accident but is a genuine theorem. This can be seen by taking j = k - 1 in the proof of Theorem 3. Since the degree of the right side of (15) must be $\leq 2k - 2$, the B must be zero in (16). This forces Y_1 and Y_0 to be equal and leads at once to a solution of (17) in the form described above.

REFERENCES

- 1. G. H. Hardy and E. M. Wright, An Introduction to the Theory of Numbers,
 Oxford 1938.
- 2. L. E. Dickson, History of the Theory of Numbers, V. 2, Washington 1923.

AN OUTCROPPING OF COMBINATORICS IN NUMBER THEORY

Emma Lehmer Berkeley, Calif.

ABSTRACT. This paper exhibits an unexpected connection between problems in the theory of numbers having to do with factorization of integers in the rational and cyclotomic fields and combinatorial problems involving ordinary and supplementary difference sets.

AN OUTCROPPING OF COMBINATORICS IN NUMBER THEORY

Emma Lehmer

Introduction. It will come as no surprise to anybody to say that number theory and combinatorics have many interests in common and that they depend on each other for ideas and tools and methods of proof.

Many theorems in combinatorics begin with the words "let p be a prime," where this condition is sometimes inherent to the problem and at other times only to the method of proof. However, the notion of primality and the companion topic of factorization is an undisputed problem in the realm of the theory of numbers.

It may therefore come as a surprise that a problem of factoring numbers in a rational field can be linked with the problem of Steiner

systems and therefore with block designs, Hadamard matrices and difference sets, while the problem of splitting a prime in cyclotomic fields can actually lead to new results in supplementary difference sets and therefore in block designs. It is with these two problems that this paper is concerned.

1. A Factorization Method. The next issue of Mathematics of Computation [8] will contain a joint paper with D.H. Lehmer which describes a method of factorization of an integer $N = pq \equiv r \pmod{24}$, where $(r, 2^{l_1}) = 1$ and p, q are primes, which uses binary quadratic forms of squarefree determinants $\pm D$, where D divides 2^{l_1} .

Briefly, the method consists in finding three suitable forms for each value of r such that at least one of these forms represents N, or a small multiple of N, in two distinct ways. From these representations the factors of N can be deduced by the simple greatest common divisior process.

For example, if $N \equiv 1 \pmod 8$, so that r = 1 or 17, then N is representable is a sum of two squares, (D = -1), if and only if $p \equiv q \equiv 1 \pmod 4$. Hence, failing to obtain such a representation we know that in this case $p \equiv q \equiv 3 \pmod 4$. Now, every number $N \equiv 1 \pmod 8$ is also represented by a square plus or minus twice a square, or $N = x^2 \pm 2y^2$, according as its factors are of the form 8n + 1 and 3, or 8n + 1 and 7. Since we already know that the factors are congruent to 3 modulo 4, they must be both congruent to 3, or both congruent to 7 modulo 8, and therefore N must be represented by either one or the other of the two forms with $D = \pm 2$.

. T lo sall values of r . and experts were quite sceptical as to the chances for an affirmative Surprisingly, this question does not appear to have been asked before prescribe three such forms for every remainder $\, {\tt r} \,$ of $\, {\tt N} \,$ prime to $\, {\tt 2h} \,$ before 1800. The question which we raised in [8] is whether one can This particular example has been well known from the time of Legendre,

One can begin the investigation with a table of the seven values

of $D \neq 1$ versus the remainders r for which

$$yn = x^2 - Dy^2 \qquad (\lambda = \pm \lambda, \pm 2)$$

$$y_N = x_- - p_{A_C} \qquad (y = \mp T^* \mp S)$$

which looks as follows

7° 2° 76° 53 TT 'L 'S 'T T' TT' T3' S3 T' L' TL' 53 6T 'LT 'TT 'T 1° 2° 73° TL

ue of r appears in three rows of the table thus giving a unique the value of x = 1 from further consideration we note that every value. we have already solved the problem for M \equiv L (8 bom) L \equiv M rot med by solved system . $N\equiv 1$ (mod 2μ) admits a representation by every form of the system and Several properties of this table hit the eye. In the first place

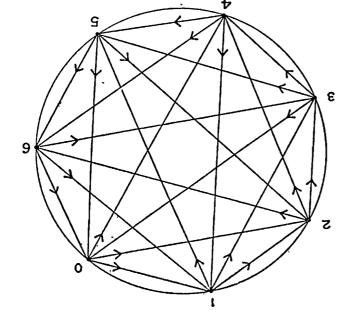


FIGURE 3

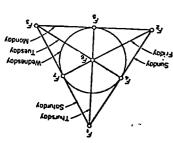


FIGURE S

selection of the three forms for every r . In [8] we proved that in every case one of these three forms must yield the factors of N=pq. What interests us more here is the fact that any two rows have exactly one r in common and every pair of r's appears—in some row so that the seven values of $r \neq 1$ form a Steiner triple system with respect to the seven blocks of three r's characterized by the determinants which are the square free divisors of 24, excluding 1.

It is interesting to note that a pictorial representation of these remainders has appeared on p. 202 of Shanks [9], as in Figure 1, while a similar picture of the Fano plane on p. 187 of Berman and Fryer [3] refers to a weekly schedule of seven firemen as in Figure 2.

 Sunday
 F_1 F_2 F_4 F_5

 Monday
 F_2 F_3 F_5 F_5

 Tuesday
 F_3 F_4 F_6 F_7

 Wednesday
 F_4 F_5 F_6 F_1

 Thursday
 F_5 F_6 F_1

 Friday
 F_6 F_7 F_2

 Saturday
 F_7 F_1 F_3

These pictures establish visually a one-to-one correspondence between the remainders r and the firemen F_i on the one hand and between the determinants and the days of the week on the other. Rearranging our remainders and determinants accordingly and including this time both r = 1 and D = 1, for which solutions may exist for every r, we obtain the usual Hadamard matrix of order eight based on the perfect

ifference set 1,2,4, of quadratic residues modulo seven in which $i_{i,j} = 1$ or -1 according as (1) may represent λN for i = r and i = 0. The inclusion of r = 1 and D = 1 might provide a justification for the usual bordering of the designs to produce Hadamard matrices.

D /	r . 1	19	11	7	17	5	· 23	13
1	1	1	1	1	ı	1	1	. 1
- 2	ı	ı	٦,	-1	1.	-1	-1	. -1
-6	1	-1	1	ı	-1	1	-1	-1
2	ı	-1	-1	ı	1	-1	1	-1
-l	1	-1	-1.	-1	ı	1	-1	ĺ
6	1	ı	-1	-1	,- 3	. 1	1	-1
3	1	-1	1	-1	-1	-1	1	1
- 3	1	ı	-1	1	-1	-1	-1	1
	}					,	•	

Thus our remainders $r \neq 1$, as well as the firemen represent a salanced incomplete block design BIBD based on a finite projective seemetry of seven points and seven lines with three points on each line and three lines through each point in which every pair of points lies in some line. Another example of such a configuration is provided by a surely graph-theory problem of Paul Erdös [5] who considered a complete directed graph on seven points called towns which were connected by one say roads in such a way that any two given towns could be reached directly by roads from some third town as in Figure 3.

We can name the seven towns by the days of the week from 1 to 7 for 0) (where Sunday is the seventh day) and make each fireman live in the town indicated by his subscript. Then, if we draw arrows from each town in the direction of the domiciles of the three firemen working

on that day and away from the other three we will get the desired arrange ment because each pair of firemen work together on some day of the week.

In [8] we generalized the problem of factoring N = pq by quadratic forms to that of factoring $N = p_1 p_2 \dots p_n$ by selecting $2^n - 1$ possible forms from a total of $2^{n+1} - 1$ forms corresponding to the $2^{n+1} - 1$ divisors (not equal to one) of the product of the first n primes as determinants. Hence this problem also leads to the Steiner system (2).

For n=3, for example, we can use the 15 square free divisors (different from one), of 120 for $\pm D$ and a BIBD design based on the Singer difference set (15,7,3) which has also been obtained from a different point of view by Whiteman [1], namely

Under the permutations

and

we obtain from table 4 of [8] the usual Hadamard matrix of order 16 and the usual BIBD design based on (3).

For n = 4, the Singer set (31,15,7) is [1]

(4)
$$s_{4}$$
: {1,2,3,4,6,8,12,15,16,17,23,24,27,29,30} .

This set was also obtained by Hall [7] and is composed of cubic residues together with the class of sextic non-residues containing 3.

For n = 5 the Steiner set (63,31,15) is [1]

It can be described as

(5)
$$s_5$$
: {0, 2^{α} , $2^{\alpha} \cdot 3^{\beta}, \pm 5 \cdot 2^{\alpha}$ (mod 63)}

This is one of two inequivalent sets with parameters (63,31,15). The other one is due to Gordon, Mills and Welch [6].

For n=6 there are 6 inequivalent difference sets (127,63,31) the quadratic residues modulo 127, the Hall set [7], the Singer set 8 and three sets of Baumert and Fredricksen [2]. The last four can all be described in terms of the cosets $C_{\hat{1}}$ of 18-th power residues. The Singer set is [2]

(6)
$$s_6: \{c_0, c_1, c_2, c_3, c_5, c_6, c_7, c_{10}, c_{16}\}$$

where 3 is in C_1 .

It might be of interest to use the structure suggested by (5) to attempt to find difference sets with parameters (255,127,63).

2. Factorization in Cyclotomic Fields. A prime $p \equiv 1 \pmod q$, where q = 2m + 1 is also a prime can be decomposed in the cyclotomic field of q-th roots of unity ζ into the product [4]

(2.1)
$$p = \frac{q-1}{r} \pi(\zeta^{\nu}) = \frac{m}{r} \pi(\zeta^{a}i)$$
. $m = \pi(\zeta^{-a}i) = F_{A}(\zeta)F_{A}(\zeta^{-1})$

where $a_1 = 1$, $a_i + a_j \neq 0 \pmod{q}$, and A is any set A_j defined by $(a\bar{a} \equiv 1 \pmod{p})$

(2.2)
$$A_j: \{a_1\bar{a}_j, a\bar{a}_j, ..., a_m\bar{a}_j\}_{i} (j = 1, 2, ..., m)$$
.

For q = 3 and q = 5 there is a unique set A corresponding to . the unique decomposition of p into the so called reciprocal factors $F_A(\zeta) \quad \text{and} \quad F_A(\zeta^{-1}) \quad . \quad \text{In fact} \quad F_A(\zeta) \quad \text{is the well known Jacobi function}$

(2.3)
$$R(1, 1) = \sum_{x=1}^{p-1} \chi_{q}(x) \chi_{q}(x+1) .$$

For q = 7 there are two such systems, namely

$$\hat{\Sigma}: \begin{cases}
1,2,3 \\
1,3,5 \\
1,4,5
\end{cases} and 1,2,4.$$

We note the appearance once more of the invariant residue difference set 1,2,4 (modulo 7). It leads to the Jacobi function

$$R(1, 2) = r + s(\zeta + \zeta^2 + \zeta^4) + t(\zeta^3 + \zeta^5 + \zeta^6)$$

where

$$4p = (s + t - 2r)^2 + 7(s - t)^2$$
.

The system \sum leads to R(1, 1) in (2.3).

From our point of view, it is interesting to note that the system Σ is in fact the supplementary difference set $m-(v,k,\lambda)=3-(7,3,3)$ of m=3 sets each having k=3 elements, in which the non-zero differences modulo 7 taken within each set, but not between sets, each appear $\lambda=3$ times [12]. It leads to BIBD (21,7,9,3,3).

For q = 11 there are 16 possible sets, the invariant quadratic residue difference set modulo 11, namely 1,3,4,5,9, and three systems of 5 sets each, namely

$$\Sigma_{1}: \begin{cases} 1,2,3,4,5\\ 1,2,6,7,8\\ 1,4,5,8,9\\ 1,3,4,6,9\\ 1,3,5,7,9 \end{cases} \qquad \Sigma_{2}: \begin{cases} 1,2,3,4,6\\ 1,2,3,6,7\\ 1,2,4,5,8\\ 1,3,6,7,9\\ 1,2,4,6,8 \end{cases} \qquad \Sigma_{3}: \begin{cases} 1,2,3,5,7\\ 1,6,7,8,9\\ 1,4,6,8,9\\ 1,5,6,8,9\\ 1,2,5,7,8 \end{cases}$$

The systems \sum_1 and \sum_2 lead to the two Jacobi functions R(1,1) and respectively [4]. The function $F_A(\zeta)$ corresponding to \sum_3 is usually simply discarded as superfluous. It was our original purpose to shed some light on what might be called non-Jacobi functions.

We note first of all that each of the three systems for q=11 forms a 5-(11,5,10) supplementary difference set. We next inquire whether there is some connection between these sets. In order to do so we introduce a primitive root $g(\bmod{11})$ and define

(2.4)
$$i_{\nu-1} = ind_{g} a_{\nu}$$
 ($\nu = 1, 2, ..., 10$)

The condition on a, in (2.1) becomes

(2.5)
$$i_0 = 0$$
, $i_v - i_\mu \not\equiv 0 \pmod{m}$.

With g = 2 the index sets corresponding to the sets \sum are

I₁:
$$\begin{cases} 0,1,2,4,8 \\ 0,1,3,7,9 \\ 0,2,3,4,6 \\ 0,2,6,8,9 \\ 0,4,6,7,8 \end{cases}$$
 I₂:
$$\begin{cases} 0,1,2,8,9 \\ 0,1,7,8,9 \\ 0,1,2,3,4 \\ 0,6,7,8,9 \\ 0,1,2,3,9 \end{cases}$$
 I₃:
$$\begin{cases} 0,1,4,7,8 \\ 0,3,6,7,9 \\ 0,2,3,6,9 \\ 0,3,4,6,7 \\ 0,1,3,4,7 \end{cases}$$

We note that if we replace g=2 by $g=2^3$ then i goes into I_1 and the set I_2 goes into I_3 , while I_1 remains invariant. Thus the a's which go with the unknown function $F_A(\zeta)$ are the cubes of the a's which go with R(1,2).

For q=13 there are 32 possible sets consisting of 5 systems of six sets each and of the pair of the sets

which go into each other. These consist of quartic residues module 13, namely 1,3,9 and of the coset of the quartic non-residues which contains either 2 or 8, in other words $\{C_0,C_1\}$ and $\{C_0,C_3\}$. This pair of supplementary difference sets is due to Szekeres [11]. This set corresponds to the Jacobi function R(1,3). Two of the 5 systems of six sets correspond to the Jacobi functions R(1,1) and R(1,2), two

more are related to these by replacing a_i by a_i^{\prime} . The remaining unexplained set leads to an index set which is independent of the primitive root as follows

$$\Sigma : \begin{cases} 1,2,3,4,5,7 \\ 1,2,7,8,9,10 \\ 1,5,6,9,10,11 \\ 1,4,5,7,10,11 \\ 1,3,4,6,8,11 \\ 1,2,4,6,8,10 \end{cases} \text{1:} \begin{cases} 0,1,2,3,5,10 \\ 0,1,2,4,9,11 \\ 0,1,3,8,10,11 \\ 0,2,7,9,10,11 \\ 0,5,7,8,9,10 \\ 0,2,3,4,5,7 \end{cases}$$

and to an unknown function $F_{A}(\zeta)$.

Thus, although we have not succeeded in our original quest, we have stumbled on a family of supplementary difference sets which appears to be new. Our index sets can be generalized by realizing that the i's are representatives of the cosets C_i to give the following theorem.

Theorem. Let p = 2mf + 1 be a prime. Let f be odd and let g

be a primitive root of p. Define the cosets of 2m-th power residues

of p by

(2.7)
$$C_{i} = \left\{g^{2m\mu+i} \pmod{p}\right\} \qquad (i = 0, 1, ..., 2m - 1) \\ (v = 0, 1, ..., f - 1)$$

Let

(2.8)
$$i_j = j + m\epsilon_j$$
, where $\epsilon_0 = 0$, $\epsilon_j = 0$ or 1.

Then for every choice of ϵ_j the system of m sets

(2.9)
$$S_n: \left\{ {}^{C}_{i_0-i_n}, {}^{C}_{i_1-i_n}, \cdots, {}^{C}_{i_{m-1}-i_n} \right\} \quad (n = 0, 1, \dots, m-1)$$

more are related to these by replacing a_i by a_i^7 . The remaining un- a_i is a supplementary difference set $m - (v,k,\lambda)$ and a BIBD (mv,v,mk,k,λ) with

(2.10)
$$v = p = 2mf + 1$$
, $k = (p - 1)/2 = mf$, $\lambda = m(mf - 1)/2$ (fodd)

Proof. Denote as usual by (u, v) the number of solutions (v, μ) of the congruence

(2.11)
$$g^{2m\mu+u} + 1 \equiv g^{2m\nu+v} \pmod{p}$$

ince f is odd we have

(u, v) =
$$(v + m, u + m)$$
.

Now let $\delta_t = g^{2mT+t}$ be an element of the set C_t . The number of these that δ_t is represented as the difference between elements of two sets of the set S_n is the number of solutions (v, μ) of the congruence.

$$g^{2m\mu+i-n+m(\epsilon_i-\epsilon_n)} - g^{2m\nu+j-n+m(\epsilon_j-\epsilon_n)} \equiv g^{2m\tau+t} \pmod{p}$$

Mich by (2.12) is

$$(j-n-t+m(\epsilon_j-\epsilon_n))$$
 , $i-n-t+m(\epsilon_i-\epsilon_n))$.

Therefore the number $N_n(\delta_t)$ of times that δ_t apears as the difference between the elements of $S_n^{'}$ is

by (2.12). Similarly since the sum is symmetric in i and j., it remains unaltered if ϵ_n is changed and is therefore a function of n+t Hence

(2.15)
$$N_n(\delta_t) = N_{n+r}(\delta_{t-r})$$
 for $r = 0, 1, ..., 2m-1$

Hence the total number of times N(δ_t) that δ_t appears as a difference in all the m sets S_n is

$$N(\delta_{t}) = \sum_{n=0}^{m-1} N_{n}(\delta_{t}) = \sum_{n=0}^{m-1} N_{n+r}(\delta_{t-r}) = \sum_{v=r}^{m-1+r} N_{v}(\delta_{t-r}) = \sum_{n=0}^{m-1} N_{n}(\delta_{t-r})$$

by (2.14) and is therefore independent of t , which proves the theorem We note that the normalizing condition $\varepsilon_0 = 0$ insures that C_0 is in every S_n and therefore C_m never appears so that -1 is not in any set, and if an element a is in S_n , then -a is not in S_n . The complementary sets will contain C_m and hence -1 in every set.

Corollary 2. For every prime $p \equiv 5 \pmod 8$ there exists a pair of Szekeres supplementary difference sets S_0 : $\{C_0, C_1\}$ and S_1 : $\{C_0, C_3\}$ of quartic residue cosets. [11], [12].

Corollary 3. For every prime $p \equiv 7 \pmod{12}$ there exists a supplementary set $S_0: \{C_0, C_1, C_2\}$, $S_1: \{C_0, C_1, C_5\}$, $S_2: \{C_0, C_h, C_5\}$ of

Pextic residue cosets. [This appears to be new, put m=3.]

Drollary 4. For every prime $p\equiv 9\pmod{16}$ the theorem gives two possible systems of 4 sets of octic cosets each. However, these systems go into each other if g is replaced by g^3 . The system

$$s_0:\{c_0,c_1,c_2,c_3\}, s_1:\{c_0,c_1,c_2,c_7\}, s_2:\{c_0,c_1,c_6,c_7\}, s_3:\{c_0,c_5,c_6,c_7\}$$

due to J. Wallis and Whiteman [14].

rollary 5. For m = 5 there are three systems of cosets of 10th powresidues of $p \equiv 11 \pmod{20}$. The system generated by

$$s_0: \{c_0, c_1, c_2, c_4, c_8\}$$

 \mathbf{r} invariant if g is replaced by a power of g prime to 10 , while the systems generated by

$$\mathbf{S_0} \colon \ \mathbf{C_0, C_1, C_2, C_8, C_9} \quad \text{ and } \ \mathbf{S_0'} \colon \{\mathbf{C_0, C_1, C_4, C_7, C_8}\}$$

into each other if g is replaced by g^3 . The remaining set $\{c_0, c_2, c_4, c_6, c_8\}$ is simply the set of quadratic residues as in Corary 1.

whillary 6. For m=6, there are 5 systems of cosets of 12th powersidues of $p\equiv 13\pmod{24}$. The one which is independent of the whitive root is generated by $S_0\colon \{c_0,c_1,c_2,c_3,c_5,c_{10}\}$. There is 4b a pair of Szekeres sets as in Corollary 2.

by

N. S. Mendelsohn.

- [1] Leonard D. Baumert, Cyclic Difference Sets, Lecture notes in Mathematics, 182, Springer-Verlag, 1971.
- [2] L.D. Baumert and H. Fredricksen, "The cyclotomic numbers of order eighteen with applications to difference sets," Math. Comp. 21 (1967) 204-219.
- [3] Gerald Berman and K.D. Fryer, Introduction to Combinatorics, Academic Press, 1972.
- [4] L.E. Dickson, "Cyclotomy and trinomial congruences," Amer. Math. Soc. Trans. 37 (1935) 363-380.
- [5] Paul Erdös, "On a problem in graph theory," The Art of Counting, MIT Press, 1973, p. 527-530.
- [6] B. Gordon, W.H. Mills and L.R. Welch, "Some new difference sets," Canadian Jn. Math. 14 (1962) 614-625.
- [7] M. Hall, Jr., "A survey of difference sets," Amer. Math. Soc. Proc. 7 (1956) 975-986.
- [8] D.H. and Emma Lehmer, "A new factorization technique using quadratic forms," Math. Comp. to appear.
- [9] Daniel Shanks, Solved and Unsolved Problems in Number Theory, v. 1, Spartan Books, 1962.
- [10] J. Singer, "A theorem in finite projective geometry and some applications to number theory," Amer. Math. Soc. Trans. 43 (1938) 377-385.
- [11] G. Szekeres, "Cyclotomy and complementary difference sets," Acta Arith. 18 (1971) 349-353.
- [12] Jennifer Wallia, "On supplementary difference sets," Aequationes Math. 8 (1972), 242-257.
- [13] W.D. Wallis, A.P. Street and J.S. Wallis, Combinatorics, Room Squares, Sumfree sets, Hadamard matrices, Lecture Notes in Math. 292, Springer-Verlag, 1972.
- [14] Jennifer Wallis and A.L. Whiteman, "Some classes of Hadamard matrices with constant diagonal," Australian Math. Soc. Bull. 7 (1972) 233-249.

Introduction.

In a famous paper [5], van der Waerden proved the following theorem. Let k and m be positive integers. Then there exists a positive integer n = n(m, k) such that if n consecutive integers are divided arbitrarily into k sets then at least one of these sets contains an arithmetic progression of length m.

An immediate consequence of van der Waerden's theorem is that if
the set of positive integers is partitioned into k disjoint sets at
least one of these sets contains an arithmetic progression of arbitrary
finite length. If none of the sets contains an infinite arithmetic
progression, then at least one of the sets contains an infinite collection
of arithmetic progressions such that given an integer r infinitely many
of these arithmetic progressions are of length greater than r.

Let S be a set of positive integers arranged in order of increasing magnitude, $S = \{a_1, a_2, a_3, \cdots\}$ where $a_1 < a_2 < a_3, \cdots$. We say that S has bounded gaps if there is a number T such that $a_{i+1} - a_i < T$ for $i = 1, 2, 3, \cdots$.

In this paper we give an explicit construction for the following extension. Let k be an integer $k \geq 2$. Then the positive integers can be partitioned into k disjoint subsets such that none of the subsets contains an infinite arithmetic progression but each of them contains an arithmetic progression of arbitrary finite length, and each of them has bounded gaps. The notion of a bounded gap is used to avoid trivial

PROC. 5TH S-E CONF. COMBINATORICS, GRAPH
THEORY, AND COMPUTING, pp. 93-109.