NOTES

Edited by **Jimmie D. Lawson and William Adkins**

Nilpotent Numbers

Jonathan Pakianathan and Krishnan Shankar

Introduction. One of the first things we learn in abstract algebra is the notion of a cyclic group. For every positive integer n, we have $\mathbb{Z}_n$, the group of integers modulo n. When n is prime, a simple application of Lagrange's theorem yields that this is the *only* group of order n. We may ask ourselves: what other positive integers have this property? In this spirit we call a positive integer n a *cyclic number* if every group of order n is cyclic. We define *abelian* and *nilpotent* numbers analogously. Recall that a group is nilpotent if and only if it is the (internal) direct product of its Sylow subgroups; see [**7**, 126].

This is not a new problem; the cyclic case is attributed to Burnside and has appeared in numerous articles, [**9**], [**4**], [**1**], [**2**]. The abelian case appears as a problem in an old edition of Robinson's book in group theory; see also [**6**] and the nilpotent case was also done quite some time ago (see [**5**], [**6**]). In this article we give an arithmetic characterization of the cyclic, abelian, and nilpotent numbers from a single perspective. Throughout this paper $\mathbb{Z}_n$ denotes the cyclic group of order n.

Nilpotent numbers. The smallest non-prime cyclic number is 15. This follows from [**3**, Proposition 6.1, p. 98] where it is shown that for primes p and q, if $p > q$, then pq is a cyclic number if and only if $q \nmid (p-1)$. Motivated by this arithmetic criterion we make the following definition.

Definition. A positive integer $n = p_1^{a_1} \cdots p_t^{a_t}$, p_i distinct primes, is said to have *nilpotent factorization* if and only if $p_i^k \not\equiv 1 \bmod p_j$ for all integers i, j and k with $1 \le k \le a_i$.

Examples of numbers with nilpotent factorization are all powers of prime numbers and pq where $p > q$ are prime and $q \nmid (p-1)$. For example, the number $21 = 3 \cdot 7$ does not have nilpotent factorization since $7 \equiv 1 \bmod 3$. It turns out that this rather strange looking property characterizes nilpotent numbers.

Theorem 1. *A positive integer n is a nilpotent number if and only if it has nilpotent factorization.*

Proof: Suppose $n = p_1^{a_1} \cdots p_t^{a_t}$ is a positive integer without nilpotent factorization. Then there exist i, j, and k with $1 \le k \le a_i$ such that $p_i^k \equiv 1 \bmod p_j$. Note that p_i and p_j are necessarily distinct so after relabelling we may assume $p_1^k \equiv 1 \bmod p_2$ for some $1 \le k \le a_1$. Let E be the elementary abelian group consisting of the direct product of k copies of $\mathbb{Z}_{p_1}$ i.e., $E = \mathbb{Z}_{p_1}^k$. E can also be viewed as a k-dimensional vector space over $\mathbb{F}_{p_1}$, the finite field with p_1 elements (isomorphic

to $\mathbb{Z}_{p_1}$ as a group). Then the group of vector space automorphisms of E is $\mathrm{Aut}(E) \cong GL_k(\mathbb{F}_{p_1})$. The latter is the group of $k \times k$ matrices with entries in $\mathbb{F}_{p_1}$ and non-zero determinant modulo p_1. The order of $GL_k(\mathbb{F}_{p_1})$ is $(p_1^k - 1)(p_1^k - p_1) \cdots (p_1^k - p_1^{k-1})$. By assumption $p_1^k \equiv 1 \bmod p_2$, so $p_2 | (p_1^k - 1)$ and hence p_2 divides $|GL_k(\mathbb{F}_{p_1})|$. Then $\mathrm{Aut}(E)$ has a subgroup isomorphic to $\mathbb{Z}_{p_2}$ by Cauchy's theorem and we may form a non-trivial semi-direct product, $E \rtimes \mathbb{Z}_{p_2}$. Now consider the group

$$G = \left(E \rtimes \mathbb{Z}_{p_2}\right) \times \mathbb{Z}_{p_1}^{a_1 - k} \times \mathbb{Z}_{p_2}^{a_2 - 1} \times \mathbb{Z}_{p_3}^{a_3} \times \cdots \times \mathbb{Z}_{p_t}^{a_t}.$$

By construction, G is a group of order n. In a nilpotent group, elements in Sylow subgroups corresponding to distinct primes commute with each other. The elements of E all have order p_1 and they don't commute with the elements of $\mathbb{Z}_{p_2}$ in the semi-direct product $E \rtimes \mathbb{Z}_{p_2}$, by construction. Hence G is not nilpotent and consequently n is not a nilpotent number.

For the converse, we wish to show that if n has nilpotent factorization, then it is a nilpotent number. Suppose this is not true. Let n be the smallest positive integer with nilpotent factorization that is not a nilpotent number. Then there exists a group G of order n that is not nilpotent. If H is any proper subgroup of G, then $|H|$ has nilpotent factorization also. H must be nilpotent, since we assumed n to be the smallest non-nilpotent integer with nilpotent factorization. So G is a non-nilpotent group with every proper subgroup nilpotent. By a theorem of O. J. Schmidt [**9**, 9.1.9. p. 251], such groups are rather special and we must have $n = |G| = p^a q^b$, where p, q are distinct primes and $a, b \geq 1$.

Let n_p and n_q denote the number of Sylow p-subgroups and Sylow q-subgroups, respectively, of G. By Sylow's theorem, $n_p \equiv 1 \bmod p$, but it is also equal to the index of the normalizer, $N_G(S_p)$, of some Sylow p-subgroup S_p in G. Now $S_p \subset N_G(S_p) \subset G$. So the order of $N_G(S_p)$ is $p^a q^k$ for some integer k, and has index $q^{b-k} = n_p \equiv 1 \bmod p$ in G. By assumption $|G| = p^a q^b$ has nilpotent factorization, which forces $b - k = 0$. This implies $N_G(S_p) = G$ and hence S_p is unique and normal in G. The same argument applied to q shows that the Sylow q-subgroup, S_q, is also unique and normal. Hence, $G \cong S_p \times S_q$, which contradicts our assumption that G was not nilpotent. So if n has good factorization, then it must be a nilpotent number. ∎

We will see that this also characterizes cyclic and abelian numbers since we have the containments

$$\textit{cyclic groups} \subset \textit{abelian groups} \subset \textit{nilpotent groups}.$$

Recall that a positive integer $n = p_1^{a_1} \cdots p_t^{a_t}$ is said to be *cube–free* if $a_i \leq 2$ for all i. It is said to be *square–free* if $a_i = 1$ for all i.

Abelian numbers. Given a prime p, there is always a non-abelian group of order p^3. For example,

$$T_p = \left\{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} : a, b, c \in \mathbb{Z}_p \right\},$$

where addition and multiplication of entries is performed modulo p, is one such group for every prime p. So an abelian number is necessarily cube–free. We claim that n is an abelian number if and only if it is a cube–free number with nilpotent factorization.

Suppose n is a cube–free nilpotent number and let G be a group of order n. Then G is nilpotent and $G \cong S_{p_1} \times \cdots \times S_{p_t}$, i.e., G is isomorphic to the product

of its Sylow subgroups. Since n was assumed to be cube–free, each S_{p_i} has order p_i or p_i^2 and is hence, abelian. G is then abelian, being a product of abelian groups, and n is an abelian number.

Conversely, if n is an abelian number, then it must be a nilpotent number and hence it has nilpotent factorization. We noted that n is necessarily cube–free; if not, then there exists a prime p such that $p^3|n$. Then $T_p \times \mathbb{Z}_{n/p^3}$ is a non-abelian group of order n, contradicting the assumption that n is an abelian number. This completes the argument and establishes our claim.

Cyclic numbers. We now claim that n is a cyclic number if and only if it is a square–free number with nilpotent factorization. The argument here is along the same lines as for the abelian case once we note that $\mathbb{Z}_p \times \mathbb{Z}_p$ is a non-cyclic group of order p^2.

This characterization is equivalent to another well known characterization of cyclic numbers. Let $\varphi(n)$ be the Euler totient function of n. It counts the number of positive integers less than or equal to n that are relatively prime to n. For $n = p_1^{a_1} \cdots p_t^{a_t}$,

$$\varphi(n) = \left(p_1^{a_1-1}(p_1 - 1)\right) \cdots \left(p_t^{a_t-1}(p_t - 1)\right)$$

Note that if n is square–free, then $\varphi(n) = (p_1 - 1) \cdots (p_t - 1)$. Our claim says that n is a cyclic number if and only if it has nilpotent factorization and it is square–free. This is equivalent to saying $p_i \nmid (p_j - 1)$ for all i, j, which is equivalent to saying $\gcd(n, \varphi(n)) = 1$. This yields the elegant result: A positive integer n is a cyclic number if and only if $\gcd(n, \varphi(n)) = 1$.

Remark. The only even numbers with nilpotent factorization are powers of 2. Let $f(n)$ denote the number of groups of order n. If $n = p_1^{a_1} \cdots p_t^{a_t}$ is an abelian number, then $f(n) = 2^{\Sigma(a_i-1)}$. The problem of determining $f(n)$ is quite hard in general and beyond reach even for the nilpotent numbers. This is because estimating $f(p^k)$ for all primes p and all integers k, is too difficult a problem at this time.

Remark. Using a deep result of J. Thompson's on minimal simple groups [**10**] which ultimately relies on the celebrated Feit–Thompson theorem, it is possible to characterize the solvable numbers as well. We can show that a positive integer n is a solvable number if and only if it is not a multiple of any of the following numbers:

(a) $2^p(2^{2p} - 1)$, p any prime.
(b) $3^p(3^{2p} - 1)/2$, p an odd prime.
(c) $p(p^2 - 1)/2$, p any prime greater than 3 such that $p^2 + 1 \equiv 0 \bmod 5$.
(d) $2^4 \cdot 3^3 \cdot 13$.
(e) $2^{2p}(2^{2p} + 1)(2^p - 1)$, p an odd prime.

As a corollary we see that an integer not divisible by 4 must be a solvable number. In particular, every odd number is a solvable number, as expected.

ACKNOWLEDGMENTS. We thank Jørgen Tornehave for useful discussions and we thank the mathematics department of Aarhus University, Denmark for their hospitality.

REFERENCES

1. L. E. Dickson, Definitions of a group and a field by independent postulates, *Trans. Amer. Math. Soc.* **6** (1905) 198–204.
2. J. A. Gallian and D. Moulton, When is $\mathbb{Z}_n$ the only group of order n?, *Elem. Math.* **48** (1993) 117–119.

3. T. Hungerford, *Algebra*, Graduate Texts in Math. **73**, Springer, New York, 1974.
4. D. Jungnickel, On the uniqueness of the cyclic group of order n, *Amer. Math. Monthly* **99** (1992) 545–547.
5. G. Pazderski, Die Ordnungen, zu denen nur Gruppen mit gegebener Eigenschaft gehören, *Arch. Math.* **10** (1959) 331–343.
6. L. Rédei, Das "schiefe Produkt" in der Gruppentheorie mit Anwendung auf die endlichen nichtkommutativen Gruppen mit lauter kommutativen echten Untergruppen und die Ordnungszahlen, zu denen nur kommutative Gruppen göheren, *Comm. Math. Helv.* **20** (1947) 225–264.
7. D. Robinson, *A course in the theory of groups*, Graduate Texts in Math. **80**, Springer, New York, 1993.
8. T. Szele, Über die endlichen Ordnungszahlen, zu denen nur eine Gruppe gehört, *Comm. Math. Helv.* **20** (1947) 265–267.
9. J. Szép, On finite groups which are necessarily commutative, *Comm. Math. Helv.* **20** (1947) 223–224.
10. J. G. Thompson, Nonsolvable finite groups all of whose local subgroups are solvable, *Bull. Amer. Math. Soc.* **74** (1968) 383–437.

University of Wisconsin, Madison, WI 53706
pakianat@math.wisc.edu

University of Michigan, Ann Arbor, MI 48109
shankar@umich.edu

Triangular Triples from Ceilings to Floors

Tom Jenkyns and Eric Muller

1. Introduction. A *triangular triple* is a sequence of non-negative integers (i, j, k) that gives the lengths of the sides of a triangle. Then each integer is at most the sum of the other two. We restrict our attention to incongruent triangles and therefore to triples where $i \le j \le k$ and $k \le i + j$, since any two triangles with these side-lengths are congruent. The associated triangle has perimeter, $p = i + j + k$. When one of p or k or j is fixed, just how many triangular triples are there?

In fact we shall count four types of triples. Let A denote the set of *all* triangular triples, let B denote the set of all *non-degenerate* triangular triples, let C denote the set of all *scalene* triangular triples, and let D denote the set of all triangular triples that are *both* scalene and non-degenerate. For each of these sets $\mathscr{A}$, let $\mathscr{A}(p)$ denote the subset of triples in $\mathscr{A}$ with sum equal p, and let $T_\alpha(p)$ denote the cardinality of $\mathscr{A}(p)$. The first few values of these functions appear somewhat chaotic:

Table 1

p	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
T_a	1	0	1	1	2	1	3	2	4	3	5	4	7	5	8	7	10	8
T_b	0	0	0	1	0	1	1	2	1	3	2	4	3	5	4	7	5	8
T_c	0	0	0	0	0	0	1	0	1	1	2	1	3	2	4	3	5	4
T_d	0	0	0	0	0	0	0	0	0	1	0	1	1	2	1	3	2	4

The main purpose of this note is to provide formulas for the four functions $T_\alpha(p)$. Past attention has focused on non-degenerate triangles [1]–[5], though [2]

