KIRKMAN TRIPLE SYSTEMS CONTAINING MAXIMUM SUBDESIGNS

R.C. Mullin, D.R. Stinson, and S.A. Vanstone

ABSTRACT. A necessary condition for a Kirkman triple system of order v to contain a Steiner triple system of order $(v-1)/2$ as a subsystem is that v be congruent to 3 modulo 12. It is shown that, except for 19 possible exceptions, this condition is also sufficient for the existence of such a system.

1. *Introduction.*

A *Steiner triple system* of order v is a pair (V,T), where V is a v-set and T is a collection of triples (three-element subsets) of V with the property that each pair of distinct elements of V is contained in precisely one of the triples of T. It is well-known that a necessary and sufficient condition for the existence of a Steiner triple system of order v is that v be a positive integer congruent to 1 or 3 modulo 6. A *subsystem* of a triple system (V,B) is a pair (V',B'), where $V' \subseteq V$ and $B' \subseteq B$, such that (V',B') is a Steiner triple system in its own right. It is easily shown that $|V'| \leq (v-1)/2$. If equality holds, the sub-system is said to be a *maximum* subdesign.

A Kirkman triple system of order v is a Steiner triple system of order v whose triples can be partitioned into classes (resolution classes) such that each member of the underlying v-set V occurs precisely once in each class . It is known [6] that such a system exists if and only if v is a positive integer congruent to 3 modulo 6. If a Kirkman triple system of order v, when viewed as a Steiner triple system, contains a maximum subdesign, we refer to the subdesign as a maximum subdesign of the Kirkman system, despite the fact that it may not be a Kirkman system. If v' is congruent to 3 modulo 6, then $2v'+1$ is congruent to 1 modulo 6, so any maximum subdesign of a Kirkman triple system must be of order v' congruent to 1 modulo 6, and hence is never a Kirkman system. This also shows that if v is the order of a Kirkman system which contains a maximum subdesign, then v is congruent to 3 modulo 12. We show here that that condition is also sufficient, with 19 possible exceptions, for the

UTILITAS MATHEMATICA Vol. 21C (1982), pp. 283-300.

existence of such a system.

A Kirkman system containing a maximum subdesign was constructed by Kirkman [2] in 1850, and again by Cayley [1] in 1863. Both of these constructions used a configuration now known as a Room square [3]. Mullin and Vanstone [4] have shown that a Kirkman triple system of order v with a maximum subdesign always gives rise to a Room square of side $(v-1)/2$, and conversely a Room square with certain incidence properties can be used to construct a Kirkman system containing a maximum subdesign.

For convenience, we will denote a Kirkman system of order v which contains a maximum subdesign by the symbol MK(v).

2. *Constructions.*

A number of constructions are required in order to establish results on the spectrum of MK(v)s. We first state several direct constructions.

THEOREM 2.1. *If* r *is a prime power congruent to* 1 *modulo* 6 *then there exists an* MK(2r+1).

This class of Kirkman triple systems was constructed by Ray-Chaudhuri and Wilson and can be found in [5].

Suppose v is a positive integer, and K is a set of positive integers. A (v,K)-*pairwise balanced design* (or PBD) is a pair (X,Q) of sets where $|X| = v$, $B \in Q$ implies $B \subseteq X$ and $|B| \in K$, and for any distinct x_1, x_2 in X, there is a unique $B \in Q$ with $\{x_1, x_2\} \subseteq B$. A set of positive integers A is said to be *PBD-closed* if $v \in A$ whenever there exists a (v,A) - PBD.

Define RMK = {r : there exists an MK(2r+1)}.

THEOREM 2.2. RMK *is PBD -closed.*

Proof. Let (X,Q) be a (v, RMK) PBD. Let $\infty \notin X$, and let $Z = \{\infty\} \cup X \times \{1,2\}$. For any $B \in Q$, we can construct an MK$(2|B| + 1)$ on $\{\infty\} \cup B \times \{1,2\}$ which contains blocks $\{\infty, x_1, x_2\}$, for each $x \in B$, and also contains a sub-design on $B \times \{1\}$ Do this for every block $B \in Q$, keeping exactly one copy of each block $\{\infty, x_1, x_2\}$, for each $x \in X$.

It is easy to check that we have a Steiner triple system, and that we have a subsystem on $X \times \{1\}$. Associated with each $B \in Q$

we have classes $R_{B,x}$, $x \in B$, which form a resolution of the $MK(2|B| + 1)$ on $\{\infty\} \cup B \times \{1,2\}$. We may stipulate that $\{\infty, x_1, x_2\} \in R_{B,x}$, for each $x \in B$. Define $R_x = \bigcup_{B \ni x} R_{B,x}$. It is easy to check that the R_x's form a resolution of our design.

Thus we have constructed an $MK(2v+1)$, as required. □

Before proceeding to the next construction, we require several definitions. An incomplete transversal array, denoted $ITA(m,k,s)$ is an $m \times m$ array A, and a triple $(X,\{G,H\},B)$, such that

(1) $|X| = mk$;

(2) every cell is either empty or contains a k-subset of X;

(3) the empty cells form an $s \times s$ subarray S;

(4) $G = \{G_1, G_2, \ldots, G_k\}$ is a partition of X into k subsets of size m;

(5) $H = \{H_1, H_2, \ldots, H_k\}$, where $H_i \subseteq G_i$ and $|H_i| = s$, $1 \le i \le k$;

(6) if B is the set of k-subsets in the cells of the array, the then $|G_1 \cap B| = 1$ and $|H_1 \cap B| \le 1$ for all $B \in B$ and $1 \le i \le k$;

(7) for every i and j $(i \neq j)$ and every $x,y \in X$ $(x \neq y)$ such that $x \notin H_i$ or $y \notin H_j$, the pair x,y is contained in a unique block of B.

(8) every column of A which is not a column of S contains each element of X precisely once and every column of A which is a column of S contains each element of $\bigcup_{i=1}^{k} (G_i \setminus H_i)$ precisely once.

As an example, an $ITA(6,3,2)$ is displayed.

		3cα	4dα	5eα	6fα
		6dβ	3eβ	4fβ	5cβ
3dγ	6eγ	1fγ	5bγ	2cγ	4aγ
4eδ	3fδ	5aδ	1cδ	6bδ	2dδ
5fε	4cε	2eε	6aε	1dε	3bε
6cω	5dω	4bω	2fω	3aω	1eω

$G_1 = \{1,2,3,4,5,6\}$, $H_1 = \{1,2\}$.

$G_2 = \{a,b,c,d,e,f\}$, $H_2 = \{a,b\}$.

$G_3 = \{\alpha,\beta,\gamma,\delta,\epsilon,\omega\}$, $H_3 = \{\alpha,\beta\}$.

It is easily seen that the existence of $k-1$ mutually orthogonal latin squares (MOLS) of order m which contain $k-1$ MOLS of order s implies the existence of an ITA(m,k,s). The converse is not true of course.

Let K be an MK(v). Let $r = (v-1)/2$. Define a Kirkman array KA(r) to be an $n \times r$ array, where $n = (2r+1)/3$, such that every cell contains precisely one block of K, each block of K is contained in a cell, and the triples of any column form a resolution class of K. The array shown below is a KA(7).

abc	ade	afg	bdf	bge	cdg	cef
d35	b26	b13	a47	a58	a12	a36
e17	c48	c57	c16	c23	b78	b45
f28	f15	d68	c38	d14	e56	d27
g46	g37	e24	g25	f67	f34	g18

The subdesign is defined on the symbol set {a,b,c,d,e,f,g}.

A KA(r) is said to be *normalized* if

(1) an element ∞ of K which is not in the maximum subdesign is contained in each cell of the first row of the array;

(2) KA is defined on the symbol set $V = I_r \times \{x,y\} \cup \{\infty\}$, where $x \neq y$;

(3) the entry in cell (1,i) is $\{\infty,(i,x),(i,y)\}$;

(4) the maximum subdesign is defined on the symbol set $I_r \times \{y\}$.

A KA(r), A, is said to contain an $n' \times r'$ subarray if there exists $n' = (2r'+1)/3$ rows and r' columns of A such that this

subarray is itself a KA(r') defined on a subset of the symbol set of A.

Let $K = (k_{ij})$ be an $m \times m$ array in which k_{ij} is an ordered k-tuple of some symbol set V. Let L be an ordered k-tuple $(\alpha_1,\alpha_2,\ldots,\alpha_k)$. Define

$$K \circ L = (\ell_{ij})$$

where $\ell_{ij} = \{(h_1,\alpha_1),(h_2,\alpha_2),\ldots,(h_k,\alpha_k)\}$

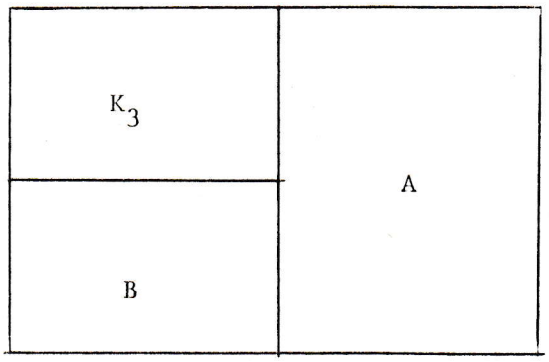
if $k_{ij} = (h_1,h_2,\ldots,h_k)$.

If $L = \phi$, then define $K \circ L$ to be an $m \times m$ empty array.

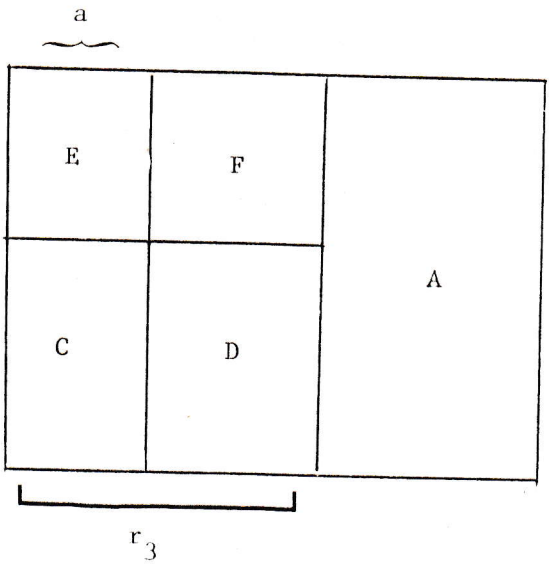
We now state and prove a recursive construction for Kirkman arrays. The construction is called a singular indirect product.

THEOREM 2.3. *Suppose there exists a* $KA(r_1)$, *and there exists a* $KA(r_2)$ *which contains a* $KA(r_3)$ *as a subarray. If for a nonnegative integer,* $a \le r_3$ *there exists an* $ITA(r_2-a,3,r_3-a)$ *and there exists a* $KA(r_1(r_3-a)+a)$ *then there exists a* $KA(r_1(r_2-a)+a)$.

Proof. Let K_1,K_2,K_3 denote $KA(r_1),KA(r_2)$, and $KA(r_3)$ respectively. Without loss of generality, assume that K_1,K_2, and K_3 are normalized. K_2 has the following form:



Let a be a nonnegative integer, $0 \le a \le r_3$. Select the first a columns of K_2 and partition the array as follows:



Let V_2 and V_3 be the symbol sets on which K_2 and K_3 are written, respectively. Clearly, $V_3 \subseteq V_2$. Define K_2^i to be the array K_2 written on the symbol set $(V_2/V_3) \times \{(i,x),(i,y)\} \cup V_3$. Of course, A_i, F_i, D_i, E_i, and C_i are defined accordingly. Let the maximum sub-design in K_2^i be written on the symbol set $(V_2/V_3) \times \{(i,y)\} \cup (I_{r_3} \times \{y\}) \cup \infty$.

Let L be an ITA(r_2-a, 3, r_3-a) written on a symbol set V_2/V_3. Form the following array N:

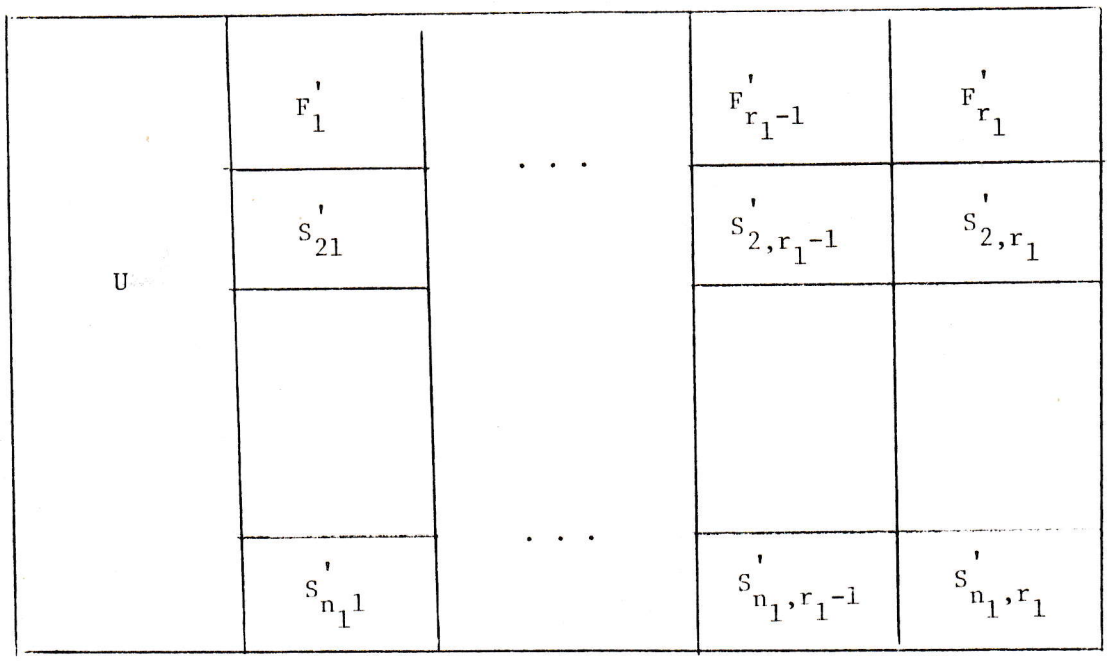
T_1	T_2		T_{r_1}
L o ℓ_{21}	L o ℓ_{22}		L o ℓ_{2r_1}
L o $\ell_{n,1}$	L o $\ell_{n,2}$		L o $\ell_{n,r}$

where $K_1 = (\ell_{ij})$ and T_i is the $n_2 \times (r_2-a)$ array consisting of F_j, A_i, and D_i of K_2^i. Let S_{ij} be the $(r_3-a) \times (r_3-a)$ empty subarray contained in $L \circ \ell_{ij}$.

Let M be a $KA(r_1(r_3-a)+a)$ written on the symbol set

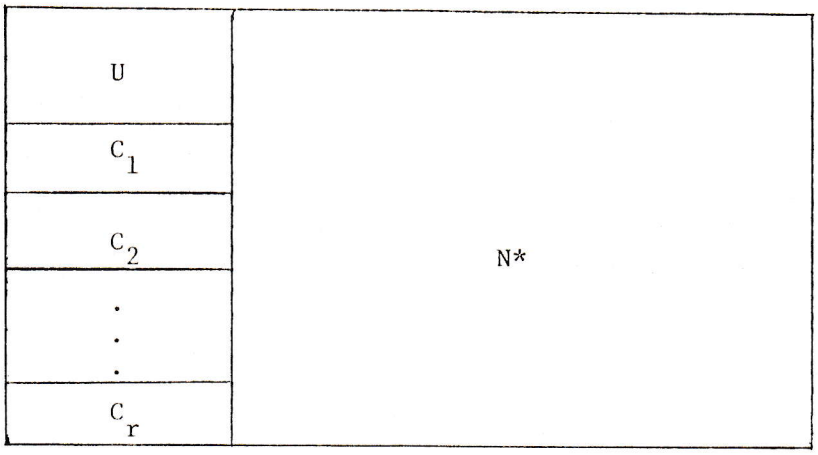
$$\{I_{r_3} \setminus I_a) \times \{x,y\}\} \times (V_1 \setminus \infty) \cup (I_a \times \{x,y\}) \cup \infty .$$

Let the maximum subdesign be defined on the symbol set $\{(I_{r_3} \setminus I_a) \times \{x,y\}\} \times (I_{r_1} \times \{y\}) \cup \infty$. Arbitrarily partition M as follows:



where F_i' is an $n_3 \times (r_3-a)$ array $(1 \le i \le r_1)$ and S_{ij}' is an $(r_3-a) \times (r_3-a)$ array $(2 \le i \le n_1,\ 1 \le j \le r_1)$.

Form the array N* from N by replacing the subarray F_i in N by the subarray F_i' of M for all i, $1 \le i \le r_1$, and replace the empty subarray S_{ij} of N by the subarray S_{ij}' of M for all i,j, $2 \le i \le n_1$, $1 \le j \le r_1$. Finally, form the following array A*.



It is a tedious but straightforward task to show that A* is a $KA(r_1(r_2-a) + a)$ defined on the symbol set

$$\{V_2-(I_a \times \{x,y\})\} \times (V_1-\infty) \cup (I_a \times \{x,y\}) \cup \infty.$$

The maximum subdesign is written on the symbol set

$$\{V_2-(I_a \times \{x,y\})\} \times \{I_{r_1} \times y\} \cup (I_a \times \{y\}) \cup \infty.$$

COROLLARY 2.4. *Suppose there exists a* $KA(r_1)$ *and there exists a* $KA(r_2)$ *which contains a* $KA(r_3)$ *as a subarray. If there exists a pair of orthogonal latin squrares of side* $r_2 - r_3$, *then there exists a* $KA(r_1(r_2-r_3) + r_3)$.

The proof follows from Theorem 2.3 with $a = 0$.

Having established the PBD-closure of RMK it is useful to have some constructions for PBD's. These constructions make use of orthogonal arrays (OA's). For a definition see [3]. Recall $OA1t) = \{n:$ there exists an $OA(n,t)\}$.

THEOREM 2.5. *Suppose* A *is a PBD-closed set,* $m \in OA(14)$, $0 \le t \le m$, *and* $\{6m+1,12m+1,6t+1,7,13\} \subseteq A$.

Then $84m+6t+1 \in A$.

Proof. See [3].

THEOREM 2.6. *Suppose* A *is a PBD-closed set,* $m \in OA(43)$, $0 \le t \le m$, *and* $\{m,m+6t,43\} \subseteq A$.

Then $43m+6t \in A$.

Proof. See [3].

We will use the following well-known result concerning the

existence of orthogonal arrays.

THEOREM 2.7. *Let* m *have prime power factorization* Πp_i^{α}. *Then* $m \in OA(k)$ *if* $k \le \min\{p_i^{\alpha} + 1\}$.

We will also make use of the following simple number-theoretic result.

LEMMA 2.8. *If* m_0 *is an integer, then there exists* m *such that* $m_0 - 13 \le m \le m_0$ *and* $(m, 2.3.5.7.11) = 1$.

Proof. We show that the maximum distance between units modulo 2.3.5.7.11 is 14. Any unit is of the form $6t + 1$ or $6t + 5$.

If $u = 6t + 1$, consider $\{u, u-2, u-6, u-8\}$. These four numbers are each relatively prime to 6, and at most one is divisible by 5, by 7, or by 11. There must be at least one element left over, which is relatively prime to 2.3.5.7.11.

If $u = 6t - 1$, consider $\{u, u-4, u-6, u-10, u-12\}$. These five numbers are each relatively prime to 6, at most two of them are divisible by 5, and at most 1 is divisible by 7, or by 11. □

We also need some constructions for incomplete transversal arrays.

LEMMA 2.9. *(1) If there exist* $k - 1$ *MOLS of orders* m *and* $m + 1$, k *MOLS of order* t, *and* $0 \le u \le t$, *then there exists an* $ITA(mt + u, k, u)$.

(2) If there exist $k - 1$ *MOLS of orders* m, $m + 1$ *and* $m + 2$, $k+1$ *MOLS of order* t, k *MOLS of order* v, *and* $0 \le u, v \le t$, *then there exists an* $ITA(mt + n + v, k, u)$.

Proof. See [5].

3. *Closing the Spectrum.*

THEOREM 3.1. *Suppose* $v \in RMK$ *if* $1825 \le v \le 44905$ *and* $v \equiv 1 \bmod 6$. *Then* $v \in S$ *if* $1825 \le v$ *and* $v \equiv 1 \bmod 6$.

Proof. Let $v \ge 1825$, $v \equiv 1 \bmod 6$. We proceed by induction. Suppose that $u \in RMK$ if $1825 \le u < v$ and $u \equiv 1 \bmod 6$. If $v \le 44905$ then $v \in RMK$ by assumption, so suppose $v \ge 44911$. Let $v = 6n + 1$, so $n \ge 7485$.

Write $n = 14m_0 + t_0$, with $304 \le t_0 \le 317$. Using Lemma 2.8, choose m such that $m_0 - 13 \le m \le m_0$ and $(m, 2.3.5.7.11) = 1$. Then $n = 14m + 1$, where $t_0 + 182 \ge t \ge t_0$.

We show that $m \ge t$. We have $m = (n-t)/14$, so $m \ge t$ if

$n \geq 15t$. But $t \leq t_0 + 182 \leq 499$, and $n \geq 7485 = 15 \cdot 499$.

Now $t \geq 304$, so $6t + 1 \geq 1825$. Thus we have □

$$v = 84m + 6t + 1 > 12m + 1 > 6m + 1 \geq 6t + 1 \geq 1825.$$

Since RMK is PBD closed, the result follows by induction, from Theorem 2.5 (note that $m \in OA(14)$ by Theorem 2.7).

In order to apply Theorem 3.1 we must show that $v \in RMK$ if $1825 \leq v \leq 44905$ and $v \equiv 1 \bmod 6$. It is desirable first to show that except for a few possible exceptions, if $v \equiv 1 \bmod 6$ and $v \leq 1819$ then $v \in RMK$.

LEMMA 3.2. *If* $v \equiv 1 \bmod 6$ *and* $v \leq 1819$ *then* $v \in RMK$ *unless* $v \in X = \{55,115,145,187,205,265,355,415,593,649,655,697,943,955,979, 1003,1243,1285,1819\}$.

Proof. We list constructions in Table 1. For brevity, we omit prime power orders (where Theorem 2.1 or Theorem 2.2 applies) and orders which are the product of two prime powers, both of which are congruent to 1 mod 6. □

Notes for Table 1.

Note 1. $8 \in OA(8)$, so there is a group-divisible design with eight groups of size 8, and blocks of size 8. Take 6 copies of each point. Replace each block by the blocks of a group-divisible design having eight groups of size 6, and blocks of size 7 (an affine plane of order 7 with a point deleted). Replace each group by an affine plane of order 7 on the 48 points existing plus on new point ∞.

To show $1537 \in B(7,193)$ start with $32 \in OA(8)$ and proceed as above.

Note 2. K. Heinrich has shown that an $ITA(n,3,2)$ exists for all $n \geq 5$.

TABLE 1.

Order	u	v	w	a	v-a	w-a	u(w-a)+a	Remarks
85	7	13	1					
275	13	19	1					
253	7	37	1					
295	7	43	1					
319	7	49	7	4	45	3	25	49=7.7,45=15.3
385								see note (1), 385ε B(7)
391	13	31	1					
445	37	13	1					
451	29	19	1					
505	7	73	1					
517	7	85	13					85=7(13-1)+1
535	7	85	13	10	75	3	31	85=7(13-1)+1,75=25.3
565	7	85	13	5	80	8	61	85=7(13-1)+1,80=8.10
583	7	85	7	2	83	5	37	85=7(13-1)+1,83=3.26+5
667	37	19	1					
685	19	37	1					
715	7	103	1					
745	13	25	1					
781	13	61	1					
799	19	43	1					
805	67	13	1					
835	7	127	19	9	116	10	79	127=7(19-1)+1,116=3.35+10+1
865	7	127	7	4	123	3	25	127=7(19-1)+1,123=41.3
895	7	133	7	6	127	1	13	133=7.19
901	25	37	1					
913	19	49	1					
985	13	85	13	10	75	3	49	85=7(13-1)+1,75=25.3
1015	13	79	1					
1045	13	85	7	5	80	2	37	85=7(13-1)+1. Note (2)
1081	7	157	13	3	154	10	73	157=13(13-1)+1,154=3.48+10
1105								84.13+6.2+1
1111								84.13+8.3+1
1135	7	163	1					
1165								84.13+6.12+1
1177	7	169	1					

TABLE 1 (continued)

Order	u	v	w	a	v-a	w-a	u(w-a)+a	Remarks
1189	7	175	7	6	169	1	13	175=7.25
1195	7	175	7	5	170	2	19	175=7.25,170=3.56+2
1207	7	175	7	3	172	4	31	175=7.25,172=3.56+4
1219	7	175	1					
1255	19	67	1					
1309	109	13	1					
1315	73	19	1					
1345	7	193	1					
1357								84.16+6.2+1
1363								84.16+6.3+1
1375								84.16+6.5+1
1405								84.16+6.10+1
1411								84.16+6.11+1
1435	7	211	7					211=7(31-1)+1
1441	7	211	7	6	205	1	13	211=7(31-1)+1
1465	7	217	31	9	208	22	163	217=7.31,208=3.64+11+5
1495	7	217	7	4	213	3	25	217=7.31,213=3.70+3
1507	7	217	7	2	215	5	37	217=7.31,215=41.5
1513	7	217	1					
1537								1537ε B(7,193),Note (1)
1555	7	223	1					
1585	7	229	13	3	226	10	73	229=19(13-1)+1,226=3.72+10
1615	7	247	19	18	229	1	25	247=13.19
1633	7	247	19	16	231	3	37	247=13.19,231=3.76+3
1639	7	247	19	15	232	4	43	247=13.19,232=2.76+4
1645	7	247	19	14	233	5	49	247=13.19,233=3.76+5
1705	7	247	13	4	243	9	67	249=13.19,243=3.78+9
1711	7	247	13	3	244	10	73	247=13.19,244=3.78+10
1717	7	247	13	2	245	11	79	247=13.19,244=3.78+11
1729	7	247	0					
1735	7	259	37	13	246	24	181	259=7.37,246=3.74+24
1765	7	259	37	8	251	29	211	259=7.37,251=3.74+29
1771	7	259	7					259=7.37
1795	13	139	1					

From Lemma 3.2 we can obtain the following.

COROLLARY 3.3. *If* $u < v \le 1819$, $v - u \equiv 0 \bmod 252$, $u,v \equiv 1 \bmod 6$, *and* $\{u,v\} \cap RMK = \emptyset$ *then* $(u,v) \in \{(55,1819),(145,649),(187,943)\}$.

Corollary 3.3 is of use in the following lemma.

LEMMA 3.4. *Suppose* $x = 43m + 6t = 43m_1 + 6t_1$, *where* m *and* m_1 *are prime powers congruent to* 1 mod 6, *and* $m < m_1$, $t \le m$, $t_1 \le m_1$. *If* $\{m + 6t, m_1 + 6t_1\} \cap RMK = \emptyset$ *and* $m + 6t, m_1 + 6t_1 \le 1819$, *then one of the following holds:*

(1) $m_1 \le 55$ *and* $m_1 - m = 42$;

(2) $m_1 \le 145$ *and* $m_1 - m = 42$ *or* 12;

(3) $m_1 \le 187$ *and* $m_1 - m = 42,18,$ *or* 12.

Proof. Since $43m + 6t = 43m_1 + 6t$, we have $m + 6t - (m_1 + 6t) = 42(m_1 - m)$. Thus $m_1 \equiv m \bmod 6$, so $m + 6t \equiv m_1 + 6t_1 \bmod 252$. Also $m + 6t \ne m_1 + 6t_1$, and both are congruent to 1 mod 6. Let $m + 6t - (m_1 + 6t_1) = 252k$. Then $m_1 - m_2 = 6k$. Corollary 3.3 implies the result. □

LEMMA 3.5. *Suppose* $m_0 < m_1 < m_2 < \ldots < m_n$, *where each* m_i *is a prime power congruent to* 1 mod 6. *Suppose* $m_i/m_{i+2} \ge 43/49$ *for* $0 \le i \le n-2$. *Then if* $43m_1 \le x \le 49m_{n-1}$, *we can write* $x = 43m_j + 6t = 43m_{j+1} + 6t_1$ *for some* j, $0 \le j \le n-1$, *and* $t \le m_j$, $t_1 \le m_{j+1}$.

Proof. Let $m = x/43$, and let m_j' be the largest m_i not exceeding m. Now, $x \le 43m_{j+1}$ and $49m_{j-1} \ge 43m_{j+1}$ so $x \le 49m_{j-1} < 49m_j$. Also $x \ge 42m_j > 43m_{j+1}$. Let $t = (x - 43m_j)/6$ and $t_1 = (x - 43m_{j+1})/6$. Both t and t_1 are integers, and $0 \le t \le m_j$, $0 \le t_1 \le m_{j+1}$, as required. □

LEMMA 3.6. *Suppose* $v \in RMK$ *if* $1825 \le v \le 6559$, *and* $v \equiv 1 \bmod 6$. *Then* $v \in RMK$ *if* $11911 \le v \le 45031$ *and* $v \equiv 1 \bmod 6$.

Proof. Let $M = \{271,277,\ldots,919,937\}$ be the set of all prime powers between 271 and 937 which are congruent to 1 modulo 6. Let the elements of M be ordered $m_0 < m_1 < \ldots < m_n$. It can be checked that $m_i/m_{i+2} \ge 43/49$ for $0 \le i \le n-1$. Let $v \equiv 1 \bmod 6$ and $11911 \le v \le 45031$. By Lemma 3.5 we can write $v = 43m_j + 6t = 43m_{j+1} + 6t_1$ with $0 \le t \le m_j$, $0 \le t_1 \le m_{j+1}$. We need only show that $\{m_j + 6t, m_{j+1} + 6t_1\} \cap RMK \ne 0$. If one of $m_j + 6t$, $m_{j+1} + 6t$, is

at least 1825, then it is in RMK by the assumption that $v \in RMK$ if $1825 \le v \le 6559$ and $v \equiv 1 \bmod 6$. Since $m_j + 6t = v - 42m_j$ and $m_{j+1} + 6t_1 = v - 42m_{n+1}$, we have $m_{j+1} + 6t \le m_{j+1} + 6t_1 \le 7m_{j+1} \le 7m_n = 6559$. Finally, if both $m_j + 6t$, $m_{j+1} + 6t_1$ are less than 1825, Lemma 3.4 guarantees that at least one of them is in RMK. □

LEMMA 3.7. $v \in RMK$ *if* $8299 \le v \le 11211$ *and* $v \equiv 1 \bmod 6$.

Proof. Let $m_0 = 181$, $m_1 = 193$, $m_2 = 199$, $m_4 = 211$, $m_5 = 211$, $m_6 = 223$, $m_7 = 229$, $m_8 = 241$. The proof is that of Lemma 3.6, mutatis mutandis. □

LEMMA 3.8. $v \in RMK$ *if* $6493 \le v \le 8281$ *and* $v \equiv 1 \bmod 6$.

Proof. Let $m_1 = 139$, $m_1 = 151$, $m_2 = 157$, $m_3 = 163$, $m_4 = 169$. The proof is that of Lemma 3.6, mutatis mutandis. (Note that $m_1 - m_0 = 12$, but $m_1 > 145$, so there is no problem with Lemma 3.4.) □

We summarize the above.

LEMMA 3.9. *Suppose* $v \in RMK$ *if* $v \equiv 1 \bmod 6$ *and either* $1825 \le v \le 6487$, $8287 \le v \le 8293$, *or* $11227 \le v \le 11905$. *Then* $v \in RMK$ *if* $1825 \le v$ *and* $v \equiv 1 \bmod 6$.

Proof. Immediate, in view of Lemmata 3.6, 3.7, and 3.8, and Theorem 3.1. □

Thus we need to show $v \in RMK$ for the above values of v. The following will be useful.

LEMMA 3.10. *Suppose* $m \le 271$ *is a prime power congruent to* 1 mod 6. *Then if* $43m \le v \le 49m$, $v \equiv 1 \bmod 6$, *and* $v \notin RMK$, *we must have* $m + 6t \in X$, *where* $v = 43m + 6t$.

Proof. The result follows from Theorem 2.6 and Lemma 3.2. Note that $m + 6t \le 7m \le 1819$. □

Similarly, we have the following.

LEMMA 3.11. *Suppose* $m \in OA(14)$, $\{6m + 1, 12m + 1\} \subseteq RMK$, *and* $m \le 49$. *If* $84m + 1 \le v \le 90m + 1$, $v \equiv 1 \bmod 6$, *and* $v \notin RMK$, *we must have* $6t + 1 \in RMK$, *where* $v = 84m + 6t + 1$.

We now make numerous applications of Lemmata 3.10 and 3.11 in Table 2 below. Each value of m used in Lemma 3.11 is in OA(14) by Theorem 2.7, and $6m + 1$ and $12m + 1$ are in RMK by Lemma 3.2.

Table 2

Lemma	m	Interval	Remarks
3.10	43	1849 - 2107	
3.10	49	2107 - 2401	
3.11	27	2269 - 2431	
3.11	29	2437 - 2611	
3.10	61	2623 - 2989	
3.10	67	2861 - 3283	
3.10	73	3139 - 3577	
3.10	79	3397 - 3871	
3.11	47	3949 - 4231	
3.10	97	4171 - 4753	
3.10	103	4429 - 5047	
3.10	109	4687 - 5341	
3.10	121	5203 - 5929	
3.10	127	5461 - 6223	
3.10	139	5977 - 6487	orders above 6487 covered
3.10	241	11227 - 11809	orders below 11227 covered
3.10	271	11653 - 11905	orders above 11905 covered

We now consider possible exceptions in the above intervals, and orders between 1819 and 11905 which are indicated in the statement of Lemma 3.9 and not contained in any interval above.

First, we note that, in the overlapping portion of two consecutive intervals, both of which are applications of Lemma 3.10, there can be no possible exceptions other than 5227 and 5983. This follows from Lemma 3.4. The only possibility is that the two values of m differ by 12, and the two values of $m + 6t$ are 145 and 649. These orders are $5227 = 43.109 + 6.90 = 43.121 + 6.4$ and $5983 = 43.127 + 6.87 = 43.139 + 6.1$. We list the remaining orders in Table 3 below and give constructions for them.

Table 3

m	Order	u	v	w	a	v-a	w-a	u(w-a)+a	Remarks
43	1861								Prime
43	1921	13	85	13	12	73	1	25	85=7(13-1)+1
43	1951								Prime
43	1993								Prime
43	2011								Prime
49	2113								Prime
49	2173	181	13	1					
49	2203								Prime
49	2245	7	325	13	5	320	8	61	325=13.25, 320=8.40
49	2263	31	73	0					
49,27	2323	7	337	7	6	331	1	13	317=7(49-1)+1
27	2383								covered (m=49)
27	2413	19	127	0					
29	2491	7	361	19	6	355	13	97	361=19.19, 355=3.114+13
29	2551								Prime
29	2581	43	61	1					
	2617								Prime
61	2677								Prime
61	2707								Prime
61	2749								Prime
61	2767								Prime
61	2827	157	19	1					
67	3001								Prime
67	3019								Prime
67	3079								Prime
73	3331								Prime
79	3583								Prime
79	3673								Prime
79	3733								Prime
79	3811	37	103						
	3877								Prime
	3883	7	559	13	5	554	8	61	559=13.43, 546=3.181+8+5
	3889								Prime

Table 3 (continued)

m	Order	u	v	w	a	v-a	w-a	u(w-a)+a	Remarks
	3895	7	559	13	3	556	10	73	559=13.43, 546=3.181+10+5
	3901	325	13	1					
	3907								Prime
	3913	43	91						
	3919								Prime
	3925	25	157						
	3931								Prime
	3937	31	127						
	3943								Prime
-47	4003								Prime
47	4063	7	589	19	10	579	9	73	589=19.31, 579=3.190+9
47	4093								Prime
47	4135	53	79	1					
47	4153								Prime
97	4189								covered(m=47)
47	4213								covered(m=97)
97	4219								covered(m=47)
97	4261								Prime
97	4279	7	625	25	16	600	9	79	625=25.25, 600=3.197+9
97	4339								Prime
109	5071	169	13	1					
109,121	5227								Prime
121	5347								Prime
121	5437								Prime
127,139	5983	31	19	30					
139	6253	521	13	1					
139	6331	211	31	1					
139	6487	13	499	0					
	8287								Prime
	8293	691	13	1					
241	11365	947	13	1					
241	11407								84.131+6.67+1
271	11875	19	625	0					

As a result of the above, and Lemmata 3.2 and 3.9, we have shown the following.

THEOREM 3.12. *If* $v \equiv 1 \bmod 6$ *is a positive integer, then* $v \in RMK$ *unless* $v \in X$.

The authors wish to thank the referee for his helpful comments.

Addendum. Alex Rosa (private communication) has recently constructed an MK(111), so $55 \in RMK$. If we now apply Theorem 2.3 with $r_1 = 7$, $r_2 = 295$, $r_3 = 43$, and $a = 41$, we obtain $1819 \in RMK$ (Note that $295 = 7(43-1) + 1$). Thus $v \in RMK$ if $v \equiv 1 \bmod 6$ and $v > 1285$.

REFERENCES

[1] A Cayley, *On a tactical theorem relating to the triads of fifteen things,* London, Edinburgh, and Dublin Phil. Magazine and J. Sci. *25* (1863), 59-61 (Collected Math. Papers *V*, 95-97).

[2] T.P. Kirkman, *Note on unanswered prize question,* Cambridge and Dublin Math. Journal *5* (1850), 255-262.

[3] R.C. Mullin, P.J. Schellenberg, D.R. Stinson, and S.A. Vanstone, *Some results on the existence of squares,* Annals of Discrete Mathematics *6* (1980), 257-274.

[4] R.C. Mullin and S.A. Vanstone, *Steiner systems and Room squares,* Annals of Discrete Math. *7* (1980), 95-104.

[5] D.K. Ray-Chaudhuri and R.M. Wilson, *Solution of Kirkman's schoolgirl problem,* Proc. Symp. Pure Math. *19* (1971), Amer. Math. Soc., Providence, R.I., 187-203.

[6] T.G. Room, *A new type of magic square,* Math. Gazette *39* (1955), 307.

Department of Combinatorics and Optimization
University of Waterloo
Ontario

Department of Computer Science
University of Manitoba
Winnipeg

Department of Combinatorics and Optimization
University of Waterloo
Ontario

Received November 17, 1980.