PACIFIC JOURNAL OF MATHEMATICS
Vo. 22, No. 3, 1967

FACTORING BY SUBSETS

S. K. STEIN

If a group G is the direct product of two of its subgroups, A and B, then every element of G is uniquely expressible in the form $ab, a \in A, b \in B$. In 1942, G. Hajós, in order to solve a geometric problem posed by Minkowski, introduced the notion of the direct product of subsets. He said that the group G is the direct product of two of its subsets, A and B, if each element of G is uniquely expressible in the form $ab, a \in A$, $b \in B$, and showed that under certain circumstances one of the sets is a group.

While Hajós's work grew out of a question concerning the partition of Euclidean n-dimensional space into congruent cubes, the present paper grew out of a question concerning partitions into congruent "crosses" and is concerned primarily with the existence of factorizations of the semigroup of integers modulo m into subsets A and B, of which A is prescibed as $\{1, 2, \cdots, k\}$ or $\{\pm 1, \pm 2, \cdots, \pm k\}$. The first three sections are algebraic and geometric, while the last two sections are number-theoretic.

Let A and B be subsets of a groupoid G. We will denote by AB the set $\{ab \mid a \in A, b \in B\}$. If each element of AB is uniquely expressible in the form $ab, a \in A, b \in B$, then we say that AB has the factoring (A, B) or briefly, $AB = (A, B)$. For instance, if G is a group, A is a subgroup of G, and B is a set of representatives of the right cosets of A in G, then $G = (A, B)$. The case when G is a finite abelian group and A and B are subsets of $G, G = (A, B)$, was examined in the classic paper of Hajós [3], later simplified by Szele [13] and Rédei [10].

When $AB = (A, B)$, there is no duplication among the elements $ab, a \in A, b \in B$. The opposite situation, when AB is "small" and there is therefore a great deal of duplication, has also been studied. See for instance Kemperman [6], [7].

For the most part the groupoid G that will concern us is S_n the multiplicative semigroup of the integers modulo n. We will be interested in factorizations $S_n - \{0\} = (A, B)$, where A is prescribed. Such factorizations, as we will show in § 2, are intimately connected with the existence of tessellations of Euclidean space by translates of certain finite collections of cubes. Before restricting the groupoid to S_n, we develop in § 1 some results that hold more generally.

1. Algebraic preliminaries.

If G is a groupoid and X is a

subset of G such that $X = (A, B)$, we will say that B *tiles* X or that B is a complement of A (in X). For any subset T of G a set of the form $Tg, g \in G$ is a *right translate* of T and a set of the form $gT, g \in G$ is a *left translate* of T.

Note that if G is a group and $G = (A, B)$, then $G = (Ax, yB)$ for any x and y in G. Thus if B tiles G, so does yB. For this reason we will assume when $G = (A, B)$ and G is a group that both A and B contain the identity element of G.

Note also that if G is a group and $G = (A, B)$ and $B = (C, D)$, then $G = (AC, D)$.

THEOREM 1.1. *Let G be a groupoid and $G = (A, B)$, where B is finite and has β elements. If $T \subset G$ has more than $(k - 1)\beta$ elements, then there is a right translate of A whose intersection with T has at least k elements.*

Proof. T is contained in the union of the β sets $Ab_1, Ab_2, \cdots, Ab_\beta$. If the cardinality of each set $T \cap Ab_i$, $i = 1, 2, \cdots, \beta$, were at most $k - 1$, then T would have at most $(k - 1)\beta$ elements, contradicting the hypothesis on T.

COROLLARY 1.2. *Let G be a group and $G = (A, B)$, where B is finite and has β elements. If $T \subset G$ has more than $(k - 1)\beta$ elements, then there is a right translate of T whose intersection with A has at least k elements.*

Proof. The identity $A \cap Tx^{-1} = (Ax \cap T)x^{-1}$, together with Theorem 1.1 yields the corollary.

Corollary 1.2 can be extended to finite quasigroups, as the following theorem shows.

THEOREM 1.3. *Let G be a finite quasigroup and $G = (A, B)$, where B has β elements. If $T \subset G$ has more than $(k - 1)\beta$ elements, then there is a right translate of T whose intersection with A has at least k elements.*

Proof. Consider the set of ordered couplets

$$Y = \{(g, a) \mid g \in G, a \in A \cap Tg\} .$$

If each Tg contains at most $k - 1$ elements of A, then Y has at most $|G|(k - 1)$ elements.

On the other hand, each element of G is uniquely expressible in the form $ab, a \in A, b \in B$. Now let T contain τ elements and A contain

α elements. Since G is a quasigroup, there are precisely τ different elements g in G, such that $a \in Tg$. Thus the cardinality of Y is precisely $\alpha\tau$ and we have $\alpha\tau \leqq |G|(k-1)$ or $\alpha\tau \leqq |G|(k-1)$. Using the equation $\alpha\beta = |G|$ we conclude that $\alpha\tau \leqq \alpha\beta(k-1)$ or $\tau \leqq \beta(k-1)$, contradicting the hypothesis on T.

We sketch an example that shows that the assumption in Theorem 1.3 that G is finite cannot be removed. The quasigroup G is defined on the set of positive integers N. We let $B = \{1, 2\}$, $T = \{1, 2, 3\}$, and A be the set of even positive integers. Define $t \circ 1$ and $t \circ 2$ in such a way that $T \circ 1 \cap T \circ 2 = \varnothing$ and each of $T \circ 1$ and $T \circ 2$ contains three elements of which at most one is even. Define $t \circ x$ for $t \in T$ and $x \in N - \{1, 2\}$ in such a way that $T \circ x$ has three elements of which at most one is even for each $x \in N - \{1, 2\}$, and such that left translation by t is a bijection of N for each $t \in T$. Define $x \circ 1$ and $x \circ 2$ for $x \in N - T$ in such a way that N is the disjoint union of $A \circ 1$ and $A \circ 2$, $x \circ 1 \neq x \circ 2$, and right translation of N by 1 or by 2 is a bijection of N. Then extend $\circ$ to a quasigroup G on N in any manner whatsoever. We have $G = (A, B)$, $\tau = |T| = 3$, $\beta = |B| = 2$, and $\tau > (2-1)\beta$. However no right translate of T meets A in two or more elements.

If B is a subset of a group G, then the existence of a factorization $G = (A, B)$ is closely related to the existence of a certain type of function on G, as we now show. Let Y be a set with the same cardinality as B. A function $f\colon G \rightarrow Y$ such that $f \mid gB\colon gB \rightarrow Y$ is a one-to-one correspondence for each $g \in G$ is a *B-coloring* of G.

THEOREM 1.4. *If B is finite and is contained in the center of G, then a B-coloring is also a B^{-1}-coloring.*

Proof. Let f be a B-coloring. We show first that f is one-to-one on each set gB^{-1}. Let $g_1, g_2 \in gB^{-1}$. Then $g_1 = gb_1^{-1}$ and $g_2 = gb_2^{-1}$ where $b_1, b_2 \in B$. Now, both g_1 and g_2 are in $g_1g_2g^{-1}B$. For we have

$$g_1g_2g^{-1}b_2 = g_1(gb_2^{-1})g^{-1}b_2 = g_1gg^{-1}b_2^{-1}b_2 = g_1$$

and

$$g_1g_2g^{-1}b_1 = g_1gb_2^{-1}g^{-1}b_1 = g_1b_2^{-1}b_1 = gb_1^{-1}b_2^{-1}b_1 = gb_2^{-1} = g_2 .$$

Since f is one-one on $g_1g_2g^{-1}B$, we see that $f(g_1) \neq f(g_2)$. Hence f is one-to-one on gB^{-1}.

THEOREM 1.5. *Let G be a group and B a subset of G. If f is a B^{-1}-coloring of G, then there is a factorization $G = (A, B)$.*

Proof. We may assume $1 \in Y$ and define $A = f^{-1}(1)$. We show that $G = (A, B)$. First of all, if

$$a_1B \cap a_2B \neq \emptyset ,$$

where $a_1, a_2 \in A$, we have $y \in a_1B \cap a_2B$, hence $yB^{-1} \ni a_1, a_2$. This is a contradiction, since f is a B^{-1}-coloring. Thus the family $[aB; a \in A]$ consists of disjoint sets. To show that this family covers G, consider any $y \in G$. Let $x \in yB^{-1}$ and $f(x) = 1$. Then $y \in xB$.

THEOREM 1.6. *If B is finite and is contained in the center of the group G, then a factorization $G = (A, B)$ induces a function f that is a B-coloring and a B^{-1}-coloring.*

Proof. Let $g \in G$. Then g is uniquely representable in the form ab, $a \in A$, $b \in B$. Define $F: B \rightarrow Y$ as some one-to-one correspondence. Then define $f: G \rightarrow Y$ by $f(ab) = F(b)$. We show that f is a B-coloring.

We show first that for any $g \in G, f \mid gB: gB \rightarrow Y$ is one-one. Indeed, assume that $x, y \in gB$ and $f(x) = f(y)$. Then $x = x_1b$ and $y = y_1b$ where x_1B and y_1B are distinct members of the B-tiling. We also have $x = gb_1$ and $y = gb_2$. Thus

$$gb_1 = x_1b \quad \text{and} \quad gb_2 = y_1b ,$$

hence

$$x_1bb_1^{-1} = y_1bb_2^{-1} .$$

Since B is in contained in the center of G, we have

$$b_1^{-1}x_1 = y_1b_2^{-1}$$

or

$$x_1b_2 = b_1y_1 = y_1b_1 ,$$

that is, $x_1B \cap y_1B \neq \emptyset$. This contradiction proves that f is a B-coloring. Theorem 1.4 implies that it is therefore a B^{-1}-coloring.

The relation between tiling and coloring provides a simple proof of the following theorem.

THEOREM 1.7. *Let G be a group and B a finite subset of the center of G. Assume that for any finite subset $S \subset G$ there is a subset X, $S \subset X \subset G$ such that X is the disjoint union of left translates of B. Then there is a factorization $G = (A, B)$.*

Proof. Note that we may assume that the X mentioned is finite. For each X mentioned in the statement of the theorem define

$\emptyset_X: X \rightarrow Y$ as in the proof of Theorem 1.6. For each $S \subset G$ define $\emptyset_S: S \rightarrow Y$ as the restriction of some $\emptyset_X$ to S where $X \supset S$. According to [2] there is a function $\emptyset: G \rightarrow Y$ such that for each $S \subset G$ there is $X \supset S$ such that $\emptyset_X | S = \emptyset | S$. We assert that $\emptyset$ is a B-coloring of G.

Let gB be a translate of B. Then $C = \bigcup \{xB \mid xB \cap gB \neq \emptyset\}$, is a finite set and thus there is a set $X \supset C$ such that $\emptyset_X | C = \emptyset | C$. The same argument used in the proof of Theorem 1.4 shows that $\emptyset_X | gB$ is one-one, hence $\emptyset | gB$ is one-one. Theorem 1.5 then shows that there is a factorization $G = (A, B)$.

THEOREM 1.8. *Let G be a group and A and B subsets of G. Then $G = (A, B)$ if and only if $A \cap gB^{-1}$ has exactly one element for each $g \in G$.*

Proof. Let G be a group and assume that A meets each member of $\{xB^{-1} \mid x \in G\}$ in one element. If $x \in G$ there is $a \in xB^{-1}$, hence $x = ab, a \in A, b \in B$. If $x = a_1b_1 = a_2b_2$, then $xB^{-1} \supset \{a_1, a_2\}$, hence $a_1 = a_2$ and $b_1 = b_2$.

Conversely, assume that $G = (A, B)$. Then for $x \in G$ $x = ab, a \in A$, $b \in B$ hence $a \in xB^{-1}$. If $a_1, a_2 \in xB^{-1}$, then $a_1 = xb_1^{-1}$ and $a_2 = xb_2^{-1}$ hence $a_1b_1 = a_2b_2$.

2. A relation between factorings in a ring.

A factoring in the multiplicative semigroup of one ring may under certain circumstances induce a factoring in the additive group of another ring, as the next theorem shows. This theorem will be used in § 3 and § 4 to obtain tessellations of Euclidean space.

THEOREM 2.1. *Let R and R^* be rings and $\emptyset: R \rightarrow R^*$ an onto ring homomorphism. Then a direct factoring, $R^* - \{0\} = (A^*, B^*)$, in the multiplicative semigroup of R^* induces a direct factoring of the additive group of R^n, $R^n = (A, B)$, where n is the order of B^*, B is any subset of R such that $\emptyset | B$ is a one-to-one correspondence between B and B^*, and A is defined below.*

Proof. We present the proof in the case that n is finite. Let a_i^* denote a typical element of A^* and b_j^* denote a typical element B^*. For each a_i^* select $a_i \in R$ such that $\emptyset(a_i) = a_i^*$ and for each b_j^* select $b_j \in R$ such that $\emptyset(b_j) = b_j^*$. Define $B \subset R^n$ as $[(r_1, \cdots, r_n) \mid r_i \in R$, $\emptyset(\sum_{j=1}^n r_jb_j) = 0]$. Define $A \subset R^n$ as $(0, 0, \cdots, 0)$ together with all elements of the form $(0, 0, \cdots, a_i, \cdots, 0)$ where $a_i \in R$ and all entries are 0 except one. (Each elements a_i thus appears as an entry in n different elements of A; A is finite if and only if A^* is finite.)

We show that $R^n = (A, B)$, where the binary operation considered is addition in R^n. Let $(r_1, \cdots, r_n)$ be an arbitrary element of R^n. If $\varnothing(\sum_{j=1}^n r_j b_i) = 0$ then $(r_1, \cdots, r_n) \in B$. Since $(0, \cdots, 0) \in A$, we have $(r_1, \cdots, r_n) \in A + B$. If $\varnothing(\sum_{j=1}^n r_j b_j) = u^* \neq 0$, then there are $a_{i_0}^* \in A^*$ and $b_{j_0}^* \in B^*$ such that $u^* = a_{i_0}^* b_{j_0}^*$. Consider $x = (r_1, \cdots, r_n) - (0, \cdots, a_{i_0}, \cdots, 0)$ where a_{i_0} is entered in the j_0th coordinate. It is easy to show that $x \in B$ and thus we have $(r_1, \cdots, r_n) \in A + B$.

Finally we show that the representation of elements of R^n in the form $a + b, a \in A, b \in B$, is unique. Assume that

$$(r_1, \cdots, r_n) + (0, \cdots, a_i, \cdots, 0) = (r_1', \cdots, r_n') + (0, \cdots, a_{i'}, \cdots, 0) ,$$

where a_i is in the jth coordinate and $a_{i'}$ is in the j'th coordinate, and $(r_1, \cdots, r_n)$ and $(r_i', \cdots, r_n')$ are in A. From the above equation it follows that $a_i^* b_j^* = a_{i'}^* b_{j'}^*$, hence $a_i = a_{i'}$ and $j = j'$. It follows also that $(r_i, \cdots, r_n) = (r_i', \cdots, r_n')$ and the proof is complete.

Theorem 2.1 will concern us most when R is the ring of integers, m is an integer, $R^* = R/(m)$ and $\varnothing$ is the natural homomorphism. Theorem 2.1 shows how a factoring $S_m - [0] = (A^*, B^*)$, where A^* has α elements and B^* has n elements, induces a direct factoring of the n-dimensional lattice R^n, $R^n = (A, B)$, where A has $n\alpha + 1$ elements, and B is a subgroup of the additive group of R^n.

This will enable us to tile the lattice R^n by translates of certain finite subsets of R^n, or equivalently, to tessellate Euclidean space E^n by translates of certain finite collections of unit cubes in E^n.

3. Tiling the lattice R^n by crosses and semicrosses.

A (k, n)-cross is a translate of the set of $2kn + 1$ elements of R^n consisting of the origin and the $2nk$ elements $(0, \cdots, \pm j, \cdots, 0)$ where $1 \leqq j \leqq k$ and j appears in any one of the n coordinates. A (k, n)-semicross is defined similarly except only j (not $-j$) appears as a coordinate. The center of a (k, n)-cross is the translate of $(0, 0, \cdots, 0)$. A (k, n)-semicross has $kn + 1$ elements. The *vertex* of a (k, n)-semicross is the translate of $(0, 0, \cdots, 0)$. As Theorem 2.1 shows, if $S_{2nk+1} - \{0\} = ([\pm 1, \cdots, \pm k], B)$, then there is a tiling of R^n by (k, n)-crosses whose centers form a subgroup, L, of the additive group of R^n and R^n/L is isomorphic to the cyclic group of order $2kn + 1$. Such a tiling we call *cyclic*. A similar remark holds for tilings by semicrosses. It is no loss of generality to consider only tilings in which one center (or vertex) is at the origin.

We now introduce several functions that record the existence or nonexistence of certain tilings. If there is a tiling of R^n by (k, n)-crosses, we shall set $g(k, n) = 1$; if there is none, we set $g(k, n) = 0$.

If there is a cyclic tiling by (k, n)-crosses, we set $c(k, n) = 1$, otherwise, $c(k, n) = 0$. Similarly we define the functions g^* and c^* for semicrosses. If $c(k, n) = 1$, then $g(k, n) = 1$. For $n = 1$ or 2 any tiling by (k, n)-crosses or (k, n)-semicrosses is cyclic. We have $g(k, 1) = c(k, 1) = 1$ for all k and $g^*(k, 1) = c^*(k, 1) = 1$ for all k. It is a simple matter to verify that $g(1, 2) = c(1, 2) = 1$ and $g(k, 2) = 0$ for all $k \geqq 2$, while $g^*(k, 2) = c^*(k, 2) = 1$ for all k. The functions c and c^* are examined in § 4 and § 5. In this section we discuss the geometric functions g and g^*. The first theorem relates g to g^*.

THEOREM 3.1. *If $g(k, n) = 1$, then $g^*(k, 2n) = 1$.*

Proof. Let $C = \{(c_1, c_2, \cdots, c_n)\}$ be the set of centers of a tiling of R_n by (k, n)-crosses. Consider the set S of (k, n)-semicrosses in R_{2n} whose vertices are at

$$\{(d_1, \cdots, d_n, d_1 - c_1, \cdots, d_n - c_n)\} ,$$

where $(d_1, \cdots, d_n) \in R_n$ is arbitrary and $(c_1, \cdots, c_n) \in C$. We show that S partitions R_{2n}.

To show that S covers R_{2n} consider a typical point $(x_1, \cdots, x_{2n})$ in R_{2n}. Then the point

$$(x_1 - x_{n+1}, x_2 - x_{n+2}, \cdots, x_n - x_{2n})$$

is in R_n. Hence for a suitable $(c_1, \cdots, c_n) \in C, \alpha \in \{0, 1, 2, \cdots, k\}$, and $i \in [1, n]$ we have

$$\begin{aligned} &x_1 - x_{n+1} = c_1, x_2 - x_{n+2} = c_2, \cdots, \\ &x_i - x_{n+i} = c_i - \alpha \text{ or } c_i + \alpha, \cdots, x_n - x_{2n} = c_n . \end{aligned}$$

If $x_i - x_{n+i} = c_i - \alpha$, then $x_{n+i} = x_i - c_i + \alpha$ and thus $(x_i, \cdots, x_{2n})$ is in the semicross whose vertex is at

$$(x_1, \cdots, x_n, x_1 - c_1, \cdots, x_i - c_i, \cdots, x_n - c_n) .$$

On the other hand, if $x_i - x_{n+i} = c_i + \alpha$, then $x_{n+i} = (x_i - c_i) - \alpha$ and $(x_1, \cdots, x_{2n})$ is in the semicross whose vertex is at

$$\begin{aligned} &(x_1, x_2, \cdots, x_i - \alpha_i, x_{i+1}, \cdots, x_n, x_1 - c_1, x_2 - c_2, \cdots, x_i - \alpha - c_i, \\ &\quad x_{i+1} - c_{i+1}, \cdots, x_n - c_n) . \end{aligned}$$

Thus S covers R_{2n}.

We next show that the elements of S are disjoint. If the semicross whose vertex is at $(x_1, \cdots, x_n, x_1 - c_1, \cdots, x_n - c_n)$ meets the semicross whose vertex is at $(y_1, \cdots, y_n, y_1 - c_1', \cdots, y_n - c_n')$, then

$$
\begin{aligned}
(3.1)\qquad &(x_1, \cdots, x_n, x_1 - c_1, \cdots, x_n - c_n) + (0, \cdots, \alpha, \cdots, 0) \\
&= (y_1, \cdots, y_n, y_1 - c'_1, \cdots, y_n - c'_n) + (0, \cdots, \beta, \cdots, 0) ,
\end{aligned}
$$

where α is in the ith coordinate and β is in the jth, $0 \leqq \alpha, \beta \leqq k$; hence

$$(3.2)\qquad (c_1, \cdots, c_i \pm \alpha, \cdots, c_n) = (c'_1, c'_2, \cdots, c'_j \pm \beta, \cdots, c'_n)$$

where the ambiguous signs in (3.2) are positive if $i \leqq n$ or $j \leqq n$, and negative if $i > n$ or $j > n$. Since the (k, n)-crosses in n-space are disjoint, $c_1 = c'_1, \cdots, c_n = c'_n, i = j, \alpha = \beta$. From (3.1) it then follows that $x_i = y_i, i = 1, 2, \cdots, n$. Thus distinct semi-crosses in R_{2n} are disjoint. The proof is complete.

THEOREM 3.2. *If $k > 2n - 2$, and $n \geqq 2$, then $g(k, n) = 0$.*

Proof. Assume that we have a tiling of R^n by (k, n)-crosses: $R^n = (A, B)$ where A is the set of centers of the crosses. Let

$$T = \{(i, j, 0, \cdots, 0) \mid 1 \leqq i \leqq k + 1, 1 \leqq j \leqq k + 1\} .$$

The cardinality of T, $(k + 1)^2$, is greater than the cardinality of a (k, n)-cross, $2kn + 1$, since the inequality

$$(k + 1)^2 > 2kn + 1$$

is equivalent, for $k > 0$, to the inequality $k > 2n - 2$.

By Theorem 1.1 at least two centers of the tiling can be assumed to be in a translate of T. But the crosses that have those two centers would intersect. From this contradiction the theorem follows.

THEOREM 3.3. *There is no tiling of R^3 by* (3, 3)*-crosses, that is,* $g(3, 3) = 0$.

Proof. A (3, 3)-cross has 19 elements. Let T consist of the 20 points: $[(i, j, 0) \mid 1 \leqq i \leqq 5, 1 \leqq j \leqq 4\}$. If there were a tiling of R^3 by (3, 3)-crosses, then there would be, by Theorem 1.1, such a tiling having at least two centers in T. Since the crosses are disjoint, we may assume that two centers are either

I: (1, 1, 0) and (5, 4, 0); or
II: (1, 1, 0) and (5, 3, 0); or
III: (1, 1, 0) and (5, 2, 0).

We show that I and II connot occur. The points (2, 2, 0), (3, 2, 0), (4, 2, 0) would lie in three crosses whose centers are not on the xy-plane. At least two of these three crosses would have their centers on the same side of the xy-plane and hence would intersect.

The remaining case, III, can be disposed of by considering the crosses that would contain the points (2, 3, 0), (2, 4, 0), (3, 3, 0), (3, 4, 0), (4, 3, 0), and (4, 4, 0).

THEOREM 3.4. *There is no tiling of R^3 by* (4, 3)-*crosses, that is,* $g(4, 3) = 0$.

Proof. A (4, 3)-cross has 25 elements. Let T consist of the 26 points: $\{(i, j, 0) \mid 1 \leqq i, j \leqq 5 \text{ and } (6, 3, 0)\}$.

If there were a tiling by (4, 3)-crosses, there would be one that has at least two of its centers in T. Since at most one of the centers can be of the form $(i, j, 0), 1 \leqq i, j \leqq 5$, one of the centers would be at (6, 3, 0). The other center we may then assume is at (1, 1, 0) or (1, 2, 0). In the first case, the points (2, 2, 0), (3, 2, 0), (4, 2, 0) could not be covered. In the second case, consider the four points (2, 1, 0), (3, 1, 0), (4, 1, 0), (5, 1, 0). At most one of these four points is covered by a cross whose center is in the xy-plane. Thus at least three of the four points are covered by crosses whose centers are not in the xy-plane. At least two of these three crosses have their centers on the same side of the xy-plane and would therefore intersect.

The factoring $G_{13} = (\{\pm 1, \pm 2\}, \{1, 3, 4\})$ shows that $c(2, 3) = 1$, hence $g(2, 3) = 1$. Thus $g(k, 3) = 1$ for $k = 1$ and 2; for $k \geqq 3$, $g(k, 3) = 0$.

It is of interest to note that in any tiling of R^3 by (1, 3)-crosses or by (2, 3)-crosses, the centers form a lattice. We outline a proof for this in the case of (1, 3)-crosses. Each (1, 3)-cross has seven elements. Let T consist of these eight elements: $\{(i, j, 0) \mid 0 \leqq i \leqq 2, 0 \leqq j \leqq 1\} \cup \{i, 2, 0) \mid i = 0, 1\}$. By Theorem 1.1 we may assume two of the centers of the tiling are in T and, by symmetry, either $\{(0, 0, 0), (1, 2, 0)\}$ or $\{(2, 0, 0), (0, 2, 0)\}$; the latter is not part of any tiling, so consider the former. For the tiling to cover (0, 1, 1) either the (1, 3)-cross with center $(-1, 1, 1)$ or the (1, 3)-cross with center (0, 1, 2) is present. Consider the case $(-1, 1, 1)$, hence the "initial configuration" (0, 0, 0), (1, 2, 0) and $(-1, 1, 1)$. Then the (1, 3)-crosses with centers $(0, 1, -2)$, $(2, 1, -1)$, (1, 1, 2), (0, 3, 1), (0, 2, 3), (3, 2, 1), (2, 3, 2), (2, 4, 0), (1, 5, 1), $(-1, 2, -1)$, $(0, 4, -1)$, $(1, 3, -2)$, $(-3, 0, 2)$, $(-3, 1, 0)$, $(-2, 3, 0)$, $(-2, 2, 2)$ are present in the tiling. Thus the translations of the initial configuration by the vectors $V_1 = (1, 2, 0)$, $V_2 = (-1, 1, 1)$ and $V_3 = (0, 1, -2)$ are also present in the tiling. We next show that the translation of the initial configuration by $-(V_1 + V_2 + V_3) = (0, -4, 1)$ is also present. For, starting from the initial configuration, we see that $(0, 1, -2)$, $(2, 1, -1)$, $(1, -1, -1)$, $(-2, 0, -1)$, $(-2, 0, -1)$, $(-1, -2, 0)$, $(-1, -1, -2)$, $(0, -3, -1)$, $(0, -1, 2)$, $(1, -2, 1)$, $(0, -4, 1)$, $(-1, -2, 0)$, $(-2, -1, 1)$, $(0, -1, 2)$,

$(-1, 0, 3)$ and $(-1, -3, 2)$ are present. Thus the set of centers contains the set $a_1 V_1 + a_2 V_2 + a_3 V_3$ where a_1, a_2, a_3 are arbitrary integers. Since the determinant of the matrix consisting of these three vectors is 7, the set of centers coincides with the lattice generated by the three vectors. The point (x, y, z) is in the lattice if and only if $x + 3y - 2z \equiv 0 \pmod 7$; this corresponds to the factoring $G_7 = (\{1, -1\}; \{1, 3, -2\})$.

We should point out that there are tilings of R^3 by $(1, 3)$-semicrosses which are not a lattice and that there is a tiling in which the centers form a lattice L, such that $R^3/L = Z_2 \times Z_2$.

4. Characters and factoring of $S_m - \{0\}$.

By a character on a groupoid G we shall mean a homomorphism $\chi: G \to R$ from G into the multiplicative semigroup of a ring R. If Z_m is the additive group of integers mod m, p is prime and m is a positive integer, then an onto homomorphism $h: G_p \to Z_m$ we shall call a (p, m)-homomorphism; note that m divides $p - 1$.

THEOREM 4.1. *Let G be a finite groupoid, $G = (A, B)$, and $\chi: G \to R$ be a character from G into the ring R. Then*

$$\Big(\sum_{a \in A} \chi(a)\Big) \cdot \Big(\sum_{b \in B} \chi(b)\Big) = \sum_{g \in G} \chi(g) .$$

Proof.

$$\sum_{g \in G} \chi(g) = \sum_{a \in A, b \in B} \chi(ab) = \sum_{a \in A\ b \in B} \chi(a)\chi(b) = \sum_{a \in A} \chi(a) \cdot \sum_{b \in B} \chi(b) .$$

In particular $\chi: S_{ab+1} \to R_{ab+1}$ given by $\chi(s) = s^r$, where r is a fixed positive integer, is a character. We have therefore $(\sum_{i=1}^{a} a_i^r)(\sum_{j=1}^{b} b_j^r) \equiv \sum_{i=1}^{ab} i^r (\mathrm{mod}\, ab + 1)$. In a similar vein, note that $(\prod_{i=1}^{a} a_i^b)(\prod_{j=1}^{b} b_j^a) \equiv (n - 1)! \pmod n$, hence if n is prime, the product is $\equiv -1 \pmod n$.

COROLLARY 4.2. *If G is a finite quasigroup, $G = (A, B)$, R has an identity element but no zero divisors, $\chi: G \to R$ is not constant with the value 1, then either $\sum_{a \in A} \chi(a) = 0$ or $\sum_{b \in B} \chi(b) = 0$.*

Proof. Select $g_0 \in G$, $\chi(g_0) \neq 1$. Then $\sum_{g \in G} \chi(g) = \sum_{g \in G} \chi(g_0 g) = \chi(g_0) \sum_{g \in G} \chi(g)$; hence $(1 - \chi(g_0)) \sum_{g \in G} \chi(g) = 0$. Since R has no zero-divisors, $\sum_{g \in G} \chi(g) = 0$, and either $\sum_{a \in A} \chi(a) = 0$ or $\sum_{b \in B} \chi(b) = 0$.

COROLLARY 4.3. *Let $G = (A, B)$ where G is the group of residue classes modulo an odd prime p. Then in at least one of A and B the number of quadratic residues equals the number of nonquadratic residues.*

Proof. Let R be the ring of integers and $\chi: G \rightarrow R$ be the Legendre symbol modulo p. We have $\sum_{g \in G} \chi(g) = 0$. The corollary follows from Theorem 4.1.

Corollary 4.2 applied to the character $\chi: G_p \rightarrow R_p$, where $\chi(g) = g$, yields the information that either $\sum_{i=1}^{m} a_i = 0$ or $\sum_{i=1}^{n} b_j = 0$, an assertion that would also follow by considering the product $\sum_{i=1}^{m} a_i \sum_{j=1}^{n} b_j$. This implies that if $kn + 1$ is prime and $n > 1$, then in a cyclic tiling of R^n by (k, n)-semicrosses, the point $(1, 1, \cdots, 1)$ is the vertex of one of the semicrosses.

THEOREM 4.4. *If n is odd and $8n + 1$ is prime, then $c(4, n) = 0$.*

Proof. The integers $1, 2, 4, -1, -2, -4$ are quadratic residues $\bmod p = 8n + 1$. Thus the number of quadratic residues in $\{\pm 1, \pm 2, \pm 3, \pm 4\}$ is not equal to the number of quadratic nonresidues there. Hence the number of quadratic residues in a complement equals the number of nonquadratic residues there; thus n is even and we have a contradiction.

As examples, we have $c(4, n) = 0$ for $n = 5, 9, 11, 17$.

THEOREM 4.5. *If $8n + 1 \equiv 0 \pmod 3$ but $8n + 1 \not\equiv 0 \pmod 9$, then $c(4, n) = 0$.*

Proof. Assume that $S_{8n+1} = (\{\pm 1, \cdots, \pm 4\}, B)$. Define $\chi: R_{8n+1} \rightarrow R_{8n+1}$ by $\chi(s) = s^2$. Let $m = 8n + 1$. From our observation it follows that

$$2(1^2 + 2^2 + 3^2 + 4^2) \sum b_i^2 \equiv 1^2 + 2^2 + \cdots + (m - 1)^2 (\mathrm{mod}\, m) .$$

Thus the equation

$$60x \equiv \frac{m(m-1)(2m-1)}{6} \pmod m$$

is solvable. Thus $(60, m)$ is a divisor of

$$m(m-1)(2m-1)/6 = (8n + 1)(8n)(16n + 1)/6 .$$

Since $8n \equiv -1 (\mathrm{mod}\, 3)$, we have $16n + 1 \equiv -1 (\mathrm{mod}\, 3)$. Thus 3 is a divisor of $(8n + 1)/3$, that is, $8n + 1 \equiv 0 (\mathrm{mod}\, 9)$, a contradiction.

Theorem 4.5 implies that $c(4, n) = 0$ for $n = 9t - 2$ and $n = 9t + 4$, in particular when $n = 4, 7, 13, 16$.

Let A be a set of m distinct positive integers less than the prime p. Let G be the group of residue classes modulo p (in which we may consider A to be imbedded). It may be that there is a subgroup $B \subset G_p$ such that A constitutes a set of representatives of all the cosets of B. Then we would have $G_p = (A, B)$. If B has n elements and A has m elements, then $mn = p - 1$. Moreover there would be a (p, m)-homomorphism, $h: G_p \rightarrow Z_m$, where Z_m is the cyclic group on m elements, which we most conveniently take to be $\{0, 1, \cdots, m - 1\}$ with addition modulo m. The kernel of h is B and $h \mid A$ is a one-one correspondence between A and Z_m. Conversely, if there is a (p, m)-homomorphism h such that $h \mid A$ is a one-one correspondence between A and Z_m, then we have $G = (A, \text{kernel } h)$.

As a special case let us consider $A = A_m = \{1, 2, 3, \cdots, m\}$. A bijection

$$\varnothing: \{1, 2, \cdots, m\} \rightarrow Z_m$$

is a *weak isomorphism* if whenever x, y, and xy are in $\{1, 2, \cdots, m\}$ then $\varnothing(xy) = \varnothing(x) + \varnothing(y)$.

THEOREM 4.6. *Let $A_m = \{1, 2, 3, \cdots, m\}$ and $\varnothing: A_m \rightarrow Z_m$ be a weak isomorphism. If there exists a (p, m)-homomorphism, h, such that $h(p_i) = \varnothing(p_i)$ for the primes in A_m, then there is a direct factorization, $G_p = (A_m, \textit{kernel } h)$.*

Proof. Since $\varnothing(p_i) = h(p_i)$, it follows that $\varnothing(x) = h(x)$ for all $x \in A_m$. By the preceding observations, we have the factorization $G_p = (A_m, \text{kernel } h)$.

THEOREM 4.7 (*Kummer-Mills*). *Let $\varnothing: A_m \rightarrow Z_m$ be a weak isomorphism. If m is odd, then $\varnothing$ is extendable to a (p, m)-homomorphism for an infinity of primes p. If m is even, then $\varnothing$ is extendable to a (p, m)-homomorphism if and only if $\varnothing$ satisfies these conditions:*

(i) *If $m = 2t$, t odd, and if $p_i \mid t$, $p_i \equiv 1 (\text{mod } 4)$, then $\varnothing(p_i)$ is even*; *and if $p_i p_j \mid t$, $p_i \equiv p_j (\text{mod } 4)$, then $\varnothing(p_i) - \varnothing(p_j)$ is even.*

(ii) *If $m = 4s$ and $p_i \mid s$, then $\varnothing(p_i)$ is even.*

Moreover if there is one extension, then there are infinitely many.

The necessity of hypotheses (i) and (ii) follows directly from the quadratic reciprocity theorem. Kummer disposed of prime m in 1859 and Mills of composite m in 1963 [9]. Their result is more general than Theorem 4.7.

A weak isomorphism $\varnothing: A_m \rightarrow Z_m$ satisfying the pertinent hypothesis in Theorem 4.7 we will call an M-function. In particular if m is of the form $2p^n$, where p is a prime of the form $4t + 3$, then any weak isomorphism is an M-function. Furthermore, if $m + 1$ is prime G_{m+1} is a group isomorphic to Z_m and there exists an M-function

$\varnothing: A \rightarrow Z_m$. The following is a consequence of these observations.

COROLLARY 4.8. *If $m+1$ is prime, then $c^*(m, n) = 1$ for an infinitude of n such that $mn+1$ is prime.*

THEOREM 5.4 shows that if $2m+1$ is prime, then $c^*(m, 4m+4) = 1$.

COROLLARY 4.9. *If m is odd and there exists a weak isomorphism $\varnothing: A_m \rightarrow Z_m$, then $c^*(m, n) = 1$ for an infinitude of n such that $mn+1$ is prime.*

THEOREM 4.10. *If $h: G_p \rightarrow Z_m$ is a homomorphism such that $h \mid A_m$ is a one-to-one correspondence between A_m and Z_m, then there is an M-function on A_m.*

Proof. Define $\varnothing(x) = h(x)$ for each $x \in A_m$. Then $\varnothing$ is a weak isomorphism from A_m to Z_m. Since $\varnothing$ has an extension h, it is an M-function.

THEOREM 4.11. *Let p be a prime, m a divisor of $p-1$, and g a primitive root* modulo *p. Let $i(x)$ denote the index of x relative to the base g. If $i(1), i(2), \cdots, i(m)$ are incongruent* modulo *m, then there is a factorization $G = (A_m, B)$ where B is a subgroup of G. Conversely, if B is a subgroup of G and $G = (A_m, B)$, then $i(1), i(2), \cdots, i(m)$ are incongruent* modulo *m.*

Proof. Observe that x is an mth power in G if and only if $m \mid i(x)$. If B consists of the mth powers, then $xB = yB$ if and only if $i(x) = i(y) (\operatorname{mod} m)$. Hence if $i(1), \cdots, i(m)$ are incongruent modulo m, $G = (A_m, B)$.

Conversely, if B is a subgroup of G such that $G = (A_m, B)$, then, since there is at most one subgroup of G of each order, B is the group of mth powers. Hence $i(1), \cdots, i(m)$ are incongruent modulo m.

For instance, consider $c^*(6, n)$. Define $\varnothing: \{1, 2, 3, 4, 5, 6\} \rightarrow \{0, 1, 2, 3, 4, 5\}$ by $\varnothing(1) = 0$, $\varnothing(2) = 1$, $\varnothing(3) = 3$ and $\varnothing(5) = 5$. Clearly $\varnothing$ satisfies the hypothesis of Theorem 4.7 and we conclude that $c^*(6, n) = 1$ for an infinite set of n. Moreover, if n is even, $h: G_{6n+1} \rightarrow Z_n$, a homomorphism of the type described in Theorem 4.7, can be used to show that $c(6, n/2) = 1$. For if n is even, -1 is a quadratic residue modulo $6n+1$. Since $(-1)^3 = -1$, we deduce that -1 is a sixth power modulo $6n+1$, hence $-1 \in$ kernel h. Thus the kernel of h has a factorization $(\{1, -1\}, B)$ and we conclude that $c(6, n/2) = 1$.

Inspection of a table of indices shows that the primes p less than

2000 for which a homomorphism $G_p \to Z_6$ exists that is one-one on $\{1, 2, 3, 4, 5, 6\}$ are: 7, 13, 103, 487, 547, 832, 967, 1063, 1663. Only in the case $p = 13$ is $n = (p - 1)/6$ even. Computations by E. Lehmer show that the next prime for which n is even is 7477. Thus $c(6, 623) = 1$.

Theorem 4.7 shows that $c^*(7, n) = 1$ for an infinity of n. In particular $c^*(7, 94) = 1$ and, as above, $c(7, 47) = 1$. Similarly, $c^*(3, 46) = 1 = c(3, 23)$.

Under certain circumstances, if $S_{kn+1} - \{0\} = (\{1, 2, \cdots, k\}, B)$ and $kn + 1$ is prime, and $1 \in B$, then B must be a group. The next theorem is thus related to Theorem 4.6. Moreover, as Theorem 3 of Sands [12] implies, if $c^*(k, n) = 1$, $(k, n) = 1$, k is a power of a prime, and $kn + 1$ is prime, then there is a charactor $\chi\colon G_{kn+1} \to Z_k$ that is one-one on $[1, 2, \cdots, k]$.

THEOREM 4.11. *If n and $nk + 1$ are prime and $G_{nk+1} = (\{1, 2, \cdots, k\}, B)$, then B is a group.*

Proof. It was proved by Sands [11] that if G is a cyclic group, $G = (A, B)$ and the order of B is prime, then either A or B is periodic, that is, there is an element $g \in G$, $g \neq 1$, such that $gA = A$ or $gB = B$. Therefore, if $G_{nk+1} = (\{1, 2, \cdots, k\}, B)$ and the order of B is prime, then either $\{1, 2, \cdots, k\}$ or B is periodic. If $g\{1, 2, \cdots, k\} = \{1, 2, \cdots, k\}$, we have $g = g \cdot 1 \in \{1, 2, \cdots, k\}$, from which it is easy to see that $g\{1, 2, \cdots, k\} \not\subset \{1, 2, \cdots, k\}$. Thus B is periodic, $gB = B$ for some $g \in G_{kn+1}$, $g \neq 1$. Since $1 \in B$, B contains the group H generated by g and is the union of cosets of H. Thus the order of H, being a divisor of the prime n, equals n, and therefore $H = B$. This ends the proof.

5. Miscellaneous results on $c(k, n)$ and $c^*(k, n)$.

In this section we examine $c(k, n)$ and $c^*(k, n)$ for small k and also special values of k and n. This table, based partly on theory and partly on computations, describes the behavior of $c(k, n)$ for $2 \leqq k \leqq 5$ and $2 \leqq n \leqq 20$.

5	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0
3	0	0	0	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0
2	0	1	1	0	1	1	0	1	1	0	0	1	0	1	1	0	0	0	0
	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20

Moreover $c(k, 5) = 0$ for all $k > 1$.

THEOREM 5.1. *If the order of 2 modulo $4n + 1$ is odd, then*

$c(2, n) = 0$. *If* $4n + 1$ *is prime and the order of* 2 *modulo* $4n + 1$ *is odd or twice an odd number, then* $c(2, n) = 0$.

Proof. Assume that the order of 2 modulo $4n + 1$ is t, an odd number and that $S_{4n+1} \equiv (\{\pm 1, \pm 2\}, B)$. We may assume that $1 \in B$, hence $-1, \pm 2 \notin B$. Since $2^2 = ab$ for some $a \in \{\pm 1, \pm 2\}, b \in B$, and since $b \neq -1, \pm 2$, we may assume $2^2 \in B$. Proceeding in this fashion inductively, we obtain $2, 2^3, 2^5, \cdots, \notin B$, hence $2^t \notin B$. But $2^t = 1 \in B$.

Assume next that $4n + 1$ is prime and that the order of 2 modulo $4n + 1$ is $2s$, where s is odd. Consider the subgroup G of S_{4n+1} generated by 2. Since $2^s \equiv -1 (\operatorname{mod} 4n + 1)\{1, 2, -1, -2\} \subset G$. If $S_{4n+1} = (\{\pm 1, \pm 2\}, B)$, then $G = (\{\pm 1, \pm 2\}, B \cap G)$. Therefore the order of $G, 2s$, is divisible by 4, contradicting the assumption that s is odd.

Incidentally, for $n = 11$, the order of 2 modulo $4n + 1 = 45$ is twice an even number namely 12, and $c(2, 11) = 0$. If the modulus is prime, however, we have the following companion of Theorem 5.1.

THEOREM 5.2. *If* $4n+1$ *is prime and the order of* 2 modulo $4n+1$ *is twice an even number, then* $c(2, n) = 1$.

Proof. Let the order of 2 be $4s$. Then $\{2^0, 2^1, \cdots, 2^{4s-1}\}$ is a subgroup of the group G_{4n+1}, hence a factor of G_{4n+1}. Now, $2^{2s} = -1$, so $\{\pm 1, \pm 2\} = \{2^0, 2^{2s}, 2^1, 2^{2s+1}\}$. We therefore have the factorization

$$\{2^0, 2^1, \cdots, 2^{4s-1}\} = \{\pm 1, \pm 2\}\{2^0, 2^2, \cdots, 2^{2s-2}\} .$$

This concludes the proof.

COROLLARY 5.3. *If* $4n + 1$ *is prime, then* $c(2, n) = 1$ *if and only if the order of* 2 modulo $4n + 1$ *is twice an even number.*

According to Bang's theorem, for any $m > 1$ there is a prime p such that $2^m \equiv 1 (\operatorname{mod} p)$ but $2^i \not\equiv 1 (\operatorname{mod} p), 1 \leqq i < m$. Thus for any integer $m \geqq 2$ there is a prime p such that the order of 2 modulo p is m. Combining this with Corollary 5.3, we see that there are an infinite number of n such that $c(2, n) = 0$ and $4n + 1$ is prime, and an infinite number of n such that $c(2, n) = 1$ and $4n + 1$ is prime.

THEOREM 5.4. *If* p *is an odd prime, then* $c((p - 1)/2, p + 1) = 1$.

Proof. Let $2k + 1 = p$, an odd prime. Let $B \subset S_{p^2} - \{0\}$ be the set

$$\{p\} \cup \{px + 1: x = 0, 1, \cdots, k\} \cup \{py - 1: y = 1, 2, \cdots, k\}$$

and let $A = \{\pm 1, \pm 2, \cdots, \pm k\}$. We assert that $S_{p^2} - \{0\} = (A, B)$.

To verify this assertion note that A has $2k$ elements, B has $2k + 2$ elements, and that $(2k)(2k + 2) = (2k + 1)^2 - 1 = p^2 - 1$. Thus to show that $S_{p^2} - \{0\} = (A, B)$, it suffices to show that $ab \equiv a'b' (\mathrm{mod}\, p^2)$, $a, a' \in A$, $b, b' \in B$, implies that $a \equiv a'$ and $b \equiv b' (\mathrm{mod}\, p^2)$. Verification of this is straightforward.

In particular

$$c(2, 6) = c(3, 8) = c(5, 12) = c(6, 14) = c(8, 18) = c(9, 20) = 1 .$$

Incidentally an alternative description of B in the preceding proof is $B = \{p\} \cup \{(p - 1)^i : i = 0, 1, \cdots, p - 1\}$.

THEOREM 5.5. *If $m = 2kn + 1$ has a divisor d such that $(d, k!) = 1$ and $d > n$, then $c(k, n) = 0$.*

Proof. Assume that $S_m - \{0\} = (A, B)$, where $A = \{\pm 1, \pm 2, \cdots, \pm k\}$, and consider the representation of d, $d \equiv ab (\mathrm{mod}\, m)$. Since $(d, a) = 1$, we have $d \mid b$, hence $b = cd$ for some integer c.

From the assumption that $d > n$ it follows that $m/d = (2kn + 1)/d \leqq 2k$. Thus there are elements $i, j \in A$ such that $i + j = m/d$. We then have

$$ib + jb = \frac{m}{d} \cdot b = mc \equiv 0 (\mathrm{mod}\, m)$$

hence

$$ib \equiv -jb (\mathrm{mod}\, m)$$

and (A, B) is not a factoring of $S_m - \{0\}$.

On the basis of Theorem 5.5 we conclude that $c(3, 14) = 0$ since $m = 5 \times 17$, and $17 > 14$; $c(3, 19) = 0$ since $m = 5 \times 23$ and $23 > 19$; $c(4, 13) = 0$ since $m = 3 \times 35$ and $35 > 13$; $c(4, 18) = 0$ since $m = 5 \times 29$ and $29 > 18$. Similarly $c(5, n) = 0$ for $n = 14, 16, 17$.

COROLLARY 5.6. *If $n = 3t + 2$, then $c(2, n) = 0$.*

THEOREM 5.7. *If $c(k, n) = 1$ and d is a divisor of $m = 2kn + 1$ such that $(d, k!) = 1$, then $c(k, (2nk + 1 - d)/2kd) = 1$.*

Proof. Let $q = m/d$ and consider $C = \{d, 2d, \cdots, (q - 1)d\} \subset S_m$. Assume that $S_m - \{0\} = (A, B)$, where $A = \{\pm 1, \cdots, \pm k\}$. For each $j, 1 \leqq j \leqq q - 1$ there is a representation $ab \equiv jd (\mathrm{mod}\, m)$, $a \in A$, $b \in B$. Since $(a, d) = 1$ we have $d \mid b$, $b = dt$ for some integer t, and thus $at \equiv j (\mathrm{mod}\, q)$. Let $B' = \{t \mid dt \in B\}$. Then $(A, B') = S_{q-1} - \{0\}$.

Thus $c(2, 20) = 0$ since $c(2, 8) = 0$.

COROLLARY 5.8. *If $m = 2kn + 1$ has a divisor d such that $(d, k!) = 1$ and $2k$ does not divide $(m/d) - 1$, then $c(k, n) = 0$.*

Thus $c(2, 19) = 1$ since 4 does not divide $(77/11) - 1$.

COROLLARY 5.9. *If $c^*(k, n) = 1$ and $kn + 1$ has a divisor d such that $(d, k!) = 1$, then $c^*(k, (nk + 1 - d)/kd) = 1$.*

COROLLARY 5.10. *If $c(2, n) = 1$, then every prime divisor of $4n + 1$ is of the form $4t + 1$.*

Proof. Let p be a prime divisor of $4n + 1$. Apply Corollary 5.8 to $d = (4n + 1)/p$.

From Corollary 5.10 we conclude that the asymptotic density of $\{n \mid c(2, n) = 1\}$ is 0. Corollary 5.8 shows that $c(2, 91) = 0$. For in this case 5 is a divisor of $4n + 1 = 365$ to which we may apply Corollary 5.8 and conclude that if $c(2, 91) = 1$ then $c(2, 18) = 1$. But $c(2, 18) = 0$.

COROLLARY 5.11. *If $c(3, n) = 1$ and d is a divisor of $m = 6n + 1$, then $c(3, (6n + 1 - d)/6d) = 1$ and 6 is a divisor of $(m/d) - 1$. Every prime divisor of $6n + 1$ is of the form $6t + 1$, (hence every divisor is of this form).*

Corollary 5.11 implies that $c(3, n) = 0$ for $n = 4, 9,$ and 14 and that $\{n \mid c(3, n) = 1\}$ has density 0.

THEOREM 5.12. *If $S_m - \{0\} = (A, B)$ and $A' = \{a \mid a \in A, (a, m) = 1\}$ and $B' = \{b \mid b \in B, (b, m) = 1\}$ then $G_m = (A', B')$, where G_m is the group of residue classes relatively prime to m.*

The proof is immediate.

COROLLARY 5.13. *If $S_m - \{0\} = (A, B)$, then the number of elements in A relatively prime to m is a divisor of $\varphi(m)$.*

If m is composite, Corollary 5.13 may be informative. For instance, it implies that $c(5, n) = 0$ when $n = 8, 9, 14, 16, 17, 20$. It also implies that $c(4, n) = 0$ for $n = 3, 4, 6, 15, 19, 20$ and $c(3, n) = 0$ for $n = 4, 9, 14, 19, 20$.

Though the geometric Theorem 3.2 implies Theorem 5.16, it is of interest to give an algebraic proof for it. The proof rests on Corollary

5.15.

LEMMA 5.14. *Let a, e, f and m be positive integers such that $ef > m$. Then there exists an $i, 1 \leqq i \leqq e-1$, such that $ai \equiv 0(\bmod m)$ or a pair $i, j, 1 \leqq i \leqq e - 1, 1 \leqq j, \leqq f - 1$ such that $ai \equiv \pm j(\bmod m)$.*

Proof. Consider the ef numbers $ai + j, 1 \leqq i \leqq e, 1 \leqq j \leqq f$. Since $ef > m$, there exist distinct pairs (i_1, j_1) and (i_2, j_2) such that

$$ai_1 + j_1 \equiv ai_2 + j_2(\bmod m) ,$$

hence

$$a(i_1 - i_2) \equiv j_2 - j_1(\bmod m) .$$

If $j_1 = j_2$, we have

$$a \mid i_1 - i_2 \mid \equiv 0(\bmod m)$$

and $1 \leqq |i_1 - i_2| \leqq e - 1$. If $j_2 \neq j_1$, we have

$$a \mid i_1 - i_2 \mid \equiv \pm \mid j_2 - j_1 \mid (\bmod m)$$

and $1 \leqq |i_1 - i_2|, |j_2 - j_1| \leqq e - 1$.

COROLLARY 5.15. (*Thue*) *Let a, e, and m be positive integers such that $e^2 > m$ and $(a, m) = 1$. Then there is a pair $i, j, 1 \leqq i, j \leqq e - 1$ such that $ai \equiv \pm j(\bmod m)$.*

THEOREM 5.16. *If $k > 2n - 2$ and $n \geqq 2$, then $c(k, n) = 0$.*

Proof. By Corollary 5.15 we see that if $(a, m) = 1$ and $e > \sqrt{m}$, then the equation $ay \equiv \pm x(\bmod m)$ has at least one solution such that $1 \leqq x \leqq e - 1$ and $1 \leqq y \leqq e - 1$. Let us apply this to the case $e = k + 1, m = 2kn + 1$. The inequality $e > \sqrt{m}$ is equivalent to $k + 1 > \sqrt{2kn + 1}$, hence to the inequality $k^2 + 2k + 1 > 2kn + 1$, which is valid for $k > 2n - 2$. Thus $ay = (\pm 1)x$, proving the theorem.

THEOREM 5.17. *If $k \geqq 2n - 2, n \geqq 3$, and $kn + 1$ is prime, then $c^*(k, n) = 0$.*

Proof. Assume that $G_{kn+1} = (\{1, 2, \cdots, k\}, \{1, b_1, \cdots, b_{n-1}\})$. Since $n(k + 1) > nk + 1$, we conclude from Lemma 5.14 that for each b_s there are $i_s, 1 \leqq i_s \leqq n - 1$ and $j_s, 1 \leqq j_s \leqq k$ such that $i_sb_s \equiv \pm j_s (\bmod kn + 1)$. If $i_sb_s \equiv j_s (\bmod kn + 1)$, we would already have the contradiction $i_sb_s \equiv j_s^1\cdot(\bmod kn + 1)$. Hence $i_sb_s \equiv -j_s (\bmod kn + 1)$. In a similar manner we deduce that $i_1, i_2, \cdots, i_{n-1}$ are distinct. For if $i_r = i_s$, we would have

$$j_r i_s b_s \equiv -j_r j_s \pmod{kn+1}$$

and

$$j_s i_r b_r \equiv -j_s j_r \pmod{kn+1} ;$$

hence

$$j_r i_s b_s \equiv j_s i_r b_r \pmod{kn+1} .$$

Cancelling $i_s(=i_r)$ yields $j_r b_s \equiv j_s b_r \pmod{kn+1}$.

We may therefore assume that $b_s = -j_s/s$, $s = 1, 2, \cdots, n-1$. Since $n \geqq 3$, there is an element b_2. We examine only b_1 and b_2 to obtain a contradiction.

If $j_1 \geqq n$, we would have $kj_1 \geqq kn$. Thus there would exist y and z, $1 \leqq y, z \leqq k$ such that $yj_1 \equiv -z \pmod{kn+1}$; in fact, let $y = \max\{u \mid uj_1 < kn+1\}$. Hence $yb_1 \equiv z \pmod{kn+1}$, a contradiction. Thus we may assume $j_1 \leqq n-1$.

Now $(2j_1)(-(j_2/2)) = j_2(-j_1)$. If $2j_1 \leqq k$, we would have a contradiction. Thus $j_1 > k/2$. We conclude that $n - 1 \geqq j_1 > k/2$, hence $k < 2(n-1) = 2n-2$. This establishes the theorem.

References

1. N. G. de Bruijn, *On the factorization of finite abelian groups*, Indag. Math. Kon Ned. Akad. Wetensch, Amsterdam **15** (1953), 258-264.

2. W. H. Gottschalk, *Choice functions and Tychonoff's theorem*, Proc. Amer. Math. Soc. **2** (1951), 172.

3. G. Hajós, *Über einfache und mehrfache Bedeckung des n-dimensionalen Raumes mit einem Würfelgitter*, Math. Zeit. **47** (1942), 427-467.

4. ———, *Sur le problème de factorization des groupes cycliques*, Acta. Math. Acad. Sci. Hungaricae **1** (1950), 189-195.

5. ———, *Sur la factorization des groupes abéliens*, Casopis **74** (1950), 157-162.

6. J. H. B. Kempermen, *On complexes in a semigroup*, Indag. Math. Kon. Ned. Akad. Wetensch, Amsterdam **18** (1956), 247-254.

7. ———, *On small sumsets in an abelian group*, Acta. Math. **103** (1960), 63-88.

8. H. B. Mann, *Addition Theorems*, Wiley, 1965.

9. W. H. Mills, *Characters with preassigned values*, Canad. J. Math. **15** (1963), 169-171.

10. L. Rédei, *Kurzer Beweis des gruppen-theoretischen Satzes von Hajós*, Comm. Math. Helv **23** (1949), 272-282.

11. A. Sands, *On the factorization of finite abelian groups*, Acta. Math. Acad. Soc. Hung. **8** (1957), 65-86.

12. ———, *On a problem of L. Fuchs*, J. London Math. Soc. **37** (1962), 277-284.

13. T. Szele, *Neuer vereinfachter Beweis des gruppen-theoretischen Satzes von Hajós*, Publ. Math. **1** (1949), 56-62.

Received April 6, 1966. This work was supported in part by NSF grant GP 4607.

UNIVERSITY OF CALIFORNIA, DAVIS