Western Number Theory Problems, 1992–12–19 & 22

Edited by Richard K. Guy

for mailing prior to 1993 (Asilomar) meeting

Summary of earlier meetings & problem sets with old (pre 1984) & new numbering.

1967 Berkeley	1968 Berkeley	1969 Asilomar	
1970 Tucson	1971 Asilomar	1972 Claremont	72:01–72:05
1973 Los Angeles	73:01–73:16	1974 Los Angeles	74:01–74:08
1975 Asilomar	75:01–75:23		
1976 San Diego	1–65	i.e., 76:01–76:65	
1977 Los Angeles	101–148	i.e., 77:01–77:48	
1978 Santa Barbara	151–187	i.e., 78:01–78:37	
1979 Asilomar	201–231	i.e., 79:01–79:31	
1980 Tucson	251–268	i.e., 80:01–80:18	
1981 Santa Barbara	301–328	i.e., 81:01–81:28	
1982 San Diego	351–375	i.e., 82:01–82:25	
1983 Asilomar	401–418	i.e., 83:01–83:18	
1984 Asilomar	84:01–84:27	1985 Asilomar	85:01–85:23
1986 Tucson	86:01–86:31	1987 Asilomar	87:01–87:15
1988 Las Vegas	88:01–88:22	1989 Asilomar	89:01–89:32
1990 Asilomar	90:01–90:19	1991 Asilomar	91:01–91:25
1992 Corvallis (present set)	92:01–92:		

[With comments on earlier problems:
70:XY, 76:15, 90:03, 91:02, 91:03, 91:06, 91:10, 91:12, 91:20, 91:21, 91:24.]

UPINT = Richard K. Guy, Unsolved Problems in Number Theory, Springer, 1981. Second edition

COMMENTS ON ANY PROBLEM WELCOME AT ANY TIME

Department of Mathematics and Statistics,
The University of Calgary,
Calgary, Alberta, Canada, T2N 1N4.

93-06-09.

COMMENTS ON EARLIER PROBLEMS

70:XY (L.J. Mordell) Let p be an odd prime. Write $f(x) = x^2$, $g(x) = ax^2$, where a is a quadratic non-residue of p. It is trivial that if n is any integer, then either the congruence $f(x) \equiv n$ or $g(x) \equiv n$ is solvable mod p. Find other functions with this property. Prove that, if d is any integer, the functions $f(x) = 2x + dx^4$, $g(x) = x - 1/4dx^2$ have this property.

Remark. See 1989 Problems set. This is a solved problem, but readers were offered an opportunity to solve it themselves, in the hope that a more general solution might be obtained, before the original solution & solver were given.

76:15 (Hugh Edgar) For primes p and q, and h an integer, how many solutions (m, n) does $p^m - q^n = 2^h$ have?

See 1989, 1990, 1991 and **92:17** below.

90:03 (Basil Gordon) Is it true that for every positive integer n there is a one-one map L of $\{1, 2, \ldots, n\}$ onto $\{0, 1, \ldots, n-1\}$ such that $L(ab) = L(a) + L(b)$ whenever a, b and ab are all in $\{1, 2, \ldots, n\}$?

Remark: It is easy to confuse this problem with one of Forcade, Lamoreaux & Pollington, *Amer. Math. Monthly*, **93**(1986) 119–121 (see also **96**(1989) 905).

Gordon's problem is a special case, so the counterexamples found by Forcade & Pollington for their problem in the case where the mapping is onto a **group** (called an FLP group below) also serve as counterexamples for Gordon's problem. Contrast the two examples for $n = 10$:

	1	2	3	4	5	6	7	8	9	10
L_P	0	1	8	2	4	9	7	3	6	5
L_G	0	1	4	2	6	5	9	3	8	7

The former is obtained by using 2 as a primitive root of $n + 1 = 11$ and the entries, which are exponents (logarithms) are the elements of the additive group of residue classes mod 10. However $L(3) + L(3) = 8 + 8 \neq 6 = L(3 \times 3)$ unless the addition is so interpreted. We can satisfy Gordon's requirements by rearranging the entries as in the second example. Forcade & Pollington gave the counterexamples 195 and 255 to their own problem and 195 is the least such. Perhaps $n = 105$ (but not $n = 35$) is the smallest counterexample to Gordon's problem; John Selfridge has done a backtrack on this by hand, but it should be confirmed by machine. Chandler (1988) has shown that every odd order FLP group is commutative.

K.A. Chandler, Groups formed by redefining multiplication, *Canad. Math. Bull.*, **31**(1988) 419–423; *MR* **89m**:20021 [1986, 119].

R.W. Forcade & A.D. Pollington, What is special about 195? Groups, nth power maps and a problem of Graham, in R.A. Mollin (editor) Number Theory, *Proc. 1st Conf. Canad. Number Theory Assoc., Banff, 1988*, de Gruyter, 1990, 147–155.

Further Remark: Blair Kelly III has done a computer search, revealing that $n = 85$ is the smallest counterexample. The next counterexamples are for $92 \leq n \leq 108$, $n = 112$,

$n = 113$, $115 \le n \le 118$ and $121 \le n \le 156$. He says that it is natural to conjecture that there are no Gordon maps for $n > 120$.

91:02 (Paul Erdős) Is it true that if $1 \le a_1 < a_2 < \ldots < a_{n+2} \le 2n$, then some a_j is a sum of consecutive a_i? In view of Pomerance's negative solution below, Erdős asks for the least replacement for $n+2$, and conjectures that this is of the form $n+c$ for some c.

A solution was given by Carl Pomerance. Further results are due to Freud and to Coppersmith & Phillips. Here's a proposed passage from section **E30** in the forthcoming second edition of *UPINT*:

If $1 \le a_1 < a_2 < \cdots < a_k \le n$ is a sequence in which no a is the sum of consecutive earlier members, then Pomerance found that $\max k \ge \lfloor \frac{n+3}{2} \rfloor$ and R. Freud later showed that $\max k \ge \frac{19}{36}n$. They notice, with Erdős, that $\max k \le \frac{2}{3}n$, even if we only forbid sums of *two* consecutive earlier members. Coppersmith & Phillips have since shown that $\max k \ge \frac{13}{24}n - O(1)$ and they lower the upper bound to $\max k \le (\frac{2}{3} - \epsilon)n + O(\ln n)$ with $\epsilon = \frac{1}{896}$.

Erdős asks if the lower density of the sequence is zero; perhaps

$$¿ \qquad \frac{1}{\ln x} \sum_{a_i < x} \frac{1}{a_i} \to 0 \qquad ?$$

Don Coppersmith & Steven Phillips, On a question of Erdős on subsequence sums, (preprint, Nov. 1992)

Róbert Freud, *James Cook Math. Notes*, Jan. 1993.

91:03 (Paul Erdős, Carole Lacampagne & John Selfridge) Obtain a good lower bound for $g(k)$, the least integer $> k+1$ such that

$$\gcd\left(\binom{g(k)}{k}, k!\right) = 1.$$

Is it true that for $k > k_0$, $g(k) > k^2$? In fact, is it true that for $k_1 > k_0$, $g(k_1) > k_1^3$?

Remark: Deficient binomial coefficients must have $n+k \ge g(k)$. In their forthcoming paper

P. Erdős, C. Lacampagne & J. L. Selfridge, Estimates of the least prime factor of a binomial coefficient, *Math. Comput.*, **60**(1993) - .

prove that $g(k) > ck^2/\ln k$ for k large, and Andrew Granville (unpublished?) uses exponential sums to prove that $g(k) > k^{\ln k/\ln\ln k}$ [he announced at Corvallis that he can prove that $g(k) > k^{c\sqrt{\ln k}}$].

91:06 (Bruce Berndt via David Boyd) We define iterated powers by

$$a_1, \quad a_1^{a_2}, \quad a_1^{(a_2^{a_3})}, \ldots$$

In his third notebook (p. 390 of vol. 2 of the Tata Institute's facsimile edition), Ramanujan states (written upside down)

"$a_1^{a_2^{a_3^{\cdot^{\cdot^{\cdot}}}}}$ is convergent when $1 + \ln\ln a_n \leq$

$$\frac{1}{2}\left\{\frac{1}{n^2} + \frac{1}{(n\ln n)^2} + \frac{1}{(n\ln n\ln\ln n)^2} + \frac{1}{(n\ln n\ln\ln n\ln\ln\ln n)^2} + \cdots\right\};$$

divergent when $1+\ln\ln a_n$ is greater than the righthand side with any 1 is replaced by $1+\epsilon$."

1. I can't prove this.
2. When does the series in { } stop? Presumably when the iterated logarithm becomes negative?
3. What is the meaning of the statement on divergence? Presumably the assumption is that $\geq$ holds for **all** n when one "1" in a numerator is replaced by $1+\epsilon$.

Notes: It is well known that if $a_n = a$, $n \geq 1$, then we have convergence for $e^{-e} \leq a \leq e^{1/e}$. This has been generalized to real and then complex a_n under same inequalities. See

R. Arthur Knoebel, Exponentials reiterated, *Amer. Math. Monthly*, **66**(1981) 235–252.

and Berndt's book, Ramanujan's Notebooks, Part I, p. 77 for references. The result for complex a_n is due to W. J. Thron in 1970.

Observe that when $a_n = e^{1/e}$, $1 + \ln\ln a_n = 0$. Thus, if Ramanujan's result is true, it is an improvement on best results that are known.

Remark: In a 92-10-18 preprint,

Gennady Bachman, On the convergence of infinite exponentials,

gives two essentially best possible tests for convergence:

If $E_n = a_1^{a_2^{a_3^{\cdot^{\cdot^{\cdot^{a_n}}}}}}$, $a_n = e^{b_n}$ and $\hat{a}_n = e^{|b_n|}$, and $\hat{E}_n$, defined analogously in terms of $\hat{a}_n$, converges, then so does E_n.

E_n converges if there exist positive integers k_0 and n_0 such that for all $n \geq n_0$ we have

$1 + \ln|\ln a_n| = 1 + \ln|b_n|$

$$\leq \frac{1}{2}\left\{\frac{1}{n^2} + \frac{1}{(nL_1(n))^2} + \frac{1}{(nL_1(n)L_2(n))^2} + \cdots + \frac{1}{(nL_1(n)L_2(n)\cdots L_{k_0}(n))^2}\right\}$$

where $L_1(x) = L(x) = \ln(x)$ for $x \geq x_1 = e$ and $L_k(x) = L_{k-1}(L(x))$ for $x \geq x_k = e^{x_{k-1}}$.

E_n diverges if $a_n > 1$ and, for $n \geq n_0$ with some positive integers k_0 and n_0, and $\epsilon > 0$, $1 + \ln\ln a_n \geq$ the above expression with the last numerator 1 replaced by $1+\epsilon$.

91:10 (Hugh Edgar) Characterize those primes p for which there exists a triple of units u_1, u_2, u_3 in $\mathbb{Z}\left[\zeta_p + \zeta_p^{-1}\right]$ for which $u_1 + u_2 + u_3 = u_1 u_2 u_3$.

Remarks: Compare **89:20**. Richard Mollin notes that the *general* question was earlier raised in

R. A. Mollin, Charles Small, K. Varadarajan & P. G. Walsh, On unit solutions of the equation $xyz = x + y + z$ in the ring of integers of a quadratic field, *Acta Arith.*, **48**(1987) 341–345; *MR* **89d**:11019.

as it was in **85:21**, the MSVW reference also being given in 1986 and 1987.

91:12 (Xingde Jia) If $a_1 < a_2 < \ldots$ is a sequence of nonnegative integers with the property that all sums $a_i + a_j + a_k$ $(i \le j \le k)$ are distinct, is it true that

$$\#\{a_i - a_j \quad | \quad i > j, \quad a_i - a_j \le x\} = O(x^{2/3}) \quad ?$$

A more general question (with more summands) can be asked.

Solution (Don Coppersmith): No. We construct an infinite sequence of a_i with infinitely many values x for which

$$\#\{a_i - a_j \mid i > j,\ a_i - a_j \le x\} = \Omega(x^{99/100}).$$

We build the sequence piece by piece. Repeat the following process infinitely often. Select a value y which is larger than three times the largest of the previously constructed values a_i and set $x = y^{100}$. Add the following values a_i to the sequence:

$$\{4^i x,\ 4_i x + iy \mid x/(2y) < i \le x/y\}.$$

Claim: for each chosen value of x there are at least $x^{99/100}/2$ pairs (a_i, a_j) whose (distinct) differences are all less than x, namely

$$\{4^i x,\ 4_i x + iy \mid x/(2y) < i \le x/y\}.$$

Claim: no two triples from this sequence have the same sum. Given two triples with the same sum, let (x, y) be the largest values of x and y associated with any of the a_i in these triples. Then for some $i \le j \le k$, $l \le m \le n$ we have

$$a_i + a_j + a_k = a_l + a_m + a_n$$

where each element is one of the following:

$$4^i x,\ 4_i x + iy\ \ z < y/3.$$

Here z represents any element belonging to a smaller (x, y). Break these elements into their high order parts, medium order parts and low order parts

$$4^i x,\ 4^i x,\ 0 \qquad 0,\ iy,\ 0 \qquad 0.\ 0,\ z.$$

Because the sum of the low order parts is less than y, which is the quantum by which medium order parts are measured, and similarly the medium order parts sum to less than x, we have that the sum of the high order parts must agree, as must the sum of the medium order parts and the sum of the low order parts. The high order parts tell us that

$$k = n, \qquad j = m \text{ or } a_j,\ a_m < y/3, \qquad i = l \text{ or } a_i,\ a_l < y/3.$$

From $x/(2y) < i \le x/y$, we know that we cannot have $iy + jy = ky$, so the medium order parts agree separately. Finally the low order parts z can be dealt with by induction. So the triples must agree identically.

This tells us that no two triples can have the same sum, and for infinitely many values of x we have

$$\#\{a_i - a_j \mid i > j,\ a_i - a_j \le x\} = \Omega(x^{99/100}).$$

Clearly the $x^{99/100}$ can be replaced by any function which is $o(x)$.

91:20 (D. H. Lehmer) Is it true that 6 is a primitive root of about 95% of primes of shape n^2+108? Andrew Odlyzko has checked this numerically for primes $p < 4\times 10^{12}$ (there appear to be 83413 such primes, 4152 of which do not have 6 as a primitive root) and has produced a heuristic argument, based on reciprocity laws, that this ought to be true.

Attribution. John Brillhart corrects this to D. H. Lehmer. He & Richard Blecksmith computed this a short way. Andrew Odlyzko did the heavy computing.

91:21 (Sinai Robbins) What groups G have $G \cong \mathcal{A}(G)$, the group of automorphisms of G ?

Remark. In addition to the remarks made last time, Nigel Boston observes that such groups can have essentially arbitrary additional structure, since any group (by a modification of Wielandt's theorem) can be imbedded subnormally in such a group.

91:24 (Dick Katz) Inscribe an equilateral triangle in a circle of unit radius. Inscribe a circle in the triangle. Inscribe a square in the second circle, and inscribe a circle in the square. Inscribe a regular pentagon in the third circle, and continue indefinitely. The radii of the circles converge to

$$\prod_{k=3}^{\infty} \cos\frac{\pi}{k}.$$

What is this number?

Comments (Richard McIntosh): (a) Abramowitz & Stegun, p. 75, give

$$\prod_{k=3}^{\infty} \cos\frac{\pi}{k} = \prod_{k=3}^{\infty}\prod_{n=1}^{\infty}\left(1 - \frac{4}{k^2(2n-1)^2}\right).$$

(b) Since $\frac{d}{dx}\ln\cos x = -\tan x$ can be expanded as a power series involving Bernoulli numbers, it follows that

$$\ln\prod_{k=3}^{\infty}\cos\frac{\pi}{k} = \sum_{k=3}^{\infty}\ln\cos\frac{\pi}{k}$$

$$= \sum_{n=1}^{\infty} \frac{(2^{2n}-1)(2\pi)^{2n}B_{2n}}{2n(2n)!}\left(\frac{(2\pi)^{2n}B_{2n}}{2(2n)!}+\frac{(-1)^n(2^{2n}-1)}{2^{2n}}\right)$$
$$= \sum_{n=1}^{\infty} \frac{(2^{2n}-1)}{n}\zeta(2n)\left(\zeta(2n)-1-\frac{1}{2^{2n}}\right)$$

where B_m is defined by

$$\frac{x}{e^x-1} = \sum_{m=0}^{\infty} B_m \frac{x^m}{m!} \quad \text{and} \quad \zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$$

Using MAPLE we get $\prod_{k=3}^{\infty} \cos\frac{\pi}{k} = 0.11494\,20448\,53296\,20070\,10401\,57469\,59874\,28307\,95337$-
$$\text{-}20086\,35168\,44023\,39651\,89660\,12825\,35305\,11779\ldots$$

(c) Since $\prod_{n=1}^{\infty} \cos\frac{x}{2^n} = \frac{\sin x}{x}$, it follows that if we use only 2^n-gons ($n = 2,\ 3,\ 4,\ \ldots$), then the radii converge to $\frac{2}{\pi}$.

PROBLEMS PROPOSED 92–12–19 & 22

92:01 (Richard Mollin via Andrew Granville) If $6k+1$, $12k+1$ and $18k+1$ are all primes, then $n = (6k+1)(12k+1)(18k+1)$ is a Carmichael number, and $p|n$ implies that $p-1|n-1$. The methods of the Alford, Granville, Pomerance paper on the infinitude of Carmichael numbers imply that there are infinitely many n such that $p|n$ implies $p^2-1|n-1$. Find such an n.

Solution: Richard Pinch has counted all Carmichael numbers less than 10^{16}.

$$443372888629441 = 17\cdot 31\cdot 41\cdot 43\cdot 89\cdot 97\cdot 167\cdot 331$$

$$[443372888629440 = 2^6 3^2 5\cdot 7^2 11\cdot 47\cdot 83\cdot 211\cdot 347]$$

and

$$582920080863121 = 41\cdot 53\cdot 79\cdot 103\cdot 239\cdot 271\cdot 509$$

$$[582920080863120 = 2^4 3^3 5\cdot 7^2 11\cdot 13\cdot 17\cdot 127\cdot 17839]$$

are the only such numbers in this range.

Sid Graham found 18 such numbers, the smallest being

$$5893983289990395334700037072001 = 29\cdot 31\cdot 37\cdot 43\cdot 53\cdot 67\cdot 79\cdot 89\cdot 97\cdot 151\cdot 181\cdot 191\cdot 419\cdot 881\cdot 883$$

and he found 17 other numbers that satisfy the slightly weaker condition $(p^2-1)/2|(n-1)$.

W. Red Alford, Andrew Granville & Carl Pomerance, (preprint, 1992).

R. G. E. Pinch, The Carmichael numbers up to 10^{15}, *Math. Comput.*, **60?**(1993) –.

92:02 (James P. Jones via Richard Guy) An analogous problem to **92:01** arose from a study of Lucas sequences. Are there any odd squarefree n such that $p^2-1|n+1$ whenever $p|n$? Apart from $n=3$ is there even an example where $(p^2-1)/2$ divides $n+1$? He gave several examples, including 5, $35 = 5\cdot 7$, $6479 = 11\cdot 19\cdot 31$, $84419 = 29\cdot 41\cdot 71$, $1930499 = 89\cdot 109\cdot 199$,

$7110179 = 37 \cdot 41 \cdot 43 \cdot 109$, $15857855 = 5 \cdot 13 \cdot 17 \cdot 113 \cdot 127$, where $(p^2-1)/4$ always divides $n+1$.

92:03 (Gene W. Smith) Define a **Pascal polynomial** as

$$\binom{k}{k}x^n + \binom{k+1}{k}x^{n-1} + \binom{k+2}{k}x^{n-2} + \cdots + \binom{k+n}{k}.$$

For example, for $n = 6$ and $k = 1$ and 3, we have

$$x^6 + 2x^5 + 3x^4 + 4x^3 + 5x^2 + 6x + 7,$$

$$x^6 + 4x^5 + 10x^4 + 20x^3 + 35x^2 + 56x + 84.$$

Each of these examples has Galois group $\mathrm{PGL}_2(5)$. Do any other Pascal polynomials have Galois group S_n? Why do these two examples behave in this way?

92:04 (Gerry Myerson) Let

$$f(n) = \frac{n!}{\frac{n}{2}!\frac{n}{3}!\frac{n}{7}!\cdots[1,2,\ldots,n]}$$

where the denominators in the denominator, 2, 3, 7, 43, 1807, ... are each one more than the product of the preceding ones, $x!$ is interpreted as $\lfloor x \rfloor !$, and [1,2,...,n] is the least common multiple of 1, 2, ..., n. Then $f(n)$ is an integer for $n = 1, 2, \ldots$. Is $f(n)$ odd infinitely often, or, given m, is there an n_0 such that for $n > n_0$, $m | f(n)$?

Remark. On 93-02-08 Gerry Myerson writes that $f(n)$ is odd only for 135 values of n, the largest of which is 1966081. He can show that, for $2 \le m \le 5$, m divides $f(n)$ for all sufficiently large n, but for general m the problem remains open.

92:05 (Russell Lyons via Jeffery Lagarias) Prove that there are no integer solutions s, y, $z \ge 2$ to the equation

$$\frac{\ln(yz)}{\ln(s)} = \frac{(yz-1)(zs^z+1)}{(s^z-1)(y+1)}$$

Solution: (found by Lagarias during the meeting) For the left side to be rational, we must have $yz = t^m$, $s = t^n$, where $m, n \ge 1$, $t \ge 2$ are integers. Left side is then m/n, which may be assumed to be in lowest terms (t may be a power).

$$\frac{m}{n} = \frac{(t^m-1)(zt^{nz}+1)}{(t^{nz}-1)(\frac{t^m}{z}+1)}$$

We will show that $t^{nz}-1$ has a large factor f not cancelling with the numerator.

If a prime p divides z, then p divides t. Hence both terms on the right are $\equiv \pm 1 \bmod p$ and p does not divide m. Thus $m \perp z = 1$ and $m \perp n = 1$ so $m \perp nz$ and $\gcd(t^m-1, t^{nz}-1) = t-1$. Also, $\gcd(t^{nz}-1, zt^{nz}+1) | z+1$ and

$$\frac{t^{nz}-1}{(t-1)(t^{nz}-1, z+1)} \text{ divides } f$$

and f divides n. But the left side

$$\geq \frac{1+t+\cdots+t^{nz-1}}{z+1} > n$$

unless $n = 1$, $z = t = 2$ and these don't work.

This will appear in a paper:

Russell T. Lyons, Equivalence of boundary measures on covering trees of finite graphs, *Ergodic Theory Dyn. Systems* (submitted).

92:06 (Michael Reid) Problem **1339**, *Math. Mag.*, **63**(1990) 56, proposed by George Gilbert, was to find all integer triples (x, y, z), $2 \leq x \leq y \leq z$, such that

$$yz \equiv 1 \bmod x, \quad zx \equiv 1 \bmod y, \quad xy \equiv 1 \bmod z.$$

The only solutions are perms of {2,3,5}. See **64**(1991) 63, where it was noted that this appeared as Problem #32 on p. 292 of Hillman & Alexanderson, *A First Undergraduate Course in Abstract Algebra*. It is the case $k = 3$ of Problem **1375** **64**(1991) 197, proposed by Lorraine L. Foster. Prove that for each integer $k \geq 3$ there exist positive integers n_1, n_2, ..., n_k such that $\prod_{i \neq j} n_i \equiv 1 \bmod n_j$, for $j = 1, 2, \ldots, k$. For a solution, see **65**(1992) 197–198.

From the sequence $a_1, a_2, \ldots = 2, 3, 7, 43, 1807, \ldots$ (see **92:04** above) we can construct two families of solutions:

$a_1, a_2, \ldots, a_{k-1}, a_k - 2$	$a_1, a_2, \ldots, a_{k-2}, 2a_{k-1} - 3, 2a_{k-1} - 1$
2, 3, 5	2, 3, 5
2, 3, 7, 41	2, 3, 11, 13
2, 3, 7, 43, 1805	2, 3, 7, 43, 3611, 3613
...	...

Question 1. Suppose that $x_1, \ldots, x_l$ are pairwisecoprime. Can this necessarily be extended to a solution $x_1, \ldots, x_k$ of the original problem for some $k \geq l$?

For example, David Moews extended the single term $a_1 = 4$ to $k = 10$:

4, 3, 5, 7, 17, 67, 16501, 52978181, 710010917562137, 1552138166758094923288555458243.

It's not hard to see that the original system is equivalent to the single congruence

$$\sum_{j=1}^{k} \prod_{i \neq j} x_i \equiv 1 \bmod \prod_{j=1}^{k} x_j \qquad (**)$$

and that this is equivalent to

$$\frac{1}{x_1} + \frac{1}{x_2} + \cdots + \frac{1}{x_k} - \frac{1}{x_1 x_2 \cdots x_k} \qquad (***)$$

being an integer. Note the connexion with Giuga's conjecture, **92:07** and **92:15** below and *UPINT* **A17**.

Some other questions that may be asked are:

Question 2. Does every integer > 1 occur as an x_i in some solution?

Question 3. Are there solutions of $(***)$ in which the integer is greater than 1 ?

Question 4. Are there solutions of $(***)$ with the integer arbitrarily large?

Question 5. Are there solutions of $(***)$ for every positive integer?

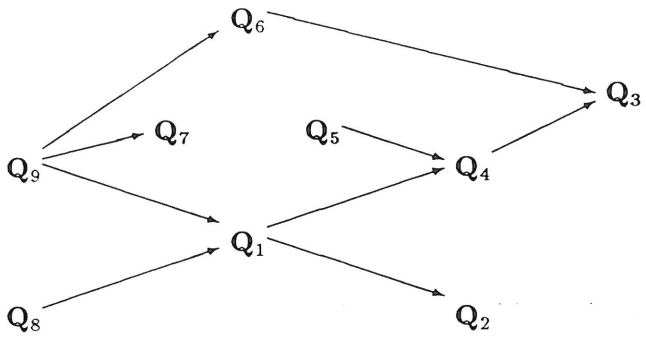
Question 6. If p_i is the i-th prime, then $p_1, p_2, \ldots, p_k$ is a solution for $k = 3$. Is it a solution for any $k > 3$?

Question 7. Are there infinitely many solutions with each x_i prime? Compare Giuga's conjecture again.

Question 8. Does the greedy algorithm work? I.e., given $x_1, \ldots, x_l$, choose x_{l+1} to be the smallest integer coprime to the previous x_i which doesn't increase the integer part of $(***)$ when it is appended. [This appears to be what Moews did in the $k = 10$ example above.]

Question 9. How about the "absent-minded algorithm" which chooses the smallest integer > 1 which is coprime to the previous x_i ?

It is easy to see that for a *fixed* k, there are only finitely many solutions to the original problem. In the following diagram, $\mathbf{Q}_i \rightarrow \mathbf{Q}_j$ means that an affirmative answer to $\mathbf{Q}_i$ implies an affirmative answer to $\mathbf{Q}_j$.



92:07 (Gerry Myerson) **Giuga's conjecture.** Compare $(***)$ in the previous problem, **92:15** below, and **A17** in *UPINT*.

$$1^{n-1} + 2^{n-1} + \cdots (n-1)^{n-1} \equiv -1 \bmod n$$

if n is prime. Is the converse true? If n is composite, then n is a Carmichael number *and*

$$\sum_{p|n} \frac{1}{p} - \frac{1}{n} \quad \text{is an integer.}$$

There is an equivalent statement involving the Bernoulli numbers:

$$nB_{n-1} \equiv -1 \bmod n.$$

92:08 (Andrew Granville) A New-Year email greeting from Hendrik Lenstra informed us that

$$1993 = 43^2 + 12^2 = 35^2 + 3 \cdot 16^2 = 29^2 + 2 \cdot 24^2 = 7^2 + 6 \cdot 18^2$$

where each second summand is divisible by only the primes 2 and 3. Find the next year which is so representable. Are there any other examples of primes p and q and positive integers a, b, c, d, A, B, C, D with

$$a^2 + A^2 = b^2 + pB^2 = c^2 + qC^2 = d^2 + pqD^2$$

and such that the only primes dividing $ABCD$ are p and q?

Solution: (Reese Scott)

$$2113 = 33^2 + 32^2 = 31^2 + 2 \cdot 24^2 = 41^2 + 3 \cdot 12^2 = 13^2 + 6 \cdot 18^2$$

92:09 (Andrew Granville) Find a more attractive proof, than that using the theory of binary quadratic forms, that for any $n \geq 1$ there are nonzero integers a_i, b_i such that

$$a_1^2 + b_1^2 = a_2^2 + 2b_2^2 = a_3^2 + 3b_3^2 = \cdots = a_n^2 + nb_n^2$$

Remark: Reese Scott has a proof which uses class numbers, but which Hugh Edgar thought qualified as *not* using the theory of binary quadratic forms. Whether it satisfies the "attractive" criterion he leaves others to judge.

92:10 (Ron Graham via Neville Robbins) The diophantine equations

$$2x^2(x^2 - 1) = 3(y^2 - 1) \quad \text{and} \quad (2x - 1)^2 = 2^n - 7$$

each have the solutions $x = 0$, 1, 2, 3, 6 and 91. Is this merely an example of the Strong Law of Small Numbers?

92:11 (John Selfridge) The proposer gave an extended lecture on "envy-free" cake-cutting and wine-pouring, in which he described the Selfridge Protocol for the division of a cake into 3 envy-free parts using at most 5 cuts. He asked for envy-free division of wine between

(A) 4 people, using 4 glasses, finishing in a bounded number (5?) of rounds

(B) 5 people, k glasses, one round. Brams & Taylor (see below) give a solution for $k = 9$. Try for $k = 6$, then $k = 5$ or 7, according as success is achieved or not.

Bibliography courtesy The Strens Collection, The University of Calgary.

[early papers copied from Singmaster's Sources.]

Ethan Akin, Vilfredo Pareto cuts the cake (preprint, Jan 1993?). [Math. Dept., The City College, 137th St. & Convent Ave., New York NY 10031, U.S.A.]

A. K. Austin, Sharing a cake, *Math. Gaz.*, **66**(1982) 212–215.

A. K. Austin & Walter R. Stromquist, in Comments and complements, *Amer. Math. Monthly*, **90**(1983) 474.

Julius B. Barbenel, Super envy-free cake division: the $N = 3$ case (preprint, Oct. 1992). [super envy-free if each believes he has $> 1/N$ and all others $< 1/N$. A measure-theoretic existence proof. Is there an algorithm?]

Julius B. Barbanel & Alan D. Taylor, Preference relations and measures in the context of fair division, preprint.

W. J. Baumol, *Superfairness: Applications and Theory*, MIT Press, Cambridge MA, 1985.

Anatole Beck, Constructing a fair border, *Amer. Math. Monthly*, **94**(1987) 157–162.

S. Bennett *et al.*, *Fair Divisions: Getting Your Fair Share*, HIMAP [High School Math. and its Applications] Module 9 (Teachers' Manual).

M. Berliant, K. Dunz & W. Thomson, On the fair division of a heterogeneous commodity, *J. Math. Econ.*, **21**(1992)

Max Black, Critical Thinking, Prentice-Hall, Englewood Cliffs NJ, 1946, 2nd ed 1952; Problem 12, pp. 12 & 432. [Raises the question but only suggests combining two persons.]

K. Borsuk, Drei Sätze über die n-dimensionale euklidische Sphäre, *Fundamenta Math.*, **20**(1933) 177–190. [Ham-sandwich theorem]

Steven J. Brams & Alan D. Taylor, An envy-free cake division algorithm (preprint), see David Gale. [requires $2^{n-2} + 1$ glasses to satisfy n people.]

Steven J. Brams & Alan D. Taylor, More envy-free cake division (preprint).

Steven J. Brams & Alan D. Taylor, An envy-free cake division protocol (preprint received Jan. 1993).

Lester E. Dubins & Edward H. Spanier, How to cut a cake fairly, *Amer. Math. Monthly*, **68**(1961) 1–17.

J. Elton, T. Hill & R. Kertz, Optimal-partitioning inequalities for nonatomic probability measures, *Trans. Amer. Math. Soc.*, **296**(1986) 703–725.

S. Even & A. Paz, A note on cake-cutting, *Discrete Appl. Math.*, **7**(1984) 285–296.

A. M. Fink, A note on the fair division problem, *Math. Mag.*, **37**(1964) 341–342.

R. Fisher, Quelques remarques sur l'estimation en statistique, *Biotypologie*, (1938) 153–159. [Ronald Aylmer Fisher?]

R. Fisher, Uncertain inference, *Proc. Amer. Acad. Arts Sci.*, **71**(1936) 245–257. [Ronald Aylmer Fisher?]

David Gale, Mathematical Entertainments, *Math. Intelligencer*, **15** No. 1 (Winter 1993) 48–52, esp. 50–52. [Selfridge's three-person, envy-free protocol. Spanier–Dubins allocation. An envy-free Stromquist allocation is automatically undominated.]

George Gamow & M. Stern, *Puzzle-Math*, Viking, New York, 1958.

Martin Gardner, Fair division, in *aha! insight*, W. H. Freeman, 1978, pp. 123–124. [describes the "envy-free" problem.]

George Gamow & M. Stern, *Puzzle-Math*, Viking, New York, 1958.

Theodore P. Hill, Determining a fair border, *Amer. Math. Monthly*, **90**(1983) 438–442.

Theodore P. Hill, A sharp partitioning-inequality for nonatomic probability measures based on the mass of the infimum of the measures, *Probab. Theory Related Fields*, **75**(1987) 143–147.

Theodore P. Hill, Partitioning general probability measures, *Ann. Probab.*, **15**(1987) 804–813.

Theodore P. Hill, A proportionality principle for partitioning problems, *Proc. Amer. Math. Soc.*, **103**(1988) 288–293.

Theodore P. Hill, Partitioning inequalities in probability and statistics, *Proc. Seattle Conf. Inequal. Probab. Statist.*, IMS Lecture Notes, 1991,

Theodore P. Hill, Fair-division problems (1992 preprint)

B. Knaster, Sur le problème du partage pragmatique de H. Steinhaus, *Ann. Soc. Polon. Math.*, **19**(1946) 228–230. [Says Steinhaus proposed the problem in a 1944 letter to Knaster. Outlines the Banach & Knaster method of one cutting $1/n$ and each being allowed to diminish it – last diminisher takes the piece. Also shows that if the valuations are different, then everyone can get $> 1/n$ in his measure. Gives Banach's abstract formulations.]

H. Kuhn, On games of fair division, in Martin Shubik (ed.) *Essays in Mathematical Economics*, Princeton Univ. Press, 1967, pp. 29–37.

J. Legut, The problem of fair division for countably many participants, *J. Math. Anal. Appl.*, **109**(1985) 83–89.

J. Legut, Market games with a continuum of indivisible commodities, *Internat. J. Game Theory*, **15**(1986) 1–7.

J. Legut, A game of fair division with a continuum of players, *Colloq. Math.*, **53**(1987) 323–331.

J. Legut, A game of fair division in the normal form, *Colloq. Math.*, **54**(1988) 179–184.

J. Legut, Inequalities for α-optimal partitioning of a measurable space, *Proc. Amer. Math. Soc.*, **104**(1988) 1249–1251.

J. Legut, On totally balanced games arising from cooperation in fair division, *Games Econ. Behavior*, **2**(1990) 47–60.

J. Legut & M. Wilcznski, Optimal partitioning of a measurable space, *Proc. Amer. Math. Soc.*, **104**(1988) 262–264.

J. Legut, J. A. M. Potters & S. H. Tijs, Economies with land: a game theoretic approach, *Games Econ. Behavior*, *4*(1992)

S. X. Levmore & E. E. Cook, *Super Strategies for Puzzles and Games*, Doubleday, Garden City NY, pp. 47–53.

A. A. Liapounoff, Sur les fonctions-vecteurs complètement additives, *Izv. Akad. Nauk USSR*, **4**(1940) 465–478; *MR* **2**, 315e.

A. A. Liapounoff, Sur les fonctions-vecteurs complètement additives, *Izv. Akad. Nauk USSR*, **10**(1946) 277–279; *MR* **8**, 157b.

Kevin McAvaney, Jack Robertson & William Webb, Ramsey partitions of integers and fair division, *Combinatorica*, **12**(1992) 193–201.

Jerzy Neyman, Un théorème d'existence, *C.R. Acad. Sci. Paris*, **222**(1946) 843–845.

Jerzy Neyman & E. Pearson, On the problem of the most efficient tests of statistical hypotheses, *Philos. Trans. Roy. Soc. London Ser. A*, **231**(1933) 289–337.

D. Olivastro, Preferred shares, *The Sciences*, Mar-Apr 1992, 52–54.

D. Olivastro, Reply to letter of Ralph G. Ranney, *The Sciences*, Jul-Aug 1992, 52.

R. Oskui, Dirty work problem, (1992 preprint)

K. Rebman, How to get (at least) a fair share of the cake, in Ross Honsberger, *Mathematical Plums*, Math. Assoc. Amer., 1979, 22–37.

J. M. Robertson & W. A. Webb, Minimal number of cuts for fair division, *Ars Combin.*, **31**(1991) 191–197.

J. M. Robertson & W. A. Webb, Approximating fair division with a limited number of cuts, (1992 preprint)

J. L. Selfridge, Four envy-free glasses of wine, MS dated 92-06-11; see also David Gale, Mathematical Entertainments, *Math. Intelligencer*, Dec. 1992.

H. Steinhaus, Remarques sur le partage pragmatique, *Ann. Soc. Polon. Math.*, **19**(1946) 230–231. [Says the problem isn't solved for irrational people and that Banach & Knaster's method can form a game.]

H. Steinhaus, The problem of fair division, *Econometrica*, **16**#1(Jan 1948) 101–104. [This is a report of a paper given on 47-09-17. Gives Banach & Knaster's method.]

Hugo Steinhaus, Sur la division pragmatique, *Econometrica* (supplement) **17**(1949) 315–319. [attributes problem to Banach & Knaster.]

H. Steinhaus, *Mathematical Snapshots*, 3rd edition, Oxford Univ. Press, 1969.

Arthur H. Stone & J. Tukey, Generalized "sandwich" theorems, *Duke Math. J.*, **9**(1942) 356–359.

Walter Stromquist, How to cut a cake fairly, *Amer. Math. Monthly*, **87**(1980) 640–644.

Walter Stromquist, Addendum to "How to cut a cake fairly", *Amer. Math. Monthly*, **88**(1981) 613–614.

Walter Stromquist & Douglas R. Woodall, Sets on which several measures agree, *J. Math. Anal. Appl.*, **108**(1985) 241–248.

K. Urbanik, Quelques théorèmes sur les mesures, *Fundamenta Math.*, **41**(1954) 150–162.

William A. Webb, A combinatorial algorithm to establish a fair border, *Europ. J. Combin.*, **11**(1990) 301–304.

William A. Webb, An algorithm for a stronger fair division problem, (1992 preprint)

D. Weller, Fair division of a measurable space, *J. Math. Econ.*, **14**(1985) 5–17.

Douglas R. Woodall, Dividing a cake fairly, *J. Math. Anal. Appl.*, **78**(1980) 233–247.

Douglas R. Woodall, A note on the cake division problem, *J. Combin. Theory Ser. A*, **42**(1986) 300–301.

92:12 (Andrew Granville) Find examples of

$$x^p + y^q = z^r \quad \text{with} \quad \frac{1}{p} + \frac{1}{q} + \frac{1}{r} < 1$$

other than $2^3 + 1^7 = 3^2$ and $7^3 + 13^2 = 2^9$. [Blair Kelly III gave $2^5 + 7^2 = 3^4$ and Reese Scott $17^3 + 2^7 = 71^2$.]

Find examples of coprime triples (A, B, C) for which there are at least 3 solutions of

$$Ax^p + By^q + Cz^r = 0 \text{ with } \frac{1}{p} + \frac{1}{q} + \frac{1}{r} < 1 \text{ and } |x|, |y|, |z| \geq 2$$

Find a solution to

$$Ax^2 + By^3 = Cz^5 \text{ in polynomials } x(A, B, C),\ y(A, B, C),\ z(A, B, C)$$

such that Ax, By, Cz have no common factors.

92:13 (Gene W. Smith) Find examples of the **Galoisean inequation**

$$\text{Gal}\left((X(X - 2n - 1)^n(X + 2n + 1)^n - t(X - 1)^n(X + n^2)) \,/\, \mathbb{Q}(t)\right) \neq S_{2n+1}$$

For example, $n = 1$ gives A_3 and $n = 3$ gives $PGL_3(2)$.

Or, find out when the discriminant of

$$(X(X-2n-1)^n(X+2n+1)^n - t(X-1)^n(X+n^2), X)$$

is a square polynomial in t.

92:14 (Richard Guy) It is well known that the rational points on an elliptic curve of rank one (or more) are dense, at least on the infinite branch. So, if P is a generator, values of n can be found such that $(n+1)P$ is arbitrarily close to P, so that n is a "near period" for the points. Several examples have been found where comparatively small n give remarkably good near periods. These are associated with large partial quotients in the continued fraction expansion of numbers associated with the curve. What is going on? Presumably something not unrelated to Stark's paper nor to Method 3 of Zagier's paper.

Harold M. Stark, An explanation of some exotic continued fractions found by Brillhart, in Atkin & Birch, *Computers in Number Theory* (Proc. S.R.C. Atlas Symp., Oxford 1969), Academic Press, 1961, 21–35.

Don Zagier, Large integral points on elliptic curves, *Math. Comput.*, **48**(1987) 425–436.

92:15 (Gerry Myerson) Comparison of Giuga's conjecture (see **92:07** above) with Wilson's theorem prompts us to let $F_n(x_1, \ldots, x_{n-1})$, $n = 1, 2, \ldots$ be a "coherent family" of symmetric functions of degree $n-1$, e.g. $F_n = x_1 x_2 \cdots x_{n-1}$ (Wilson's theorem), $F_n = x_1^{n-1} + \cdots + x_{n-1}^{n-1}$ (Giuga's conjecture), or $F_n = \sum_{j=1}^{n-1} \sum_{k=1}^{n-1} x_j^{n-2} x_k$, or .... Is there a number A, depending on the family, but not on n, such that $F_n(1, 2, \ldots, n-1) \equiv A \bmod n$ if and only if n is prime?

What happens if we ask only that F_n be invariant under the cyclic group?

92:16 (Yang Wang – from my notes) If $0 \in S$, $\gcd(S) = 1$ and $T_{S,N} = \{\sum_{i=0}^{N} a_i 2^i | a_i \in S\}$, how many consective integers can $T_{S,N}$ contain? E.g., if $S = \{0, p, 2q\}$ then there are quite a lot.

92:17 (Reese Scott via Hugh Edgar) Theorem: If p, q are given primes, h is fixed and $p^m - q^n = 2^h$ has two solutions with m, n positive integers, then $q^2 | 2^q - 2$, $q^2 | p^q - p$, $2|h$, $2^h \| (p-1)$ and $2^{h+1} | (q-1)$.

Show that these conditions exclude all possibilities.

Remarks: Reese Scott writes that if the equation has two solutions, then $q^2 | (2^q - 2)$, and, as it has only one for $q = 1093$ or 3511, then for two solutions $q > 3 \cdot 10^9$. Cao & Wang have shown that if there are two solutions, one of them has $m = 1$. For latest results see his *J. Number Theory* paper, especially Theorems 1 & 6.

Cao Zhen-Fu, Hugh Edgar's problem on exponential Diophantine equations (Chinese), *J. Math. (Wuhan)*, **9**(1989) 173–178; *MR* **90i**:11035.

Cao Zhen-Fu & Wang Du-Zheng, On the Diophantine equation $a^x - b^y = (2p)^z$ (Chinese). *Yangzhou Shiyuan Xuebao Ziran Kexue Ban*, **1987** no. 4 25–30; *MR* **90c**:11020.

Reese Scott, On the equations $p^x - b^y = c$ and $a^x + b^y = c^z$, *J. Number Theory*, **43**(1993) 153–165.

92:18 (Harold Davenport via Andrew Granville) For any group G find $n(G)$, the length of the longest sequence of (not necessarily distinct) elements of G such that the products of all subsequences are different from the identity.

$$1.\ \text{If } G = \mathbb{Z}/p^{a_1}\mathbb{Z} \times \mathbb{Z}/p^{a_2}\mathbb{Z} \times \cdots \times \mathbb{Z}/p^{a_k}\mathbb{Z}$$
$$\text{then } n(G) = (p^{a_1} - 1) + (p^{a_2} - 1) + \cdots + (p^{a_k} - 1)$$

$$2.\ \text{If} \qquad G = C_{m_1} \times C_{m_2} \times \cdots \times C_{m_k}$$
$$\text{then } n(G) \geq (m_1 - 1) + (m_2 - 1) + \cdots + (m_k - 1)$$

$$3.\ \text{and} \qquad n(G) \leq m_1(1 + \ln \frac{|G|}{m_1})$$

Improve 3. It's known that there is a G giving strict inequality in 2.

Variant in class groups. Consider $G = C/C^p$ where C is the class group of the pth cyclotomic field. Given an ideal I, let

$$\Gamma_I = \{I^\sigma : \sigma \in \Gamma\}$$

Find as small a subset as possible of Γ_I, say $\{I_1, \ldots, I_t\}$, with $I_1^{a_1} \cdots I_t^{a_t}$ principal. Trivially we can take $t = p$-rank of $C/C^p + 1$, but can we do better, given that our set is so large?

92:19 (Erdős & Heilbronn via John Selfridge) (**C15** in *UPINT*) E. & H. asked for the largest number $k = k(m)$ of distinct residue classes, modulo m, so that no subset has sum zero. For example, the set

$$1,\ -2,\ 3,\ 4,\ 5,\ 6$$

shows that $k(20) \geq 6$, and in fact equality holds. The pattern of this example shows that

$$k \geq \lfloor(-1 + \sqrt{8m + 9})/2\rfloor \qquad (m \geq 5)$$

Equality holds for $5 \leq m \leq 24$. However, S. observes that if m is of the form $2(l^2 + l + 1)$, the set

$$1,\ 2,\ \ldots,\ l - 1,\ l,\ \tfrac{1}{2}m,\ \tfrac{1}{2}m + 1,\ \ldots,\ \tfrac{1}{2}m + l$$

implies that

$$k \geq 2l + 1 = \sqrt{2m - 3}$$

In fact he conjectures that, for any even m, this set or the set with l deleted always gives the best result. For example, $k(42) \geq 9$.

On the other hand, if p is a prime in the interval

$$\tfrac{1}{2}k(k + 1) < p < \tfrac{1}{2}(k + 1)(k + 2)$$

he conjectures that $k(p) = k$, where the set can be simply

$$1,\ 2,\ \ldots,\ k$$

The case $k(43) = 8$ was confirmed by Clement Lam, so k is not a monotonic function of m.

The only case where a better inequality is known than $k \geq \lfloor\sqrt{2m-3}\rfloor$ is $k(25) \geq \sqrt{50-1} = 7$, as is shown by the set 1, 6, 11, 16, 21, 5, 10. If m is of the form $25l(l+1)/2$ and *odd*, then it is possible to improve on the set 1, -2, 3, 4, ..., but if m is of that form and *even*, then the construction already given for m even is always better.

Is $k = \lfloor(-1+\sqrt{8m+9})/2\rfloor$ for an infinity of values of m?

For which values of m are there realizing sets none of whose members are prime to m? For example, $m = 12$: {3,4,6,10} or {4,6,9,10}. Is there a value of m for which *all* realizing sets are of this type?

E. & H. proved that if $a_1,\ a_2,\ \ldots,\ a_k,\ k \geq 3(6p)^{1/2}$, are distinct residues mod$p$, where p is prime, then every residue mod$p$ can be written in the form $\sum_{i=1}^{k} \epsilon_i a_i,\ \epsilon_i = 0$ or 1. They conjectured that the same holds for $k > 2\sqrt{p}$ and that this is best possible and Olsen proved this. They further conjectured that the number, s, of distinct residues of the form $a_i + a_j,\ 1 \leq i \leq j \leq k$, is at least $2k-3$. [By coincidence, on return from Corvallis, my accumulation of mail contained a submission on this problem (for possible publication in the Unsolved Problems section of the MONTHLY) by Rødseth. The rest of this paragraph is correspondingly amended, and his bibliography used to amplify my own.] In this connexion Rødseth has used Pollard's extension of the Cauchy-Davenport Theorem to show that if $m = p$, a prime, then $s \geq \min(p, 2k - \sqrt{4k+1})$ and a deep result of Freiman to show that there is an absolute constant c such that if $p > ck$, then s is indeed $\geq 2k-3$.

W. Brakemeier, *Ein Beitrag zur additiven Zahlentheorie*, Dissertation, Tech. Univ. Braunschweig 1973.

W. Brakemeier, Eine Anzahlformel von Zahlen modulo n, *Monatsh. Math.*, **85**(1978) 277–282.

A. L. Cauchy, Recherches sur les nombres, *J. École Polytech.*, **9**(1813) 99–116.

H. Davenport, On the addition of residue classes, *J. London Math. Soc.*, **10**(1935) 30–32.

H. Davenport, A historical note, *J. London Math. Soc.*, **22**(1947) 100–101.

P. Erdős, Some problems in number theory, in *Computers in Number Theory*, Academic Press, London & New York, 1971, 405–413.

P. Erdős & H. Heilbronn, On the addition of residue clesses mod p, *Acta Arith.*, **9**(1969) 149–159.

G. A. Freiman, *Foundations of a Structural Theory of Set Addition*, Transl. Math. Monographs, **37**(1973), Amer. Math. Soc., Providence RI.

Henry B. Mann & John E. Olsen, Sums of sets in the elementary abelian group of type (p,p), *J. Combin. Theory*, **2**(1967) 275–284.

John E. Olsen, An addition theorem modulo p, *J. Combin. Theory*, **5**(1968) 45–52.

John E. Olsen, An addition theorem for the elementary abelian group, *J. Combin. Theory*, **5**(1968) 53–58.

J. M. Pollard, A generalisation of the theorem of Cauchy and Davenport, *J. London Math. Soc.*, **8**(1974) 460–462.

J. M. Pollard, Addition properties of residue classes, *J. London Math. Soc.*, **11**(1975) 147–152.

U.-W. Rickert, *Über eine Vermutung in der additiven Zahlentheorie*, Dissertation, Tech. Univ. Braunschweig 1976.

Øystein J. Rødseth, Sums of distinct residues mod p, Preprint, Dec. 1992.

C. Ryavec, The addition of residue classes modulo n, *Pacific J. Math.*, **26**(1968) 367–373.

E. Szemerédi, On a conjecture of Erdős and Heilbronn, *Acta Arith.*, **17**(1970-71) 227–229.