Die Aufzählung der 11 inkongruenten Netze des Würfels bei beidseitig gleich gefärbtem Papier sei dem Leser überlassen.

Die Reinzeichnungen zu den Figuren hat Herr C. Niederberger hergestellt, wofür ihm an dieser Stelle herzlich gedankt sei. M. Jeger, Zürich

LITERATURVERZEICHNIS

[1] C. Berge, *Principes de Combinatoire*, (Paris 1968).

[2] N. G. de Bruijn, *Polyas Abzähltheorie. Muster für Graphen und chemische Verbindungen.* Selecta Mathematica III, Heidelberger Taschenbücher, Band 86, p. 1–26. (Berlin–Heidelberg–New York, 1971).

[3] M. Jeger, *Einführung in die Kombinatorik*, Band 2, (Stuttgart 1975; erscheint demnächst).

[4] H. Sachs, *Einführung in die Theorie der endlichen Graphen*, (Teil I, Leipzig 1970; Teil II, Leipzig 1972).

Groups and Fields in Z_n

It can easily be verified that $\{2, 4, 6, 8\}$ is a group under multiplication mod 10 with 6 as the identity and that $\{0, 2, 4, 6, 8\}$ is a field under addition mod 10 and multiplication mod 10. The purpose of this paper is to characterize the subsets of Z_n which are groups under multiplication mod n and those which are fields under addition and multiplication mod n. Some of the results on subgroups of Z_n given here are equivalent to some of the results given by Hewitt and Zuckermann [1], but are of a substantially different form.

In the following $U_n = \{m \mid (n, m) = 1\}$ will denote the group of units in Z_n, ϕ will denote the Euler phi function and a small Roman letter will denote an integer or the residue class of the integer in Z_n; the context will indicate which is intended.

Proposition 1. If $n = ab$ and $(a, b) = 1$, then $a^{\phi(b)}$ is idempotent in Z_n.

Proof: $a^{\phi(b)} \equiv 1 \pmod{b}$ by Euler's theorem. Hence, multiplying through by $a^{\phi(b}$ we have $(a^{\phi(b)})^2 \equiv a^{\phi(b)} \pmod{n}$ since $n = ab$ and $(a, b) = 1$. Therefore, $(a^{\phi(b)})^2 = a^{\phi(b)}$ in Z_n.

Lemma 1. If $(x, n) = d$ and $(d, n/d) = 1$, then $x \equiv du \pmod{n}$ where $u \in U_n$. Hence, $x \in d\,U_n$.

Proof: Since $(d, n/d) = 1$, there exists a t_0 such that $x/d + t_0 n/d \equiv 1 \pmod{d}$. Let $u = x/d + t_0 n/d$. Then $(u, d) = (1, d) = 1$ and $(u, n/d) = (x/d, n/d) = 1$. Hence, $(u, n) = 1$ and $u \in U_n$. Also, $du = x + t_0 n \equiv x \pmod{n}$.

Proposition 2. If $(c, n) = d$ and $(d, n/d) = 1$, then $c\,U_n = d\,U_n$.

Proof: By Lemma 1, there is a $u \in U_n$ such that $c \equiv du \pmod{n}$. Hence, $c\,U_n = du\,U_n = d\,U_n$.

Proposition 3. If $n = ab$ and $(a, b) = 1$, then $a^{\phi(b)}\,U_n = a\,U_n$.

Proof: This follows immediately from Proposition 2 by observing $(a^{\phi(b)}, n) = a$ and $(a, n/a) = (a, b) = 1$.

The following theorem gives a method for constructing subsets of Z_n which are groups. The example in the first paragraph is obtained by taking $n = 10$ and $a = 2$.

Theorem 1. If $n = ab$ and $(a, b) = 1$, then $a U_n$ is a group under multiplication mod n with $a^{\phi(b)}$ as the identity. The order of this group is $\phi(b)$.

Proof: We will repeatedly make use of the fact $a U_n = a^{\phi(b)} U_n$ obtained in Proposition 3. Let $x, y \in U_n$. Then $(a^{\phi(b)} x)(a^{\phi(b)} y) = (a^{\phi(b)})^2 xy = a^{\phi(b)} xy$ by Proposition 1 and $xy \in U_n$. Hence, $a U_n$ is closed under multiplication mod n. Also, $a^{\phi(b)}(a^{\phi(b)} x) = (a^{\phi(b)})^2 x = a^{\phi(b)} x$ by Proposition 1. Hence, $a^{\phi(b)}$ is the identity for $a U_n$. Now let z be the inverse of x in U_n. Then $(a^{\phi(b)} x)(a^{\phi(b)} z) = (a^{\phi(b)})^2 xz = a^{\phi(b)}$. Hence, $a^{\phi(b)} z$ is the inverse of $a^{\phi(b)} x$ in $a U_n$. Therefore, $a U_n$ is a group under multiplication mod n. Furthermore, $ax \equiv ay \pmod{n}$ if and only if $x \equiv y \pmod{b}$ since $(a, n) = a$. Also, if $(w, b) = 1$, then $(aw, n) = a$ and $(a, n/a) = 1$. Hence, by Lemma 1, $aw \in a U_n$. Therefore, there is a one-to-one correspondence between the elements of Z_b which are relatively prime to b and the elements of $a U_n$. Hence, $a U_n$ has $\phi(b)$ elements.

Theorem 2. Let $(c, n) = d$. $c U_n$ is a group if and only if $(d, n/d) = 1$. In this case $c U_n = d U_n$.

Proof: If $(d, n/d) = 1$, then $c U_n = d U_n$ by Proposition 2 and, by Theorem 1, $d U_n$ is a group. Conversely, if $c U_n$ is a group, then it has an identity of the form ce where $e \in U_n$. Then $cec = c$ in Z_n. Hence, $c^2 e \equiv c \pmod{n}$. Therefore, $ce \equiv 1 \pmod{n/d}$. Consequently c is a unit in $Z_{n/d}$ and hence, $(c, n/d) = 1$. Therefore, $(d, n/d) = 1$ since d is a factor of c.

The next theorem shows that all subsets of Z_n which are groups under multiplication mod n are subgroups of the groups given in Theorem 1 and hence the groups in Theorem 1 are maximal. These groups can indeed have proper subgroups which are not obtained by the method in Theorem 1 as is seen by considering the subgroup $\{4, 6\}$ of the group in the example of the first paragraph.

Theorem 3. Let G be a subset of Z_n which is a group under multiplication mod n. If e is the identity for G and $(e, n) = d$, then

(i) $(x, n) = d$ for every $x \in G$,

(ii) $(d, n/d) = 1$,

(iii) G is a subgroup of $d U_n$.

Proof: Let $x \in G$ with $(x, n) = d'$. Now $ex \equiv x \pmod{n}$. Hence, $e \equiv 1 \pmod{n/d'}$. Since $d \mid e$, $(d, n/d') = 1$ and therefore $d \mid d'$. Also, $x^k \equiv e \pmod{n}$ for some integer $k \geqslant 2$, if $x \neq e$. Hence, $x^k/d \equiv e/d \pmod{n/d}$. Now $(e/d, n/d) = 1$ and thus $(x^k/d, n/d) = 1$. But d' is a factor of x^k/d since $k \geqslant 2$. Hence, $(d', n/d) = 1$ and therefore $d' \mid d$. Thus $d = d'$ and $(d, n/d) = 1$. Now, using Lemma 1, we see that if $x \in G$, then $x \in d U_n$; i.e. $G \subseteq d U_n$. Also, by Theorem 2, $d U_n$ is a group and hence G is a subgroup of $d U_n$.

As an interesting side result we can now show that every idempotent element of Z_n is of the form given in Proposition 1. This characterization of the idempotents of Z_n is quite different from that given in [1].

Corollary 1. Every idempotent element of Z_n is of the form $a^{\phi(b)}$ where $n = ab$ and $(a, b) = 1$.

Proof: If x is an idempotent element of Z_n, then $\{x\}$ is a subset of Z_n which 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 $\{x\}$ is a subgroup of $a U_n$. Then x must be the identity of $a U_n$. Letting $b = n/a$, Theorem 1 tells us $a^{\phi(b)}$ is the identity of $a U_n$. Hence, $x = a^{\phi(b)}$ in Z_n.

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

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