Kleine Mitteilungen

We now turn to the problem of determining the subsets of Z_n which are fields. In the following $\overline{U}_n$ will denote $U_n \cup \{0\}$ and if F is a field, F^* will denote the non-zero elements of F.

Theorem 4. If F is a subset of Z_n which is a field, then there is an a such that $a \mid n$, $(a, n/a) = 1$ and $F = a\,\overline{U}_n$.

Proof: If F is a subset of Z_n which is a field, then F^* is a group under multiplication mod n. Hence, by Theorem 3 there is an a such that $a \mid n$, $(a, n/a) = 1$ and $F^* \subseteq a\,U_n$ which is equivalent to $F \subseteq a\,\overline{U}_n$. Now let e be the multiplicative identity of F, and hence of $a\,U_n$. Then $a = a\,e = e + e + \cdots + e$ (a summands) must be in F. Also, if $u \in U_n$, $u\,a = a + a + \cdots + a$ (u summands) must be in F. Consequently $a\,U_n \subseteq F$. Also, $0 \in F$ and thus $F = a\,\overline{U}_n$.

Theorem 5. Assume $n = a\,b$ where $(a, b) = 1$. $a\,\overline{U}_n$ is a field if and only if b is a prime.

Proof: If b is not a prime then $b = c\,d$ where $c, d > 1$. Now $(c\,a, n) = c\,a$ and hence $c\,a \notin a\,U_n$ by Theorem 3i. Also $c\,a \not\equiv 0 \pmod{n}$. Hence, $c\,a \notin a\,\overline{U}_n$. But adding a to itself c times gives $c\,a$. Therefore, $a\,\overline{U}_n$ is not closed under addition mod n and hence is not a field. Now assume b is a prime. First of all we observe that $0\,a, 1\,a, 2\,a, \ldots, (b-1)\,a$ are b distinct elements mod n. Also, since $(i\,a, n) = a(i, b) = a$ for $i = 1, 2, \ldots, b-1$ and $(a, n/a) = 1$, $i\,a \in a\,U_n$ for $i = 1, 2, \ldots, b-1$ by Lemma 1. Since the number of elements in $a\,U_n$ is $\phi(b) = b - 1$, we have $a\,U_n = \{1\,a, 2\,a, \ldots, (b-1)\,a\}$. Hence, $a\,\overline{U}_n = \{0\,a, 1\,a, 2\,a, \ldots, (b-1)\,a\}$ and this set clearly forms a group under addition mod n. Hence, $a\,\overline{U}_n$ is a field.

Combining the last two theorems we have the following characterization of the subsets of Z_n which are fields.

Corollary 2. Z_n has subsets which are fields if and only if there exists a prime p such that $p \mid n$ and $p^2 \nmid n$. Moreover, for every such prime p, the set $(n/p)\,\overline{U}_n$ is a field and all subsets of Z_n which are fields are obtained in this way.

J. E. Nymann, University of Texas, El Paso

REFERENCE

[1] Edwin Hewitt and H. S. Zuckermann, *The multiplicative semigroup of integers modulo m*, Pacific J. Math. *10* 1291–1308 (1960).

Kleine Mitteilungen

Ein elementarer Beweis für die Integraldarstellung der Laplaceschen Zahlen

In der numerischen Analysis haben die Laplaceschen Zahlen $L_1, L_2, L_3, \ldots$, neben den Eulerschen und Bernoullischen Zahlen eine grosse Bedeutung erlangt [1]. Sie werden üblicherweise durch die Koeffizienten der Taylor-Reihe

$$-\frac{x}{\ln(1-x)} = 1 - L_1 x - L_2 x^2 - L_3 x^3 - \cdots, \quad x \in (-1, 1), \tag{1}$$

oder, was auf dasselbe hinausläuft, durch die Rekursionsformel

$$\sum_{\nu=1}^{n} \frac{L_\nu}{n-\nu+1} = \frac{1}{n+1}, \quad n \in \boldsymbol{N}, \tag{2}$$

erklärt. Für die Laplaceschen Zahlen gilt auch die Integraldarstellung

$$L_\nu = (-1)^{\nu-1} \int_0^1 \binom{t}{\nu}\, dt, \quad \nu \in \boldsymbol{N}, \tag{3}$$

die gewöhnlich durch gliedweise Integration der gleichmässig konvergenten Reihe

$$(1-x)^t = \binom{t}{0} - \binom{t}{1}x + \binom{t}{2}x^2 - \binom{t}{3}x^3 + \cdots, \quad t \in [0,1],$$

über das Intervall [0,1] bei festem $x \in (-1,1)$ und anschliessendem Koeffizientenvergleich mit (1) bewiesen wird. Im folgenden soll die Integraldarstellung (3) auf der Basis der Rekursionsformel (2) in dem Sinne elementar bewiesen werden, als nur die Differentiation und Integration von Polynomen benutzt werden; insbesondere werden eine Bezugnahme auf die Theorie der Potenzreihen und die Problematik bei der Vertauschung von Grenzprozessen vermieden.

Ausgehend von den bestimmten Integralen

$$\int_0^1 (t-1)^\mu t^{n-\mu}\, dt = (-1)^\mu \frac{\mu!\,(n-\mu)!}{(n+1)!}, \quad \mu \in \{0,\ldots,n\}, \quad n \in \boldsymbol{N},$$

die man durch μ-malige partielle Integration unmittelbar verifiziert, entsteht

$$\int_0^1 \sum_{\nu=0}^{\mu} (-1)^\nu \binom{\mu}{\nu} t^{n-\nu}\, dt = \frac{(-1)^n}{(n+1)!} \prod_{\substack{\nu=0 \\ \nu \neq \mu}}^{n} (\mu-\nu), \quad \mu \in \{0,\ldots,n\}, \quad n \in \boldsymbol{N},$$

und damit weiter

$$\sum_{\nu=0}^{n} \frac{(-1)^\nu \binom{\mu}{\nu}}{n-\nu+1} = \frac{(-1)^n}{(n+1)!} \frac{d}{dt} \prod_{\nu=0}^{n} (t-\nu)\Bigg|_{t=\mu}, \quad \mu \in \{0,\ldots,n\}, \quad n \in \boldsymbol{N}. \tag{4}$$

Es folgt die Identität zweier Polynome n-ten Grades,

$$\sum_{\nu=0}^{n} \frac{(-1)^\nu \binom{t}{\nu}}{n-\nu+1} = \frac{(-1)^n}{(n+1)!} \frac{d}{dt} \prod_{\nu=0}^{n} (t-\nu), \quad n \in \boldsymbol{N}, \quad t \in \boldsymbol{R}, \tag{5}$$

da diese laut (4) an den $n+1$ Stellen $t = 0,1,\ldots,n$ übereinstimmen. Integration von (5) über das Intervall [0,1] ergibt

$$\frac{1}{n+1} - \sum_{\nu=1}^{n} \frac{L_\nu^*}{n-\nu+1} = 0, \quad n \in \boldsymbol{N}, \tag{6}$$

mit

$$L_\nu^* := (-1)^{\nu-1} \int_0^1 \binom{t}{\nu}\, dt, \quad \nu \in \boldsymbol{N}. \tag{7}$$

Die Rekursionsformeln (2) und (6) liefern dann die gesuchte Identität

$$L_\nu = L_\nu^*, \quad \nu \in \boldsymbol{N}. \tag{8}$$

Walter Gerdes, Universität Karlsruhe

LITERATUR

[1] J. F. STEFFENSEN, *Interpolation* (Chelsea Publ. Co., New York 1950).

Area Preserving Homeomorphisms

W. J. Firey [1965] has shown that an affinity of d-dimensional euclidean space E^d which preserves k-dimensional volume, for some $k = 1, 2, \ldots, d-1$, is an isometry. Here we shall generalize the case $k = d-1$ of this result to arbitrary homeomorphisms of E^d. Specifically, we shall prove:

Theorem. Let Φ be a homeomorphism of E^d onto itself, which preserves surface area. Then Φ is an isometry.

Before proceeding with the proof, we must make our terms more explicit. We shall take surface area in the Cantor-Minkowski sense. That is, if A is a set in E^d, and A_ρ denotes the set of points of E^d whose distance from A is at most ϱ, then the surface area $S(A)$ of A is defined in terms of the volume V by

$$S(A) = \lim_{\varrho \to 0} \frac{1}{2\varrho} V(A_\varrho),$$

if this limit exists. In saying that Φ preserves surface area we shall mean that, for each set A in E^d, $S(A) = S(A\Phi)$ if either surface area is defined. In fact, we shall only use this property when A or $A\Phi$ is the boundary of a ball, so the assumption of the theorem is unnecessarily strong.

To prove the theorem, we shall use, as did Firey, the isoperimetric theorem, which states that, among all bodies (compact sets which are the closures of their interiors) with the same surface area in E^d, the balls, and only the balls, have the maximum volume. However, since we cannot so easily use the underlying linear structure of E^d, our proof must necessarily be a little less direct than Firey's.

Firstly, let B be any (euclidean) ball in E^d. Then $B\Phi$ has the same surface area as B, and so, by the isoperimetric theorem, it has no greater volume than B. (For brevity, we talk about the surface area of B, rather than of its boundary.) Now let D be an arbitrary body in E^d, with volume V, say. Then, for any preassigned $\varepsilon > 0$, we can cover D with balls, whose total volume does not exceed $V + \varepsilon$. It follows that the volume of $D\Phi$ cannot exceed $V + \varepsilon$ also, and since ε was arbitrary, we deduce that Φ cannot increase volume.

The same argument applied to the inverse homeomorphism Φ^{-1}, which also preserves surface area, shows that Φ must preserve volume. A second application of the isoperimetric theorem, this time characterizing the cases of equality, shows that, for each ball B, $B\Phi$ is a congruent ball. Since two points of E^d determine the ball

with the segment joining them as diameter, we now see that Φ cannot increase distance. Again considering Φ^{-1}, we conclude that Φ preserves distance; that is, Φ is an isometry of E^d, as was claimed.

The proof above does not extend to the cases of homeomorphisms which preserve volume of some intermediate dimension (except that length preserving homeomorphisms are obviously isometries). So, it is natural to ask:

Problem: Is it true that a homeomorphism of E^d onto itself which preserves k-dimensional volume, for some $k = 2, \ldots, d-2$, is an isometry?

P. McMullen, University College London

REFERENCE

[1] W. J. FIREY, *Affinities which Preserve Lower Dimensional Volume*, Amer. Math. Monthly *72*, 645 (1965).

Even Perfect and Super Perfect Numbers

If $\sigma(n)$ is the sum of the divisors of n and k a natural number then the *k-th* iterate of $\sigma(n)$ is denoted by $\sigma^k(n)$: that is, $\sigma^1(n)$ equals $\sigma(n)$ and for k exceeding 1, $\sigma^k(n)$ is defined recursively as $\sigma(\sigma^{k-1}(n))$. The solutions in even natural numbers, n, of the equation $\sigma^k(n) = 2n$ are for $k = 1$ the even perfect numbers, the Euclid numbers $2^a(2^{a+1} - 1)$, where $2^{a+1} - 1$ is a (Mersenne) prime. D. Suryanarayana defined super perfect numbers to be the solutions of $\sigma(\sigma(n)) = 2n$, the preceding identity with $k = 2$, and he showed that the even super perfect numbers were precisely $n = 2^a$ where, as before, $2^{a+1} - 1$ is prime [2].

It will be shown here that for no other value of k does $\sigma^k(n) = 2n$ have a solution in even natural numbers. Needed in the proof of this result is the weak inequality $\sigma^j(n) \geq j + n$, for $n \geq 2$, with equality if and only if $j = 1$ and n is prime or $j = 2$ and $n = 2$. The latter is easily established by repeated application of the inequality $\sigma(n) \geq 1 + n$, with equality iff n is prime.

Theorem. The equation $\sigma^k(n) = 2n$ has a solution in even natural numbers if and only if either $k = 1$ and $n = 2^a(2^{a+1} - 1)$ or $k = 2$ and $n = 2^a$ where in both cases $2^{a+1} - 1$ is prime.

Proof. The case of $k = 1$, Euler's characterisation of even perfect numbers, appears in most elementary number theory texts, for example [1], so only $k \geq 2$ will be considered in the proof.

Let $n = 2^a m$ where m is odd and greater than 1.

Then

$$\begin{aligned}\sigma^k(n) &= \sigma^{k-1}[(2^{a+1} - 1) \cdot \sigma(m)] \\ &\geq (k-2) + 1 + \sigma(m) + (2^{a+1} - 1) \cdot \sigma(m) \\ &> 2n .\end{aligned}$$

Hence a solution of $\sigma^k(n) = 2n$ is possible only if $m = 1$, that is, if $n = 2^a$, in which case:

$$\sigma^k(n) = \sigma^{k-1}(2^{a+1} - 1)$$
$$\geq (k-1) + (2^{a+1} - 1) .$$

The last inequality forces k to be equal to 2 and $2^{a+1} - 1$ to be prime.

To conclude the proof it suffices to note that if p is a Mersenne prime then $(p+1)/2$ satisfies $\sigma(\sigma(n)) = 2n$.

Graham Lord, Temple University, Philadelphia, Pennsylvania, U.S.A.

LITERATURVERZEICHNIS

[1] G. H. HARDY and E. M. WRIGHT, *An Introduction to the Theory of Numbers* (Oxford 1960), p. 240.

[2] D. SURYANARAYANA, *Super Perfect Numbers*. El. Math. *24*, 16–17 (1969).

Aufgaben

Aufgabe 721. The question whether, for an integer $n > 1$, $\varphi(n) \mid (n-1)$ implies that n is a prime, is open (cf., e.g., American Math. Monthly *80*, 192–193 [1973]). Show that if $n = 2^{2^s} + 1$ $(s \geq 0)$ and $\varphi(n) \mid (n-1)$, then n is a prime.

J. Steinig, Genève

Solution: We show the more general result that n is a prime whenever $n = 1 + q^t$ ($t > 0$, q prime) and $\varphi(n) \mid (n-1)$. (If this is true then we must have $q = 2$, for otherwise n is even and $n > 2$, since $t > 0$, so n cannot be a prime.) Let $n = 1 + q^t = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_l^{\alpha_l}$, $\alpha_i \geq 1$. Clearly, $p_i \nmid q$. From the condition $\varphi(n) = p_1^{\alpha_1 - 1} p_2^{\alpha_2 - 1} \ldots p_l^{\alpha_l - 1} \prod_{i=1}^{l} (p_i - 1) \mid (n-1) = q^t$, it follows that $\alpha_1 = \alpha_2 = \ldots = \alpha_l = 1$ and $p_i = q^{t_i} + 1$, $t_i \geq 0$. Without loss of generality $p_1 < p_2 < \cdots < p_l$ and consequently $t_1 < t_2 < \cdots < t_l$. If $l > 1$ then $n = p_1 p_2 \ldots p_l = 1 + q^{t_1} + q^{t_2} + \cdots + q^{t_l} + q^{t_1 + t_2} + \cdots + q^{t_1 + t_2 + \cdots + t_l}$

and

$$n - 1 = q^t = q^{t_1} + q^{t_2} + \cdots + q^{t_l} + q^{t_1 + t_2} + \cdots + q^{t_1 + t_2 + \cdots + t_l} \equiv q^{t_1} \pmod{q^{t_1 + 1}} ,$$

a contradiction.

Apparently $l = 1$, $t = t_1$ and $n = p_1$.

O. P. Lossers, Eindhoven, The Netherlands

Weitere Lösungen sandten A. Bager (Hjørring, Dänemark), E. P. Bauhoff (Mannheim, BRD), C. Bindschedler (Küsnacht, ZH), O. Buggisch (Darmstadt, BRD), P. Bundschuh (Köln, BRD), L. Carlitz (Durham, N.C., USA), J. Fehér (Pécs, Ungarn), L. Hämmerling (Aachen, BRD), H. Harborth (Braunschweig, BRD), H. Kappus (Rodersdorf, SO), P. Kiss (Eger, Ungarn), A. Marshall (Madison, Wisconsin, USA), Chr. A. Meyer (Bern), H. Müller (Berlin), R. Shantaram (Flint, Michigan, USA), M. Vowe (Therwil, BL) und R. Wyss (Flumenthal, SO).