CAYLEY NUMBERS WITH ARBITRARILY MANY DISTINCT PRIME FACTORS

TED DOBSON AND PABLO SPIGA

Abstract. A positive integer \( n \) is a Cayley number if every vertex-transitive graph of order \( n \) is a Cayley graph. In 1983, Dragan Marušić posed the problem of determining the Cayley numbers. In this paper we give an infinite set \( S \) of primes such that every finite product of distinct elements from \( S \) is a Cayley number. This answers a 1996 outstanding question of Brendan McKay and Cheryl Praeger, which they “believe to be the key unresolved question” on Cayley numbers. We also show that, for every finite product \( n \) of distinct elements from \( S \), every transitive group of degree \( n \) contains a semiregular element.

1. Introduction

In this paper, all groups considered are finite and all graphs and digraphs are finite and have no multiple edges or arcs. (They may have loops and they may be disconnected.) A (di)graph \( \Gamma \) is vertex-transitive if the automorphism group \( \text{Aut}(\Gamma) \) of \( \Gamma \) acts transitively on the vertices of \( \Gamma \). Let \( R \) be a group and let \( S \) be a subset of \( R \), the Cayley digraph on \( R \) with connection set \( S \), denoted \( \text{Cay}(R, S) \), is the digraph with vertex-set \( R \) and with \( (g, h) \) being an arc if and only if \( gh^{-1} \in S \). It is easy to see that \( \text{Cay}(R, S) \) is a graph if and only if \( S \) is inverse-closed, that is, \( S = \{ s^{-1} | s \in S \} \). It is also clear that the action of \( R \) on itself by right multiplication gives rise to a group of automorphisms of \( \text{Cay}(R, S) \) which is transitive on its vertex-set; thus \( \text{Cay}(R, S) \) is vertex-transitive. With a slight abuse of terminology, we say that a (di)graph \( \Gamma \) is a Cayley (di)graph if \( \Gamma \) is isomorphic to some Cayley (di)graph: it is well-known and easy to prove \cite{10} Lemma 4] that this happens if and only if \( \text{Aut}(\Gamma) \) contains a subgroup \( R \) with \( R \) transitive on the vertices of \( \Gamma \) and with the identity being the only element of \( R \) fixing some vertex of \( \Gamma \).

A positive integer \( n \) is called a Cayley number if every vertex-transitive graph of order \( n \) is a Cayley graph. In 1983, Dragan Marušić \cite{13} asked for a concrete determination of the positive integers \( n \) for which every vertex-transitive graph of order \( n \) is a Cayley graph, that is, Marušić posed the problem of determining Cayley numbers. Clearly, every prime number is a Cayley number, and 10 is not a Cayley number because the Petersen graph is not a Cayley graph.

The question of Marušić has generated a fair amount of interest, with most results giving explicit numbers that are not Cayley. In fact, it seems to be easier to provide integers that are not Cayley numbers: to show that \( n \) is not a Cayley number it suffices to exhibit one single vertex-transitive graph of order \( n \) that is...
not a Cayley graph, but to show that $n$ is a Cayley number one needs to prove that each vertex-transitive graph of order $n$ is a Cayley graph.

It is useful to observe that the integers which are not Cayley numbers, called non-Cayley numbers, are closed under multiplication, that is, if $n$ is a non-Cayley number and $m$ is a positive integer, then $nm$ is also a non-Cayley number. This is easy to see as, if $\Gamma$ is a graph of order $n$ that is not a Cayley graph, then for every positive integer $m$ the disjoint union of $m$ copies of $\Gamma$ yields a graph of order $nm$ that is also not a Cayley graph. The reader is referred to [10,13,15,17] for many examples of non-Cayley numbers and to [2,8,9,14] for work towards establishing that certain integers are Cayley numbers.

In this paper, we answer a question of Brendan McKay and Cheryl Praeger [15, Question] that they “believe to be the key unresolved question” concerning the structure of the set of Cayley numbers; namely, there exist Cayley numbers that are product of arbitrarily many distinct primes.

**Theorem 1.1.** There exists an infinite set $S$ of primes such that for every finite product $n$ of distinct elements from $S$, every vertex-transitive digraph of order $n$ is a Cayley digraph. Consequently, $n$ is a Cayley number and there exist Cayley numbers that are a product of arbitrarily many distinct primes.

The proof of Theorem 1.1 follows from Theorem 1.2, which we believe to be of independent interest. (A transitive permutation group $G$ is quasiprimitive if every non-identity normal subgroup of $G$ is transitive.)

**Theorem 1.2.** There exists an infinite set of primes $S$ such that, for every finite product $n$ of distinct elements from $S$ with $n$ not prime, the only quasiprimitive groups of degree $n$ are the alternating and the symmetric groups.

Theorem 1.2 combined with [6, Theorem 4.7] gives the following interesting corollary.

**Corollary 1.3.** There exists an infinite set of primes $S$ such that, for every finite product $n$ of distinct elements from $S$, every transitive group of degree $n$ contains a transitive solvable subgroup.

These results can be used to obtain a new contribution to elusive groups, see Corollary 4.5.

1.1. **Structure of the paper.** In Section 2 we collect our main tools, namely, a number theoretic result and a few group theoretic lemmas. We then prove Theorems 1.1 and 1.2 and Corollary 1.3 in Section 3. We conclude the paper with some comments and problems in Section 4.

2. **Basics**

2.1. **Number theory.** We start by proving a number theoretic lemma, which depends on Dirichlet’s Theorem on primes in arithmetic progressions and on the Prime Number Theorem. (We denote by $\phi(m)$ the Euler’s totient function.)

**Lemma 2.1.** There exists an infinite set $S$ of prime numbers such that, for each $\kappa \in \mathbb{N}$ and for each $p_1, \ldots, p_\kappa \in S$ with $p_1 < p_2 < \cdots < p_\kappa$, we have

(i): $(p_1 p_2 \cdots p_\kappa - 1)^4 < p_\kappa,
(ii): \gcd(p_i, p_j - 1) = 1$ for every $i, j \in \{1, \ldots, \kappa\}$,
(iii): the product $p_1p_2\cdots p_\kappa$ is not equal to $\frac{q^d-1}{q-1}$, for any prime power $q$ and any $d \geq 1$.

Proof. We construct the set $S$ inductively: we show that there exists an infinite family of sets of prime numbers $\{S_\ell\}_{\ell \in \mathbb{N}\setminus\{0\}}$ such that, for every $\ell \in \mathbb{N}\setminus\{0\}$:

(a) $|S_\ell| = \ell$,
(b) $S_\ell \subseteq S_{\ell+1}$,
(c) for each $\kappa \in \{1, \ldots, \ell\}$ and for each $p_1, \ldots, p_\kappa \in S_\ell$ with $p_1 < p_2 < \cdots < p_\kappa$, the primes $p_1, \ldots, p_\kappa$ satisfy the conditions (i), (ii) and (iii).

Then the proof follows immediately by taking $S := \bigcup_{\ell \in \mathbb{N}\setminus\{0\}} S_\ell$.

Define $S_1 := \{11\}$ and observe that 11 is not of the form $(q^d-1)/(q-1)$, for any prime power $q$ and any $d \geq 1$. Now, suppose that $\ell \in \mathbb{N}\setminus\{0\}$, and that $S_\ell = \{p_1, \ldots, p_\ell\}$ has been defined. We construct $S_{\ell+1}$ by carefully choosing a suitable prime $p_{\ell+1}$ and by setting $S_{\ell+1} := S_\ell \cup \{p_{\ell+1}\}$.

Set $m := p_1 \cdots p_\ell$. For $N \in \mathbb{N}\setminus\{0\}$, define

\[ T_N := \{x \in \mathbb{N} \mid x > m^4, x \text{ prime, } x \leq N \text{ and } x \equiv -1 \pmod{m}\}, \]
\[ S_N := \left\{ x = \frac{q^d-1}{q-1} \mid \text{for some prime power } q \text{ and some } d \geq 1, x \text{ odd, } x \leq mN \right\}. \]

We claim that

\begin{equation}
|T_N| \sim \frac{N}{\phi(m) \log(N)}.
\end{equation}

(Here, given a set $X$ we denote by $|X|$ its cardinality, moreover, by abuse of notation, we let $|T_N|$ denote the function in the variable $N$ given by $N \mapsto |T_N|$. Finally, $\sim$ denotes Landau’s notation for two asymptotic functions in the variable $N$.) Write

\[ T'_N := \{x \in \mathbb{N} \mid x \text{ prime, } x \leq N \text{ and } x \equiv -1 \pmod{m}\}. \]

As there are at most $m^4$ primes less than or equal to $m^4$, we get $|T'_N| \geq |T_N| - m^4$. From [18, Part II, §4, Theorem 2] and the Prime Number Theorem, we have

\[ \lim_{N \to \infty} \frac{|T'_N|}{N/(\phi(m) \log(N))} = 1 \]

and Eq. (2.1) is proven.

We claim that

\begin{equation}
|S_N| \leq (1 + \log_2(mN)) \sqrt{mN} + \log_2(mN) + 1.
\end{equation}

Let $x \in S_N$ with $x = (q^d-1)/(q-1)$ for some prime power $q$ and some $d \geq 1$. Now, $q^{d-1} \leq (q^d-1)/(q-1) = x \leq mN$ and hence $d-1 = \log_q(q^{d-1}) \leq \log_q(mN) \leq \log_2(mN)$. It follows that $d \leq 1 + \log_2(mN)$, that is, we have at most $1 + \log_2(mN)$ choices for $d$.

When $d \geq 3$, from $q^{d-1} \leq mN$, we get $q \leq (mN)^{1/2}$ and hence we have at most $(mN)^{1/2}$ choices for $q$. This shows that we have at most $(1 + \log_2(mN))(mN)^{1/2}$ choices for $x$ when $d \geq 3$: this accounts for the first summand in the right-hand-side of Eq. (2.2). Suppose that $d = 2$. Then $x = q + 1$ is odd and hence $q = 2^t$, for some $t \geq 1$. Now, $2^t < x \leq mN$ and hence $t \leq \log_2(mN)$. Thus we have at most $\log_2(mN)$ choices for $x$ in this case. Clearly, we have only one element when $d = 1$.

Using Landau’s notation, Eq. (2.2) yields

\begin{equation}
|S_N| \in o\left(\frac{N}{(\phi(m) \log(N))}\right).
\end{equation}
Let $N_\ell$ be the smallest positive integer with $0 < |S_{N_\ell}| < |T_{N_\ell}|$ and observe that $N_\ell$ is well-defined from Eqs. (2.3) and (2.1).

Observe that every element $x \in T_{N_\ell}$ is prime and, together with $p_1, \ldots, p_\ell$, satisfies (i) and (ii). In fact, if $x \in T_{N_\ell}$, then $x > m^4$ and $x \equiv -1 \pmod{m}$.

Hence, for every $i \in \{1, \ldots, \ell\}$, $x \equiv -1 \pmod{p_i}$ and so $\gcd(x, p_i - 1) = 1$. Suppose that, for every $y \in T_{N_\ell}$, the set $\{p_1, \ldots, p_\ell, y\}$ fails to satisfy (iii). Then, for every $y \in T_{N_\ell}$, there exist $i_1, \ldots, i_\ell \in \{1, \ldots, \ell\}$ with

$$p_{i_1} \cdots p_{i_\ell} \cdot y = \frac{q^d - 1}{q - 1},$$

for some prime power $q$ and some $d \geq 1$. Now,

$$p_{i_1} \cdots p_{i_\ell} \cdot y \leq p_1 \cdots p_\ell \cdot y = my \leq mN_\ell$$

and $p_{i_1} \cdots p_{i_\ell} \cdot y \in S_{N_\ell}$. Therefore $|S_{N_\ell}| \geq |T_{N_\ell}|$, which is a contradiction. Thus there exists $p_{\ell+1} \in T_{N_\ell}$ such that $\{p_1, \ldots, p_\ell, p_{\ell+1}\}$ satisfies (i), (ii) and (iii). \hfill \Box

2.2. Group theory. Let $G$ be a transitive permutation group on a set $X$, and let $B \subseteq X$ with $B \neq \emptyset$. We say $B$ is a block for $G$ if $B^g = B$ or $B^g \cap B = \emptyset$ for every $g \in G$. The whole set $X$ and the singleton sets $\{x\}$ are always blocks for $G$ and so are called trivial blocks. If $G$ has a non-trivial block, then $G$ is imprimitive, and primitive otherwise. If $B$ is a block for $G$, then $\{B^g \mid g \in G\}$ is a $G$-invariant partition of $X$ or system of imprimitivity for $G$.

In the following lemma we use a result of Liebeck and Saxl \cite{11} Corollary 1]: this was one of the first cases where the classification of the finite simple groups had made possible the solution of an outstanding classical problem in the theory of permutation groups. Namely, the classification of the primitive groups of degree $mp$ with $p$ prime and $m < p$. (Here $\text{soc}(G)$ denotes the socle of the group $G$.)

**Lemma 2.2.** Let $G$ be a primitive permutation group of degree $n$ with $n$ not prime and let $p$ be the largest prime divisor of $n$. Then one of the following holds:

(i): $p < (n/p)^4$;

(ii): $\text{soc}(G) = \text{PSL}(d, q)$, $n = \frac{q^d - 1}{q - 1}$ and $G$ is endowed with one of its natural 2-transitive actions;

(iii): $\text{soc}(G) = A_n$ and $G$ is endowed with its natural 2-transitive action.

**Proof.** We suppose that $p \geq (n/p)^4$. Observe that $p \geq n^{4/5} > n^{1/2}$ because $n > 1$. In particular, $n = mp$ with $1 < m < p$ and hence the work of Liebeck and Saxl \cite{11} applies.

Let $T$ be the socle of $G$. Now, $T$, $n$ and some information on $p$ are given in the first, second and fourth columns of \cite{11} Table 3. We assume that Cases (ii) and (iii) do not occur. With a careful case-by-case examination of each of the remaining lines of \cite{11} Table 3 we obtain that no primitive group may arise: all computations are straightforward and here, to give an idea of the proof, we deal only with the fifth row of \cite{11} Table 3 (all other rows are similar).

We have $S = \text{PSL}(d, q)$, $d \geq 4$, $n = \frac{q^d - 1}{q - 1}$ and $p \geq \frac{q^{d-1} - 1}{(q^2 - 1)(q - 1)}$ or $p$ divides $\frac{q^d - 1}{(q - 1)}$. If $p = \frac{q^{d-1} - 1}{(q - 1)}$, we have $p < (n/p)^4$, and hence $p$ must divide $\frac{q^d - 1}{(q - 1)}$. In particular,

$$\left(\frac{q^{d-1} - 1}{q^2 - 1}\right)^4 \leq \left(\frac{n}{p}\right)^4 \leq \frac{q^d - 1}{q - 1}.$$
However, this inequality is never satisfied when \( d \geq 4 \).

In Lemma 2.2 the reader should not take too seriously the exponent 4 in \( p < (n/p)^4 \). With more effort, one can prove a similar lemma with a smaller exponent; however, for the scope of this paper we content ourselves with our weaker statement.

**Lemma 2.3.** Let \( S \) be as in Lemma 2.1 and let \( n \) be a finite product of distinct elements from \( S \) with \( n \) not prime. Then the only primitive groups of degree \( n \) are \( A_n \) and \( S_n \).

**Proof.** Let \( G \) be a primitive group of degree \( n \) and let \( S \) be its socle. Recall that the largest prime divisor \( p \) of \( n \) satisfies \( (n/p)^4 < p \) (from Lemma 2.1 (i)) and that \( n \) is not of the form \((q^d - 1)/(q - 1)\), for any prime power \( q \) and any \( d \geq 1 \) (from Lemma 2.1 (iii)). Then \( S = A_n \) by Lemma 2.2. \( \square \)

### 3. PROOF OF THEOREMS 1.1 AND 1.2 AND COROLLARY 1.3

Every primitive group is quasiprimitive, however there are imprimitive groups that are quasiprimitive: for example the automorphism group of the line graph of the Petersen graph. For the proof of Theorem 1.2 we are only interested in quasiprimitive groups \( G \) that are almost simple. In this case, \( G \) is quasiprimitive if the socle of \( G \) is transitive.

**Proof of Theorem 1.2.** Let \( S \) be as in Lemma 2.1 let \( n \) be a finite product of distinct elements from \( S \) with \( n \) not prime and let \( G \) be a quasiprimitive group of degree \( n \). By Lemma 2.3 the only primitive groups of degree \( n \) are \( A_n \) or \( S_n \). We argue by contradiction and we suppose that \( G \not\sim A_n \). In particular, \( G \) is imprimitive. Let \( B \) be a non-trivial system of imprimitivity for \( G \) with blocks of maximal size and let \( H \) be the permutation group induced by \( G \) in its action on \( B \). Set \( r := |B| \). Observe that \( H \) is primitive by our choice of \( B \).

As \( n \) is square-free, we see that \( G \) is almost simple (see for example [10]) and hence \( H \cong G \).

As \( H \) is primitive of degree \( r \) and \( r \) is a finite product of distinct elements from \( S \), we get that either \( r \) is prime, or \( H \in \{ A_r, S_r \} \) by Lemma 2.3. Suppose that \( H \not\in \{ A_r, S_r \} \). Since \( r \) is not of the form \((q^d - 1)/(q - 1)\), for any prime power \( q \) and any \( d \geq 1 \), from [7, Theorem 1.49] we obtain \( r = 11 \) and \( H = PSL(2, 11) \), or \( r = 23 \) and \( H = M_{23} \). In both cases, \( r \) is the largest prime divisor of \(|H| = |G| \) and hence \( r > (n/r)^4 \). A direct inspection on \(|H| \) and \( n \) shows that this is impossible. Thus \( H \in \{ A_r, S_r \} \) and the action of \( H \) on \( B \) is the natural action of \( A_r \) or \( S_r \).

From Lemma 2.1 there exists a prime divisor \( p \) of \( n \) with \( p > (n/p)^4 \). Let \( B \in B \), let \( b \in B \), and denote by \( G_{(B)} \) the setwise stabiliser of \( B \) in \( G \) and by \( G_b \) the stabiliser of the point \( b \). As \( G \cong H \in \{ A_r, S_r \} \) and as \( n \mid |G| \), we obtain that \( p \mid r! \) and hence \( p \leq r \). If \( p \nmid r \), then \( p > (n/p)^4 \geq r^4 \geq p^4 \), a contradiction. Thus \( p \mid r \) and hence \( r > (n/r)^4 \).

From above, \(|G : G_{(B)}| = r, |G_{(B)} : G_b| = n/r \) and \( G_{(B)} \in \{ A_{r-1}, S_{r-1} \} \). In particular, we have \( n/r = |G_{(B)} : G_b| \geq r - 1 \). Thus \( r > (n/r)^4 \geq (r - 1)^4 \), a contradiction. \( \square \)

**Proof of Corollary 1.3.** Let \( S \) be as in Lemma 2.1 and let \( n \) be a finite product of distinct elements from \( S \). From Lemma 2.1 we have \( \gcd(n, \phi(n)) = 1 \). Now, if \( n \) is prime, then every transitive group of degree \( n \) contains a cyclic transitive
subgroup. If $n$ is not prime, the proof follows immediately combining Theorem 1.2 and [6, Theorem 4.7] and using $\gcd(n, \phi(n)) = 1$. □

Proof of Theorem 1.1 Let $S$ be as in Corollary 1.3. Now, for every finite product $n$ of distinct elements from $S$, we have $\gcd(n, \phi(n)) = 1$ and the only quasiprimitive groups of degree $n$ are $A_n$ and $S_n$. Now [6, Corollary 4.10] immediately gives that every vertex-transitive digraph of order $n$ is a Cayley digraph. □

4. Comments

Theorem 1.1 finally proves that the arithmetic structure of some Cayley numbers is much more rich than the cases that have been investigated so far. It is now interesting, in our opinion, to estimate the density of Cayley numbers. It is fairly straightforward using the group theoretic and the number theoretic results already available in the literature to prove that Cayley numbers have density zero in the natural numbers, that is,

$$\lim_{n \to \infty} \frac{|\{m \in \mathbb{N} \mid m \text{ Cayley number}, m \leq n\}|}{n} = 0.$$ 

Therefore we pose the following problem.

Problem 4.1. Determine the rate of growth of the function

$$n \mapsto |\{m \in \mathbb{N} \mid m \text{ Cayley number}, m \leq n\}|.$$ 

To see the importance of Corollary 1.3 we need a term introduced by Hassani, Iranmanesh and Praeger [8] in a paper on Cayley numbers.

Let $G$ be transitive of degree $n$. If $B$ and $C$ are systems of imprimitivity for $G$ and every block of $C$ is a union of blocks of $B$, we write $B \preceq C$ (and $B \prec C$ when $B \neq C$). Let $n = p_1^{a_1}p_2^{a_2}\cdots p_r^{a_r}$ be the prime factorisation of $n$ and define $\Omega : \mathbb{N} \setminus \{0\} \mapsto \mathbb{N}$ by $\Omega(n) = \sum_{i=1}^{r} a_i$ (thus $\Omega(n)$ is the number of prime divisors of $n$). We say $G$ is $\Omega(n)$-step imprimitive if there exists a sequence of systems of imprimitivity $B_0 \prec B_1 \prec \cdots \prec B_{\Omega(n)}$ for $G$. Observe that, if $B_{i+1} \subset B_i$ and $B_i \in B_i$, then $|B_{i+1}|/|B_i|$ is prime for every $i \in \{1, \ldots, m-1\}$, and that $B_0$ and $B_{\Omega(n)}$ are the trivial systems of imprimitivity. If, in addition, each $B_i$ is formed by the orbits of a normal subgroup of $G$, we say that $G$ is normally $\Omega(n)$-step imprimitive.

Theorem 4.2 ([4, Theorem 1.9]). A transitive group of square-free degree $n$ contains a normally $\Omega(n)$-step imprimitive subgroup if and only if it contains a transitive solvable subgroup.

Hassani, Iranmanesh and Praeger [8, Theorem 1.1] showed that a vertex-transitive graph of order $pqr$, where $p$, $q$, and $r$ are distinct primes satisfying some additional arithmetic conditions, is a Cayley graph provided its automorphism group contains a normally 3-step imprimitive subgroup (and hence a transitive solvable subgroup in view of Theorem 4.2). The first author proved a similar result: a vertex-transitive graph of order $n$, with $\gcd(n, \phi(n)) = 1$ or with $\gcd(n, \phi(n)) = q$ where $q$ is a prime such that $q^2 \nmid (p - 1)$ for every prime $p \mid (n/q)$, is isomorphic to a Cayley graph if and only if its automorphism group contains a transitive solvable subgroup (or equivalently, is normally $\Omega(n)$-step imprimitive); see [3, 4]. It is also known that any group of square-free order is solvable. Thus the set $T$ of square-free integers for which every 2-closed transitive group of degree $n \in T$ contains a transitive solvable
subgroup is related to the set of square-free Cayley numbers, and if additional arithmetic conditions are imposed on the integers \( n \in T \), the property of any 2-closed permutation group of degree \( n \) containing a transitive solvable subgroup implies \( n \) is a Cayley number. Thus the following problem is a natural one.

**Problem 4.3.** Determine the square-free integers \( n \) with the property that every 2-closed transitive group of degree \( n \) contains a transitive solvable subgroup.

We observe that it is not the case that if \( n \) is a Cayley number then every transitive group of degree \( n \) contains a transitive solvable subgroup. Indeed, 14 is a Cayley number (see [14, Table 1]), but \( \text{PSL}(3,2) \) has a transitive permutation representation of degree 14 containing no transitive solvable subgroup. Thus, we would like to pose another problem.

**Problem 4.4.** Determine the square-free integers \( n \) with the property that every transitive group of degree \( n \) contains a transitive solvable subgroup.

There is one more problem to which our work supplies a partial solution: the problem of finding elusive groups. This problem originated with a conjecture of Marušić: he conjectured that the automorphism group of every vertex-transitive graph contains a semiregular element [12] Problem 2.4. Klin generalised this conjecture to the conjecture that all 2-closed groups contain a semiregular element [1] Problem BCC15.12. Since heuristically most transitive groups contain semiregular elements, a transitive group which does not contain a semiregular element is called elusive. While it is already known that every 2-closed group of square-free degree contains a semiregular element [5], it is not known in general if every transitive group of square-free degree is elusive. Much is known on this topic, see [2] for a list of partial results as well as for undefined terminology. Combining Theorem 1.2 and [6, Corollary 4.9] we have the following result.

**Corollary 4.5.** Let \( S \) be as in Lemma 2.21 and let \( n \) be a finite product of distinct elements from \( S \). Then no permutation group of degree \( n \) is elusive.

**References**

[1] P. J. Cameron, Problems from the Seventeenth British Combinatorial Conference, *Discrete Math.* 167/168 (1997), 605–615.

[2] E. Dobson, Classification of vertex-transitive graphs of order a prime cubed. I, *Discrete Math.* 224 (2000), no. 1–3, 99–106.

[3] E. Dobson, On solvable groups and circulant graphs, *European J. Combin.* 21 (2000), no. 7, 881–885.

[4] E. Dobson, On solvable groups and Cayley graphs, *J. Combin. Theory Ser. B* 98 (2008), no. 6, 1193–1214.

[5] E. Dobson, A. Malnič, D. Marušić, L. A. Nowitz, Minimal normal subgroups of transitive permutation groups of square-free degree, *Discrete Math.* 307 (2007), no. 3–5, 373–385.

[6] E. Dobson, D. Marušić, On semiregular elements of solvable groups, *Comm. Algebra* 39 (2011), no. 4, 1413–1426.

[7] D. Gorenstein, *Finite simple groups*, University Series in Mathematics, Plenum Publishing Corp., New York, 1982.

[8] A. Hassani, M. A. Iranmanesh, C. E. Praeger, On vertex-imprimitive graphs of order a product of three distinct odd primes, *J. Combin. Math. Combin. Comput.* 28 (1998), 187–213.

[9] M. A. Iranmanesh, C. E. Praeger, On non-Cayley vertex-transitive graphs of order a product of three primes, *J. Combin. Theory Ser. B* 81 (2001), no. 1, 1–19.

[10] C. H. Li, A. Seress, On vertex-transitive non-Cayley graphs of square-free order, *Des. Codes Cryptogr.* 34 (2005), no. 2–3, 265–281.
[11] M. W. Liebeck, J. Saxl, Primitive permutation groups containing an element of large prime order, J. London Math. Soc. (2) 31 (1985), no. 2, 237–249.
[12] D. Marušič, On vertex symmetric digraphs, Discrete Math. 36 (1981), no. 1, 69–81.
[13] D. Marušič, Cayley properties of vertex symmetric graphs, Ars Combin. 16 (1983), 297–302.
[14] B. D. McKay, C. E. Praeger, Vertex-transitive graphs which are not Cayley graphs. I, J. Austral. Math. Soc. Ser. A 56 (1994), no. 1, 53–63.
[15] B. D. McKay, C. E. Praeger, Vertex-transitive graphs that are not Cayley graphs. II, J. Graph Theory 22 (1996), no. 4, 321–334.
[16] G. Sabidussi, On a class of fixed-point-free graphs, Proc. Amer. Math. Soc., 9 (1958), 800–804.
[17] Á. Seress, On vertex-transitive, non-Cayley graphs of order \( pqr \), Discrete Math. 182 (1998), no. 1-3, 279–292.
[18] J-P. Serre, A course in arithmetic, Springer-Verlag, New York, 1973.

Ted Dobson, Mississippi State University,
PO Drawer MA, Mississippi State, MS 39762, USA, and
University of Primorska, IAM, Muzejska trg 2, 6000 Koper, Slovenia
E-mail address: dobson@math.msstate.edu

Pablo Spiga, Dipartimento di Matematica Pura e Applicata,
University of Milano-Bicocca, Via Cozzi 55, 20126 Milano, Italy.
E-mail address: pablo.spiga@unimib.it