MATHEMATICS OF COMPUTATION
Volume 67, Number 223, July 1998, Pages 1199–1206
S 0025-5718(98)00929-6

FACTORING ELEMENTARY GROUPS OF PRIME CUBE ORDER INTO SUBSETS

SÁNDOR SZABÓ AND COBURN WARD

ABSTRACT. Let p be a prime and let G be the 3-fold direct product of the cyclic group of order p. Rédei conjectured if G is the direct product of subsets A and B, each of which contains the identity element of G, then either A or B does not generate all of G. The paper verifies Rédei's conjecture for $p \leq 11$.

1. INTRODUCTION

Let G be a finite abelian group written multiplicatively with identity e. Let A, B and C denote subsets of G. Assume that each element c of C is uniquely expressible in the form $c = ab$, where $a \in A$, $b \in B$ and that each product ab, $a \in A$, $b \in B$ belongs to C. Thus C is a direct product of A and B; we alternatively express this by saying that the equation $C = AB$ is a *factorization* of C. The subsets A and B are called *factors*. Any subset of G is said to be *normed* if it contains the identity e. A factorization $C = AB$ is also called *normed* if both A and B are normed subsets. We extend the definition of "factorization" in the obvious way to more than two factors: the equation $C = A_1A_2 \cdots A_k$ is a *factorization* when each $c \in C$ is expressible in exactly one way as a product of k elements $a_1a_2 \cdots a_k$ where $a_i \in A_i\,, 1 \leq i \leq k$.

Each finite abelian group is a direct product of cyclic groups of prime power orders, and this factoring is unique apart from the order of the factors. If G is a direct product of cyclic groups of prime power orders $t_1, \ldots, t_n$ respectively, then the non-ordered n-tuple $(t_1, \ldots, t_n)$ is called the *type* of the group G. We will let $\langle A \rangle$ denote the smallest subgroup of G containing the subset A, that is, the generatum or span of A.

Rédei [3] proved that for any factorization of a finite abelian group into two or more normed subsets of prime cardinality, at least one of the factors must be a subgroup. The following special case plays an important part of the proof and has interesting geometric and combinatorial applications. (For further details see [2] and [4].) If G is a group of type (p, p), where p is a prime, and $G = AB$ is a normed factorization, then either A or B is a subgroup of G.

Rédei formulated a conjecture which appears as Problem 5 in the Open Problems section of his book [4]:

Conjecture. Let G be a group of type (p, p, p) where p is prime. If $G = AB$ is a normed factorization, then either $\langle A \rangle \neq G$ or $\langle B \rangle \neq G$.

Received by the editor June 17, 1994 and, in revised form, January 23, 1997.
1991 *Mathematics Subject Classification.* Primary 20K01; Secondary 52C22.
Key words and phrases. Factorization of groups, Latin squares.

In this paper we describe how Latin squares can be used to investigate Rédei's conjecture. With this tool we verify the conjecture for $p \leq 11$.

If Rédei's conjecture holds, then we can easily describe all normed factorizations $G = AB$ of groups of type (p, p, p) where p is prime. The product of the cardinalities of A and B must equal p^3. If $|A| = 1$ or $|A| = p^3$, then the conjecture trivially holds. Thus we may assume without loss of generality that $|A| = p$ and $|B| = p^2$. The conjecture implies that either $\langle A\rangle \neq G$ or $\langle B\rangle \neq G$. If $\langle A\rangle$ is of order p, then $\langle A\rangle = A$, and, therefore, B must be a complete set of representatives modulo A which contains the identity element. Similarly if $\langle B\rangle$ is of order p^2, then A must be a complete set of representatives modulo B which contains the identity element. The last case to consider is when $\langle A\rangle$ is of order p^2. Let $H = \langle A\rangle$. Let $z \in G\backslash H$. Since no power of z is in H, the collection $\{eH, zH, z^2H, \cdots, z^{p-1}H\}$ is a partition of G. Set $B_i = z^iH \cap B$ for each i, $0 \leq i \leq p-1$. The sets B_i partition B.

We will show that $A(z^{-i}B_i) = H$ is a factorization. Clearly

$$A(z^{-i}B_i) = A(H \cap z^{-i}B) \subseteq HH = H.$$

To show the reverse inclusion, suppose that $h \in H$. Since $G = AB$, $z^ih = ab$ for some $a \in A$ and $b \in B$. Now $z^{-i}b = a^{-1}h \in H$ and, hence, $h = a(z^{-i}b) \in A(H \cap z^{-i}B) = A(z^{-i}B_i)$ which implies that $H \subseteq A(z^{-i}B_i)$. The product AB_i is direct and so $A(z^{-i}B_i)$ is a factorization of H.

According to Rédei's theorem, either A is a subgroup of G or $z^{-i}B_i$ is a coset of a subgroup of H. (Keep in mind that the factor $z^{-i}B_i$ is not necessarily normed.) Since A is not a subgroup, $K_i = z^{-i}B_i$ is a coset modulo a subgroup of H. We conclude that for any $z \in G\backslash H$, there are sets $K_0, K_1, \cdots, K_{p-1}$ such that $AK_0, AK_1, \cdots, AK_{p-1}$ are factorizations of H and $\{z^0K_0, z^1K_1, \cdots, z^{p-1}K_{p-1}\}$ is a partition of B and each K_i is a coset of a subgroup of H.

A factorization $G = AB$ is called *quasi-periodic* if one of the factors, say B, can be partitioned into $r > 1$ subsets $B_1, \ldots, B_r$ and if there is a subgroup $H = \{h_1, \ldots, h_r\}$ of G such that $AB_i = AB_1h_i$ for each i, $1 \leq i \leq r$. This definition comes from G. Hajós [1] who conjectured that each factorization of a finite abelian group is quasi-periodic. Sands [5] gave a counterexample to Hajós' conjecture but also pointed out that whenever either $\langle A\rangle$ or $\langle B\rangle$ is a proper direct factor of G, the factorization $G = AB$ must be quasi-periodic. In a group of type (p, p, p) each subgroup is a direct factor, thus for these groups, Rédei's conjecture implies Hajós' conjecture.

2. Replaceable and reducible factors

Let A and A' be subsets of the finite abelian group G. We say that the factor A can be replaced by A' in the factorization $G = AB$, if $A'B$ is also a factorization of G. If A can be replaced by A' in every factorization of G in which A is a factor, then we say that A *is replaceable* by A' in G.

We will use two results on replaceable factors. The first one is that for each $a \in A$, the normed factor A is replaceable by the normed factor $a^{-1}A$. This is because $a^{-1}G = G$, and so if $G = AB$ is a normed factorization, then $G = (a^{-1}A)B$ is one as well.

The next result on replaceable factors is proved by Rédei [3]; the proof exploits group characters and group rings. Let p be a prime and let G be a finite abelian p-group. Consider a normed factorization $G = AB$ such that $|A| = p$. Denote the

elements of A by $\{e, a_1, a_2, \ldots, a_{p-1}\}$. Rédei's result is that factor A is replaceable by $\langle a_i \rangle$ for each i, $1 \leq i \leq p-1$.

A normed subset B of a finite abelian group is said to be *reducible* if there are proper subsets C, D of B such that $B = CD$ is a normed factorization. In a counterexample to Rédei's conjecture, the factors must be irreducible. To prove this, consider the factorization $G = AB$, where $|A| = p$ and $|B| = p^2$. Clearly A is irreducible. Assume that B can be factored into CD, where $|C| = |D| = p$. From the factorization $G = ACD$, it follows (from Rédei's theorem) that at least one of these factors is a subgroup of G. If this is A, then $\langle A \rangle \neq G$. Thus we may assume that either C or D is a subgroup of G. For the sake of concreteness, assume that D is a subgroup of G. From the factorization $G = ACD$, we get the factorization $G/D = \big((AD)/D\big) \cdot \big((CD)/D\big)$ of the factor group G/D. Again by Rédei's theorem, one of these factors is a subgroup of G/D. Hence, either AD or CD is a subgroup of G, and so either $\langle A \rangle \neq G$ or $\langle B \rangle \neq G$.

3. Latin squares

Henceforth we will let $G = AB$ be a normed factorization of a group of type (p, p, p) where p is prime. We will suppose that $|A| = p$ and $|B| = p^2$ and we will assume that $\langle A \rangle = G$. As a consequence, there are elements x, y, z of A such that $\langle x, y, z \rangle = G$. This means that all elements of G are of the form $x^i y^j z^k$ where i, j, k are integers in the range $0, 1 \ldots, p-1$. For convenience, we will code the element $x^i y^j z^k$ by the ordered triple (i, j, k). We will show that in the set of all (i, j, k) representing all elements of B, any given combination of i and j determines k uniquely. Thus the p^2 triples corresponding to B can be conveniently viewed as a p by p table whose ith row and jth column entry is k.

A previously mentioned result by Rédei shows that in the normed factorization $G = AB$, the factor A can be replaced by $\langle z \rangle$ to get the normed factorization $G = \langle z \rangle B$. Multiplying by arbitrary g, we get the factorization $G = (g\langle z \rangle)B$. Although this latter factorization is not necessarily normed, it is still true that the two factors can have at most one element in common. Therefore, each of the p^2 cosets modulo subgroup $\langle z \rangle$ intersects factor B in at most one element. Since $|B| = p^2$, each coset contains precisely one element from B. This means for each combination of i and j, there is exactly one k such that $x^i y^j z^k \in B$.

We can repeat the previous argument with either $\langle x \rangle$ or $\langle y \rangle$ in the role of $\langle z \rangle$. We conclude that for triples (i, j, k) coding factor B, each (i, k) determines j and each (j, k) determines i. Thus each row and each column of the table for B contains each of $0, 1, \ldots, p-1$ exactly once. In summary, $\langle A \rangle = G$ implies that factor B can be described using a p by p Latin square. In fact, this can be done in three ways since the roles of elements x, y and z are symmetric.

Let f be a permutation on $\{0, 1, \ldots, p-1\}$. We shall use the expression " the ith row of the Latin square contains (is) permutation f " to mean that the entry in row i column j of the Latin square is $f(j)$ for $0 \leq j \leq p-1$. A similar expression will be used for columns. Some geometric terminology is also useful. The triple $\big(i, j, k\big)$ can be viewed as a point in the 3-dimensional affine space over the modulo p finite field. When the triples for a row (column) form a straight line, we shall call that row (column) *linear* and a *straight line*. A permutation on $\{0, 1, \ldots, p-1\}$ will be called *linear* if its ordered pairs form a line in $AG(2, p)$.

There are some major restrictions on the Latin square for B. A permutation f of the elements of a finite abelian group H is called a *complete mapping* of H if $a \to af(a)$, $a \in H$, is again a permutation on H. Using this terminology, we now show that the rows and columns of the Latin square for B are complete mappings of the additive group modulo p.

Note that $(z^{-1}A)B$ is a normed factorization of G since $z \in A$; the first factor contains $z^{-1}y$ since $y \in A$. Thus the result of Rédei implies that $G = \langle z^{-1}y\rangle B$ is a normed factorization. Consequently, each coset of $\langle z^{-1}y\rangle$ contains exactly one element of B. (Otherwise an element of B could be represented in two distinct ways as an element of $\langle z^{-1}y\rangle$ times an element of B.) This means that if a and b are entries in the uth and vth columns in the same row of the Latin square for B, then

$$b - a \not\equiv (-1)(v - u) \pmod{p}. \tag{1}$$

Similarly, since $x, z \in A$ it follows that if a and b are entries in the uth and vth rows in the same column, then (1) holds. These results imply that the Latin square describing B can contain only complete mappings in its rows and columns.

This Latin square has p positions which contain a given fixed element k. Consider the permutation on $\{0, 1, \ldots, p-1\}$ which maps i to j precisely when k is the entry in row i, column j. We refer to this permutation as the *kth transversal*. Because $x, y \in A$, each coset modulo subgroup $\langle y^{-1}x\rangle$ contains exactly one element from B. Hence, whenever the ath and the bth positions in the uth and vth columns contain the same element, inequality (1) must hold. We conclude that the transversals are complete mappings.

We now make a further reduction that will be used systematically later. We claim that if there is a counterexample to Rédei's conjecture, then there is one such that the Latin square for factor B contains nonlinear complete mappings in the first column, first row and 0th transversal. The argument follows: If each column is a straight line, then the lines must be parallel, and so factor B is a product of two smaller subsets, namely, the elements of the first column and the first row. This would imply that B is reducible, which it cannot be if it provides a counterexample. Thus there is a nonlinear column; the same argument gives us the existence of a nonlinear row. Since factor B can be replaced by $b^{-1}B$ for each $b \in B$, we may assume that the nonlinear row and nonlinear column correspond to $i = 0$ and $j = 0$ respectively. (Refer to these as the *first* row and column.) Assume that the 0th transversal is linear—otherwise, we are done. Let u, v, w be the permutations in the first column, first row and the 0th transversal respectively. If each transversal is linear, then factor B is reducible. Therefore, there is an i such that the $u(i)$th transversal is not linear. We may assume that the ith row is linear because the other alternative would mean that the Latin square for $x^{-i}z^{-u(i)}B$ in the factorization $G = A(x^{-i}z^{-u(i)})B$ would have the desired properties.

Let P be the plane spanned by the triples in ith row and the 0th transversal and consider $u(j)$, the entry in the jth row of the first column. Again, either the jth row or the $u(j)$th transversal is linear since otherwise we are done. If the jth row is linear, it must be parallel to the ith row. Furthermore, this row intersects the 0th transversal, and so the triples representing the jth row lie in plane P. In particular, the triple $\big(j, 0, u(j)\big)$ lies in P. In case the $u(j)$th transversal is linear, it must be parallel to the 0th transversal and it must intersect the ith row. Thus the triples representing the $u(j)$th transversal lie in plane P. So, in either case,

$\big(j, 0, u(j)\big)$ lies in P. Since j was arbitrary, the first column is the intersection of P with the coordinate plane $j = 0$. We conclude that u is linear; this contradicts our choice of u.

4. When $p \leq 5$

When $p = 2$ or $p = 3$, the factor A contains only 1 or 2 nonidentity elements. On the other hand, G cannot be generated by less than 3 elements. Therefore $\langle A \rangle \neq G$.

Let us turn to the case $p = 5$. As always we assume $\langle A \rangle = G$, and so, there exist $x, y, z \in A$ such that $\langle x, y, z \rangle = G$. Consider the 5 by 5 Latin square associated with the factor B. We have seen that we can assume that the first row, first column and 0th transversal represent nonlinear complete mappings. When $p = 5$, the complete mappings are all linear, therefore $p = 5$ yields no counterexample to Rédei's conjecture.

5. When $p = 7$

Assume that $G = AB$ is a counterexample to Rédei's conjecture where $\langle A \rangle = G$. The complete mappings on the additive group modulo 7 constitute the candidates for the rows, columns and transversals of the Latin square corresponding to factor B. We need to focus only on those mappings which fix 0, since each of the other ones is the result of adding an arbitrary constant modulo p to one of these mappings. There are 19 such complete mappings. Five of them are linear; Table 1 shows the cycle notation for the remaining ones which are denoted $\gamma_1, \ldots, \gamma_{14}$.

Table 1

γ_1:(0)(1)(24653)	γ_7:(0)(1)(23564)
γ_2:(0)(3)(12654)	γ_8:(0)(3)(14562)
γ_3:(0)(2)(15364)	γ_9:(0)(2)(14635)
γ_4:(0)(6)(12453)	γ_{10}:(0)(6)(13542)
γ_5:(0)(4)(12365)	γ_{11}:(0)(4)(15632)
γ_6:(0)(5)(13624)	γ_{12}:(0)(5)(14263)
γ_{13}:(0)(124)(356)	γ_{14}:(0)(142)(365)

For each γ_i in Table 1, let $\phi_1(\gamma_i)$ be the permutation on $\{0, \cdots, p-1\}$ that takes j to $3\gamma_i(3^{-1}j)$. (The multiplications and inverse are taken modulo 7.) Note that $\phi_1(\gamma_i)$ can be found in Table 1, since ϕ_1 and its inverse fix 0 and preserve the properties of linearity and completeness. Thus ϕ_1 is a permutation on the elements of Table 1 which in cycle notation can be represented as

$$(\gamma_1\gamma_2\gamma_3\gamma_4\gamma_5\gamma_6)(\gamma_7\gamma_8\gamma_9\gamma_{10}\gamma_{11}\gamma_{12})(\gamma_{13}\gamma_{14}) \; . \tag{2}$$

Let ψ_1 be the automorphism of G that takes g to g^3. This automorphism takes the counterexample $G = AB$ into another one $G = \psi_1(A)\psi_1(B)$. Note that if u is the first column of the Latin square corresponding to factor B, then $\phi_1(u)$ is the first column of the Latin square that codes factor $\psi_1(B)$.

The automorphism ψ_2 of G defined by $\psi_2(x) = x$, $\psi_2(y) = z$, $\psi_2(z) = y$ takes a counterexample to Rédei's conjecture $G = AB$ into another one $G = \psi_2(A)\psi_2(B)$. Note that if u is the first column of the Latin square for B, then u^{-1} is the first column of the square for $\psi_2(B)$. Also note that the class of nonlinear complete

mappings fixing 0 is invariant under inversion. Thus the inverse mapping can be viewed as a permutation on the elements of Table 1. In cycle notation, this is

$$(\gamma_1\gamma_7)(\gamma_2\gamma_8)(\gamma_3\gamma_9)(\gamma_4\gamma_{10})(\gamma_5\gamma_{11})(\gamma_6\gamma_{12})(\gamma_{13}\gamma_{14})\ . \tag{3}$$

Permutations (2) and (3) generate a group which separates the elements of Table 1 into two transitivity classes $\{\gamma_1, \gamma_2, \gamma_3, \gamma_4, \gamma_5, \gamma_6, \gamma_7, \gamma_8, \gamma_9, \gamma_{10}, \gamma_{11}, \gamma_{12}\}$ and $\{\gamma_{13}, \gamma_{14}\}$. Earlier we argued that if there is a counterexample to Rédei's conjecture, then there is one in which the first column, row and 0th transversal are all found in Table 1. The transitivity class analysis shows that we can assume without loss of generality that the first column is either γ_1 or γ_{13}.

We lay some groundwork before we consider these two cases. Let u, v, and w be the complete mappings represented by the the 1st column, 1st row and the 0th transversal respectively. For a given $i \neq 0$, suppose $w(i) = j$. This means that element 0 is found in row i column j. Note that $j \neq 0$. Let β_i and γ_j denote the complete mappings represented by row i and column j respectively. We have $\beta_i(0) = u(i)$, $\gamma_j(0) = v(j)$, and $\beta_i(j) = \gamma_j(i) = 0$. Hence, $u(i) = \beta_i(0) - \beta_i(j) \neq j$ since β_i is a complete mapping and $j \neq 0$. Thus for each $i \neq 0$, $u(i) \neq w(i)$. Furthermore, $v(j) = \gamma_j(0) - \gamma_j(i) \neq i$ since γ_j is a complete mapping and $i \neq 0$. Thus for each $i \neq 0$, $v\big(w(i)\big) \neq i$.

Now take the case where $u = \gamma_1$. Only $v = \gamma_8$, $v = \gamma_{10}$, and $v = \gamma_{12}$ satisfy $u(i) \neq v(i)$, $1 \leq i \leq p-1$. If $v = \gamma_8$, w can only be γ_8, γ_{10}, or γ_{12}, since $u(i) \neq w(i)$. Because $v\big(w(i)\big) \neq i$, all of these possibilities are excluded by $v\big(w(3)\big) = 3$, $v\big(w(5)\big) = 5$, and $v\big(w(2)\big) = 2$ respectively. If $v = \gamma_{10}$, w can only be γ_8, γ_{10}, or γ_{12}. All of these possibilities are excluded by $v\big(w(4)\big) = 4$, $v\big(w(6)\big) = 6$, and $v\big(w(3)\big) = 3$ respectively. If $v = \gamma_{12}$, the only possibilities for w are γ_8, γ_{10}, and γ_{12} which are excluded by $v\big(w(6)\big) = 6$, $v\big(w(1)\big) = 1$, and $v\big(w(5)\big) = 5$ respectively.

Finally, consider the case where $u = \gamma_{13}$. Since $u(i) \neq w(i)$, we must have $v = \gamma_{14}$. At this point, there is no consistent choice available for the second column.

This contradiction shows that there is no counterexample to Rédei's conjecture when $p = 7$.

6. When $p = 11$

Suppose there is a counterexample to Rédei's conjecture for $p = 11$. We have argued that there is an 11 by 11 Latin square which has complete mappings for its rows, columns and transversals. Furthermore, there exists one in which the initial row, column and 0th transversal are nonlinear and fix 0. Any such Latin square will be called *qualified*. A counterexample to Rédei's conjecture implies the existence of a qualified Latin square where factor B is non-reducible. We will show that no such Latin square exists, but the numbers involved require the use of a computer to assist in the search.

As before we regard a Latin square as a collection of triples (i, j, k) where k is the entry in row i, column j. Consider the permutation on triples which takes (i, j, k) to $(3i, 3j, 3k)$ where multiplication is performed modulo 11. This acts on the set of qualified Latin squares and preserves the property of non-reducibility. We note that if u is the complete mapping representing the initial column of a Latin square, then the initial column u' of the permuted one will satisfy $u'(i) = 3u(3^{-1}i)$.

In a similar fashion, the transformation taking (i, j, k) to (i, k, j) acts on the set of all qualified Latin squares, preserves non-reducibility and changes the square's

TABLE 2

$f(0)f(1)\cdots f(9)f(10)$	(β,δ)
0 1 2 4 5 7 10 3 6 8 9	$(8,6)$ $(0,6)$ $(9,0)$
0 1 2 5 6 9 3 10 4 7 8	$(5,4)$ $(4,0)$ $(0,8)$
0 1 2 5 10 4 6 3 8 9 7	$(4,4)$ $(8,7)$ $(3,0)$ $(1,4)$ $(0,6)$ $(0,7)$ $(9,0)$ $(7,0)$
0 1 3 4 8 5 9 2 6 10 7	$(7,0)$ $(0,3)$ $(3,2)$
0 1 3 5 6 4 8 10 7 9 2	$(8,7)$ $(0,6)$ $(9,0)$
0 1 3 5 6 4 9 7 10 8 2	$(4,0)$ $(0,8)$ $(5,4)$
0 1 3 5 6 10 8 2 4 9 7	$(7,0)$ $(0,3)$ $(3,2)$
0 1 3 5 10 7 4 2 9 6 8	$(9,8)$ $(3,10)$ $(0,4)$ $(8,7)$ $(0,6)$ $(9,0)$ $(3,3)$ $(8,0)$
0 1 4 7 5 9 2 8 10 3 6	$(5,4)$ $(7,6)$ $(1,3)$ $(4,0)$ $(3,0)$ $(0,7)$ $(0,8)$ $(8,10)$
0 1 7 5 3 10 4 9 6 8 2	$(4,10)$ $(0,3)$ $(0,4)$ $(9,8)$ $(8,0)$ $(3,2)$ $(1,7)$ $(7,0)$

initial column u to u^{-1}. The group generated by both of these permutations partitions the 3441 complete mappings that fix 0 into 23 transitivity classes of nonlinear mappings and 6 classes containing linear mappings. Thus our search for a counterexample needs to consider only 23 cases; each case uses a representative nonlinear mapping from a transitivity class as the initial column of the Latin square representing factor B. There are exactly 389 complete mappings that fix 1 as well as 0 and at least one of these belongs to each of the 23 transitivity classes. So in our calculations, we chose a representative from each class that fixes both 0 and 1.

We performed an exhaustive computer search for all qualified Latin squares having an initial column equal to one of the 23 representatives discussed above. The search was performed in a depth-first fashion. At stage 1 the initial row was chosen from the nonlinear complete mappings that fix 0. Subsequently, the columns were chosen, one per stage. Backtracking occurred whenever a candidate column or row had no more instantiations consistent with the previously established parts of the Latin square.

The search revealed exactly 50 qualified Latin squares meriting further consideration as possible counterexamples. We checked each one to see if factor B was reducible or not. An interesting pattern was observed. Suppose there exist integers α, β, ω, δ, and complete mappings f and g on the additive group modulo p such that all the triples (i,j,k) constituting the Latin square satisfy the relationship

$$k = f(\alpha i + \beta j) + g(\omega i + \delta j), \tag{4}$$

where the operations are taken modulo p. If the matrix $\left(\begin{smallmatrix}\alpha & \beta\\ \omega & \delta\end{smallmatrix}\right)$ has an inverse modulo p, say $\left(\begin{smallmatrix}a & b\\ c & d\end{smallmatrix}\right)$, then the collection of triples in the Latin square is the direct sum of

$$\Big\{\big(am, cm, f(m)\big) \mid 0 \le m \le p-1\Big\} \quad \text{and} \quad \Big\{\big(bn, dn, g(n)\big) \mid 0 \le n \le p-1\Big\}.$$

All 50 qualified Latin squares satisfied a special case of equation (4), namely where $k = f(i+\beta j)+\delta j$. The roster in Table 2 gives the complete mappings f and the (β,δ) pairs that generate these 50 Latin squares.

Thus we are able to conclude there is no counterexample to Rédei's conjecture when $p = 11$ because all qualified Latin squares represent reducible factors.

When $p \ge 13$, the size of the search space precludes using the exact approach discussed above. Some further simplifications are necessary to make additional progress.

References

[1] G. Hajós, *Sur la factorisation des groupes abeliens*, Casopis **74** (1949), 157–162. MR **13:**623a
[2] L. Lovász and A. Schrijver, *Remarks on a theorem of Rédei*, Studia Sci. Math. Hungar. **16** (1983), 449–454. MR **85e:**51017
[3] L. Rédei, *Die neue Theorie der endlichen abelschen Gruppen und Verallgemeinerung des Hauptsatzes von Hajós*, Acta Math. Acad. Sci. Hungar. **16** (1965), 329–373. MR **32:**4187
[4] L. Rédei, *Lacunary Polynomials over Finite Fields*, Akadémia Kiadó, Budapest, Hungary, 1973. MR **50:**4548
[5] A. D. Sands, *On a conjecture of G. Hajós*, Glasgow Math. J. **15** (1974), 88–89. MR **51:**13078

Department of Mathematics, University of Bahrain, ISA Town, State of Bahrain
Current address: General Science and Mathematics Department, College of Health Sciences, Manama, State of Bahrain

Department of Mathematics, University of the Pacific, Stockton, California 95211
E-mail address: cward@uop.edu