ELSEVIER Discrete Mathematics 200 (1999) 165–179

DISCRETE MATHEMATICS

On the orders of directly indecomposable groups

Paul Erdős, Péter P. Pálfy*,[1]

Mathematical Institute of the Hungarian Academy of Sciences, Budapest, P.O. Box 127, H-1364 Hungary

Received 23 September 1997; accepted 21 April 1998

Abstract

We investigate the set of those integers n for which directly indecomposable groups of order n exist. For even n such groups are easily constructed. In contrast, we show that the density of the set of odd numbers with this property is zero. For each n we define a graph whose connected components describe uniform direct decompositions of all groups of order n. We prove that for almost all odd numbers (i.e., with the exception of a set of density zero) this graph has a single 'big' connected component and all other vertices are isolated. We also give an asymptotic formula for the number of isolated vertices of the graph, i.e., for the number of prime divisors q of n such that every group of order n has a cyclic direct factor of order q. © 1999 Elsevier Science B.V. All rights reserved

Keywords: Indecomposable group; Uniform factorization; Density

1. Introduction

In this paper we will call a finite group *indecomposable* if it cannot be decomposed into the direct product of two proper subgroups. Sudler [9] asked the question for which positive integers n there exists an indecomposable group of order n. If n is even then it is very easy to find an indecomposable group of order n (Proposition 1.1). On the other hand, we prove that the density of the set of odd numbers for which an indecomposable group exists is zero, that is, for *almost all* odd numbers n (i.e., with the exception of a set of density zero) every group of order n can be decomposed into a proper direct product (Corollary 4.2).

It seems to be difficult to describe those numbers for which indecomposable groups of that order exist. We do this only in the cases when n is square-free (Theorem 5.2) or $n = p^a q^b$ with p, q primes, $a, b \geqslant 1$ (Theorem 6.1). We get, for example, that there

* Corresponding author. E-mail: ppp@math-inst.hu.

[1] Research supported by OTKA grant No. 16432.

PII: S0012-365X(98)00325-2

are indecomposable groups of order 3×7 and 7×29 but there is no indecomposable group of order $3 \times 7 \times 29$; there are indecomposable groups of order $3^5 \times 11$ and 3^6 but none of order $3^6 \times 11$. Therefore we will rather consider *uniform factorizations*, i.e., factorizations $n = n_1 n_2 \cdots n_m$ such that every group of order n is the direct product of groups of order $n_1, n_2, \ldots, n_m$. The number theoretic characterization of these factorizations is given in Proposition 2.1. It turns out that every number has a unique such factorization with a maximum number of factors. Our main result is that for almost all odd numbers all but one of these factors is a prime number (Theorem 3.1) and we give an asymptotic formula for the number of these prime factors as well (Theorem 4.1).

This paper is an extended version of the Hungarian original [2]. The structure of the paper has been somewhat modified. The introduction of the graph $\Gamma(n)$ in Definition 2.2 is new, making it easier to describe the results, in particular Theorem 3.1. Corollary 2.4 is also new, as well as the graph theoretic Problem 5.3 and the proofs of Theorems 5.2 and 6.1 which were omitted in [2]. Paul Erdős expressed several times his interest in rewriting and publishing the paper in English; it is sad that this will happen only posthumously.

To begin with, notice that any cyclic group of prime-power order or any simple group is directly indecomposable. However, the set of orders of these groups has density zero. More examples can be constructed using metacyclic groups.

Proposition 1.1. *Let $n = 2^k m$ with $k \geqslant 1$, m odd. Then the group*

$$G = \langle a, b \mid a^m = 1,\ b^{2^k} = 1,\ b^{-1}ab = a^{-1} \rangle$$

is directly indecomposable of order n.

Proof. Assume that $G = G_1 \times G_2$, and let $a = a_1 a_2$, $b = b_1 b_2$ with $a_i, b_i \in G_i$ $(i = 1, 2)$. Since the order of b is the least common multiple of the orders of b_1 and b_2, it follows that one of them, say, b_1 has order 2^k. Then 2^k divides the order of G_1, hence G_2 has odd order, thus $b_2 = 1$. The relation $b^{-1}ab = a^{-1}$ yields $(b_1^{-1} a_1 b_1) a_2 = a_1^{-1} a_2^{-1}$, from which we infer that $a_2^2 = 1$. However, we have already observed that G_2 has odd order, hence $a_2 = 1$. Thus $G_2 = 1$, so G has only a trivial direct decomposition, indeed. □

All groups considered in this paper are finite. Throughout we use p and q to denote primes, and $c_1, \ldots, c_6$ will denote absolute constants.

2. Uniform factorizations

Proposition 2.1. *Let $n = n_1 n_2$ be an odd number. Every group of order n can be decomposed into the direct product of groups of order n_1 and n_2 if and only if the following three conditions are satisfied:*

(i) *n_1 and n_2 are coprime numbers,*

(ii) *there are no primes p and q, and $k \geqslant 1$ such that $p \mid n_1$, $q^k \mid n_2$, and $p \mid q^k - 1$; and symmetrically,*

(iii) *there are no primes p and q, and $k \geqslant 1$ such that $p^k \mid n_1$, $q \mid n_2$, and $q \mid p^k - 1$.*

(Remarks. The exponent k in (ii) and (iii) need not be the highest power of q or p dividing the order of G. Obviously, no even number can have a proper factorization satisfying the conditions of the proposition. We formulated the result for odd numbers in order to emphasize the use of special properties of groups of odd order.)

Proof. The necessity of the conditions is shown by the following groups: (i) C_n, the cyclic group of order n; (ii) $\{x \mapsto ax + b \mid a,\ b \in \mathrm{GF}(q^k),\ a^p = 1\} \times C_{n/pq^k}$, where $\mathrm{GF}(q^k)$ denotes the field of q^k elements; (iii) symmetrically, by interchanging the role of p and q.

Now let us assume that the conditions (i), (ii), and (iii) are satisfied and let G be an arbitrary group of order n. Since n is odd, the celebrated result of Feit and Thompson [3] yields that G is solvable. By Hall's theorem (see [4, p. 232]) one can find a suitable Sylow p_i-subgroup P_i for each prime divisor p_i of n such that $P_iP_j = P_jP_i$ holds for each pair of indices. Let G_1 be the product of all those P_i's for which p_i divides n_1, and let G_2 be constructed analogously. Condition (i) gives $|G_1| = n_1$, $|G_2| = n_2$. Let now p be a prime divisor of n_1 and P the Sylow p-subgroup in the chosen Hall-system, q a prime divisor of n_2 with Sylow q-subgroup Q. Then $PQ = QP$ is a subgroup of G. By a result of Pazderski [7] (see also [6, p. 285]) the conditions (ii) and (iii) imply that PQ is nilpotent, i.e., P and Q centralize each other elementwise. This holds for every pair of prime divisors of n_1 and n_2, hence G_1 and G_2 commute, so $G = G_1 \times G_2$. □

Definition 2.2. Let $n > 1$ be an integer. We define an undirected graph $\Gamma(n)$ with vertices corresponding to the prime divisors of n, with an edge between p and q iff for some exponent $k \geqslant 1$ either $p \mid q^k - 1$ and $q^k \mid n$ or $q \mid p^k - 1$ and $p^k \mid n$. (Here p^k (or q^k) need not be the highest power of p (or q) dividing n.)

Proposition 2.1 easily yields the following:

Corollary 2.3. *The number n has a proper factorization $n = n_1n_2$ such that every group of order n can be decomposed into the direct product of groups of order n_1 and n_2 if and only if the graph $\Gamma(n)$ is not connected.*

Corollary 2.4. *Every number $n > 1$ has a uniquely determined factorization $n = n_1n_2 \ldots n_m$ with maximum number of factors such that every group of order n can be decomposed into the direct product of groups of order $n_1, n_2, \ldots, n_m$.*

Proof. Clearly, in virtue of Proposition 2.1, the connected components of $\Gamma(n)$ determine the factors n_i. □

Making use of Dirichlet's theorem on prime numbers in arithmetic progressions it is easy to see that every graph can be represented as $\Gamma(n)$ for a suitable n. However, this wealth of different graphs is produced by a rare set of integers. We will show that for almost all odd numbers n (i.e., with the exception of a set of density zero) the graph $\Gamma(n)$ consists of a single 'big' connected component and a large number of isolated vertices.

3. The unique 'big' factor

Theorem 3.1. *For almost all numbers n the graph $\Gamma(n)$ has a unique connected component containing more than one vertex.*

Proof. We will show that for any fixed $\eta > 0$ the lower density of the set of those numbers n for which the graph $\Gamma(n)$ has only one connected component which is not an isolated point is at least $1 - \eta$. Since this will hold for any positive η, this set of numbers has density 1, indeed.

Later we will choose the parameters ε $(0 < \varepsilon < 1)$ and A $(A > 2)$ suitably, but let now ε and A be fixed and consider the set of those numbers n which satisfy the following five requirements:

(a) n has a prime divisor less than A,

(b) for every divisor $d < (\log\log n)^{1-\varepsilon}$ of n there exists a prime $q \mid n$ such that $q \equiv 1 \pmod{d}$,

(c) n has no prime divisors in the interval $((\log\log n)^{1-\varepsilon}/A, (\log\log n)^{1+\varepsilon})$,

(d) there is no prime $p > (\log\log n)^{1+\varepsilon}$ such that p^2 divides n,

(e) n has no prime divisors q and r such that $qr^k \mid n$, $q > (\log\log n)^{1+\varepsilon}$, and $r^k \equiv 1 \pmod{q}$.

We show that for every such number n the graph $\Gamma(n)$ has only one non-singleton component. So suppose that n satisfies (a)–(e). Let p be the smallest prime divisor of n, and let Δ denote the connected component of $\Gamma(n)$ containing p. We are going to show that every prime outside Δ is an isolated vertex of $\Gamma(n)$. In addition, we show that every such prime occurs to the first power in the prime decomposition of n.

By (a) we have that $p < A$. Let r be a prime divisor of n such that $p < r < (\log\log n)^{1-\varepsilon}/A$. Then (b) yields a prime $q \mid n$ such that $pr \mid q - 1$. Now both p and r are joined to q with an edge in $\Gamma(n)$, so each such prime r belongs to Δ. Hence by (c) every prime q outside Δ is at least $(\log\log n)^{1+\varepsilon}$. By (d) each such prime occurs to the first power in the prime decomposition of n. None of them is connected to any prime in Δ by the definition of the connected component. Moreover, there is no edge between any two such primes by condition (e). (Actually, we do not use the full strength of (e) here, that will be needed only in the proof of Theorem 4.1.)

It remains to estimate the lower density of the set of numbers satisfying (a)–(e). We will give upper bounds for the upper density of the sets of numbers not satisfying (a), …, (e) separately.

Lemma 3.2. *Let $A>2$. The density of the set of those numbers which have no prime divisor less than A is at most $c_1/\log A$ for some constant $c_1>0$.*

Proof. The density of this set is obviously

$$\prod_{p<A}\left(1-\frac{1}{p}\right)<\exp\left(-\sum_{p<A}\frac{1}{p}\right)\leqslant \exp(-\log\log A+\log c_1)=\frac{c_1}{\log A}. \qquad \square$$

Lemma 3.3. *Let $0<\varepsilon<1$. Almost all numbers n have the property that for every $d<(\log\log n)^{1-\varepsilon}$ there exists a prime $q\,|\,n$ such that $q\equiv 1\,(\operatorname{mod} d)$.*

Proof. We give an upper bound for the proportion of those numbers $n\leqslant x$ for which there exists a $d<(\log\log x)^{1-\varepsilon}$ such that $q\not\equiv 1\,(\operatorname{mod} d)$ for all prime divisors q of n. First let us fix d. Then Brun's method (see [5]) yields that the proportion of those $n\leqslant x$ which are not divisible by any prime $q\equiv 1\,(\operatorname{mod} d)$ is at most

$$c_2\prod_{\substack{q\equiv 1(d)\\ q\leqslant x}}\left(1-\frac{1}{q}\right)<c_2\exp\left(-\sum_{\substack{q\equiv 1(d)\\ q\leqslant x}}\frac{1}{q}\right),$$

with some absolute constant c_2. From the Siegel–Walfisz Theorem (see [8]) it follows by partial summation that

$$\sum_{\substack{q\equiv 1(d)\\ q\leqslant x}}\frac{1}{q}=(1+o(1))\frac{\log\log x}{\varphi(d)}\geqslant(1+o(1))\frac{\log\log x}{(\log\log x)^{1-\varepsilon}}\geqslant c_3(\log\log x)^{\varepsilon}$$

holds for every $d<(\log\log x)^{1-\varepsilon}$ with some constant $c_3>0$. Hence the proportion of the exceptional numbers n is at most

$$(\log\log x)^{1-\varepsilon}c_2\exp(-c_3(\log\log x)^{\varepsilon}),$$

which goes to 0 as $x\to\infty$. □

Lemma 3.4. *Let $0<\varepsilon<1$. The upper density of the set of those numbers n which have a prime divisor in the interval $((\log\log n)^{1-\varepsilon},(\log\log n)^{1+\varepsilon})$ is at most $\log((1+\varepsilon)/(1-\varepsilon))$.*

Proof. The method of [1] yields that the average number of prime divisors of a number n in the interval $((\log\log n)^{1-\varepsilon},(\log\log n)^{1+\varepsilon})$ is

$$\log\log(\log\log n)^{1+\varepsilon}-\log\log(\log\log n)^{1-\varepsilon}+o(1)=\log\frac{1+\varepsilon}{1-\varepsilon}+o(1).$$

Our claim follows immediately. □

Lemma 3.5. *Almost all numbers n have the property that every prime divisor $p>\log\log n$ of n occurs to the first power in the prime decomposition of n.*

Proof. The number of those integers $n\leqslant x$ which are divisible by the square of a number greater than log log $\sqrt{x}$, or are less than $\sqrt{x}$ is at most

$$\sum_{\log\log\sqrt{x}<k\leqslant\sqrt{x}} \frac{x}{k^2}+\sqrt{x}<\frac{x}{\log\log\sqrt{x}}+\sqrt{x}=\mathrm{o}(x). \qquad \square$$

Lemma 3.6. *Let $\varepsilon>0$. Then almost all numbers n have the property that n has no such divisors p and q^k, where p and q are primes, $k\geqslant 1$, $p>(\log\log n)^{1+\varepsilon}$ and $q^k\equiv 1 \pmod p$.*

Proof. The number of those integers $n\leqslant x$ for which there exist primes p, q, and $k\geqslant 1$ such that $pq^k\mid n$, $p>(\log\log\sqrt{x})^{1+\varepsilon}$ and $q^k\equiv 1 \pmod p$, or $n\leqslant\sqrt{x}$ is at most

$$\sum_{\substack{p>(\log\log\sqrt{x})^{1+\varepsilon}\\ q^k\equiv 1 \pmod p\\ q^k\leqslant x}} \frac{x}{pq^k}+\sqrt{x}=x\sum_{p>(\log\log\sqrt{x})^{1+\varepsilon}}\frac{1}{p}\sum_{\substack{q^k\equiv 1(p)\\ q^k\leqslant x}}\frac{1}{q^k}+\mathrm{o}(x)$$

$$\leqslant x\sum_{p>(\log\log\sqrt{x})^{1+\varepsilon}}\frac{1}{p}\frac{c_4\log\log x}{p-1}+\mathrm{o}(x)$$

(cf. [8, Theorem 2.4.1]; here we have $p<\sqrt{x}$)

$$\leqslant x\frac{c_4\log\log x}{(\log\log\sqrt{x})^{1+\varepsilon}}+\mathrm{o}(x)=\mathrm{o}(x). \qquad \square$$

Now we can finish the proof of Theorem 3.1. Using Lemmas 3.2–3.6 we see that the lower density of the set of numbers satisfying all conditions (a)–(e) is at least

$$1-\left(\frac{c_1}{\log A}+\log\frac{1+\varepsilon}{1-\varepsilon}\right)>1-\eta,$$

if ε is sufficiently small and A is sufficiently large. $\square$

4. The number of isolated prime factors

In the previous section we proved that for almost all odd numbers n the graph $\Gamma(n)$ has a single 'big' connected component and all other vertices are isolated, moreover these correspond to primes p that divide n to the first power and all of them are greater than $(\log\log n)^{1+\varepsilon}$. Now we determine the number of such prime divisors.

Theorem 4.1. *Almost all odd numbers n have*

$$(1+\mathrm{o}(1))\prod_{p|n}\left(1-\frac{1}{p-1}\right)\log\log n$$

isolated prime divisors, i.e., prime divisors q such that every group of order n is the direct product of the cyclic group of order q and a group of order n/q.

Since the number of isolated prime divisors as given in Theorem 4.1 is almost always positive, we obtain the following.

Corollary 4.2. *For almost all odd numbers n every group of order n can be decomposed into a proper direct product.*

The following lemmas pave the way to proving Theorem 4.1.

Lemma 4.3. *Let $p_1,\dots,p_t$ be fixed distinct odd primes. Then, as $x\to\infty$,*

$$\sum_{\substack{q \text{ prime}\\ q\leqslant x\\ p_i\nmid q-1}}\frac{1}{q}=(1+\mathrm{o}(1))\prod_{i=1}^{t}\left(1-\frac{1}{p_i-1}\right)\log\log x.$$

Proof. Let $k=p_1\cdots p_t$. Those primes $q\neq p_i$ for which $p_i\nmid q-1$ for each $i=1,\dots,t$ lie in one of the $(p_1-2)\cdots(p_t-2)$ residue classes among the $\varphi(k)=(p_1-1)\cdots(p_t-1)$ residue classes coprime to k. The quantitative form of Dirichlet's theorem (see [8, p. 138]) gives that the number of primes $<x$ in any of these residue classes is asymptotically

$$\frac{1}{\varphi(k)}\frac{x}{\log x}.$$

Now our claim easily follows by partial summation. □

Proposition 4.4. *Let $g(n)$ denote the number of those prime divisors q of the integer n for which $q-1$ and n are coprime. Then for almost all odd n we have*

$$g(n)=(1+\mathrm{o}(1))\prod_{p|n}\left(1-\frac{1}{p-1}\right)\log\log n.$$

Proof. It is enough to show that for arbitrary positive ε and η the inequality

$$\left|\frac{g(n)}{\prod_{p|n}(1-1/(p-1))\log\log n}-1\right|<\varepsilon$$

holds with the exception of a set of upper density less than 2η. For the proof of this we will fix a sufficiently large number A.

Let M denote the product of the primes not exceeding A (including 2). On the residue class $n \equiv a (\operatorname{mod} M)$, where $1 \leqslant a < M$ is an odd number, we will consider the function $g_A(n)$ denoting the number of prime divisors q of the (odd) number n such that $q > A$ and $q-1$ is not divisible by any prime divisor $p \leqslant A$ of n.

We will employ Turán's method to determine the normal order of the function $g_A(n)$. Every number in the fixed residue class has the same prime divisors not exceeding A, let these be $p_1, \ldots, p_t$. Now we have

$$\sum_{\substack{n \equiv a(M) \\ n \leqslant x}} g_A(n) = \sum_{\substack{n \equiv a(M) \\ n \leqslant x}} \sum_{\substack{q \mid n \\ q > A \\ p_i \nmid q-1}} 1 = \sum_{\substack{A < q \leqslant x \\ p_i \nmid q-1}} \sum_{\substack{n \equiv a(M) \\ q \mid n \\ n \leqslant x}} 1 = \sum_{\substack{A < q \leqslant x \\ p_i \nmid q-1}} \left(\frac{x}{Mq} + \delta_q \right),$$

where $|\delta_q| < 1$. Hence the average of the values of $g_A(n)$ on the residue class $n \equiv a (\operatorname{mod} M)$ in the interval $[1, x]$ is

$$\sum_{\substack{A < q \leqslant x \\ p_i \nmid q-1}} \frac{1}{q} + \mathrm{O}\left(\frac{1}{\log x} \right).$$

Lemma 4.3 yields

$$K = \sum_{\substack{A < q \leqslant x \\ p_i \nmid q-1}} \frac{1}{q} = (1 + \mathrm{o}(1)) \prod_{i=1}^{t} \left(1 - \frac{1}{p_i - 1} \right) \log \log x.$$

For the summed square deviation of $g_A(n)$ from K we obtain (with all $|\delta_i| < 1$)

$$\begin{aligned}
&\sum_{\substack{n \equiv a(M) \\ n \leqslant x}} (g_A(n) - K)^2 \\
&\quad = \sum_{\substack{n \equiv a(M) \\ n \leqslant x}} g_A(n)^2 - 2K \sum_{\substack{n \equiv a(M) \\ n \leqslant x}} g_A(n) + \left(\frac{x}{M} + \delta_1 \right) K^2 \\
&\quad = \sum_{\substack{A < q_1 \leqslant x \\ p_i \nmid q_1 - 1}} \sum_{\substack{A < q_2 \leqslant x \\ p_i \nmid q_2 - 1}} \sum_{\substack{n \equiv a(M) \\ n \leqslant x \\ q_1 \mid n, \\ q_2 \mid n}} 1 - K^2 \frac{x}{M} + \mathrm{o}(x) \\
&\quad = \sum_{\substack{A < q \leqslant x \\ p_i \nmid q-1}} \left(\frac{x}{Mq} + \delta_q \right) + \sum_{\substack{A < q_1 \leqslant x \\ p_i \nmid q_1 - 1}} \sum_{\substack{A < q_2 \leqslant x \\ p_i \nmid q_2 - 1}} \left(\frac{x}{Mq_1 q_2} + \delta_{q_1 q_2} \right) \\
&\qquad - \sum_{\substack{A < q \leqslant x \\ p_i \nmid q-1}} \left(\frac{x}{Mq^2} + \delta_{q^2} \right) - K^2 \frac{x}{M} + \mathrm{o}(x) \\
&\quad \leqslant K \frac{x}{M} + K^2 \frac{x}{M} - K^2 \frac{x}{M} + \mathrm{O}(x) = K \frac{x}{M} + \mathrm{O}(x).
\end{aligned}$$

Hence the average square deviation of $g_A(n)/K$ from 1 is

$$\leqslant \frac{1}{K} + \mathrm{O}\left(\frac{1}{K^2}\right),$$

so Chebyshev's inequality yields that for almost all odd n

$$g_A(n) = (1+\mathrm{o}(1)) \prod_{\substack{p\mid n\\ p\leqslant A}} \left(1 - \frac{1}{p-1}\right) \log\log n$$

holds.

Now we can consider our original function $g(n)$. In $g_A(n)$ we did not count those primes which do not exceed A, hence $g(n) \leqslant g_A(n) + \pi(A)$. On the other hand, we have counted those primes $q\mid n$ for which there exists a prime $p\mid n$ such that $p>A$ and $p\mid q-1$. Estimating the average number of such primes from above we obtain

$$\frac{1}{x}\sum_{n\leqslant x}\sum_{\substack{p>A\\ q\equiv 1(p)\\ pq\mid n}} 1 \leqslant \frac{1}{x}\sum_{\substack{p>A\\ p\leqslant\sqrt{x}}}\sum_{\substack{q\equiv 1(p)\\ q\leqslant x/p}} \frac{x}{pq} < \sum_{p>A}\frac{1}{p}\sum_{\substack{q\equiv 1(p)\\ q\leqslant x}}\frac{1}{q}$$

$$\leqslant \sum_{p>A} \frac{1}{p}\frac{c_4\log\log x}{p-1} < \frac{c_4\log\log x}{A},$$

cf. the proof of Lemma 3.6. Thus, with the exception of a set of at most ηx elements, we have, for $n\leqslant x$,

$$g(n) \geqslant g_A(n) - \frac{c_4\log\log x}{A}\frac{1}{\eta}.$$

For the remaining $(1-\eta)x - \mathrm{o}(x)$ numbers the inequalities

$$1+\mathrm{o}(1) \geqslant \frac{g(n)}{g_A(n)} \geqslant 1 - (1+\mathrm{o}(1))\frac{c_4}{A\prod_{3\leqslant p\leqslant A}\left(1-\frac{1}{p-1}\right)}\frac{1}{\eta}$$

hold. Notice that

$$A\prod_{3\leqslant p\leqslant A}\left(1-\frac{1}{p-1}\right) \geqslant A\exp\left(-(\log 8)\sum_{3\leqslant p\leqslant A}\frac{1}{p}\right)$$

$$\geqslant c_5 A\exp(-(\log 8)\log\log A) = \frac{c_5 A}{(\log A)^{\log 8}}.$$

We must also take into account that in the formulation of the proposition we multiply $(1-1/(p-1))$ for all prime divisors of n. Let us estimate the product

$$\prod_{\substack{p\mid n\\ p>A}}\left(1-\frac{1}{p-1}\right) \geqslant 1 - \sum_{\substack{p\mid n\\ p>A}}\frac{1}{p-1}.$$

In average we have

$$\frac{1}{x}\sum_{n\leqslant x}\sum_{\substack{p|n\\p>A}}\frac{1}{p-1}\leqslant\frac{1}{x}\sum_{A<p\leqslant x}\frac{x}{p}\frac{1}{p-1}\leqslant\frac{1}{A}.$$

Hence, with the exception of at most ηx numbers n in the interval $[1,x]$,

$$\sum_{\substack{p|n\\p>A}}\frac{1}{p-1}\leqslant\frac{1}{A}\frac{1}{\eta},$$

that is the inequality

$$\prod_{\substack{p|n\\p>A}}\left(1-\frac{1}{p-1}\right)>1-\frac{1}{A}\frac{1}{\eta}$$

holds. Summarizing, we obtain that, with the exception of a set of upper density at most 2η, for every odd number n

$$\left|\frac{g(n)}{\prod_{p|n}(1-1/(p-1))\log\log n}-1\right|$$

$$=\left|\frac{g(n)}{g_A(n)}\frac{g_A(n)}{\prod_{\substack{p|n\\p\leqslant A}}(1-1/(p-1))\log\log n}\cdot\frac{1}{\prod_{\substack{p|n\\p>A}}(1-1/(p-1))}-1\right|$$

$$\leqslant c_6\left\{\left|\frac{g(n)}{g_A(n)}-1\right|+\left|\frac{g_A(n)}{\prod_{\substack{p|n\\p\leqslant A}}(1-1/(p-1))\log\log n}-1\right|\right.$$

$$\left.+\left|\prod_{\substack{p|n\\p>A}}\left(1-\frac{1}{p-1}\right)-1\right|\right\}$$

$$\leqslant c_6\left\{\frac{(1+o(1))c_4(\log A)^{\log 8}}{c_5A}\frac{1}{\eta}+o(1)+\frac{1}{A}\frac{1}{\eta}\right\}<\varepsilon,$$

if we choose A large enough. □

For the order of magnitude of $\prod(1-1/(p-1))$ we have the following estimate.

Lemma 4.5. *Let $\omega(n)$ be an arbitrary function such that $\omega(n)\to 0$. Then for almost all odd n we have*

$$\prod_{p|n}\left(1-\frac{1}{p-1}\right)>\omega(n).$$

Proof. For every odd n the inequality

$$\prod_{p|n}\left(1-\frac{1}{p-1}\right) \geqslant \exp\left(-(\log 8)\sum_{p|n}\frac{1}{p}\right)$$

holds, and in average we have

$$\frac{1}{x}\sum_{n\leqslant x}\sum_{p|n}\frac{1}{p} \leqslant \frac{1}{x}\sum_{p\leqslant x}\frac{1}{p}\frac{x}{p} < \sum_{p}\frac{1}{p^2} < 1.$$

Hence our claim follows. □

Proof of Theorem 4.1. By Proposition 2.1 a prime divisor q of n is isolated, i.e., every group of order n has a direct factor of order q, if and only if the following three requirements are satisfied:

(i) q divides n to the first power,

(ii) $q-1$ is coprime to n,

(iii) there is no prime-power divisor $p^k \mid n$ such that $q \mid p^k - 1$.

Proposition 4.4 gives the number of prime divisors satisfying (ii). For almost all n every prime divisor $q > (\log\log n)^{1+\varepsilon}$ automatically satisfies (i) and (iii) (see Lemmas 3.5 and 3.6). For almost all n the number of prime divisors less than $(\log\log n)^{1+\varepsilon}$ is $O(\log\log\log\log n)$ (see [1]) and this is negligible compared to the formula given in Proposition 4.4 as Lemma 4.5 shows. □

5. Square-free numbers

In this section we characterize those square-free numbers n for which indecomposable groups of order n exist. For this description we use another graph.

Definition 5.1. Let a and b be coprime square-free numbers. We define the bipartite graph $\Delta(a,b)$ to have the prime divisors of a and b as vertices and we draw an edge $\{p,q\}$ for each pair of primes such that $p \mid a$, $q \mid b$, and $q \mid p-1$. (Note that the roles of a and b are not symmetric.)

Theorem 5.2. *Let n be a square-free number. Then there exists an indecomposable group of order n if and only if n has a divisor d such that the bipartite graph $\Delta(d,n/d)$ is connected.*

Proof. First we prove the sufficiency of the condition. So let n be a square-free number and $d \mid n$ such that $\Delta(d,n/d)$ is connected. For each prime divisor p_i of d let Q_i be the set of prime divisors of n/d connected with p_i in $\Delta(d,n/d)$, i.e., those $q \mid n/d$ for which $q \mid p_i - 1$ hold. Furthermore, let $r_i = \prod_{q\in Q_i} q$, then $r_i \mid p_i - 1$. Hence there exists a k_i such that the multiplicative order of k_i modulo p_i is r_i, i.e., r_i is the least positive integer such that $k_i^{r_i} \equiv 1 \pmod{p_i}$ holds. The Chinese Remainder Theorem yields a k with $k \equiv k_i \pmod{p_i}$ for all p_i. Now we take the metacyclic group

$$G = \langle a, b \mid a^d = 1, b^{n/d} = 1, b^{-1}ab = a^k \rangle.$$

We will show that G is indecomposable. Assume that $G = G_1 \times G_2$. If $\{p,q\}$ is an edge in $\Delta(d, n/d)$, then by our construction a Hall $\{p,q\}$-subgroup of G, $\langle a^{d/p}, b^{n/dq} \rangle$ is non-commutative, hence both p and q divide the order of the same factor G_1 or G_2. Since $\Delta(d, n/d)$ is connected, it follows that all prime divisors of n divide the order of the same factor, hence the other one is trivial, i.e., G is indecomposable, indeed.

For the converse let G be an arbitrary indecomposable group of order n. By a theorem of Zassenhaus (see [6, p. 420]) G is metacyclic of the form

$$G = \langle a, b \mid a^d = 1, b^{n/d} = 1, b^{-1}ab = a^k \rangle,$$

for some $d \mid n$ and k with $(d, k-1) = 1$. Let us define a graph Δ on the set of prime divisors of n by connecting p and q with an edge if and only if the (up to conjugation unique) Hall $\{p,q\}$-subgroup of G is non-commutative.

We claim that Δ is connected. Assuming the contrary, let $\Delta = \Delta_1 \cup \Delta_2$ be a decomposition of the vertex set into disjoint subsets such that there is no edge between the vertices of Δ_1 and Δ_2. Now let G_i $(i = 1,2)$ be a Hall Δ_i-subgroup of G. Then, for every prime divisor $p_1 \mid |G_1|$ and every prime divisor $p_2 \mid |G_2|$, a suitable Sylow p_1-subgroup in G_1 and a suitable Sylow p_2-subgroup in G_2 commute with each other, hence G_1 and G_2 commute, i.e., we obtain a direct decomposition $G = G_1 \times G_2$, contradicting the indecomposability of G. So we have shown that Δ is connected, indeed. If $\{p,q\}$ is an edge of Δ and, say, $p \mid d$, then $q \mid n/d$ and $q \mid p-1$, hence Δ is a subgraph of $\Delta(d, n/d)$. Thus the latter is also connected, as we wanted to show. □

The characterization given in Theorem 5.2 raises an algorithmic problem. For a square-free number n let us define a directed graph $\vec{\Gamma}(n)$ on the set of prime divisors of n with a directed edge (p,q) iff $q \mid p-1$. Obviously, $\vec{\Gamma}(n)$ does not contain any directed cycle, but there is no other restriction on the isomorphism type of $\vec{\Gamma}(n)$, as one can easily see by applying Dirichlet's theorem. Now if we take a divisor d of n then $\Delta(d, n/d)$ becomes the graph with the set of (undirected) edges $\vec{\Gamma}(n) \cap (\Gamma_1 \times \Gamma_2)$, where Γ_1 and Γ_2 denote the set of prime divisors of d and n/d, respectively. So our question is the following.

Problem 5.3. Let $\vec{\Gamma}$ be a directed graph without directed cycles. Can one efficiently decide whether there exists (and if exists, find) a partition $\Gamma_1 \cup \Gamma_2$ of the vertex set of $\vec{\Gamma}$ such that the bipartite graph $\vec{\Gamma} \cap (\Gamma_1 \times \Gamma_2)$ is connected?

6. The case $n = p^a q^b$

In this section we determine for which numbers of the form $n = p^a q^b$ (p, q distinct primes, a, $b \geqslant 1$) there exist indecomposable groups of order n. To formulate the result, recall that r is called the order of p modulo q if r is the least positive integer such that $p^r - 1$ is divisible by q.

Theorem 6.1. *Let p and q be distinct primes, and let r denote the order of p modulo q, and s the order of q modulo p. Then there exists a directly indecomposable group of order $p^a q^b$ (a, $b \geqslant 1$) if and only if one of the following holds:*

(i) $r = 1$,
(ii) *r is even, $a \geqslant r$,*
(iii) *$r \geqslant 3$ is odd, $a = r$ or $a \geqslant 2r$,*
and symmetrically
(i′) $s = 1$,
(ii′) *s is even, $b \geqslant s$,*
(iii′) *$s \geqslant 3$ is odd, $b = s$ or $b \geqslant 2s$.*

Proof. First we construct indecomposable groups in the cases (i), (ii), (iii).

(i) Now $r = 1$, i.e., $q \mid p - 1$. Hence $q \mid \varphi(p^a)$, so there exists a $k \not\equiv 1 \pmod{p^a}$ with $k^q \equiv 1 \pmod{p^a}$. The group $\langle x, y \mid x^{p^a} = 1, y^{q^b} = 1, y^{-1}xy = x^k \rangle$ is directly indecomposable of order $p^a q^b$ (cf. Proposition 1.1).

(ii) First let $a = r$. Then the multiplicative group of the p^r-element field contains a primitive qth root of unity α, which we consider as an automorphism of the additive group A of the field. Then we form the semidirect product $A\langle y \rangle$, where y has order q^b and acts on A as α. This group is indecomposable of order $p^r q^b$.

Next let $a = r + 1$. Since r is even, there is an extraspecial p-group P of order p^{r+1} and of exponent p. (Here we can assume $p > 2$; otherwise we have $s = 1$.) Now $|\mathrm{Aut}(P)| = |\mathrm{Sp}(r, p)| p^r (p - 1)$ is divisible by $p^r - 1$, hence P has a nontrivial automorphism α of order q. We take the semidirect product $P\langle y \rangle$ with y of order q^b acting on P as α.

Finally, if $a > r + 1$, we form the central product of the previously constructed group $P\langle y \rangle$ with a cyclic group of order p^{a-r}.

(iii) Now let $r \geqslant 3$ be odd. For $a = r$ we can do the same as in case (ii). For $a = 2r$ we can proceed similarly, using the field of p^{2r} elements. For $a = 2r + 1$ we use an extraspecial group of order p^{2r+1}, and for $a > 2r + 1$ we take its central product with a cyclic group of order p^{a-2r}.

Now we have to show that in all the remaining cases every group of order $p^a q^b$ is a proper direct product. So we have either $a < r$ or r is odd and $r < a < 2r$, and symmetrically, $b < s$ or s is odd and $s < b < 2s$.

By Burnside's Theorem (see [4, p. 131]) G is solvable. We consider chief series of G, i.e.,

$$1 = N_0 \lhd N_1 \lhd N_2 \lhd \cdots \lhd N_{n-1} \lhd N_n = G,$$

where each N_i is normal in G and the series is not refinable. By solvability of G every chief factor N_i/N_{i-1} is an elementary abelian group. We look at the action of G on N_i/N_{i-1}. Either G acts trivially, in which case we say that the chief factor N_i/N_{i-1} is *central*, or G acts as a non-trivial irreducible linear group on N_i/N_{i-1}. In the latter case let, say, N_i/N_{i-1} be a p-group. Then $G/C_G(N_i/N_{i-1})$ cannot have a non-trivial normal p-subgroup (see [4, p. 62]), hence it contains a non-trivial normal q-subgroup. Then by Clifford's theorem the dimension of N_i/N_{i-1} over the p-element field is a multiple of r. Since $a<2r$, we get $|N_i/N_{i-1}|=p^r$, and there can be at most one such chief factor in any chief series. (In this case we have, of course, $r<a<2r$, r odd.) Similarly, there is at most one non-central chief factor of q-power order, namely of order q^s.

If all chief factors are central, then G is nilpotent, so it is the direct product of its (unique) Sylow p-subgroup and Sylow q-subgroup. So assume that there is a non-central chief factor, say, N_i/N_{i-1} of order p^r. We are going to prove that G has a non-central minimal normal subgroup of order p^r, i.e., there is another chief series $1=N_0^* \lhd N_1^* \lhd \cdots$ such that $N_1^*/N_0^* \cong N_i/N_{i-1}$. If $i=1$, then there is nothing to prove, so let $i>1$. Clearly, it is enough to show the existence of a normal subgroup $N_{i-1}^* \lhd G$ with $N_{i-2} \lhd N_{i-1}^* \lhd N_i$ and $N_i/N_{i-2}=N_{i-1}/N_{i-2} \times N_{i-1}^*/N_{i-2}$. By induction we may assume $i=2$. We have to distinguish several cases.

If N_1 is central of order q then N_2 is nilpotent, so $N_2=N_1 \times N_1^*$, where N_1^* is the (unique) Sylow p-subgroup of N_2. If N_1 is a non-central chief factor of order q^s, then $C_{N_2}(N_1)$ is a normal subgroup of G containing N_1, so it is either N_1 or N_2. However, the Sylow p-subgroup of $\mathrm{Aut}(N_1) \cong \mathrm{GL}(s,q)$ is cyclic, but N_2/N_1 is not, hence only $C_{N_2}(N_1)=N_2$ is possible. Now N_2 is again nilpotent.

There remains the case when N_1 is central of order p. Now N_2 is abelian, since otherwise it would be an extraspecial p-group, contrary to $|N_2/N_1|=p^r$ with r odd (cf. [6, p. 354]). Were N_2 of exponent p^2, then $\{x \in N_2 \mid x^p=1\}$ would be a normal subgroup lying properly between N_1 and N_2 (as $r>1$), which is impossible. Hence N_2 is an elementary abelian p-group. Let $C_2=C_G(N_2/N_1) \lhd G$ and $C_1=C_G(N_2) \lhd G$. Then C_2/C_1 is a p-group of order dividing p^r. However, as $N_2 \leqslant C_1$ and $|G|=p^a q^b$ with $a<2r$, we have $|C_2/C_1|<p^r$. Hence $N_1<C_{N_2}(C_2) \lhd G$, therefore $C_{N_2}(C_2)=N_2$, so $C_2=C_1$. Now let M/C_2 be a minimal normal subgroup of G/C_2. As $\mathrm{GL}(r,p)$ has a cyclic Sylow q-subgroup, it follows that $|M/C_2|=q$. Then $N_2=C_{N_2}(M) \times [N_2,M]=N_1 \times [N_2,M]$ (see [4, p. 177]). So we have finished showing that if there is a non-central chief factor, then it is G-isomorphic to a minimal normal subgroup of G.

Now let us consider the case when there is a non-central chief factor of order p^r, but no chief factor of order q^s exists in G. Let P_0 be a minimal normal subgroup of G such that $|P_0|=p^r$. In G/P_0 every chief factor is central, hence G/P_0 is nilpotent: $G/P_0=P/P_0 \times QP_0/P_0$, where P is a Sylow p-subgroup, Q a Sylow q-subgroup of G. Hence we have $P \lhd G$ and $[P,Q]=P_0$. Now $P=C_P(Q)[P,Q]$ (see [4, p. 180]). Since P_0 is a minimal normal subgroup of G, it follows that $P_0 \leqslant Z(P)$. As $C_P(Q) \cap [P,Q]=C_{P_0}(Q)=1$, we obtain that $P=C_P(Q) \times P_0$ and $G=C_P(Q) \times P_0Q$, a proper direct decomposition since $|C_P(Q)|=|P:P_0|=p^{a-r}>1$.

If there are chief factors of order both p^r and q^s, then we can find minimal normal subgroups P_0 and Q_0 of order p^r and q^s, respectively. By the previous paragraph there are subgroups P_1 and Q_1 such that $G/Q_0 = P_1Q_0/Q_0 \times P_0Q_1Q_0/Q_0$ and $G/P_0 = Q_1P_0/P_0 \times Q_0P_1P_0/P_0$. Hence we get a direct decomposition $G = Q_0P_1 \times P_0Q_1$. □

Acknowledgements

The authors are indebted to J. Pintz and especially to M. Szalay for their valuable comments.

References

[1] P. Erdős, On the distribution of prime divisors, Aequationes Math. 2 (1969) 177–183.

[2] P. Erdős, P.P. Pálfy, Direkt szorzatra nem bontható csoportok rendjéről, Matematikai Lapok 33 (1986) 289–298.

[3] W. Feit, J.G. Thompson, Solvability of groups of odd order, Pacific J. Math. 13 (1963) 755–1029.

[4] D. Gorenstein, Finite Groups, Harper & Row, New York, 1968.

[5] H. Halberstam, H.E. Richert, Sieve Methods, Academic Press, New York, 1974.

[6] B. Huppert, Endliche Gruppen, vol. I, Springer, Berlin, 1967.

[7] G. Pazderski, Die Ordnungen, zu denen nur Gruppen mit gegebenen Eigenschaften gehören, Archiv Math. 10 (1959) 331–343.

[8] K. Prachar, Primzahlverteilung, Springer, Berlin, 1957.

[9] C. Sudler, Query #331, Notices Amer. Math. Soc. 32 (1985) 472.