MATHEMATICS OF COMPUTATION
Volume 80, Number 274, April 2011, Pages 1155–1162
S 0025-5718(2010)02417-2
Article electronically published on September 17, 2010

VERIFYING A CONJECTURE OF L. RÉDEI FOR $p = 13$

SÁNDOR SZABÓ

Abstract. In 1970 L. Rédei conjectured that if an elementary p-group G of order p^3 is a direct product of its subsets A and B such that both A and B contain the identity element of G, then at least one of the factors A and B cannot span the whole G. We will verify this conjecture for $p = 13$.

1. Introduction

Let G be a finite abelian group. In this paper we will use multiplicative notation in connection with abelian groups. We refer to the group operation as multiplication. The neutral element will be called identity element and will be denoted by e. Let A and B be subsets of G. The product AB is defined to be $\{ab : a \in A,\ b \in B\}$. In a typical situation equal elements occur in the list

$$ab,\ a \in A,\ b \in B \tag{1}$$

and so, in a typical situation, $|AB| \leq |A||B|$ holds. If the elements in the list (1) are distinct, that is, if $|AB| = |A||B|$, then we say that the product AB is direct. When the product AB is direct and is equal to G, then we say that $G = AB$ is a factorization of G.

Let p be a prime. If G is a direct product of k groups of order p, then we say that G is an elementary p-group of rank k. A group of order p is necessarily commutative. The direct product of commutative groups is commutative again. Therefore elementary p-groups are necessarily abelian groups.

A subset A of G is called normalized if $e \in A$. A factorization $G = AB$ is called normalized if the factors A and B are both normalized subsets of G. For a subset A of G the intersection of all subgroups of G that contain A, that is, the span of A in G is denoted by $\langle A \rangle$. If $\langle A \rangle = G$, then A is called a full-rank subset of G. If a factor is not full-rank, then it is contained in a maximal subgroup of G. A factorization $G = AB$ is called a full-rank factorization if the factors A and B are full-rank factors. A subset A of G is called periodic if there is an element $g \in G \setminus \{e\}$ such that $Ag = A$. A convenient way to test that a given subset A is periodic is to compute

$$L = \bigcap_{a \in A} Aa^{-1}.$$

If $|L| = 1$, then A is not periodic and if $|L| \geq 2$, then A is periodic. (For a proof see Lemma 1.2.1 of [3].)

Received by the editor September 1, 2009 and, in revised form, February 4, 2010.
2010 *Mathematics Subject Classification.* Primary 20K01; Secondary 05B45, 52C22, 68R05.
Key words and phrases. Factorization of finite abelian groups, periodic subset, full-rank factorization.

In 1970 L. Rédei [2] advanced the following conjecture.

Conjecture 1. *Let p be a prime and let G be an elementary p-group of order p^3. If $G = AB$ is a normalized factorization of G, then $\langle A\rangle \neq G$ or $\langle B\rangle \neq G$.*

The conjecture appears as Problem 5 in the Open Problems section of [2]. It can be rephrased such that an elementary p group of rank 3 does not admit any full-rank normalized factorizations.

The conclusion of the conjecture plainly holds when $A = \{e\}$ or $B = \{e\}$ and so it is enough to consider the cases when $|A| \neq 1$ and $|B| \neq 1$. In fact, we may assume that $|A| = p$, $|B| = p^2$. When $p = 2$, then $A \setminus \{e\}$ contains only one element and so $\langle A\rangle = G$ cannot hold. Similarly, in the $p = 3$ case, $A \setminus \{e\}$ contains only two elements and consequently A cannot possibly span the entire G. Therefore, Rédei's conjecture is interesting for $p \geq 5$. S. Szabó and C. Ward [4] settled the $p \leq 11$ cases. The $p = 5$, $p = 7$ cases required only paper and pencil. In the $p = 11$ case the assistance of a computer was needed. The $p = 13$ case of the computation was highly infeasible.

In this paper we propose a new approach. Interestingly, in this way even the $p = 5$ case is not well suited for hand computation. However, a computer handles the $p = 13$ case without difficulty.

2. The exact cover problem

In this section we define three problems. They are the simultaneous complement factor, the exact cover, and the simultaneous transversal problems.

Problem 1. Given a finite abelian group G and subgroups $H_1, \ldots, H_r$ of G such that $|H_1| = \cdots = |H_r|$. The problem is to decide if there is a normalized subset B of G for which $G = H_1B, \ldots, G = H_rB$ are factorizations of G.

Here B is a complement factor to the subgroups $H_1, \ldots, H_r$ simultaneously. Perhaps we may refer to this problem as the simultaneous complement factor problem. In this form the problem is a decision problem. The answer is "yes" or "no". We need that variant of the problem that finds B. In fact, we are looking for all possible B.

The exact cover problem is the following.

Problem 2. Given a universal set U and a family of subsets $D_1, \ldots, D_n$ of U. The task is to decide if there are disjoint subsets $E_1, \ldots, E_s \in \{D_1, \ldots, D_n\}$ such that $U = E_1 \cup \cdots \cup E_s$.

The sets $E_1, \ldots, E_s$ form an exact cover of U; whence the name of the problem. Again the problem in this form is a decision problem and we need that version, which searches for all possible exact covers of U.

It is known from the theory of computations that the decision version of the exact cover problem is NP complete. So we cannot expect a polynomial running time algorithm for this problem. D. E. Knuth [1] presents an algorithm for the exact cover problem. This is what we will use in this paper.

In order to apply the exact cover algorithm to Rédei's conjecture we describe yet another problem that we call the simultaneous transversal problem.

Problem 3. Given a set V and given r partitions $P_1, \ldots, P_r$ of V, say, $P_i = \{C_{i,1}, \ldots, C_{i,s}\}$, here $C_{i,j}$ is a subset of V and each P_i has the same number of elements. The simultaneous transversal problem questions the existence of elements

$v(1), \ldots, v(s)$ of V that form a transversal of the partitions $P_1, \ldots, P_r$ simultaneously.

We need that version of the simultaneous transversal problem that lists all possible simultaneous transversals of the partitions $P_1, \ldots, P_r$. We will see in Section 4 how the simultaneous transversal problem helps in checking Rédei's conjecture.

Lemma 1. *The simultaneous transversal problem can be reduced to the exact cover problem.*

Proof. Let us construct an incidence matrix with $m = |V|$ rows and $n = rs$ columns. The rows are labeled with the elements of V and the columns are labeled with the sets $C_{i,j}$. For each element v of V we put a bullet into the cell in the row of v and in the column of $C_{i,j}$ if $v \in C_{i,j}$. We can now construct an exact cover problem. Set the universal set U to be

$$\{C_{1,1}, \ldots, C_{1,s}, \ldots, C_{r,1}, \ldots, C_{r,s}\}.$$

To each element v of V we define a subset D_v of U by the assignment

$$C_{i,j} \in D_v \text{ exactly when } v \in C_{i,j}.$$

Using the incidence matrix constructed above one can check that if $v(1), \ldots, v(s)$ is a transversal to the partitions $P_1, \ldots, P_r$ simultaneously, then the subsets $D_{v(1)}, \ldots, D_{v(s)}$ form an exact cover of U. It can also be checked that if $v(1), \ldots, v(s) \in V$ for which $D_{v(1)}, \ldots, D_{v(s)}$ is an exact cover of U, then the elements $v(1), \ldots, v(s)$ form a transversal for each partition $P_1, \ldots, P_r$ simultaneously. □

In order to illustrate the construction we worked out an example. Let $V = \{1, 2, 3, 4, 5, 6, 7, 8\}$ and let the partitions P_1, P_2, P_3 be the following:

$$P_1 = \{\underbrace{\{1, 2, 3, 4\}}_{=C_{1,1}}, \underbrace{\{5, 6, 7, 8\}}_{=C_{1,2}}\},$$
$$P_2 = \{\underbrace{\{1, 3, 5, 7\}}_{=C_{2,1}}, \underbrace{\{2, 4, 6, 8\}}_{=C_{2,2}}\},$$
$$P_3 = \{\underbrace{\{1, 2, 7, 8\}}_{=C_{3,1}}, \underbrace{\{3, 4, 5, 6\}}_{=C_{3,2}}\}.$$

The incidence matrix associated with these partitions is depicted in Table 1.

TABLE 1. The incidence matrix

	$C_{1,1}$	$C_{1,2}$	$C_{2,1}$	$C_{2,2}$	$C_{3,1}$	$C_{3,2}$
1	•		•		•	
2	•			•	•	
3	•		•			•
4	•			•		•
5		•	•			•
6		•		•		•
7		•	•		•	
8		•		•	•	

TABLE 2. The $p = 5$ case

(u, v, w)	μ	ν	(u, v, w)	μ	ν
$(0, 0, 2)$	49	2	$(1, 1, 1)$	3	0
$(0, 1, 1)$	49	2	$(1, 1, 2)$	49	2
$(0, 1, 2)$	25	1	$(4, 4, 4)$	133	6
$(0, 2, 2)$	1	0			

TABLE 3. The $p = 7$ case

(u, v, w)	μ	ν	(u, v, w)	μ	ν
$(0, 0, 2)$	529	12	$(1, 1, 1)$	277	6
$(0, 0, 3)$	529	12	$(1, 1, 2)$	361	8
$(0, 1, 1)$	529	12	$(1, 1, 3)$	361	8
$(0, 1, 2)$	397	9	$(1, 2, 2)$	445	10
$(0, 2, 2)$	265	6	$(3, 3, 3)$	583	12
$(0, 3, 6)$	265	6			

3. Dealing with the symmetries

Let p be a prime greater than 3. Let G be an elementary p-group of order p^3. Consider a normalized factorization $G = AB$, where $|A| = p$, $|B| = p^2$. In order to verify Rédei's conjecture we assume on the contrary that $\langle A\rangle = \langle B\rangle = G$. Our purpose is to show that such a factorization does not exist. (We can carry this plan to completion only when $p \leq 13$.) Let us choose an element a of A. Multiplying the normalized factorization $G = AB$ by a^{-1} we get the normalized factorization $G = Ga^{-1} = (Aa^{-1})B$ of G. Let us choose an element $a'a^{-1}$ of (Aa^{-1}). In the factorization $G = (Aa^{-1})B$, by Lemma 1.4.3 of [3], the factor (Aa^{-1}) can be replaced by the subgroup $\langle a'a^{-1}\rangle$ to get the normalized factorization $G = \langle a'a^{-1}\rangle B$ for each distinct $a', a \in A$. Suppose for a moment that we know the elements of A. Among the subgroups $\langle a'a^{-1}\rangle$, $a', a \in A$ there may be equal ones. Let $H_1, \ldots, H_r$ be all the distinct elements among these subgroups of order p. This means that B is a transversal to the cosets modulo the subgroups $H_1, \ldots, H_r$ simultaneously. By Lemma 1, the simultaneous transversal problem can be reduced to an exact cover problem. With the exact cover algorithm one can compute all possible choices for B and it remains to check if $\langle B\rangle = G$ holds. But, in fact, we do not know the elements of A. We will be able to locate five elements of A. As a consequence the value of r will be 10.

Since $\langle A\rangle = G$, we can choose a basis x, y, z of G such that $x, y, z \in A$. Together with e there are four fixed elements in A. As $p \geq 5$, there is an element a in $A \setminus \{e, x, y, z\}$. We partition A in the form $A = A_1 \cup A_2$, where $A_1 = \{e, x, y, z, a\}$. Since the product AB is direct, it follows that the product A_1B is also direct. Our strategy is the following. For each fixed A_1 we compute each normalized subset B of G for which $|B| = p^2$ and the product A_1B is direct. If it turns out that each such B is either periodic or it is not full-rank, then we are done since in this case there cannot be a counterexample for Rédei's conjecture. Let $x^u y^v z^w$, $0 \leq u, v, w \leq p-1$ be the representation of a in the basis x, y, z. For the sake of brevity we will represent a by the exponents (u, v, w) only. In a similar way the basis elements x, y, z can be represented by the exponents $(1, 0, 0)$, $(0, 1, 0)$, $(0, 0, 1)$.

TABLE 4. The $p = 11$ case

(u, v, w)	μ	ν	(u, v, w)	μ	ν
$(0, 0, 2)$	8 821	56	$(1, 1, 5)$	5 517	44
$(0, 0, 3)$	164 272	232	$(1, 2, 2)$	5 932	46
$(0, 1, 1)$	17 470	144	$(1, 2, 3)$	12 328	68
$(0, 1, 2)$	8 395	71	$(1, 2, 4)$	12 379	68
$(0, 1, 3)$	22 111	115	$(1, 3, 3)$	5 928	46
$(0, 2, 2)$	9 236	86	$(1, 3, 4)$	6 168	46
$(0, 2, 3)$	7 305	64	$(2, 2, 2)$	28 198	48
$(0, 2, 5)$	9 185	86	$(2, 2, 3)$	41 421	136
$(0, 3, 10)$	5 406	42	$(2, 2, 4)$	37 395	92
$(0, 5, 8)$	5 391	42	$(2, 5, 8)$	36 235	92
$(1, 1, 1)$	5 219	42	$(2, 6, 7)$	53 848	180
$(1, 1, 2)$	8 403	44	$(3, 3, 7)$	36 992	92
$(1, 1, 3)$	19 338	132	$(5, 5, 5)$	35 194	48
$(1, 1, 4)$	7 864	44	$(7, 7, 10)$	53 290	180

The number of choices for a is $p^3 - 4$ since G has p^3 elements and four elements of G have already been chosen to be in A. We may assume that $0 \le u \le v \le w \le p-1$ since the basis elements x, y, z can be interchanged among each other. This leaves

$$\binom{p+2}{3} - 2 = (1/6)(p+2)(p+1)(p) - 2$$

choices for a as the elements e and z have already been chosen to be in A.

We need to further reduce the number of choices for the element a. We will sort the possible A_1 subsets into equivalence classes. It will be enough to work with one representative from each equivalence class.

Note that if $w \neq 0$, then among the elements x, y, z, a the elements x, y, a can also be used as a basis for G. Setting

$$x_1 = x,\ y_1 = y,\ z_1 = a,\ a_1 = z$$

we get that

$$a_1 = x_1^{-w^{-1}u} y_1^{-w^{-1}v} z_1^{w^{-1}}.$$

In other words, (u, v, w) can be replaced by $(-w^{-1}u, -w^{-1}v, w^{-1})$. Here the operations are understood in Z_p.

Similarly, if $v \neq 0$, then (u, v, w) can be replaced by $(-v^{-1}u, v^{-1}, -v^{-1}w)$ and if $u \neq 0$, then (u, v, w) can be replaced by $(u^{-1}, -u^{-1}v, -u^{-1}w)$.

Multiplying the factorization $G = AB = (A_1 \cup A_2)B$ by x^{-1} we get the normalized factorization $G = Gx^{-1} = (Ax^{-1})B = (A_1x^{-1} \cup A_2x^{-1})B$ of G. Therefore, the product $(A_1x^{-1})B$ is direct. This means that the elements e, x, y, z, a of A_1 can be replaced by the elements

$$x^{-1},\ e,\ yx^{-1},\ zx^{-1},\ ax^{-1}$$

of A_1x^{-1} when A is replaced by Ax^{-1} in the factorization $G = AB$. Setting

$$x_1 = x^{-1},\ y_1 = yx^{-1},\ z_1 = zx^{-1},\ a_1 = ax^{-1}$$

we get that

$$a_1 = x_1^{1-u-v-w} y_1^v z_1^w.$$

In short (u, v, w) can be replaced by $(1-u-v-w, v, w)$.

Similarly, (u, v, w) can be replaced by $(u, 1-u-v-w, w)$ and $(u, v, 1-u-v-w)$.

Let us define a graph Γ. The nodes of Γ are the elements of Z_p^3. We send a directed edge from the node

$$(u, v, w) \tag{2}$$

to the node

$$(u', v', w') \tag{3}$$

of Γ if u', v', w' is only a rearrangement of the elements u, v, w. Further, we connect the node (2) with a directed edge to the node (3) if (u', v', w') is equal to one of the following:

$$(-w^{-1}u, -w^{-1}v, w^{-1}),\ (w \neq 0),$$
$$(-v^{-1}u, v^{-1}, -v^{-1}w),\ (v \neq 0),$$
$$(u^{-1}, -u^{-1}v, -u^{-1}w),\ (u \neq 0),$$
$$(1-u-v-w, v, w),\ (u, 1-u-v-w, w),\ (u, v, 1-u-v-w).$$

One can verify easily that if there is a directed edge from node (2) to node (3), then there is a directed edge from node (3) to node (2). The two directed edges can be replaced conveniently by a single undirected edge. Thus the edges of the graph Γ are finally not directed. We decompose Γ into connected components and we choose one representative from each component. The symmetry reduction part of the argument can be summarized in the following result.

Lemma 2. *The equivalence classes and the nodes of the connected components of the graph* Γ *are identical.*

The equivalence classes can be described in a more formal way. We define a relation $\sim$ on Z_p^3. Namely, the element (2) is in relation to the element (3) if there is a directed edge from node (2) to node (3). One can see that the $\sim$ relation is symmetric. The reflexive and transitive closure of $\sim$ is an equivalence relation. The equivalence classes are the same as the nodes of the connected components in Γ.

We discard the elements of the components of $(0,0,0)$, $(1,0,0)$, $(0,1,0)$, $(0,0,1)$, $(p-1, p-1, p-1)$. The reason for the last exclusion is that among the elements of $A \setminus \{e, x, y, z\}$ the element a can be chosen such that the quantity $u+v+w$ is as small as possible. Now in the $u = v = w = p-1$ case there are no choices left for the elements in $A \setminus \{e, x, y, z\}$ if $p \geq 7$.

4. The computations

We describe the set U and the subsets $D_1, \ldots, D_n$ of U in the exact cover problem more explicitly. There is an incidence matrix associated with the exact cover problem and we describe this incidence matrix. There are ten subgroups $H_1, \ldots, H_{10}$ such that $G = H_1 B, \ldots, G = H_{10} B$ are normalized factorizations of G. The subgroups $H_1, \ldots, H_{10}$ are spanned by the elements

$$ex^{-1},\ ey^{-1},\ ez^{-1},\ ea^{-1},\ xy^{-1},\ xz^{-1},\ xa^{-1},\ yz^{-1},\ ya^{-1},\ za^{-1},$$

respectively. The incidence matrix has $|G| = p^3$ rows and $(10) \cdot p^2$ columns. The rows are labeled by the elements of G. Each of the first p^2 columns contains a translated copy of the subgroup H_1, that is, a coset modulo H_1. These cosets are

TABLE 5. The $p = 13$ case

(u, v, w)	μ	ν	(u, v, w)	μ	ν
$(0, 0, 2)$	5 473 284	1 260	$(1, 2, 3)$	109 045	154
$(0, 0, 3)$	968 556	454	$(1, 2, 4)$	101 386	128
$(0, 0, 4)$	4 298 656	480	$(1, 2, 5)$	363 248	232
$(0, 1, 1)$	13 917 302	1 052	$(1, 3, 3)$	109 054	102
$(0, 1, 2)$	145 575	315	$(1, 3, 4)$	157 195	102
$(0, 1, 3)$	46 613	211	$(1, 3, 5)$	259 315	258
$(0, 1, 5)$	57 472	289	$(1, 4, 4)$	352 851	180
$(0, 2, 2)$	105 918	306	$(2, 2, 2)$	1 870 787	156
$(0, 2, 3)$	34 129	176	$(2, 2, 3)$	2 716 963	286
$(0, 2, 4)$	41 198	228	$(2, 2, 4)$	2 281 198	234
$(0, 2, 6)$	34 515	176	$(2, 2, 5)$	2 874 367	468
$(0, 3, 3)$	35 224	176	$(2, 3, 3)$	2 628 622	208
$(0, 3, 12)$	122 517	462	$(2, 3, 4)$	2 362 932	182
$(0, 4, 4)$	34 189	176	$(2, 4, 4)$	2 376 057	312
$(1, 1, 1)$	144 796	50	$(2, 5, 10)$	2 284 413	156
$(1, 1, 2)$	84 748	152	$(3, 3, 4)$	3 615 745	624
$(1, 1, 3)$	157 783	152	$(3, 4, 8)$	2 352 047	182
$(1, 1, 4)$	58 055	126	$(3, 6, 6)$	3 746 063	676
$(1, 1, 5)$	63 713	152	$(3, 8, 8)$	2 830 535	234
$(1, 1, 6)$	206 530	464	$(5, 5, 5)$	4 040 525	1 092
$(1, 2, 2)$	152 439	206			

pairwise disjoint. Similarly, each of the second p^2 columns contains a coset modulo H_2 and the cosets are pairwise disjoint. Finally, each of the tenth p^2 columns contains a coset modulo H_{10}. These cosets are pairwise disjoint as well. The columns are labeled by the elements of the universal set U. Therefore, $|U| = (10) \cdot p^2$. A solution to this simultaneous transversal problem is the same as the solution to the simultaneous complement factor problem for the subgroups $H_1, \ldots, H_{10}$. The incidence matrix provides the definition of the subsets $D_1, \ldots, D_n$. As a consequence n must be equal to p^3.

The $p = 5, 7, 11, 13$ cases are handled separately but in a similar manner. In each case the computation can be divided into four steps.

(1) Constructing a transversal for the equivalence classes.
(2) Setting up the incidence matrix for the exact cover.
(3) Finding all possible exact covers.
(4) Inspecting the arising complement factors.

The source code is available at [5] .

In the $p = 5$ case the graph Γ splits into 8 connected components. We discard the component containing $(0, 0, 0)$. In the remaining 7 cases using the exact cover algorithm we compute all possible factors B. The result is summarized in Table 2. The μ stands for the number the nodes of the searching tree and ν denotes the number of the possible B's found. In each case the resulting B was periodic. We know from the last paragraph of Section 2 of [4] that if B is periodic, then it cannot be part of a full-rank factorization. We point out that in this case we cannot rule out the component containing $(4, 4, 4)$.

In the $p = 7$ case the graph Γ consists of 13 connected components. Two of them we discard and in the remaining 11 cases we used the exact cover algorithm to compute all possible B. The result is in Table 3. Again all B were periodic and so there is no counterexample for Rédei's conjecture when $p = 7$.

In the $p = 11$ case the graph Γ has 30 connected components, two of which we discarded. Then we computed the possible B sets. All of them were periodic. The details are presented in Table 4.

When $p = 13$ the graph Γ has 43 connected components. We sort out two of them and so we end up with 41 instances of the exact cover problem. The results are summarized in Table 5. Each of the computed B proved to be periodic.

We spell out the result of the computer aided search more formally.

Theorem 1. *Conjecture* 1 *holds for* $p \leq 13$.

References

[1] D. E. Knuth, Dancing links, in *Millennial Perspectives in Computer Science*, J. Davies, B. Roscoe, and J. Woodcock, Eds., Palgrave Macmillan, Basingstoke, 2000, pp. 187–214.

[2] L. Rédei, *Lückenhafte Polynome über endlichen Körpern*, Birkhäuser Verlag, Basel, 1970, (English translation: *Lacunary Polynomials over Finite Fields*, North-Holland, Amsterdam, 1973.) MR0294297 (45:3366)

[3] S. Szabó, *Topics in Factorization of Abelian Groups*, Birkhäuser Verlag, 2004. MR2105798 (2005k:20125)

[4] S. Szabó and C. Ward, Factoring elementary groups of prime cube order into subsets, *Mathematics of Computation* **67** (1998), 1199–1206. MR1451328 (98j:20078)

[5] `http://www.ttk.pte.hu/mii/alkmatematika/anyagok/demo.zip`

Institute of Mathematics and Informatics, University of Pécs, Ifjúság u. 6, 7624 Pécs, Hungary

E-mail address: `sszabo7@hotmail.com`