10,000 and $q < 10{,}485{,}760$. The purpose of this note is to present an extension of this table for $10{,}000 < p < 15{,}000$ and $q < 10{,}485{,}760$.

The table presents the value of K for which $q = 2Kp + 1$ is the smallest divisor of M_p rather than presenting the divisor, q. This has been done because, first, the value of K indicates more about the character of the divisor than q does, and, second, to save space. All primes between 10,000 and 15,000 were examined. If any such prime is not listed in the table, it means that $2^p - 1$ has no prime factor $< 10 \cdot 2^{20}$.

Several criteria have been discovered concerning the divisors of the Mersenne numbers, M_p. The best known of these (for $K = 1$) is due to Euler [2]. It states that if $p = 4L + 3$ and $q = 8L + 7$ are both primes then q divides M_p. For $K = 3$, Pellet was the first to state [3] that $q = 6p + 1$ divides M_p if q can be expressed in the form $4(2a + 1)^2 + 27b^2$, and p and q are both prime. For $K = 4$, Reuschle stated and Western proved [4] that $q = 8p + 1$ divides M_p if q can be expressed in the form $d^2 + 64(2c + 1)^2$ and p and q are both prime.

These calculations were performed on an IBM 650 system at Picatinny Arsenal. The program used was as follows: all prime factors q of M_p $(p > 2)$ are of the form $q = 2Kp + 1$, and of one of the two forms $8L \pm 1$. Thus, either $K = 0 \bmod 4$ or $p + K = 0 \bmod 4$. Each prime p was expressed in binary form, $p = \sum_{i=0} a_i 2^i$, $a_i = 0$ or 1. The residues $R_i = R_{i-1}^2 \bmod q$, $R_0 = 2$, were found. Finally the residue $\prod_{i=0} (R_i)^{a_i} \bmod q$ was evaluated. If this product is congruent to one $(\bmod q)$ then q is a divisor of M_p.

Picatinny Arsenal
Dover, New Jersey

1. H. Riesel, "Mersenne Numbers," *MTAC*, v. 12, July 1958, p. 207.
2. G. H. Hardy & E. M. Wright, *An Introduction to the Theory of Numbers*, 3rd edition, 1956, Oxford University Press, p. 80.
3. L. E. Dickson, *History of the Theory of Numbers*, v. I, Chelsea Publishing Co., 1952, p. 25.
4. A. E. Western, "Some criteria for the residues of 8th and other powers, "*Proc. London Math. Soc.* (2) 9 (1911) p. 244–272.

On a Theorem of Mann on Latin Squares

By R. T. Ostrowski and K. D. Van Duren

Mann [1] proved the following theorem: *If a Latin square L of order $4t + 2$ has a $(2t + 1) \times (2t + 1)$ block with as many as $(2t + 1)^2 - t$ cells containing digits in a list of $2t + 1$, then there exists no Latin square orthogonal to L.* This theorem seemed until lately to give theoretical evidence for the truth of Euler's conjecture that no pair of orthogonal Latin squares exists of any order $4t + 2$. Now that Euler's conjecture has been shown to be false [2], [3], a more detailed investigation of Latin squares of orders $4t + 2$ seems worthwhile.

The chief goal of the work reported in this note was to find an example indicating that Mann's theorem is the best possible of its type for order 10—or conversely, to

Received July 30, 1960.

accumulate experimental evidence suggesting that a more stringent theorem of the same nature remains to be proved. With the aid of the UNIVAC M-460 Computer, the former alternative was achieved. Displayed below is a pair of orthogonal Latin squares of order 10; the upper left 5×5 block of the first Latin square has $5^2 - 2 - 1 = 22$ cells containing digits 0, 1, 2, 3, 4. (Note three italicized digits in each of the four separated 5×5 blocks of the left Latin square.)

01234	56789	01923	84657
34012	79865	67895	23104
43120	97658	93746	58210
1240*7*	85*3*96	38254	79061
203*7*5	689*4*1	14507	36982
57698	34120	25619	40873
89756	12034	40138	62795
6598*1*	4320*7*	56480	17329
9856*3*	0147*2*	82071	95436
7684*9*	2051*3*	79362	01548

The second of the above Latin squares resembles either of the first pair of orthogonal Latin squares of order 10 constructed by Parker [2]; it is disguised by permutation of rows and columns. A UNIVAC M-460 program, coded by Parker [4], generated the first of the above pair as an orthogonal mate of the second. Considering the results discussed near the end of this note it was largely luck that such an example as the above was found among the moderate number of cases examined.

An observation shortened the computation time by a factor of four. In a Latin square of order 10 any 5×5 block contains each digit the same number of times as the block whose sets of rows and columns are complements of the sets of rows and columns for the first block. Further, the block with the same five rows and the complementary set of columns has the same sum of incidences for the set of five digits complementary to the set tallied in the initial block. Hence it is sufficient to inspect $\frac{1}{4}\binom{10}{5}^2 = 15{,}876$ blocks. This was implemented in the program by choosing all sets of five rows including the first, and all sets of five columns including the first.

The authors' program for the UNIVAC M-460 Computer carries out the following steps:

1. Read into the computer a tape of one Latin square of order 10.

2. For a 5×5 block tally the incidence of each digit 0, 1, $\cdots$, 9.

3. Sort out a set of five highest counts of the ten. Sum these five counts, and record this sum. If the sum for the block just run is the largest found for the Latin square, record the row and column indices.

4. On completion of 15,876 (see above) passes through 2 and 3, generate an output tape. The information presented is the number of 5×5 blocks with sums of 25, 24, $\cdots$, 15; and the row and column indices for the first block giving the highest sum.

5. Return to 1 or stop.

Running time, including input and output, was about 40 seconds per Latin square. A repetitive process of this magnitude is barely thinkable without a computer; human scanning ability is not nearly good enough to locate a 5×5 block of highest sum of incidences of five digits.

The program was run for some sixty Latin squares of order 10 known to have orthogonal mates. Of these only one had a sum of 22—and this occurred for only one partitioning of rows and columns into fives.

Another routine was written for the same computer to generate random Latin squares of order 10. Digits 0 through 9 were produced by an appropriately modified random number generator; cells were filled in sequentially subject to the required conditions, and changes made when completion became impossible. One hundred Latin squares were produced and processed by the first program. The highest sums of counts of five digits in 5×5 blocks were 19 for 76 Latin squares, 20 for 23 squares, and 21 for one; no Latin square of the hundred had a sum over 21. Of the hundred Latin squares, no two produced the same list of counts in 15,876 blocks; this evidence supports the claim of randomness. Before this study it had seemed plausible that most Latin squares of order 10 have sums over 22, since considerable searching by computer in recent years suggests that pairs of orthogonal Latin squares of order 10 are rare. Almost certainly there are necessary conditions for Latin squares of order 10 to possess orthogonal mates, aside from falsity of the hypothesis of Mann's theorem.

The problem was suggested by E. T. Parker. The authors thank him for help on various points.

Control Data Corporation
Minneapolis, Minnesota, and
Remington Rand Univac Division
Sperry Rand Corporation
St. Paul, Minnesota

1. HENRY B. MANN, "On orthogonal Latin squares," *Bull. Amer. Math. Soc.*, v. 50, 1944, p 249–257.
2. E. T. PARKER, "Orthogonal Latin squares," *Proc. Nat. Acad. Sci. U.S.A.*, v. 45, 1959, p. 859–862.
3. R. C. BOSE, S. S. SHRIKHANDE & E. T. PARKER, "Further results on the construction of mutually orthogonal Latin squares and the falsity of Euler's conjecture," *Canad. J. Math.*, v. 12, 1960, p. 189–203.
4. E. T. PARKER, "A computer search for Latin squares orthogonal to Latin squares of order ten," *Notices Amer. Math. Soc.*, v. 6, 1959, abstract 564-71, p. 798.

Complete Factorization of $2^{159} - 1$

By K. R. Isemonger

Algebraic factors of $2^{159} - 1$ are $2^3 - 1 = 7$ and $2^{53} - 1 = 6361 \cdot 69431 \cdot 20394401$, the latter factorization having been first published by F. Landry in 1869.

R. M. Merson of Farnborough, Hants, England has found 13960201 to be a prime factor of $(2^{106} + 2^{53} + 1)/7 \cdot 6679$. The resulting quotient is the integer

$$N = 124\ 302\ 977\ 331\ 586\ 210\ 969,$$

whose factorization was completed by me on 15 May 1960.

The procedure employed was to exhibit N as the difference of two squares, namely,

Received May 19, 1960; revised November 14, 1960.