counterexample to the statement of the theorem and let N be a minimal normal subgroup of G. By Proposition 3.2 we know that G cannot be nilpotent. Then $|N| = r$ for some prime r. Clearly, G/N is isomorphic to C_p, C_{pq}, or $C_p : C_q$ for some primes p and q.

First suppose that $G/N \cong C_p$. If $r = p$ then $G = C_{p^2}$ or $C_p \times C_p$. This is a contradiction since G cannot be nilpotent. If $r \neq p$ then $G = C_r : C_p$, a contradiction.

Now let $G/N \cong C_{pq}$. By our assumption on $\delta(G)$, the prime r must be less than both p and q. Then N is central in G and so G is abelian; a contradiction.

Finally let $G/N \cong C_p : C_q \neq C_{pq}$ with $p \neq q$. Then $p > q$. By our assumption on $\delta(G)$, the prime r must be less than q (and also p). Then N is central in G and $G \cong C_r \times (C_p : C_q)$. But then the subgroup $C_p : C_q$ is normal in G of order larger than $|G|^{2/3}$. This is also a contradiction. This proves the theorem. □

REMARK 3.5. (i) The bound in the previous theorem is sharp. For let both $(p-1)/2$ and p be primes (Sophie Germain primes). Then for the supersolvable Frobenius group $G = (C_p \times C_p) : C_{(p-1)/2}$ the invariant $\delta(G)$ is only slightly bigger than $1 + |G|^{-1/3}$.

(ii) The word "supersolvable" cannot be replaced by "solvable" in the above theorem. For let $p = 2^t - 1$ be a Mersenne prime, let V be a t-dimensional vector space over the field with 2 elements, let H be a Singer cycle acting on V, and let G be the primitive permutation group $V \times H$. Then $\delta(G) < 1 + |G|^{-1/3}$.

Now we impose an even stronger restriction on $\delta(G)$ for solvable groups G to conclude that the group is cyclic.

PROPOSITION 3.6. *If G is a non-trivial solvable group with $\delta(G) \leq 1 + |G|^{-1/2}$ then G is simple (and hence cyclic of prime order).*

PROOF. Let G be a minimal counterexample and let N be a minimal normal subgroup of G of order p^n where p is a prime. Then the factor group G/N is simple, isomorphic to C_r where r is a prime. If $r = p$ then G is a cyclic group of order $p^{n+1} = p^2$, by Proposition 3.2, and as such $\delta(G) = 1 + |G|^{-1/2} + |G|^{-1}$, a contradiction. So $r \neq p$, and N has a complement C_r in G. If $C_r \lhd G$ then $n = 1$ and G is cyclic of order pr. Hence $\delta(G) = 1 + (1/r) + (1/p) + (1/pr) > 1 + (1/\sqrt{pr})$, a contradiction. Finally, if C_r is not normal in G then $G = N \rtimes C_r$ and C_r acts faithfully and irreducibly on N. Hence $r \leq |N| - 1$ and $\delta(G) = 1 + (1/r) + (1/|G|) > 1 + |G|^{-1/2}$, a contradiction. □

REMARK 3.7. The word "solvable" cannot be omitted from the statement of Proposition 3.6, as is illustrated by the affine special linear group $\mathsf{ASL}(n, p)$, or by the wreath product $S \wr A_n$ where S is some non-abelian finite simple group.

We now present a classification result of a certain class of Leinster groups, namely those of order $p^t q$ for p, q prime.

PROPOSITION 3.8. *Let G be a group of order $p^t q$ where p and q are primes and t is a positive integer. Then G is a Leinster group if and only if $p = 2$ and one of the following occurs:*

(1) *$q = 2^{t+1} - 1$ is a Mersenne prime and G is cyclic;*
(2) *$q = 2^t - 1$ is a Mersenne prime and $G \cong M_{q,t}$.*

PROOF. The "if"-part is clear by Euclid's result and Proposition 2.2.

Conversely, suppose that G is a Leinster group of order $p^t q$ where p and q are primes and t is a positive integer. Notice that $p \neq q$ because otherwise $D(G)$ would be congruent to 1 modulo p. A similar observation yields that $O_q(G) \neq 1$ and $O_p(G) \neq 1$. Hence $|O_q(G)| = q$ and $|O_p(G)| = p^k$ for some positive integer k at most t. Let $N = O_q(G)$ and let H be a Sylow p-subgroup of G. Then $G = N \rtimes H$. By Corollary 3.3, the group H is cyclic.

We claim that p and q cannot be both odd. For if $p \geq 3$ and $q \geq 3$ then we have

$$\delta(G) \leq \frac{p^{t+1}-1}{p^t(p-1)} \cdot \frac{q+1}{q} < \frac{p}{p-1} \cdot \frac{q+1}{q} \leq 2,$$

which is a contradiction.

Let $q = 2$. Then H is a cyclic subgroup of index 2 in G hence normal in G and so $G = H \times N$ is cyclic. In this case $|G|$ is even but not divisible by 4. By Euler's theorem, this implies that $|G| = 6$ and case (1) occurs.

We can assume that $q \geq 3$. Then $p = 2$. In this case

$$\begin{aligned} 2^{t+1}q = D(G) = (1+2+\cdots+2^k)(1+q) + (2^{k+1}+\cdots+2^t)q \\ = (2^{t+1}-1)q + (2^{k+1}-1), \end{aligned}$$

which implies that $q = 2^{k+1} - 1$.

If $k = t$ then G is cyclic, $|G|$ is an even perfect number, and hence, by Euler's result, case (1) occurs.

We can assume that $k < t$. Now the cyclic group $H/O_2(G)$ of order 2^{t-k} can be considered as a subgroup of $\mathrm{Aut}(N)$ which has order $q - 1 = 2^{k+1} - 2$. Hence 2^{t-k} must divide $2^{k+1} - 2$ which can only occur if $t = k + 1$. Since $\mathrm{Aut}(N)$ has exactly one element of order 2, namely the element which inverts a generator of N, we see that $G \cong M_{q,t}$. We conclude that case (2) occurs. □

4. Cyclic extension method

The functions D and δ are multiplicative in the integers in the sense that whenever n and m are coprime integers we have $D(nm) = D(n)D(m)$ and $\delta(nm) = \delta(n)\delta(m)$. The functions D and δ that we have introduced for groups, are also multiplicative, even in a broader sense.

DEFINITION 4.1. Let G, H be finite groups. Following Leinster [5], we say that G and H are *coprime* if they have no common composition factor. In particular, if G and H are finite groups with coprime orders, then they are coprime.

PROPOSITION 4.2 ([5]). *Let G, H be coprime finite groups. Then*

$$D(G \times H) = D(G)D(H) \quad \textit{and} \quad \delta(G \times H) = \delta(G)\delta(H).$$

Using this result, three Leinster groups were constructed in [5], namely $S_3 \times C_5$, $A_5 \times C_{15128}$, and $A_6 \times C_{366776}$.

In this section we take this method further by finding more Leinster groups of this type. The idea is the following. For each group G, we try to find a cyclic group C, coprime to G, such that $G \times C$ is a Leinster group. In order to achieve this, we compute $\delta(G)$ and we keep track of the list of prime divisors of the cyclic composition factors of G; we call this list A. Our goal is to find a positive integer n not divisible by any of the primes in A, such that $\delta(n) = 2/\delta(G)$; it will then follow from Proposition 4.2 that the group $G \times C_n$ is a Leinster group. This reduces the problem to the following purely number theoretical question.

QUESTION 4.3. *Given $q \in \mathbb{Q}$ and a list $A = \{p_1, \dots, p_k\}$ of primes, try to find a positive integer n such that $\delta(n) = q$, and such that $p_i \nmid n$ for all $i \in \{1, \dots, k\}$.*

Even if $A = \emptyset$, this question is known to be extremely hard, and it is related to very fundamental open questions about perfect numbers. For instance, the question whether there exists a positive integer n with $\delta(n) = 5/3$ is known to be equivalent to the existence of odd perfect numbers [1]. We also mention that there is an ongoing effort to try to determine for as many rationals q as possible whether they are contained in the image of δ; see, for example, [8].

We have implemented a relatively straightforward backtracking algorithm for Question 4.3, the details of which we have diverted to Appendix A.

We have applied our algorithm on a few specific cases:

- dihedral groups of order $2n$ with n odd, up to order 10^{10} (100 examples), for instance

$$D_{9798637554} \times C_{204150168209} = D_{2\cdot 3^4\cdot 19\cdot 37\cdot 97\cdot 887} \times C_{13^2\cdot 61^2\cdot 324641};$$

- a list of 950 simple groups, including the 26 sporadic groups (15 examples), for instance

$$\mathsf{M}_{22} \times C_{55009909630} = \mathsf{M}_{22} \times C_{2\cdot 5\cdot 13\cdot 79\cdot 109\cdot 157\cdot 313};$$

- all groups of order ≤ 2015, only excluding order 1536 (for which there are 408 641 062 different groups) (192 examples). Note that we can omit groups of prime power order, since every nilpotent quotient of a Leinster group has to be cyclic by Corollary 3.3.

The interested reader can find the complete lists of these examples on our webpage [9].

In Section 5, we will use the cyclic extension method to find even more examples, but only after we have developed some theoretical results about the normal subgroup structure of Zassenhaus metacyclic groups.

REMARK 4.4. The Leinster groups of the form $D_{2n} \times C_m$ that we found, all have the peculiar property that n contains a lot of small prime factors, whereas m is usually prime or a small square times a prime. We do not know how to make this observation more formally explicit, nor do we have an explanation for this behaviour.

Notice that up to now, only one Leinster group of odd order is known, namely the group

$$G = (C_{127} \rtimes C_7) \times C_{3^4 \cdot 11^2 \cdot 19^2 \cdot 113} \tag{4.1}$$

of order 355 433 039 577. The existence of odd order Leinster groups was stated as an open question by Tom Leinster on MathOverflow, and the example above was first discovered by François Brunault only one day after the question was asked [6].

5. Zassenhaus metacyclic groups

Many of the Leinster groups that we found so far, are Zassenhaus metacyclic groups (or ZM-groups for short), i.e. groups with the property that all Sylow subgroups are cyclic; in particular such a group is metacyclic. The goal of this section is to investigate the normal subgroup structure of these groups, and to use our results in order to find more examples of Leinster groups.

The structure of these groups has been completely determined by Zassenhaus.

DEFINITION 5.1. A triple (m, n, r) satisfying the conditions

$$\gcd(m, n) = \gcd(m, r - 1) = 1 \quad \text{and} \quad r^n \equiv 1 (\mathrm{mod}\, m)$$

will be called a *ZM-triple*, and the corresponding group

$$\langle a, b \mid a^m = b^n = 1, b^{-1}ab = a^r \rangle$$

will be denoted by $\mathsf{ZM}(m, n, r)$.

REMARK 5.2. If (m, n, r) is a ZM-triple, then m is necessarily odd. Indeed, if m were even, then the relation $r^n \equiv 1 \pmod m$ would force r to be odd, contradicting $\gcd(m, r - 1) = 1$.

THEOREM 5.3 (Zassenhaus). *Let G be a ZM-group. Then there exists a ZM-triple (m,n,r) such that $G \cong \mathsf{ZM}(m,n,r)$. We have $|G| = mn$ and $G' = \langle a \rangle$ (so $|G'| = m$), and G/G' is cyclic of order n.*

Conversely, every group isomorphic to $\mathsf{ZM}(m,n,r)$ is a ZM-group.

PROOF. See, for example, [4, IV, Satz 2.11]. □

LEMMA 5.4. *Let* $G = \mathsf{ZM}(m,n,r) = \langle a, b \mid a^m = b^n = 1, b^{-1}ab = a^r \rangle$. *Then*

$$(b^s a^t)^d = b^{sd}\, a^{t\left(1+r^s+r^{2s}+\ldots+r^{(d-1)s}\right)},$$

for all natural numbers s, t, d.

PROOF. This is an easy computation, using induction on d. □

COROLLARY 5.5. *Let* $G = \mathsf{ZM}(m,n,r) = \langle a, b \mid a^m = b^n = 1, b^{-1}ab = a^r \rangle$. *Then*

$$(a^{-1}ba)^d = b^d a^{1-r^d},$$

for every natural number d.

PROOF. For $d = 1$, this follows from the defining relation $b^{-1}ab = a^r$. For $d > 1$, the result then follows from Lemma 5.4 with $s = 1$ and $t = 1 - r$. □

THEOREM 5.6. *Let* $G = \mathsf{ZM}(m,n,r) = \langle a, b \mid a^m = b^n = 1, b^{-1}ab = a^r \rangle$. *For every divisor d of n, we write*

$$e(d) := \gcd(r^d - 1, m).$$

Then for every divisor d of n and every divisor k of $e(d)$, the group

$$N_{k,d} := \langle a^k, b^d \rangle$$

is a normal subgroup of G. Conversely, every normal subgroup N of G is of the form $N = N_{k,d}$ for some divisor d of n and some divisor k of $e(d)$. The group $N_{k,d}$ has order mn/kd.

PROOF. Let d be a divisor of n, and let k be a divisor of $e(d) = \gcd(r^d - 1, m)$. The group $N_{k,d} := \langle a^k, b^d \rangle$ is normalized by b because

already a is normalized by b. On the other hand, $a^{-1}b^d a = b^d a^{1-r^d} = b^d (a^{-1})^{e(d)}$ by Corollary 5.5; and since $k \mid e(d)$, this element is again contained in $N_{k,d}$. Hence $N_{k,d}$ is also normalized by a, and we conclude that $N_{k,d}$ is a normal subgroup of G.

Conversely, let N be an arbitrary normal subgroup of G. We first claim that N is necessarily of the form $N = \langle a^k, b^d \rangle$ for certain natural numbers k and d dividing m and n respectively. Indeed, let $g = b^s a^t$ be an arbitrary element of N. Then $[g, b] = g^{-1}b^{-1}gb = a^{t(r-1)}$, and hence $a^{t(r-1)} \in N$. Since $\gcd(r-1, m) = 1$, it follows that $a^t \in N$ as well, and then also $b^s \in N$. This proves our claim.

Observe that it follows from Lemma 5.4 that k is the smallest positive integer such that $a^k \in N$, and similarly d is the smallest positive integer such that $b^d \in N$.

It remains to show that $k \mid e(d)$. Since $b^d \in N$, Corollary 5.5 shows again that $a^{e(d)} \in N$. Since k is the smallest positive integer such that $a^k \in N$, this implies that $k \mid e(d)$. We conclude that $N = N_{k,d}$ for some divisor d of n and some divisor k of $e(d)$.

Finally, we show that the order of $N_{k,d}$ is mn/kd. Indeed, we have already observed that every element $g \in N_{k,d}$ can be written as $g = b^s a^t$ where s is a multiple of d and t is a multiple of k; we conclude that there are precisely $(n/d)(m/k)$ such elements. □

We now have a complete understanding of the normal subgroups of a ZM-group, and this allows us to compute $D(G)$ for any ZM-group G.

THEOREM 5.7. *Let $G = \mathsf{ZM}(m, n, r)$ be an arbitrary Zassenhaus metacyclic group. Then*

$$\delta(G) = \sum_{d \mid n} \frac{\delta(e(d))}{d} = \sum_{d \mid n} \frac{\delta\big(\gcd(r^d - 1, m)\big)}{d} .$$

PROOF. We simply add up the orders of all normal subgroups. By Theorem 5.6, every divisor d of n gives rise to normal subgroups $N_{k,d}$ for each divisor k of $e(d)$, and

$$\sum_{k \mid e(d)} N_{k,d} = \sum_{k \mid e(d)} \frac{mn}{kd} = \frac{mn}{d} \cdot \frac{D(e(d))}{e(d)} .$$

Summing over all divisors d of n, and observing that $|G| = mn$, we obtain the required formula. □

Notice that if $d = 1$, then $e(d) = \gcd(r-1, m) = 1$, and if $d = n$, then $e(d) = \gcd(r^n - 1, m) = m$. As a corollary, we get a very simple formula for the case where n is a prime.

COROLLARY 5.8. *Let $G = \mathsf{ZM}(m, p, r)$ be a Zassenhaus metacyclic group where p is a prime. Then*

$$D(G) = |G| + D(m) \quad \textit{and hence} \quad \delta(G) = 1 + \frac{\delta(m)}{p}\,.$$

PROOF. This follows immediately from Theorem 5.7 and the previous observation. □

The case where m is prime also gives rise to a simpler formula.

COROLLARY 5.9. *Let $G = \mathsf{ZM}(p, n, r)$ be a Zassenhaus metacyclic group where p is a prime, and let α be the order of r modulo p. Then $1 < \alpha \mid \gcd(n, p-1)$, and*

$$D(G) = pD(n) + D(n/\alpha) \quad \textit{and hence} \quad \delta(G) = \delta(n) + \frac{\delta(n/\alpha)}{p\alpha}\,.$$

PROOF. The fact that (p, n, r) is a ZM-triple implies that $p \nmid r - 1$ while $p \mid r^n - 1$; hence $1 < \alpha \mid n$. Observe that $\delta(e(d)) = 1 + 1/p$ or $\delta(e(d)) = 1$ depending on whether $p \mid r^d - 1$ or $p \nmid r^d - 1$, or equivalently, whether $\alpha \mid d$ or $\alpha \nmid d$. It thus follows from Theorem 5.7 that

$$\begin{aligned}
\delta(G) &= \sum_{d \mid n} \frac{\delta(e(d))}{d} \\
&= \Big(1 + \frac{1}{p}\Big) \sum_{d \mid n, \alpha \nmid d} \frac{1}{d} + \sum_{d \mid n, \alpha \mid d} \frac{1}{d} \\
&= \sum_{d \mid n} \frac{1}{d} + \frac{1}{p} \sum_{d \mid n, \alpha \mid d} \frac{1}{d} \\
&= \delta(n) + \frac{\delta(n/\alpha)}{p\alpha}.
\end{aligned}$$

The resulting formula for $D(G)$ follows since $|G| = pn$. □

Another interesting case is the case $r = m - 1$.

COROLLARY 5.10. *Let $G = \mathsf{ZM}(m, n, m-1)$, and write $n = 2^t s$ with s odd. Then*

$$\delta(G) = \delta(s) \cdot \left(1 + \delta(m)\left(1 - \frac{1}{2^t}\right)\right).$$

PROOF. Recall that m is always odd. On the other hand, $1 \equiv r^n \equiv (-1)^n \pmod m$, and since m is odd, this can only be true if n is even; hence $t \geq 1$. Next, observe that for every divisor d of n,

$$e(d) = \gcd\big((-1)^d - 1, m\big) = \begin{cases} 1 & \text{if } d \text{ is odd;} \\ m & \text{if } d \text{ is even.} \end{cases}$$

It now follows from Theorem 5.7 that

$$\begin{aligned} \delta(G) &= \sum_{d|n} \frac{\delta(e(d))}{d} \\ &= \sum_{d|n,d \text{ odd}} \frac{1}{d} + \sum_{d|n,d \text{ even}} \frac{1}{d} \cdot \delta(m) \\ &= \sum_{d|s} \frac{1}{d} + \sum_{d|s} \sum_{k=1}^{t} \frac{1}{2^k d} \cdot \delta(m) \\ &= \left(\sum_{d|s} \frac{1}{d}\right)\left(1 + \left(\sum_{k=1}^{t} \frac{1}{2^k}\right) \cdot \delta(m)\right) \\ &= \delta(s) \cdot \left(1 + \delta(m)\left(1 - \frac{1}{2^t}\right)\right). \end{aligned}$$

□

We have used Corollaries 5.8, 5.9 and 5.10 in order to try to find examples of Leinster groups that are Zassenhaus metacyclic. In order to make our search more efficient, we have combined our theoretical results with the "cyclic extension method" that we have introduced in Section 4.

EXAMPLE 5.11. There is little hope to find examples of Leinster groups of the form $\mathsf{ZM}(m, p, r)$ with p prime. Indeed, suppose that $\mathsf{ZM}(m, p, r)$ is a Leinster group; then it follows from Corollary 5.8 that $\delta(m) = p$, i.e. m is a so-called multiperfect number. But m is odd, and the existence of odd multiperfect numbers is still unknown.

EXAMPLE 5.12. We have tried to apply the cyclic extension method on groups of the form $\mathsf{ZM}(m, p, r)$. Note that for $p = 2$, a group of the form

$\mathsf{ZM}(m,p,r)$ is necessarily a dihedral group, and we have already dealt with such groups separately in Section 4. If p is odd, however, we have not found any other example than the odd order Leinster group (4.1). (We have tried all odd values for m up to 10^7, and every prime p dividing the exponent of the group of units modulo m.)

EXAMPLE 5.13. We now use Corollary 5.9 to find Leinster groups by extending groups of the form $G = \mathsf{ZM}(p,n,r)$. Note that it is impossible to extend a group G to a Leinster group (using the cyclic extension method) if $\delta(G) > 2$. Also observe that G has the structure of a semidirect product $C_p \rtimes C_n$ and that $\mathrm{Aut}(C_p) \cong C_{p-1}$; we will therefore restrict to values of n of the form $n = 2^t \cdot d$ with $d \mid p-1$, d odd. (The reason for the factor 2^t is that our cyclic extension method can only find cyclic factors that are coprime to G, and in particular it will never find cyclic factors of even order as soon as n is even.)

It is interesting to observe that given p (and $d \mid p-1$), we can compute an upper bound for t (and hence for n) from the observation that $\delta(G) \leq 2$. Indeed, we claim that

$$t \leq \log_2(pd+1) + v_2(p-1) - 1, \tag{5.1}$$

where $v_2(x)$ is the 2-valuation of x, i.e. the exponent of 2 in the factorization of x. To prove our claim, let $s = v_2(p-1)$, so that $p-1 = 2^s \cdot \ell$ for some odd ℓ, and suppose to the contrary that $t > \log_2(pd+1) + s - 1$. Then $2^{t-s+1} > pd+1$; in particular $t > s$. Let α be the order of r modulo p, as in Corollary 5.9; then $\alpha \mid \gcd(n, p-1)$, hence we can write $\alpha = 2^k c$ with $k \leq s$ and $c \mid d$. It follows that

$$\begin{aligned}
\delta(G) &= \delta(n) + \frac{\delta(n/\alpha)}{p\alpha} \\
&= \delta(2^t) \cdot \delta(d) + \frac{\delta(2^{t-k}) \cdot \delta(d/c)}{2^k pc} \\
&= \frac{(2^{t+1}-1) \cdot \delta(d)}{2^t} + \frac{(2^{t-k+1}-1) \cdot \delta(d/c)}{2^t pc} \\
&> \frac{2^{t+1}-1}{2^t} + \frac{pd \cdot \delta(d/c)}{2^t pc} \geq 2\,,
\end{aligned}$$

contradicting the fact that $\delta(G) \leq 2$. This proves the inequality (5.1). Notice that our bound is sharp, in the sense that equality can hold when $d = 1$ and p is equal to a Mersenne prime $p = 2^t - 1$; in that case, we get precisely the groups $M_{p,t}$ that we found in Section 2. It is also useful to notice that if $d > 1$,

then already the bound arising from $\delta(n) \leq 2$, namely

$$t \leq \log_2\bigl(1 + (\delta(d) - 1)^{-1}\bigr) - 1, \tag{5.2}$$

is often stronger than the bound in (5.1), and taking both bounds (5.1) and (5.2) into account helps to reduce the computation time.

We have implemented our ideas, and we ran the program for all primes less than 5×10^7; we found 51 examples of Zassenhaus metacyclic Leinster groups in this fashion, for instance

$$\mathsf{ZM}(2622511, 2^{20}, \alpha = 2) \times C_{5245021 \cdot 10490041 \cdot 5370900991 \cdot 171868831711 \cdot 343737663421}\,.$$

(Note that we have not computed r explicitly, which explains our slightly different notation involving α.)

Example 5.14. Finally, we have applied our cyclic extension method on groups of the form $\mathsf{ZM}(m, n, -1)$. Surprisingly, all the examples that we found, have n equal to a power of 2, with the only exception of the case $m = 127$ and $n = 7$, resulting again in the only known odd order Leinster group (4.1). We ran the program for all values of m less than 10^8, and we found 125 examples, for instance

$$\mathsf{ZM}(92571007, 2^6, -1) \times C_{5215267} = \mathsf{ZM}(71 \cdot 1021 \cdot 1277, 2^6, -1) \times C_{5215267}\,.$$

(There is, of course, some overlap with our earlier lists.)

Again, the interested reader can consult the complete lists on our webpage [9].

Appendix A. An algorithm for Question 4.3

In this appendix, we provide some details for our implementation of the algorithm that, given $q \in \mathbb{Q}$, tries to find $n \in \mathbb{N}$ such that $\delta(n) = q$, where n is subject to certain conditions, as explained in Question 4.3. Because of this inherent difficulty of the problem, we provide a backtracking algorithm that starts in a systematic way to try to find solutions, but that tracks back as soon as one of several parameters reaches a certain bound.

The basic idea of the algorithm is the following; we will discuss the parameters afterwards. The algorithm takes three input arguments:

- the value for q of which we want to find a preimage for δ,
- a list M of "forbidden prime divisors", and
- a depth parameter d.

We begin our algorithm with $q = a/b$ with $\gcd(a, b) = 1$ and $M = A$. If $b = 1$, then n has to be a multiperfect number; we have simply hard-coded the first few cases in our algorithm.

Assume now that $b > 1$. Observe that $\delta(n)$ can only be equal to $t = a/b$ if n is a multiple of b; moreover, we then have that $\delta(n) \geq \delta(b)$. It follows that if $q = a/b < \delta(b)$, or in other words, if $a < D(b)$, then we can never find a solution to the equation $\delta(n) = q$.

If $a = D(b)$, then of course $n = b$ is a solution to the equation $\delta(n) = t$. We are left with the case $a > D(b)$; since n has to be a multiple of b, we proceed by trying values of the form $n = bc$. The values for c that we try, are of the form $c = b'c'$, where $\gcd(b, c') = 1$, and such that every prime divisor of b' is a prime divisor of b. Then $\delta(n) = \delta(bb')\delta(c')$, and so $\delta(n) = a/b$ if and only if $\delta(c') = ab'/D(bb')$.

For each of the choices for b' that we will consider (the choice of which will be bounded by several of our parameters), we call our algorithm recursively, with

- q replaced by $ab'/D(bb')$,
- M extended with the list of prime divisors of b, and
- depth d increased by one.

We continue this process until we find a solution (because at some point $q = a/b$ is such that $a = D(b)$), or until one of the parameter bounds is exceeded or one of the constraints (namely the divisibility conditions $p_i \nmid n$ and the inequalities $a \geq D(b)$) is no longer fulfilled.

The parameters that we use in order to decide when to track back, are the following; we mention a possible sensible bound between parentheses as an example, but depending on the situation it might be useful to change these bounds:

- the value of the denominator b (10^{30}),
- the number of different prime divisors of the denominator b (9),
- the highest exponent in the factorization of b (7),
- the number of different prime divisors in the list of forbidden primes (12),
- the sum of the exponents in the factorization of b' (5 in depth 0 and 2 in higher depths),
- the maximal recursion depth (10).

We have implemented our ideas in Sage [7], and the interested reader can consult the program code on our webpage [9].

Acknowledgments. We are grateful to Tom Leinster for starting the discussion about these groups on MathOverflow [6]. We thank François Brunault for providing the first example of an odd order Leinster group, and for his simple yet very effective idea of gradually increasing the exponents in our backtracking algorithm for Question 4.3, in a comment to another MathOverflow discussion [2]. Finally, many of our computations were performed on the Stevin Supercomputer Infrastructure of Ghent University, whose support is gratefully acknowledged. All our programs were written in Sage [7].

REFERENCES

[1] C. W. Anderson, *The solution of $\Sigma(n) = \sigma(n)/n = a/b$, $\Phi(n) = \varphi(n)/n = a/b$ and some related considerations*, unpublished manuscript (1974).
[2] T. De Medts, *Recovering n from $\sigma(n)/n$*, MathOverflow, http://mathoverflow.net/questions/56376.
[3] T. De Medts - M. Tărnăuceanu, *Finite groups determined by an inequality of the orders of their subgroups*, Bull. Belg. Math. Soc. Simon Stevin **15**, no. 4 (2008), pp. 699–704.
[4] B. Huppert, *Endliche Gruppen I*, Die Grundlehren der Mathematischen Wissenschaften, Band **134**, Springer-Verlag, Berlin, New York, 1967.
[5] T. Leinster, *Perfect numbers and groups*, arXiv:math/0104012.
[6] T. Leinster, *Is there an odd-order group whose order is the sum of the orders of the proper normal subgroups?*, Math. Overflow, http://mathoverflow.net/questions/54851.
[7] W. A. Stein et. al., *Sage Mathematics Software* (Version 4.6.1), The Sage Development Team, 2011, http://www.sagemath.org.
[8] W. G. Stanton - J. A. Holdener, *Abundancy outlaws of the form $(\sigma(N) + t)/N$*, J. Integer Sequences **10** (2007), Article 09.7.6.
[9] http://java.ugent.be/∼tdemedts/leinster.

Manoscritto pervenuto in redazione il 30 Agosto 2011.