DENSITY OF SINGULAR PAIRS OF INTEGERS

Roman Nedela
Faculty of Applied Sciences, University of West Bohemia, Pilsen, Czech Republic
nedela@savbb.sk

Carl Pomerance
Department of Mathematics, Dartmouth College, Hanover, NH 03755, USA
carl.pomerance@dartmouth.edu

Received: , Revised: , Accepted: , Published:

Abstract

A positive integer n is called cyclic if there is a unique group of order n, which is necessarily cyclic. Using a characterisation of the cyclic integers as those n satisfying $\gcd(n, \varphi(n)) = 1$, P. Erdős (1947) proved that the number of cyclic integers $n \le x$ is asymptotic to $z(x) = e^{-\gamma}\frac{x}{\log\log\log x}$, as $x \to \infty$, where γ is Euler's constant. An ordered pair of integers (m, n) is called singular if $\gcd(m, \varphi(n)) = 1$ and $\gcd(n, \varphi(m)) = 1$, a concept which is relevant to pairwise products of cyclic groups and to embeddings of complete bipartite graphs. In this note we show that the number of singular pairs of integers (m, n), $m, n \le x$, is asymptotic to $z(x)^2$.

1. Introduction

Say a positive integer n is *cyclic* if there is just one group, up to isomorphism, of order n, which of course is necessarily cyclic. A number-theoretic characterisation of cyclic integers is given by the following theorem.

Theorem 1.1. *[17] The positive integer n is cyclic if and only if n and $\varphi(n)$ are coprime.*

Here, φ is Euler's totient function. Theorem 1.1 has some history. According to our knowledge it first appears explicitly in a paper by Szele [17] published in 1947. In 1992 another simple proof of Theorem 1.1 was published in [9]. There are signs that the result was known to Burnside and Hölder already around the year 1900, for instance it appears as an exercise in the monograph by Robinson [16, 10.1, Exercise 12] attributed to Burnside. Moreover, in 1885 Hölder in [7] proved that the number

of groups of squarefree order n is given by

$$g(n) = \sum_{d|n} \prod_{p|d} \frac{p^{\nu_p(n/d)} - 1}{p - 1},$$

where the product is over the primes p dividing d, and $\nu_p(m)$ is the number of primes $\equiv 1 \pmod{p}$ dividing m. Theorem 1.1 follows immediately. Indeed, for n squarefree, since the summand with $d = 1$ always contributes 1 to the sum (as an empty product), we have $g(n) = 1$ exactly when the other terms are all 0, which occurs exactly when $\gcd(n, \varphi(n)) = 1$. Further if n is not squarefree, one can easily construct a group of order n that is not cyclic.

Another related result was proved by Dickson [1] in 1905, where he characterised the integers n such that all groups of order n are abelian. This result can be found in papers by Szep [18] and Rédei [16] as well. In particular, the abelian criterion is that n is cube-free and for $p^k q \mid n$ with p, q primes, we have $q \nmid p^k - 1$. A result of G. Padzerski [12] from 1959 further characterises those numbers n such that every group of order n is nilpotent: Such n satisfy the same condition as the abelian condition without the requirement that n be cube-free. Also see Müller [11] for more in this vein.

Erdős proved in [2] that the number of cyclic integers is asymptotically $z(x) := e^{-\gamma} x/\log\log\log x$, where γ is Euler constant. Call a positive integer n abelian (nilpotent), if every group of order n is abelian (nilpotent). It is interesting that the number of abelian $n \le x$ is also $\sim z(x)$ and the same is true for the number of nilpotent $n \le x$, even though there are more of these integers than there are cyclic integers. Erdős and Mays [3] found asymptotics for the number of abelian $n \le x$ that are not cyclic and also for the number of nilpotent $n \le x$ that are not abelian.

The cyclic integers were rediscovered in the context of topological graph theory [8], where it was proved that the complete bipartite graph $K_{n,n}$ has a unique regular embedding into an orientable surface if and only if n is cyclic. Here, a 2-cell embedding of a graph into an orientable surface is regular if the group of orientation-preserving automorphisms is regular on the set of arcs.

We discuss some of these terms. In topological graph theory a graph is usually considered as a 1-dimensional cell complex. An embedding $i : G \to S$ of a connected graph G into a closed orientable surface S is cellular, if each component of $S \setminus i(G)$ is homeomorphic to an open disc. A graph automorphism that extends to a self-homeomorphism of S preserving the embedded graph is an automorphism of the embedding. An embedding of a graph G is edge-transitive if the group of orientation-preserving automorphisms acts transitively on the edges of G. The embedding is regular if the group of orientation-preserving automorphisms is regular on the set of arcs of G.

The main topic of this note is the concept of a singular pair. An ordered pair of positive integers (m, n) is *singular* if $\gcd(m, \varphi(n)) = \gcd(n, \varphi(m)) = 1$. Observe

that the pair (n, n) is singular if and only if n is cyclic. Generalizing the result of [8] mentioned above about embeddings of $K_{n,n}$, Fan and Li [4] proved that the complete bipartite graph $K_{m,n}$ has a unique edge-transitive embedding into an orientable surface if and only if the pair (m, n) is singular. Independently, the following statement was proved in [5].

Theorem 1.2. *[5] Let m and n be positive integers. Then the following statements are equivalent:*

1. *the pair (m, n) is singular,*
2. *every product of disjoint cyclic groups C_m and C_n of orders m and n is the direct product $C_m \times C_n$,*
3. *every product of cyclic groups of orders m and n is abelian,*
4. *the complete bipartite graph $K_{m,n}$ admits a unique edge-transitive embedding into an orientable surface.*

Recall that a group G is a product of groups A and B, $G = AB$, if for every $g \in G$ there exist $a \in A$ and $b \in B$ such that $g = ab$. Two subgroups A and B of G are disjoint if $A \cap B = \{1\}$.

We will prove in the next section that the number of singular pairs (m, n) with $m, n \leq x$ is $\sim z(x)^2$ as $x \to \infty$.

Remark 1.3. Cellular embeddings of bipartite bicoloured graphs into orientable surfaces form a combinatorial counterpart to algebraic curves defined by polynomial equations in two complex variables. In the context of algebraic geometry Grothendieck called such maps "dessins d'enfant". The correspondence between the dessins and algebraic curves is explained by a non-trivial Belyĭ theorem, see [10] for details. If $m = n$ the unique embedding of $K_{n,n}$ in Theorem 1.2(4) corresponds to the famous Fermat curve defined by the equation $x^n + y^n = 1$.

2. Main result

In this section we are concerned with the number of singular pairs with $m, n \leq x$. The problem of determining this number was mentioned by G. Jones in a personal communication with one of the authors. Let x be a large number, and let

$$\begin{aligned} y &= y(x) = \log\log x, \\ z &= z(x) = e^{-\gamma} x/\log y, \text{ where } \gamma \text{ is Euler's constant}, \\ \epsilon &= \epsilon(x) = 1/\log\log y. \end{aligned}$$

Observe that the Erdős result [2] can be stated as follows: the number of cyclic integers $\leq x$ is $\sim z$ as $x \to \infty$. We prove the following theorem.

Theorem 2.1. *The number of singular pairs (m,n) with $m,n \le x$ is $\sim z^2$ as $x \to \infty$.*

When we use O-notation, the implied constant is assumed to be absolute. We let p, q, r denote primes.

Proof. We shall use a few results about primes in residue classes.

1. If a, m are integers with $m > 0$ and $\gcd(a,m) = 1$, then
$$\sum_{\substack{p \le x \\ p \equiv a \pmod m}} \frac{1}{p} = \frac{y}{\varphi(m)} + O(1).$$

2. If a, m are as above, then
$$\sum_{\substack{n \le x \\ p \mid n \implies p \not\equiv a \pmod m}} 1 = O\left(x \exp\left(-\frac{y}{\varphi(m)}\right)\right).$$

3. If a, m are as above, then
$$\sum_{\substack{|a| < p \le x \\ p \equiv a \pmod m}} \frac{1}{p} = O\left(\frac{y}{\varphi(m)}\right).$$

The first of these results with a non-uniform O-constant is already implicit in the work of Dirichlet (see [13, Prop. 5]). The version here, where the O-constant is uniform, can be found, for example, in [14, Theorem 1]. The second item follows as a consequence of the first item and from Brun's method, see [6, Theorem 2.2]. The Brun–Titchmarsh inequality is used for the third statement; or see [14, Remark 1].

We begin with the upper bound implicit in the theorem. If $p \nmid \varphi(n)$, then n is not divisible by any prime $q \equiv 1 \pmod p$. So, for any prime p, the second item above implies that the number of $n \le x$ with $p \nmid \varphi(n)$ is $O(x \exp(-y/p))$. We sum this inequality for all $p \le y^{1-\epsilon}$, so finding that the number of $n \le x$ such that $\varphi(n)$ is not divisible by every prime $p \le y^{1-\epsilon}$ is $O(xy \exp(-y^\epsilon))$. Thus, the number of pairs (m,n) with $m,n \le x$ and either $\varphi(m)$ or $\varphi(n)$ not divisible by every prime $p \le y^{1-\epsilon}$ is $O(x^2 y \exp(-y^\epsilon))$. This expression is $o(z^2)$ as $x \to \infty$, so we may assume that the pairs we are counting have both $\varphi(m), \varphi(n)$ divisible by every prime to $y^{1-\epsilon}$. For such a pair to be singular it is necessary that m, n be coprime to every prime to $y^{1-\epsilon}$. By a simple sieve (i.e., inclusion-exclusion) and Mertens' theorem, the number of integers $n \le x$ not divisible by any prime to $y^{1-\epsilon}$ is $\sim e^{-\gamma} x / \log(y^{1-\epsilon}) \sim z$ as $x \to \infty$. Hence the number of pairs of such integers is at most $(1 + o(1))z^2$ as $x \to \infty$.

For the lower bound implicit in the theorem we take pairs (m,n) with $m,n \le x$ and mn not divisible by any prime $p \le y^{1+\epsilon}$. As in the upper bound argument, the number of such pairs is $\sim z^2$ as $x \to \infty$, so it suffices to show that most of these pairs are singular. If such a pair is not singular then there is a prime $p > y^{1+\epsilon}$ dividing $\gcd(m,\varphi(n))$ or $\gcd(n,\varphi(m))$.

For a given prime p, if $p \mid \varphi(n)$, then either $p^2 \mid n$ or there is a prime $q \mid n$ with $q \equiv 1 \pmod{p}$. By the third result above, the number of $n \le x$ with $p \mid \varphi(n)$, where $p > y^{1+\epsilon}$, is thus

$$O\left(\frac{x}{p^2} + \frac{xy}{p}\right) = O\left(\frac{xy}{p}\right).$$

We conclude that the number of pairs (m,n) with $m,n \le x$ and with p dividing $\gcd(m,\varphi(n))$ is

$$O\left(\frac{x^2y}{p^2}\right),$$

and the same estimate pertains to the number of pairs with $p \mid \gcd(n,\varphi(m))$. We sum this for $p \ge y^{1+\epsilon}$ getting

$$O\left(\frac{x^2y}{y^{1+\epsilon}\log y}\right) = O\left(\frac{x^2}{y^{\epsilon}}\right).$$

Since this expression is $o(z^2)$ as $x \to \infty$, the result is established. □

Remark 2.2. We note that the above proof can be amended to show that the number of ordered k-tuples $(m_1,\dots,m_k)$ of positive integers $\le x$, where each pair (m_i,m_j) with $i \ne j$ is singular, is $\sim z^k$ as $x \to \infty$. Here we assume that k is arbitrary, but fixed. The same asymptotic holds where we do not insist that $i \ne j$, which is then equivalent to $m_1 \dots m_k$ being cyclic, even though this condition is slightly stronger.

The set of k-tuples defined above, suggests that a generalisation of Theoren 1.2 could hold. However, a direct extension is not possible. The problem is that if a group $G = X_1X_2\dots X_k$ decomposes as a product of more than two groups, then the product of two factors X_iX_j may not form a subgroup. Further, it is not clear how one might generalize the concept of singular to complete multipartite graphs. However, we can say something about groups along the following lines. Say an ordered k-tuple $(m_1,\dots,m_k)$ is singular if there is no non-abelian group which is the product of pairwise disjoint subgroups $C_{m_1},\dots,C_{m_k}$. It is easy to see from Theorem 1.2 that this generalizes the concept of singular pairs. Further, using the thoughts in Remark 2.2 we have that for k fixed, the number of singular k-tuples with coordinates at most x is $\sim z^k$ as $x \to \infty$.

Acknowledgments

The authors thank Prof. Gareth Jones (Univ. Southampton) for his assistance with the history of the singular integers. We also thank Prof. John Voight (Dartmouth Coll.) for his interest in the topic and Prof. Paul Pollack for assistance regarding the provenance of item (1) in the proof of Theorem 2.1 and also for reminding us of [3].

The first author is supported by the grants APVV-15-0220, VEGA 1/0150/14, and Project P202/12/G061 of the Czech Science Foundation.

References

[1] L. E. Dickson, Definitions of a group and a field by independent postulates, Trans. Amer. Math. Soc. 6 (1905), 198–204.

[2] P. Erdős, Some asymptotic formulas in number theory, J. Indian Math. Soc. 12 (1948) 75–78.

[3] P. Erdős and M. E. Mays, On nilpotent but not abelian groups and abelian but not cyclic groups, J. Number Theory 28 (1988), 363–368.

[4] W. Fan, C.-H. Li, The complete bipartite graphs with a unique edge-transitive embedding, J. Graph Theory, DOI: 10.1002/jgt.22176.

[5] Y-Q. Feng, K. Hu, R. Nedela, M. Škoviera, and N. Wang, Complete regular dessins and skew-morphisms of cyclic groups, preprint.

[6] H. Halberstam and H.-E. Richert, Sieve methods, Academic Press, London, 1974.

[7] O. Hölder, Die Gruppen mit quadratfreien Ordnungszahl, Nachr. Akad.Wiss. Goettingen Math.-Phys. Kl. II 2 (1895) 211–229.

[8] G. Jones, R. Nedela, and M. Škoviera, Complete bipartite graphs with a unique regular embedding, J. Comb. Theory B 98 (2008), 241–248.

[9] D. Jungnickel, On the uniqueness of the cyclic group of order n, Amer. Math. Monthly, 99 (1992), 545–547.

[10] S. Lando and A. Zvonkin, Graphs on surfaces and their applications. With an appendix by Don B. Zagier. Encyclopaedia of Mathematical Sciences, 141. Low-Dimensional Topology, II. Springer-Verlag, Berlin, 2004.

[11] T. Müller, An arithmetic theorem related to groups of bounded nilpotency, J. Algebra 300 (2006), 10–15.

[12] G. Pazderski, Die Ordnungen, zu denen nur Gruppen mit gegebener Eigenschaft gehren, Arch. Math. 10 (1959) 331–343.

[13] P. Pollack, Euler and the partial sums of the prime harmonic series, Elem. Math 70 (2015), 13–20.

[14] C. Pomerance, On the distribution of amicable numbers, J. Reine Angew. Math. 293/294 (1977), 217–222.

[15] 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 gehören, Comment. Math. Helv. 20, (1947). 225–264.

[16] D. J. S. Robinson, A Course in the Theory of Groups, Springer, New York, 1996.

[17] T. Szele, Über die endlichen Ordnungszahlen, zu denen nur eine Gruppe gehort, Comm. Math. Helv. 20 (1947), 265–267.

[18] J. Szep, On finite groups which are necessarily commutative, Comm. Math. Helv. 20 (1947), 223–224.