CORRIGENDUM TO "PATHS AND CIRCUITS IN FINITE GROUPS", DISCR. MATH. 22 (1978) 263

MAXIMILIAN F. HASLER AND RICHARD J. MATHAR

Abstract. We remove 52 from the set of prime partitionable numbers in a paper by Holsztyński and Strube (1978), which also appears in a paper by Erdős and Trotter in the same year. We establish equivalence between two different definitions in the two papers, and further equivalence to the set of Erdős-Woods numbers.

1. The paper by Holsztyński and Strube

In their paper about paths and circuits in finite groups, Holsztyński and Strube define prime partitionable numbers as follows [5, Defn. 5.3]:

Definition 1. *An integer n is said to be prime partitionable if there is a partition $\{\mathbb{P}_1, \mathbb{P}_2\}$ of the set of all primes less than n such that, for all natural numbers n_1 and n_2 satisfying $n_1 + n_2 = n$, we have $\gcd(n_1, p_1) > 1$ or $\gcd(n_2, p_2) > 1$, for some $(p_1, p_2) \in \mathbb{P}_1 \times \mathbb{P}_2$.*

Remark 1. *According to this definition, only integers $n \geq 4$ can be prime partitionable, because one cannot have a partition $\{\mathbb{P}_1, \mathbb{P}_2\}$ of the primes less than 3, since there is only one. The condition involving the greatest common divisors (GCD's) can also be written as "$p_1 \mid n_1$ or $p_2 \mid n_2$", since the GCD is necessarily equal to the prime if it is larger than 1.*

Example 1. *The smallest prime partitionable number is 16. The set of primes less than 16 is $\mathbb{P} = \{2, 3, 5, 7, 11, 13\}$. There are two partitions $\mathbb{P} = \{\mathbb{P}_1, \mathbb{P}_2\}$ that demonstrate that 16 is prime partitionable, these are*

$$\{\mathbb{P}_1 = \{2, 5, 11\},\ \mathbb{P}_2 = \{3, 7, 13\}\} \tag{1}$$

and

$$\{\mathbb{P}_1 = \{2, 3, 7, 13\}, \mathbb{P}_2 = \{5, 11\}\}\ . \tag{2}$$

Following Definition 1, the authors give the following (wrong!) list of prime partitionable numbers,

$$\{16, 22, 34, 36, 46, 52, 56, 64, 66, 70, ...\} \tag{3}$$

which erroneously includes the 52.

The paper by Holsztyński and Strube is cited, and the wrong list (3) is explicitly reprinted, in a paper of Trotter and Erdős [7], where they show that the Cartesian product of two directed cycles of respective lengths n_1 and n_2 is hamiltonian iff the

Date: October 28, 2015.
2010 *Mathematics Subject Classification.* Primary 11P70; Secondary 05C45.
Key words and phrases. Errata, prime partitionable, paths, circuits, cycles, hamiltonian.

GCD of the lengths is $d \geq 2$ and can be written as sum $d = d_1 + d_2$, where the d_i are coprime to the respective lengths.

Using two independent computer programs written in Maple and PARI/GP we verified that the list of prime partitionable numbers according to Definition 1 should rather be equal to

$$\{16, 22, 34, 36, 46, 56, 64, 66, 70, 76, 78, 86, 88, 92, 94, 96, 100, ...\} . \tag{4}$$

(With contemporary computer power it is easier to inspect all possible 2-partitions of the prime sets beyond what could be done at the time of publication of the original paper.)

Remark 2. *If n is prime partitionable with a representation $n = q^l + n_2$ where q^l is a prime power with $l \geq 1$, then at least one of the prime factors of n_2 is in the same set $\mathbb{P}_j$ as q. [Proof: If q is in $\mathbb{P}_1$, then $n = q^l + n_2$ is supported by $\gcd(n_1, q) > 1$ on $\mathbb{P}_1$. The commuted $n = n_2 + q^l$ is obviously not supported on $\mathbb{P}_2$ because q is not member of $\mathbb{P}_2$, so it must be supported via $\gcd(n_2, p_1) > 1$ through a prime member p_1 on $\mathbb{P}_1$; so n_2 must have a common prime factor with an element of $\mathbb{P}_1$. Alternatively, if q is in $\mathbb{P}_2$, n_2 must have a common prime factor with an element of $\mathbb{P}_2$. In both cases, one of the prime factors of n_2 is in the same partition $\mathbb{P}_j$ as q.]*

Remark 3. *As a special case of Remark 2, if n is prime partitionable and $n = q_1 + q_2$ with q_1 and q_2 both prime, then q_1 and q_2 are either both in $\mathbb{P}_1$ or both in $\mathbb{P}_2$.*

Remark 4. *As a corollary to Remark 2, if n is one plus a prime power, n is not prime partitionable.*

Remark 5. *If n is prime partitionable with a representation $n = 1 + q_1^{e_1} q_2^{e_2}$, one plus an integer with two distinct prime factors, then the two prime factos q_1 and q_2 are not in the same $\mathbb{P}_j$. The proof is elementary along the lines of Remark 2. $n = 106 = 1 + 3 \times 5 \times 7$ and $n = 196 = 1 + 3 \times 5 \times 13$ are the smallest prime partitionable numbers not of that form.*

We see that 52 is not prime partitionable given the following contradiction:

- $52 = 5^2 + 3^3$ which forces 3 and 5 into the same $\mathbb{P}_j$ according to Remark 2: $\mathbb{P}_j = \{3, 5, \ldots\}$.
- $52 = 3 + 7^2$ which forces 3 and 7 into the same $\mathbb{P}_j$ according to Remark 2: $\mathbb{P}_j = \{3, 5, 7, \ldots\}$.
- $52 = 17 + 5 \times 7$ which requires that 5 or 7—which are already in the same $\mathbb{P}_j$—are in the same $\mathbb{P}_j$ as 17 according to Remark 2: $\mathbb{P}_j = \{3, 5, 7, 17, \ldots\}$.
- $52 = 1 + 3 \times 17$ which requires that 3 and 17 are in distinct sets according to Remark 5.

In overview, we establish the equivalence between the set of prime partitionable numbers of Definition 1 and two other sets, the prime partitionable numbers of Trotter and Erdős (Section 2) and the Erdős–Woods numbers (Section 3).

2. The Paper by Trotter and Erdős

2.1. **The Trotter–Erdős definition.** Although the authors of [7] cite the—at that time unpublished—work of Holsztyński and Strube [5], they give the following seemingly different definition of "prime partitionable:"

Definition 2. *An integer d is prime partitionable if there exist n_1, n_2 with $d = \gcd(n_1, n_2)$ so that for every $d_1, d_2 > 0$ with $d_1 + d_2 = d$ either $\gcd(n_1, d_1) \neq 1$ or $\gcd(n_2, d_2) \neq 1$.*

Example 2. *$d = 16 = 2^4$ is prime partitionable according to Definition 2 based for example on $n_1 = 880 = 2^4 \times 5 \times 11$ and $n_2 = 4368 = 2^4 \times 3 \times 7 \times 13$.*

According to this definition, any integer $d < 2$ is "vacuosly" prime partitionable since there are no representations $d = d_1 + d_2$ with $d_1, d_2 > 0$. So we tacitly understand $d > 1$ in Definition 2 when we talk about equivalence with Definition 1.

It is easy to see that a "witness pair" n_1 and n_2 in Definition 2 has the following properties:

- (P1) $d = \gcd(n_1, n_2)$ implies factorizations $n_1 = dk_1$, $n_2 = dk_2$ with $\gcd(k_1, k_2) = 1$. We still may have $\gcd(d, k_1) > 1$ or $\gcd(d, k_2) > 1$.
- (P2) One can construct derived "witness pairs" where n_2 is replaced by $n_2' = dk_2'$, where k_2' is the product of all primes less than d that do not divide n_1. [Keeping k_2' coprime to n_1 ensures that $\gcd(n_1, n_2')$ still equals d. The construction also ensures that the prime factor set of n_2' is a superset of the prime factor set of n_2, so the d_2 in Definition 2 which need a common prime factor with n_2 still find that common prime factor with n_2'.] n_1 may be substituted in the same manner.
- (P3) One can reduce a witness pair by striking prime powers in k_1 and k_2 until k_1 and k_2 are square-free, coprime to d, and contain only prime factors less than d.
- (P4) The integer dk_1k_2 does *not* need to have a prime factor set that contains all primes $\leq d$. (Example: $d = 46 = 2 \times 23$ is prime partitionable established by $k_1 = 3 \times 19 \times 37 \times 43$ and $k_2 = 5 \times 7 \times 11 \times 13 \times 17 \times 29 \times 41$, where the prime 31 is not in the prime factor set of dk_1k_2). The missing prime factors may be distributed across the n_1 and n_2 (effectively multiplying k_1 or k_2 but not both with a missing prime) to generate "fatter" prime witnesses. [$\gcd(n_1, n_2)$ does not change if either n_1 or n_2 is multiplied with absent primes. Furthermore the enrichment of the prime factor sets of the n_j cannot reduce the common prime factors in $\gcd(d_j, n_j)$. So the witness status is preserved.]
- (P5) Prime factors of n_1 or n_2 larger than d have no impact on the conditions $\gcd(n_j, d_j) \neq 1$ and can as well be removed from n_j without compromising the witness status.

2.2. **Equivalence With The Holsztyński–Strube Definition.**

Lemma 1. *If a number is prime partitionable according to Definition 1 it is prime partitionable according to Definition 2.*

Proof. Assume that a partition $\{\mathbb{P}_1, \mathbb{P}_2\}$ establishes that d is prime partitionable according to Definition 1. Let k_j be the product of all $p \in \mathbb{P}_j$ which do not divide d. Then the pair $n_1 = dk_1$, $n_2 = dk_2$ satisfies the condition of Definition 2. [Because the k_j and d are coprime, $d = \gcd(n_1, n_2)$. The prime factor sets of n_j are supersets of $\mathbb{P}_j$, so the d_j find matching prime factors according Definition 1.] □

Lemma 2. *If a number is prime partitionable according to Definition 2 it is prime partitionable according to Definition 1.*

Proof. Assume that n_1, n_2 is a witness pair conditioned as in Definition 2, propped up with with the aid of (P4) if the union of their prime sets is incomplete. Then let $\mathbb{P}_1$ contain all prime factors of n_1 smaller than d and let $\mathbb{P}_2$ contain the prime factors of n_2/d smaller than d: This yields a partition $(\mathbb{P}_1, \mathbb{P}_2)$ with the properties of Definition 1. Because we have (asymmetrically) assigned all the prime factors of n_1 to $\mathbb{P}_1$, the decompositions of d where $\gcd(d_1, n_1) > 1$ find the associated p_1 in Definition 1. The nontrivial part is to show that if $\gcd(d_1, n_1) = 1$ and therefore $\gcd(d_2, n_2) > 1$, then $\gcd(d_2, p_2) > 1$ for some $p_2 \in \mathbb{P}_2$. Observe that a prime factor p_2 of $\gcd(d_2, n_2)$—known to exist for $\gcd(d_2, n_2) > 1$—cannot divide k_1 (coprime to n_2); it cannot divide d either, else it would also divide $d - d_2 = d_1$ and thus divide $\gcd(d_1, n_1) = \gcd(d_1, dk_1)$, contradicting the assumption on the $\gcd(d_1, n_1)$. So p_2 cannot divide the product $k_1 d = n_1$ and therefore p_2 is in $\mathbb{P}_2$. □

We have shown in the two lemmas above that the two sets of prime partitionable numbers are mutually subsets of each other; therefore they are equal:

Theorem 1. *An integer $d > 3$ is prime partitionable in the sense of Definition 1 iff it is prime partitionable in the sense of Definition 2.*

Remark 6. *This also implies that if a number is* not *prime partitionable according to one of the definitions, it neither is according to the other.*

This proof establishes a bijection, for any given $d > 3$, between (i) 2-partitions of the primes less than d and (ii) pairs (n_1, n_2) with the properties that $d = \gcd(n_1, n_2)$, $k_1 = n_1/d$ and $k_2 = n_2/d$ square-free and coprime to d and without prime factors $> d$.

3. Erdős–Woods numbers

This is the definition given for sequence A059756 of the OEIS [3], entitled "Erdős–Woods numbers:"

Definition 3. *An Erdős–Woods number is a positive integer $w = e_2 - e_1$ which is the length of an interval of consecutive integers $[e_1, e_2] = \{k \in \mathbb{N} \mid e_1 \le k \le e_2\}$ such that every element k has a factor in common with one of the end points, e_1 or e_2.*

Example 3. *The smallest, $w = 16$, refers to the interval $[2184, 2185, ..., 2200]$; others are listed in* [3, A194585]. *The end points are $e_1 = 2184 = 2^3 \times 3 \times 7 \times 13$ and $e_2 = 2200 = 2^3 \times 5^2 \times 11$, and each number $2184 \le k \le 2200$ has at least one prime factor in the set $\{2, 3, 5, 7, 11, 13\}$.*

Woods was the first to consider this definition [8], Dowe proved that there are infinitely many [2] and Cegielski, Heroult and Richard have shown that the set is recursive [1].

Lemma 3. *An Erdős–Woods number is prime partitionable according to Definition 1.*

Proof. Place all prime factors of e_1 into a set $\mathbb{P}_1$ and all prime factors of e_2 that are not yet in $\mathbb{P}_1$ into $\mathbb{P}_2$. This guarantees that the two $\mathbb{P}_j$ do not overlap. Place any primes $< w$ that are missing in one of the $\mathbb{P}_j$. Taking $n_1 = k - e_1$, $n_2 = e_2 - k$, each k defines 1-to-1 a partition $w = n_1 + n_2$. If k has a common prime factor with e_1, say p_1, then $p_1 \in \mathbb{P}_1$ and then n_1 has a non-trivial integer factorization

$n_1 = p_1(k/p_1 - e_1/p_1)$, which satisfies the $\gcd(w, p_1) > 1$ requirement of Definition 1 via $\mathbb{P}_1$. If k has a common prime factor with e_2, say p_2, then p_2 is either in $\mathbb{P}_1$ (as a common prime factor of e_1 and e_2) or in $\mathbb{P}_2$. The subcases where p_2 is in $\mathbb{P}_1$ lead again to the non-trivial integer factorization $n_1 = p_2(k/p_2 - e_1/p_2)$, satisfying the requirement of Definition 1 via $\mathbb{P}_1$; the subcases where p_2 is in $\mathbb{P}_2$ lead to the non-trivial integer factorization $n_2 = p_2(e_2/p_2 - k/p_2)$, satisfying Definition 1 via $\mathbb{P}_2$. □

Lemma 4. *A prime partitionable number laid out in Definition 1 is an Erdős–Woods number.*

Proof. The prime partitionable number n of Definition 1 defines for each $1 \le j < n$ a prime p_j which is either the associated $p_1 \in \mathbb{P}_1$ if $\gcd(j, p_1) > 1$ or the associated $p_2 \in \mathbb{P}_2$ if $\gcd(n-j, p_2) > 1$ (or any of the two if both exist). The associated Erdős–Woods interval with lower limit e_1 exists because the set of modular equations $e_1 + j \equiv 0 \pmod{p_j}$, $1 \le j < n$, can be solved with the Chinese Remainder Theorem [6, 4]. Duplicates of the equations are removed, so there may be less than $n - 1$ equations if some p_j appear more than once on the right hand sides. [Note that each p_j is associated with matching j in the equations, meaning for fixed p_j all the j are in the same modulo class because they have essentially been *fixed* in Definition 1 demanding $j \equiv 0 \pmod{p_j}$. No contradicting congruences arise in the set of modular equations.] □

Having shown the two-way mutual inclusion in the two lemmas and joining in Theorem 1 yields:

Theorem 2. *A number is an Erdős–Woods number iff it is prime partitionable according to Definition 1 (and therefore iff it is prime partitionable according to Definition 2).*

References

1. Patrick Cégielski, François Heroult, and Denis Richard, *On the amplitude of intervals of natural numbers whose every element has a common prime divisor with at least an extremity*, Theor. Comp. Sci. **303** (2003), no. 1, 53–62. MR 1990741
2. David L. Dowe, *On the existence of sequences of co-prime pairs of integers*, J. Austral. Math. Soc. Ser. A **47** (1989), no. 1, 84–89. MR 0998882 (90e:11005)
3. OEIS Foundation Inc., *The On-Line Encyclopedia Of Integer Sequences*, (2013), http://oeis.org/. MR 1992789 (2004f:11151)
4. Aviezri S. Fraenkel, *New proof of the general chinese remainder theorem*, Proc. Amer. Math. Soc. **14** (1963), no. 5, 790–791. MR 0154841 (27 #4785)
5. W. Holsztyński and R. F. E. Strube, *Paths and circuits in finite groups*, Discrete Math. **22** (1978), no. 3, 263–272. MR 0522721 (80e:20052)
6. Oystein Ore, *The general chinese remainder theorem*, Am. Math. Monthly **59** (1952), no. 6, 365–370.
7. William T. Trotter, Jr. and Paul Erdős, *When the Cartesian product of directed cycles is Hamiltonian*, J. Graph Theory **2** (1978), no. 2, 137–142. MR 0493392
8. Alan Robert Woods, *Some problems in logic and number theory, and their connections*, Ph.D. thesis, University of Machester, 1981, reprinted in New Studies in Weak Arithmetics, Sep. 2013, CSLI.

URL: `http://www.univ-ag.fr/~mhasler`
E-mail address: `mhasler@univ-ag.fr`

CEREGMIA & D.S.I., Université des Antilles, B.P. 7209, 97275 Schoelcher cedex, Martinique (F.W.I.)

URL: http://www.mpia.de/~mathar
E-mail address: mathar@mpia.de

Max Planck Institute of Astronomy, Königstuhl 17, 69117 Heidelberg, Germany