# ON THE MAXIMAL NUMBER OF PAIRWISE ORTHOGONAL LATIN SQUARES OF A GIVEN ORDER

S. CHOWLA, P. ERDÖS, AND E. G. STRAUS

**1. Introduction.** In the preceding paper Bose, Shrikhande, and Parker give their important discovery of the disproof of Euler's conjecture on Latin squares. In this paper we show that their results can be strengthened to imply that $N(n)$, the maximal number of pairwise orthogonal Latin squares of order $n$, tends to infinity with $n$. In fact there exists a positive constant $c$, such that $N(n) > n^c$ for all sufficiently large $n$.

Our proof involves no new combinatorial insights, but is based entirely on a number-theoretical investigation of the following inequality due to Bose and Shrikhande.

THEOREM A. *If* $k \leqslant N(m) + 1$ *and* $1 < u < m$ *then* $N(km + u) \geqslant \min\{N(k), N(k+1), 1 + N(m), 1 + N(u)\} - 1$.

The only other results on Latin squares which we need are due to H. F. MacNeish.

THEOREM B. (1) $N(ab) \geqslant \min\{N(a), N(b)\}$.
(2) $N(q) = q - 1$ *if* $q$ *is the power of a prime.*

In § 2 we give a proof of the fact that $N(n)$ tends to infinity, using only the most elementary tools. In § 3 we use Brun's method to obtain quantitative results on the lower bound of $N(n)$. Finally, in § 4, we discuss the theoretical limitations on the results that can be derived from Theorem A.

**2. Proof that**

$$\lim_{n\to\infty} N(n) = \infty.$$

Let $x$ be an arbitrarily large positive integer. Let

$$k + 1 = \prod_{p \leqslant x} p^x \qquad (p \text{ prime}). \tag{1}$$

Then by Theorem B we have

$$N(k+1) \geqslant 2^x - 1 \geqslant x \tag{2}$$

and

Received August 8, 1959. This paper was written while the authors were members of the Number Theory Institute (Summer, 1959) in Boulder, Colorado. The authors wish to acknowledge with gratitude the opportunity for collaboration given them by this Institute.

$$N(k) \geqslant x \tag{3}$$

since all prime factors of $k$ are greater than $x$. Now set

$$m_1 = k^k \prod_{\substack{q \nmid n \\ q \leqslant x}} q^k \qquad (q \text{ prime}). \tag{4}$$

Note that while $m_1$ is defined in terms of $n$, it has an upper bound which depends on $x$ alone. If $n$ is sufficiently large then the interval $(n/(k+1)m_1, (n-1)/km_1)$ contains a number $m_2$ such that

$$m_2 \equiv 1 \pmod{k!}. \tag{5}$$

Thus the least prime factor of $m_2$ is greater than $k$.

If we set $m = m_1 m_2$ then from Theorem B and equations (4), (5) we obtain

$$\begin{aligned} N(m) &\geqslant \min\{N(m_1), N(m_2)\} \geqslant \min\{2^k - 1, k\}. \\ &\geqslant k. \end{aligned} \tag{6}$$

Thus the first condition of Theorem A is satisfied. Finally we set $u = n - km$. Since we had chosen $n/(k+1)m_1 < m_2 < (n-1)/km_1$ we have $km + 1 < n < (k+1)m$, so that

$$1 < u < m \tag{7}$$

which satisfies the second condition of Theorem A. From (1), (4), and (5) we see that $n$ and $km$ are incongruent module any prime less than $x$ and therefore $u$ has no divisors less than $x$. Thus

$$N(u) \geqslant x. \tag{8}$$

Combining (2), (3), (6), and (8) we obtain from Theorem A

$$N(n) \geqslant x - 1 \tag{9}$$

for arbitrary $x$ and sufficiently large $n$.

**3. Numerical estimates on the lower bound of** $N(n)$. In addition to Theorems A and B we need a result of Brun's sieve method. We shall use the following theorem due to H. Rademacher **(1)**.

THEOREM C. *Let $P(D; x; p_1, \ldots, p_r)$ denote the number of positive integers, $y$, no greater than $x$ which lie in an arithmetic progression $\Lambda + tD (t = 0, 1, \ldots,)$ where $0 < \Lambda < D$ and $(\Lambda, D) = 1$ and so that $y \not\equiv a_i \pmod{p_i}$, $y \not\equiv b_i \pmod{p_i}$ $(i = 1, \ldots, r)$.*

*If $p_1 < \ldots < p_r$ are primes with $p_i \geqslant 7$, then*

$$P(D; x; p_1, \ldots, p_r) > \frac{Cx}{D \log^2 p_r} - C' p_r^{79/10}$$

*where $C$ and $C'$ are positive constants.*

We shall also need the following simple fact.

LEMMA D. *The number of integers, $y$, no greater than $x$ which are divisible by a prime factor $p$ of $n$ so that $p > n^c$, is no greater than $x/cn^c$.*

*Proof.* Obviously there are at most $x/p$ numbers $y$ divisible by $p$ and therefore the number in question is no greater than

$$x \sum_{\substack{p \mid n \\ p > n^c}} \frac{1}{p} \leqslant x \sum_{p/n} \frac{1}{n^c} < x \frac{1}{n^c} \cdot \frac{1}{c} = x/cn^c$$

since there are less than $1/c$ prime factors of $u$ which exceed $n^c$.

*Case I. $n$ is even.* Pick $k$ so that

$$(10) \qquad \begin{aligned} &k \equiv -1 \pmod{2^{\left[\frac{1}{91} \log_2 n\right]}},\ k \equiv 1 \pmod{15}; \\ &k \not\equiv 0 \text{ or } -1 \pmod{p} \text{ for } p \text{ prime}, 7 \leqslant p \leqslant n^{1/90};\ k < n^{1/10}. \end{aligned}$$

We note that this restricts $k$ to an arithmetic progression with difference

$$D = 15.2^{\left[\frac{1}{91} \log_2 n\right]} < c_1 n^{1/91}.$$

Thus by Theorem C there are at least

$$(11) \qquad \frac{C n^{1/10}}{c_1 n^{1/91} \log^2 n\ (1/90)^2} - C' n^{\frac{79}{10} \cdot \frac{1}{90}}$$

$$= c_2 n^{81/910}/\log^2 n - C' n^{79/900} > c_3 n^{81/910}/\log^2 n$$

choices of $k$.

According to Lemma D the number of natural numbers below $n^{1/10}$ which have a prime factor greater than $n^{1/90}$ in common with $n$ does not exceed $90\, n^{8/90}$. Since $81/910 > 8/90$, it follows from (11), and the fact that $k$ has no factors less than $n^{1/90}$, that we can choose $k$ so that

$$(12) \qquad (k, n) = 1.$$

From (10) and Theorem B it follows that

$$(13) \qquad \begin{aligned} &N(k) > n^{1/90} - 1 > \tfrac{1}{3} n^{1/91}, \\ &N(k+1) > \min\{\tfrac{1}{2} n^{1/91}, n^{1/90}\} - 1 > \tfrac{1}{3} n^{1/91}, \end{aligned}$$

for $n$ sufficiently large.

We now set $n = n_1 + n_2 k$ where $0 < n_1 < k$ and let $u = n_1 + u_1 k$, where we pick $u_1$ subject to the following conditions.

$$(14) \qquad \begin{aligned} &u_1 \not\equiv n_1 \pmod 2; \\ &\left.\begin{aligned} &u_1 \not\equiv -n_1/k \pmod p,\ p \nmid k \\ &u_1 \not\equiv n_2 \pmod p \end{aligned}\right\} \quad p \text{ prime}, 3 \leqslant p \leqslant k; \\ &u_1 < n^{159/200}. \end{aligned}$$

Note that the incongruence (mod 2) implies that $u$ is odd.

The incongruences modulo 2, 3, and 5 can be satisfied by restricting $u_1$ to a progression with difference 30. In order to apply Theorem C we need $(u_1, 30) = 1$. If $(u_1, 30) > 1$ we write $u_1 = u_1' \cdot (u_1, 30)$ with $(u_1', 30) = 1$; then according to Theorem C, the number of such choices of $u_1'$ is at least

$$\frac{C\, n^{159/200}}{30 \log^2 k} - C'\, k^{79/10} > c_4\, n^{159/200}/\log^2 n - C'\, n^{79/100} > 0 \tag{15}$$

for $n$ sufficiently large.

From (14) we see that $u$ is not divisible by any prime less than $k$ and prime to $k$. If $u$ were divisible by a prime $p$ which divides $k$, then $n_1$, and hence $n$, would be divisible by $p$, in contradiction to (12). Hence from (13) we obtain

$$N(u) \geqslant k > N(k) > \tfrac{1}{3} n^{1/91} \text{ for sufficiently large } n. \tag{16}$$

Also, if we set $m = (n - u)/k$, then

$$\begin{aligned} m &> n/n^{1/10} - (1 + n^{159/200}) > \tfrac{1}{2} n^{9/10} \\ &> n^{1/10} + (1 + n^{159/200}) > u > 1 \end{aligned} \tag{17}$$

for sufficiently large $n$. Finally, according to (12) and (14), all prime factors of $m$ exceed $k$ so that

$$N(m) \geqslant k > N(k) > \tfrac{1}{3} n^{1/91}. \tag{18}$$

According to (17) and (18) our choice of $k$, $u$, $m$ satisfies the conditions of Theorem A. Thus by (13), (16), and (18) we have

$$N(n) > \tfrac{1}{3} n^{1/91} \text{ for all sufficiently large even } n. \tag{19}$$

*Case II. n odd.* Instead of applying Theorem C to $k$ we apply it to $k + 1$ with equation (10) replaced by

$$\begin{aligned} &k + 1 \equiv 1 \pmod{2^{\left[\frac{1}{91} \log_2 n\right]}}\ k + 1 \equiv 2 \pmod{15}; \\ &k + 1 \not\equiv 0 \text{ or } 1 \pmod{p} \text{ for } 7 \leqslant p \leqslant n^{1/90}; \\ &k + 1 \leqslant n^{1/10}. \end{aligned} \tag{10'}$$

The rest of the argument on $k$ proceeds as before and equation (12) remains unchanged, while (13) becomes

$$\begin{aligned} &N(k) > \min\{\tfrac{1}{2} n^{1/91}, n^{1/90}\} - 1 > \tfrac{1}{3} n^{1/91}, \\ &N(k + 1) > n^{1/90} - 1 > \tfrac{1}{3} n^{1/91}. \end{aligned} \tag{13'}$$

The choice of $u$ is modified so that (14) is replaced by

$$u_1 \not\equiv n_2 \pmod 2; \qquad u_1 \not\equiv -n_1/k \pmod p \tag{14'}$$

for all primes $3 \leqslant p \leqslant k$ which do not divide $k$; while $u_1 \not\equiv n_2 \pmod p$ for all primes $3 \leqslant p \leqslant k$; $u_1 < n^{159/200}$.

It then follows from (13′) and (14′) that both $n$ and $m = (n - u)/k$ are odd, and the remainder of the argument proceeds exactly as before to yield the following.

THEOREM. *There exists a number $n_0$ so that for all $n > n_0$ we have*

$$N(n) > \tfrac{1}{3}n^{1/91}.$$

**4. Remarks.** The exponent 1/91 in our result is far from best possible. We have not used the best available sieve method, nor have we even squeezed the last drop out of the sieve method quoted. It seems, however, reasonable to defer such efforts in the hope that other theorems of the type of Theorem A can be developed, which may eliminate the twofold use of the double sieve of Theorem C. This would be accomplished, for example, if either the occurrences of both $N(k)$ and $N(k + 1)$ or the inequality $N(m) + 1 \geqslant k$ could be eliminated.

Theorem A can never lead to $N(n) \geqslant n^{1/2}$ since we must have $n > mk$ and $N(m) + 1 \geqslant k$ so that $k \leqslant m \leqslant n^{1/2}$ and $N(k) < n^{1/2}$.

On the other hand, our result seems to eliminate the possibility of a reasonable modification of MacNeish's conjecture which would express $N(n)$ in terms of prime power divisors of $n$; since for any positive $c$ there are infinitely many $n$ for which even the greatest prime power divisor is less than $n^c$.

REFERENCE

1. H. Rademacher, *Beiträge zur Viggo Brunschen Methode in der Zahlentheorie*, Abbh. Math. Sem. Hamburg, *3* (1924), 12–30.

*Number Theory Institute* (1959), *Boulder, Colorado*
*University of Colorado*
*University of California, Los Angeles*