Zeitschrift: Elemente der Mathematik
Band: 30 (1975)
Heft: 1

Rubrik: Kleine Mitteilungen

P_3' and P_3'' respectively denote the $x - v$ and $v - z$ subpaths of P_3. Then, P_3'' has the same length as P. Hence, the paths P_1, P_3', and $\langle\{w, x\}\rangle$ constitute a $u - w$ walk of at most $e(z)$. Since this is impossible, it must be the case that $u \in Z(G)$. As such, the theorem follows.

As a special case of the preceding theorem, we have the following corollary.

Corollary 10. If a graph G is randomly eulerian from any vertex, then the center $Z(G)$ induces a connected subgraph.

John Roberts, Western Michigan Univ., Kalamazoo, USA

REFERENCES

[1] F. Bäbler, *Über eine spezielle Klasse Euler'scher Graphen.* Comment. Math. Helv. *27*, 81–100 (1953).

[2] M. Behzad and G. Chartrand, *Introduction to the Theory of Graphs.* Allyn and Bacon, Boston (1972).

[3] L. Euler, *Solutio problematis ad geometriam situs pertinentis.* Comment. Academiae Sci. I. Petropolitanae *8*, 128–140 (1736). Opera omnia I_7, 1–10.

[4] O. Ore, *A problem regarding the tracing of Graphs.* Elem. Math. *6*, 49–53 (1951).

Kleine Mitteilungen

When is the divisibility relation in a monoid a partial ordering?

1. Let $\langle M, \cdot, e\rangle$ be a monoid, i.e., a semigroup $\langle M, \cdot\rangle$ with an identity element e. We define the *divisibility relation* $\le$ in M by

$$x, y \in M;\ x \le y \ :\leftrightarrow\ xu = y \quad \text{for some} \quad u \in M\,.$$

By a non-trivial group we mean a group consisting of two or more elements. For $x \in M$, we denote the principal right ideal $\{xu;\ u \in M\}$ by xM. It is easily seen that, for arbitrary $x, y \in M$,

$$x \le y \ \leftrightarrow\ yM \subset xM \ \leftrightarrow\ y \in xM \qquad (1)$$

and that $\le$ is reflexive and transitive. Shwu-Yeng T. Lin [5] raised the problem to find a necessary and sufficient condition on M for $\le$ to be a partial ordering. In this note we present an answer to this question and several remarks about it.

2. Criterion 1: *For a monoid $\langle M, \cdot, e\rangle$, the following statements are equivalent:*

(*) $x, u, v \in M;\ xuv = x \rightarrow xu = x\,,$

(*′) $x, y \in M;\ xM = yM \rightarrow x = y\,,$

(*″) *the divisibility relation $\le$ in M is a partial ordering.*

Proof: (*) → (*′): Assume that $xM = yM$. Then $x = xe \in xM = yM$ and, analogously, $y \in xM$. Therefore there exist $u, v \in M$ such that $y = xu$, $x = yv$, hence $xuv = x$, and (*) implies $xu = x$, i.e., $x = y$. – (*′) → (*″): Suppose that $x \le y$ and $y \le x$. From (1) we conclude $xM = yM$, and by virtue of (*′) we get $x = y$. – (*″) → (*): Let be $xuv = x$. Then $xu \le x$ and $x \le xu$, and antisymmetry yields $xu = x$.

Corollary 1: *The following conditions are necessary for* $\leq$ *to be a partial ordering*:

M has no non-trivial subgroups. (2)

$u, v \in M;\ uv = e \rightarrow u = v = e$. (3)

The subgroup U of invertible elements of M is $\{e\}$. (4)

$\langle M, \cdot, e\rangle$ *is not a non-trivial group* . (5)

Proof: (2): Assume that M has a non-trivial subgroup L with identity element e' (notice that e' need not be equal to e; cf. Remark 6 below). Let be $u \in L$, $u \neq e'$. Then $e'uu^{-1} = e'$, but $e'u = u \neq e'$, a contradiction to (*). – (3): Let be $uv = e$, hence $euv = e$. (*) implies $eu = e$, i.e., $u = e$. Now $uv = e$ yields $v = e$. – (4) follows from (3) and (5) from (4). For (5) in this connection see [1], p. 176, Theorem 6.

On the other hand, it is quite natural to ask for what familiar classes of monoids condition (*) does hold. $\langle M, \cdot, e\rangle$ is called

left cancellative if, for any $x, y, z \in M$, $xy = xz$ implies $y = z$, (6)

idempotent if $xx = x$ for any $x \in M$. (7)

Corollary 2: *Each of the following two conditions* a), b) *is sufficient for* $\leq$ *to be a partial ordering*:

a) (4) *and* (6) (see also [6], p. 123),

b) (7) *and commutativity* of $\cdot$.

Proof: a) $xuv = x$ implies $(xu)vu = xu$, and (6) leads to $uv = e$, $vu = e$, i.e., by virtue of (4), to $v = e$. Therefore $xu = xuv = x$. Thus, (*) holds. – b) $xuv = x$ and (7) imply $xux = xu(xuv) = (xuxu)v = (xu)v = xuv = x$. With the additional help of commutativity we get $xu = xxu = xux = x$.

3. Remark 1: Any semilattice (with or without identity element), i.e., any commutative idempotent semigroup, satisfies (*) (see [2], p. 22, Lemma 2); reflexivity is ensured by (7). For idempotent semigroups the divisibility relation equals the so-called natural partial ordering $\leq_n$ defined by $x \leq_n y :\leftrightarrow xy = y$ ([3], p. 23–24).

Remark 2: Condition a) in Corollary 2 is not necessary for (*): Let E be a non-empty set and $\mathfrak{P}(E)$ the collection of all subsets of E. Then the monoid $\langle \mathfrak{P}(E), \cup, \phi\rangle$ is a semilattice, so satisfies (*). But it is not left cancellative. Here $\leq$ is set-theoretical inclusion.

Remark 3: Condition b) in Corollary 2 is not necessary for (*): Let $\boldsymbol{N}$ denote the set of positive integers. Then $\langle \boldsymbol{N}, \cdot, 1\rangle$ satisfies (4) and (6), thus (*) holds. Here $\leq$ turns out to be the usual divisibility relation in $\boldsymbol{N}$. Since $\langle \boldsymbol{N}, \cdot, 1\rangle$ is not idempotent, we have a negative answer to an additional question in [5].

Remark 4: Let be $E = \{a, b\}$ $(a \neq b)$. Let $e, \underline{a}, \underline{b}$ mappings from E into E, namely: e identical, $\underline{a}(E) = \{a\}$, $\underline{b}(E) = \{b\}$. If $M = \{e, \underline{a}, \underline{b}\}$, and if we define $\cdot$ in M by $xy := y \circ x$, then $\langle M, \cdot, e\rangle$ is an idempotent noncommutative monoid; it is not left cancellative, but (2) and (3) hold: The subgroups of M are $\{e\}$, $\{\underline{a}\}$, and $\{\underline{b}\}$. The equations $\underline{a}\,\underline{b}\,\underline{a} = \underline{a}$, $\underline{a}\,\underline{b} = \underline{b}$ violate (*). Therefore none of the conditions (2), (3), (7) and of their conjunctions is sufficient for (*). However, in the commutative case, (7) is (Corollary 2b)).

Remark 5: (6) does not imply (*): Consider a non-trivial group M and notice that (*) implies (5). Here $\leq$ is the universal relation on M: $x \leq y$ for any $x, y \in M$.

Remark 6: Even for commutative monoids, (3) is not sufficient for (*): For any real number a denote the matrix $\begin{pmatrix} a & a \\ a & a \end{pmatrix}$ by m_a. For $e := \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, $M := \{e, m_a;\ a \in \mathbf{R}\}$ and the usual matrix multiplication, $\langle M, \cdot, e\rangle$ is a commutative monoid satisfying (3). But $\{m_a;\ a \in \mathbf{R}\setminus\{0\}\}$ forms a non-trivial subgroup of M, its identity element being $m_{1/2}$. So M does not satisfy (2), a fortiori not (*).

4. Finally we discuss the question about necessary and sufficient conditions on the monoid $\langle M, \cdot, e\rangle$ for $\leq$ to have other important properties. The proofs of the following three criteria are left to the reader.

Criterion 2: *The following statements are equivalent:*

$$x, y \in M \rightarrow xM \cap yM \neq \phi, \text{ i.e., } M \text{ is left reversible ([4], p. 194)}, \tag{8}$$

$$x, y \in M \rightarrow x \leq z,\ y \leq z \text{ for some } z \in M \text{ (Moore-Smith property)}. \tag{8'}$$

Commutativity of $\cdot$ is sufficient for (8) but by no means necessary: Consider a non-abelian group.

Criterion 3: *The following statements are equivalent:*

$$x, y \in M \rightarrow \{x, y\} \cap xM \cap yM \neq \phi, \tag{9}$$

$$x, y \in M \rightarrow x \leq y \quad \text{and/or} \quad y \leq x. \tag{9'}$$

Criterion 4: *The following statements are equivalent:*

$$x, y \in M \rightarrow xM \cap yM = zM \quad \text{for some} \quad z \in M, \tag{10}$$

$$x, y \in M \rightarrow x \leq z \quad \text{and} \quad y \leq z \quad \text{for some} \quad z \in M, \quad \text{and}$$
$$w \in M, x \leq w, y \leq w \quad \text{imply} \quad z \leq w. \tag{10'}$$

Evidently, (9) implies (10), and (10) implies (8). (9), (10), (8) correspond to the situations in totally ordered, semilattice-ordered and directed sets, respectively.

Corollary 3: *Let $\langle M, \cdot, e\rangle$ be a monoid for which* (*) *and* (10) *hold. Then there exists a binary operation* $*$ *on* M *such that*

a) *$\langle M, *, e\rangle$ is a commutative idempotent monoid,*

b) *the divisibility relations $\leq'$ and $\leq$ in $\langle M, *, e\rangle$ and $\langle M, \cdot, e\rangle$ are the same.*

Proof: a) Let x, y be arbitrary elements of M. By (10), there exists $z \in M$ such that $xM \cap yM = zM$. By (*'), z is uniquely determined by x and y. Thus $*$ is well-defined by

$$x * y = z \quad \text{where} \quad xM \cap yM = zM.$$

Therefore, the mapping $f: M \rightarrow \{xM;\ x \in M\}$ defined by $f(x) = xM$ for every $x \in M$ is bijective and has the property $f(x * y) = f(x) \cap f(y)$ ($\langle M, *, e\rangle$ is the 'transplant' of $\langle\{xM; x \in M\}, \cap, M\rangle$ under f^{-1}; see [7], p. 43/44). Since $\langle\{xM; x \in M\}, \cap, M\rangle$ is a semilattice with identity, so is $\langle M, *, e\rangle$ (For a different proof cf. [2], p. 10, Corollary). – b) For arbitrary elements $x, y \in M$ we have $x \leq' y \leftrightarrow x * u = y$ for some $u \in M \leftrightarrow xM \cap uM = yM$ for some $u \in M \leftrightarrow yM \subset xM \leftrightarrow x \leq y$, the last step being ensured by (1).

Remark 7: Of course, $x * y = \sup\{x, y\}$ with respect to $\leq$. For $\langle \boldsymbol{N}, \cdot, 1\rangle$ ($\boldsymbol{N}$ the set of positive integers), $*$ is the least common multiple operation, and both operations $\cdot$ and $*$ lead to the usual divisibility relation.

J. Rätz, Bern

REFERENCES

[1] J. Aczél, *The Monteiro-Botelho-Teixeira axiom and a 'natural' topology in abelian semigroups.* Portug. Math. *24*, 173–177 (1965).

[2] G. Birkhoff, *Lattice theory.* Third edition. Amer. Math. Soc. Colloq. Publ. Vol. XXV. Providence, R.I., 1967.

[3] A. H. Clifford and G. B. Preston, *The algebraic theory of semigroups*, Vol. I. Amer. Math. Soc. Math. Surveys No. 7. Providence, R.I., 1961.

[4] A. H. Clifford and G. B. Preston, *The algebraic theory of semigroups*, Vol. II. Amer. Math. Soc. Math. Surveys No. 7. Providence, R.I., 1967.

[5] Shwu-Yeng T. Lin, *On a functional equation arising from the Monteiro-Botelho-Teixeira axioms for a topological space.* Aeq. Math. *9* (1973) 118–119. Problem 110, Aeq. Math. *9*, 298 (1973).

[6] A. Rosenfeld, *An introduction to algebraic structures.* Holden-Day San Francisco 1968.

[7] S. Warner, *Modern algebra*, Vol. I. Prentice-Hall Englewood Cliffs, N.J., 1965.

A formula for the least prime greater than a given integer

We shall prove the following theorem, which gives an apparently new formula for the nth prime p_n.

Theorem. Let m be any natural number ≥ 2. Put

$$d = \left((m!)^{m!} - 1, (2m)!\right),$$

$$t = \frac{d^d}{(d^d, d!)}$$

and define α by the condition $d^\alpha \| t$. Then the integer

$$p = \frac{d}{(t/d^\alpha, d)}$$

is the least prime greater than m.

In particular, taking $m = p_{n-1}$, we see that $p = p_n$. So, in principle, this formula enables us to compute p_n once p_{n-1} is known. Of course the result is purely of theoretical interest, since even computing the number d (by the Euclidean algorithm) is, in general, completely impractical.

Some years ago Gandhi (see [1]) proved the following result: if Q is the product of the first $n-1$ primes, then the inequality

$$1 < 2^{p_n}\left[-\frac{1}{2} + \sum_{d|Q}\left(\frac{\mu(d)}{2^d - 1}\right)\right] < 2$$

(μ denotes the Möbius function) gives p_n explicitly in terms of $p_1, \cdots, p_{n-1}$. There are also older formulas for p_n (see [2, p. 344], [3]).

Lemma. The representation of d as a product of primes is

$$d = q_1 q_2 \cdots q_n \quad (n \geq 1),$$

where $m < q_1 < q_2 < \cdots < q_n < 2m$ and q_1 is the least prime $p > m$.

Proof. Obviously d is square-free, and each of its prime factors is between m and $2m$. Thus we have only to show that d is divisible by p, the smallest prime which exceeds m. By Bertrand's theorem [2, p. 343] $m < p < 2m$. Therefore, if $m > 3$, $\varphi(p) = 2[(p-1)/2] \mid m!$, so that Euler's theorem gives $(m!)^{m!} \equiv 1 \pmod{p}$. It is easy to see that this congruence also holds for $m = 2, 3$. Since $p \mid (2m)!$ the proof of the lemma is complete.

Proof of the theorem. For $i = 1, \cdots, n$, the exponent e_i of the highest power of q_i which divides $d!$, is

$$e_i = \sum_{j=1}^{\infty} \left[\frac{d}{q_i^j}\right] < \sum_{j=1}^{\infty} \frac{d}{q_i^j} < d$$

[2, p. 342]. Since for $1 \leqq i \leqq n-1$

$$\left[\frac{d}{q_{i+1}}\right] = \frac{d}{q_{i+1}} < \frac{d}{q_i} = \left[\frac{d}{q_i}\right],$$

$$\left[\frac{d}{q_{i+1}^j}\right] \leq \left[\frac{d}{q_i^j}\right] \quad (j = 2, 3, \cdots),$$

we have $d > e_1 > e_2 > \cdots > e_n$. Hence $t = q_1^{\alpha(1)} q_2^{\alpha(2)} \cdots q_n^{\alpha(n)}$, where $0 < \alpha(1) < \alpha(2) < \cdots < \alpha(n)$. This completes the proof.

Reijo Ernvall, University of Turku, Finland

REFERENCES

[1] C. V. Eynden, *A Proof of Gandhi's Formula for the nth Prime*, Amer. Math. Monthly *79*, 625 (1972).

[2] G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers*, 4th ed. (Oxford University Press, Oxford 1960).

[3] W. Sierpiński, *Sur une Formulae Donnant tous les Nombres Premiers*, C. R. Acad. Sci (Paris) *235*, 1078–1079 (1952).

Aufgaben

Aufgabe 709. It is well known (cf. e.g. H. Hadwiger, H. Debrunner, V. Klee, Combinatorial Geometry in the Plane, New York 1964, p. 4, Problem 5) that no three distinct points of a square lattice can be the vertices of an equilateral triangle. Show that no four distinct points of an equilateral triangular lattice can be the vertices of a square.

M. S. Klamkin, Dearborn, Michigan, USA

Erste Lösung: Wir beweisen allgemeiner den folgenden Satz:

Ein rechtwinkliges Dreieck kann genau dann in ein reguläres Dreiecksgitter eingelagert werden (d.h., die Ecken sind Gitterpunkte), wenn das Verhältnis seiner Katheten die Form $r\sqrt{3}$ mit einer positiven rationalen Zahl r hat.

Daraus folgt unmittelbar die Behauptung der Aufgabe 709, aber z.B. auch der Satz: Kein pythagoräisches Dreieck kann in ein reguläres Dreiecksgitter eingelagert werden.

Beweis: I. $\boldsymbol{a}$ und $\boldsymbol{b}$ seien zwei Einheitsvektoren, die das Gitter aufspannen, $\boldsymbol{a} \cdot \boldsymbol{b} = 1/2$. A, B und C seien drei verschiedene Gitterpunkte, die ein bei C rechtwinkliges Dreieck bilden. Ist dann etwa $\boldsymbol{BC} = x\boldsymbol{a} + y\boldsymbol{b}$, $\boldsymbol{CA} = u\boldsymbol{a} + v\boldsymbol{b}$ mit ganzen Zahlen x, y, u, v, so ist $\boldsymbol{BC} \cdot \boldsymbol{CA} = 0$, folglich $x(2u+v) + y(u+2v) = 0$. Es gibt also