Western Number Theory Problems, 1990–12–17 & 20

Edited by Richard K. Guy & Gerry Myerson

for mailing prior to 1991 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 (present set)	90:01–90:19		

[With comments on earlier problems: 76:15, 88:09, 88:12, 88:17, 89:18, 89:20, 89:29, 89:31, 89:32.]

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

COMMENTS ON ANY PROBLEM WELCOME AT ANY TIME

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

91-06-10 to 91-07-13, with helpful correspondence from Paul Bateman, Hugh Edgar, Jeff Lagarias, Emma Lehmer & Gerry Myerson.

COMMENTS ON EARLIER PROBLEMS

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? At most one? Only finitely many? Examples are $3^2 - 2^3 = 2^0$; $5^3 - 11^2 = 2^2$; $5^2 - 3^2 = 2^4$.

This appeared as Advanced Problem 6110* in *Amer. Math. Monthly*, **83**(1976) 661, proposed by David M. Battany, Oceanside, California, with the suggestion "at most one". It is also in section **D9** on page 87 of UPINT.

Reese Scott, in an as-yet-to-be-published paper, "On the equation $|p^n - q^m| = c$", goes a fair way towards settling the question. He observes that the finiteness of the number of solutions for given (p, q, c) follows from a result of Pillai. The reference is

S. Sivasankaranarayana Pillai, On the inequality "$0 < a^x - b^y \leq n$", *J. Indian Math. Soc.*, **19**(1931) 1–11; Zbl. **1** 268b.

There are also:

S.S. Pillai, On $a^x - b^y = c$, *ibid.* (N.S.) **2**(1936) 119–122; Zbl. **14** 392e.

S.S. Pillai, A correction to the paper "On $A^x - B^y = C$", *ibid.* (N.S.) **2**(1937) 215; Zbl. **16** 348b.

The review of the former mentions

Aaron Herschfeld, The equation $2^x - 3^y = d$, *Bull. Amer. Math. Soc.*, **42**(1936) 231–234; Zbl. **14** 8a.

which in turn refers to the earlier Pillai paper and mentions Siegel's theorem.

Reese Scott's paper has been examined by one or two people, and has now been submitted for publication.

88:09 (Brian Conrey) Let $P(z)$ be a polynomial with real non-negative coefficients and $P(0) \neq 0$. Then P has no real positive zeros. Let ζ be a complex zero of P such that $|\arg \zeta|$ is minimal, where $-\pi < \arg \leq \pi$. Define

$$P_1(z) = \frac{P(z)}{(z-\zeta)(z-\bar{\zeta})}$$

where $\bar{\zeta}$ is the complex conjugate of ζ. Then $P_1(z)$ has real coefficients: are they all non-negative?

Remarks: Brian Conrey & Kevin McCurley each since reported that a group at Texas Tech. are rumored to have proved that the answer is "yes". Ron Evans (90-09-05) & Andrew Odlyzko (90-09-14) supply the reference:

Roger W. Barnard, W. Dayawansa, K. Pearce & David A. Weinberg, Polynomials with nonnegative coefficients, *Proc. Amer. Math. Soc.*, (to appear).

88:12 (Emma Lehmer: revision of **86:12** — and compare **90:14** below) $p = ef + 1$ is prime and

$$\eta_j = \sum_{i=0}^{f-1} \zeta_p^{g^{ei+j}}$$

are the Gaussian periods of order e.

(1) Find constants c_i, $0 \le i \le e-1$, not all 1 or -1, such that

$$\theta_j = \sum_{i=0}^{e-1} c_i \eta_{i+j}$$

are units.

For $e = 5$, $p = 25n^4 + 25n^3 + 15n^2 + 5n + 1$, $\prod \eta_i = n^{10}$.

For $e = 6$, $p = 144n^2 + 12n + 1$, $\prod \eta_i = n^6$.

For $e = 7$, $p = n^6 + 7n^5 + 21n^4 + 49n^3 + 147n^2 + 343n + 343$.

For $e = 8$, $p = 16n^4 + 1$.

Last year's remark was:

Remark. replace the original remark by: Another example for $e = 5$, $p = 25n^4 - 25n^3 + 165n^2 - 95n + 211$ gives $\prod_{i=0}^{4} \theta_i = 1$, for $p = 211$ and $\theta_i = \eta_i - \eta_{i+1} - 1$. In terms of Dickson's form

$$16p = x^2 + 50u^2 + 50v^2 + 125w^2 \quad \text{with} \quad xw = v^2 - u^2 - 4uv$$

we have $u + v = 1$, $w = 5$. We note that for $\theta_i = \eta_i + c$ we have $u + v = 1$, $w = \pm 1$.

n	p	x	u	v	w	q
0	211	1	2	-1	5	31
1	281	11	-3	4	5	37
-1	521	31	7	-6	5	29
2	881	61	-8	9	5	29
5	16361	451	-23	24	5	7
-5	23561	551	-26	27	5	41
8	99611	1201	-38	39	5	7

where q is the least quintic residue.

(2) Are there primes for which $\prod \eta_i = n^e$ for $e = 7$ and $e = 8$?

Emma Lehmer, Connection between Gaussian periods and cyclic units, *Math. Comput.*, **50**(1988) 535–541.

Andrew Earnest asked for references to "Dickson's form". Gerry Myerson (90-10-05) wrote:

Let $p \equiv 1 \bmod 5$ be prime, $\theta = e^{2\pi i/p}$, $K = \mathbb{Q}(\theta)$, E be the field of index 5 in K, and $\eta = Tr_E^K(\theta)$. Then η and its conjugates are the cyclotomic periods of order 5. The product of any two is an integer linear combination of the others, and the integer coefficients are the cyclotomic constants of order 5. It turns out that there are formulas for the cyclotomic constants in terms of the x, u, v, w in $16p = x^2 + 50u^2 + 50v^2 + 125w^2$. Dickson's work on this, and much more, can be found in three papers on cyclotomy that he published in the 1930s. [Emma Lehmer has supplied references:

L. E. Dickson, Cyclotomy, higher congruences and Waring's problem, *Amer. J. Math.*, **57**(1935) 391–424.

L. E. Dickson, Cyclotomy and trinomial congruences, *Trans. Amer. Math. Soc.*, **37**(1935) 363–380.

Thomas Storer, Cyclotomy and Difference Sets, Lectures in Advanced Mathematics **2**, Markham, Chicago, 1967, which contains 41 references.]

There might also be something in

A.R. Rajwade, The period equation for primes p congruent to 1 (mod 5), *Proc. Cambridge Philos. Soc.*, **69**(1971) 153–155; MR **43** #1917; rNT T20-48.

Albert Leon Whiteman, The cyclotomic numbers of order ten, *Proc. Symp. Appl. Math.*, **10** 95–111, AMS, Providence RI, 1960; MR **22** #4682; rNT T20-24.

88:17 (Dick Katz via John Selfridge) Is $\frac{1}{8} + \frac{1}{16} + \frac{1}{64} + \frac{1}{128} + \frac{2}{256} + \frac{1}{512} + \frac{1}{2048} + \ldots$ rational, where the numerators are the numbers of "large" digits, 5, 6, 7, 8 or 9, in the decimal representation of 2^k?

Remark: The problem is to find generalizations, to other sets of digits, since Eugene Levine [Problem 386, *Coll. Math. J.*, **19**(1988) 448; solution, John P. Quinn, *ibid.* **21**(1990) 151–152, with generalizations by Levine and by Dave Ohlsen], asks readers to show that the sum is 2/9, as do Doug Bowman & Tad White in Advanced Problem 6609, *Amer. Math. Monthly*, **96**(1989) 743. In their original submission, Bowman & White also gave the example

$$\sum_{n\geq 0} \frac{f(n)}{2^n} = \frac{20}{89}$$

where, for each n, $f(n)$ is the sum of the Fibonacci numbers F_i over those i for which the i-th digit in the base 10 representation of 2^n is greater than 4. They asked for generalizations to other sets of digits and other bases. Unfortunately their paper, "On a problem of Levine", has run afoul of the large *Monthly* backlog. However, their discussion has been incorporated into the solution of Problem 6609, mentioned above [**98**(1991) 279–281].

89:18 (Sun Qi) If

$$f(x_1, \ldots, x_m) \in \mathrm{GF}(p)[x_1, \ldots, x_m]$$

and there are primitive roots $\alpha_1, \ldots, \alpha_m$ mod p such that $f(\alpha_1, \ldots, \alpha_m) \equiv 0 \bmod p$, then are there always primitive roots $\beta_1, \ldots, \beta_m$ mod p^l such that $f(\beta_1, \ldots, \beta_m) \equiv 0 \bmod p^l$?

Andy Granville, Andrew Odlyzko & Gerry Myerson have been looking into this. The last named writes (90-10-01):

Let g be an integer which is a primitive root mod p, but not mod p^2. Let $f(x_1, \ldots, x_m) = x_1 - g$. Then $f(x_1, \ldots, x_m) \in \mathbb{Z}[x_1, \ldots, x_m]$, and there are primitive roots $\alpha_1, \ldots, \alpha_m$ mod p such that $f(\alpha_1, \ldots, \alpha_m) \equiv 0 \bmod p$, but there are no primitive roots $\beta_1, \ldots, \beta_m$ mod p^2 such that $f(\beta_1, \ldots, \beta_m) \equiv 0 \bmod p^2$. It is this trivial counterexample that makes me feel that I don't understand the problem.

89:20 (Hugh Edgar) Characterize those positive integers n for which

$$\alpha + \beta + \gamma = \alpha\beta\gamma = 1 \tag{*}$$

is solvable in $\mathbb{Z}[\zeta_n]$.

Remarks. Since $1+i+(-i) = 1 \cdot i \cdot (-i) = 1$, all positive integer multiples of 4 qualify. The equations (*) are solvable in the ring of integers of $\mathbb{Q}(\theta)$, where $\mathrm{Irr}(\theta, X, \mathbb{Q}) = X^3 - X^2 - 4X - 1$. $\mathbb{Q}(\theta)$ is a cyclic cubic extension of $\mathbb{Q}$, and $\mathbb{Q}(\theta)$ is a subfield of $\mathbb{Q}(\zeta_{13})$ so all positive integer multiples of 13 qualify. Edgar notes that Andrew Bremner, *Manuscripta Math.*, **65**(1989) 479–487, shows that the field arising from $X^3 - X^2 - 4X - 1$ is the one and only cyclic cubic extension of $\mathbb{Q}$ on which (*) have solutions.

Solution (Bill McCallum via Hugh Edgar)

$$\epsilon_1 + \epsilon_2 + \epsilon_3 = \epsilon_1\epsilon_2\epsilon_3$$

if

$$\epsilon_k = \left(\frac{\zeta^{\frac{p+1}{2}}}{\eta_1\eta_2}\right)\eta_k \qquad (1 \le k \le 3)$$

where $\eta_1 = \zeta + \zeta^2$, $\eta_2 = \zeta^3 + \zeta^6 + \ldots + \zeta^{3(a-1)}$, $\eta_3 = \eta_1\eta_2$ and $\zeta = \zeta_p$ is a primitive p-th root of unity, p prime > 3, and $a \in \mathbb{Z}$ is chosen to satisfy $3a \equiv 2 \bmod p$. Thus the problem has solutions in $U_{\mathbb{Q}(\zeta_p)}$, the unit group of the p-th cyclotomic field for every prime $p > 3$.

Hugh Edgar would also like to know those primes for which (*) has a solution in $U_{\mathbb{Q}(\zeta_p+\zeta_p^{-1})}$, the unit group of the maximal real subfield of $\mathbb{Q}(\zeta_p)$. For $p = 5$ and $p = 13$ there are solutions, but he doesn't know what happens for any other odd prime $p \ge 7$.

89:29 (Mike Filaseta — from Emil Grosswald, Mar. '88, but not originating with him) For odd n the Legendre polynomials are divisible by x, but otherwise they are irreducible. Can two Legendre polynomials share the same non-trivial factor? Similar question for Hermite polynomials.

Mike Filaseta (90-10-15) sends two letters of Emil Grosswald, dated 88-03-30 & 88-05-16. He would state the problem and comments as follows:

Let $L_n(x)$ denote the n-th Legendre polynomial. Then it it not known if $L_n(x)$ is irreducible if n is even, or if $L_n(x)/x$ is irreducible if n is odd. Is it true that $\gcd(L_m(x), L_n(x))$ is either 1 or x whenever m and n are distinct integers ≥ 1?

(Emil Grosswald mentioned this problem to M. Filaseta in a letter dated 88-03-30. Later, in a letter dated 88-05-16, Emil states, "To the best of my knowledge, the first time [this problem was raised was] in a letter of Stieltjes to Hermite." He goes on to add, "If my memory is correct and Stieltjes's statement is more or less what I believe to remember, then the coprimality of any two Legendre polynomials was known to Stieltjes." What was Stieltjes's argument?)

89:31 (Gerry Myerson) A **covering set** is a set of $m \times m$ integer matrices such that $\bigcup_{A \in S} \mathbb{Z}^m A = \mathbb{Z}^m$, that is, for every integer row m-vector $\mathbf{h}$ there exists an integer row m-vector $\mathbf{k}$ and an element $A \in S$ such that $kA = h$.

(1) Find conditions on $\Delta_1, \Delta_2, \ldots$ such that there exists a covering set $S = [A_1, A_2, \ldots]$ with $\det A_j = \Delta_j$ for all j. (E.g., for every prime p there is a covering set of $p + 1$ matrices of determinant p)

(2) Is every left-covering a right-covering? I.e., does

$$\bigcup_{A \in S} \mathbb{Z}^m A = \mathbb{Z}^m \quad \text{imply} \quad \bigcup_{A \in S} A\mathbb{Z}^m = \mathbb{Z}^m?$$

A negative solution of (2) was given last year by Gerry Myerson who noted the particular case of (1): is there a finite covering (say in the case $m = 2$) with no two determinants equal in absolute value? Todd Cochrane of Kansas St. Univ. has answered this in the affirmative, using a set of covering congruences in which all the moduli are composite.

89:32 (Leo Chouinard via Bart Goddard) Let $0 < a_1 < a_2 < \ldots < a_n$ be integers. Consider inequalities of the forms $a_i + a_j < a_k$ or $a_i + a_j > a_k$. Note that the systems

$$\left\{ \begin{array}{rcl} a_i + a_j & < & a_k \\ a_i + a_j & > & a_{k+m} \end{array} \right. \quad \text{and} \quad \left\{ \begin{array}{rcl} a_i + a_j & > & a_k \\ a_{i+m} + a_j & < & a_k \end{array} \right.$$

are "obviously unsolvable".

(1) Are there any systems of inequalities of these forms which are unsolvable, but contain no obviously unsolvable subsystems?

(2) How about if $0 \leq a_1 \leq a_2 \leq \ldots \leq a_n$?

Remark: Andrew Odlyzko writes (90-09-14) that the answer to both parts is yes, at least in the stated form. Take the inequalities to be $a_5 < a_1 + a_2$ and $a_3 + a_4 < a_5$. These imply $a_3 + a_4 < a_1 + a_2$, which is clearly impossible. We need a better version of the problem.

PROBLEMS PROPOSED 90–12–17 & 20

90:01 (M.V. Subbarao via Dick Lehmer) Let $n \geq 1$ be an integer. Construct a sequence n_1, n_2, ... by $n_1 = n$,

$$n_{i+1} = \begin{cases} \frac{1}{2}d(n_i) & \text{if } n_i \text{ is not a square,} \\ \frac{1}{2}((2n_i - 1)d(n_i) + 1) & \text{if } n_i \text{ is a square,} \end{cases}$$

where $d(n)$ is the number of divisors of n.

1. Is it true that for each n the sequence leads to 1, 1, ... ?
2. Is it true that the number of distinct terms in the sequence is bounded, independent of n ?

Remark: John Rickert answered 2. in the negative: let $b_1 = 4$, $b_{j+1} = 2^{2b_j - 1}$ (so that $b_2 = 2^7 = 128$, $b_3 = 2^{255}$, ...) and take $n_1 = b_r$ so that $n_2 = b_{r-1}$, ... $n_r = b_1 = 4$, $n_{r+1} = 11$, $n_{r+2} = 1$, with $r + 2$ distinct terms.

90:02 (Dick Katz via Grigori Kolesnik) Let S be the set of all reals of the form $\sum_{n=0}^{\infty} a_n/n!$, $a_n = 0$ or 1. Are there any algebraic irrationals in S ?

Remark: Erdős & Spiro solved a related problem in the MONTHLY in the mid-80's.

Remark: (Paul Bateman) The same real numbers are considered in Problem 6634 , *Amer. Math. Monthly*, **97**(1990) 553, but from a totally different point of view. [R. W. Zeamer lets K be the field generated by S and asks if $K = \mathbf{R}$?]

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.

90:04 (from Florida via John Brillhart) For $n \geq 0$, let $N_n = \prod_{k=0}^{n}(k^2 + 1)$.

1. Is there an $n > 3$ for which N_n is square?

2. Do there exist $1 < n_1 < n_2$ such that N_{n_2}/N_{n_1} is square?

Solution: to 1. for sufficiently large n (Jeff Lagarias): Let P_n be the largest prime dividing N_n. Hooley [*Acta Math.*, **117**(1967) 281–299] proved

$$(1) \qquad P_n > n^{11/10}$$

for all sufficiently large n. See C. Hooley, *Applications of Sieve Methods to the Theory of Numbers*, Cambridge Univ. Press, 1976, Chap. 2, for a history of this problem.

If $P_n > 2n$ then P_n *exactly divides* N_n. Indeed, if P_n divides $j^2 + 1$, then, since $j \leq n$, $P_n^2 > 4n^2 \geq j^2 + 1$ so $P_n^2 \nmid (j^2 + 1)$. Moreover, the only residue classes m mod P_n with $P_n|(m^2 + 1)$ are $m \equiv \pm j$ mod P_n, and since $P_n > 2n$ the class $-j$ mod P_n has smallest representative $P_n - j > n$. Thus $P_n \| N_n$.

With (1) this shows that N_n is not a square for all $n > n_0$. Since the method of proof of (1) uses the Selberg sieve, it gives an effective constant and, in principle, one can find n_0 effectively. It remains to do this and check that $n = 3$ is the only solution with $n < n_0$.

90:05 (Neville Robbins) Are there arbitrarily large gaps between consecutive sums of two squares?

Solution: (Andy Odlyzko) Yes, since there are only $x/\sqrt{\ln x}$ sums of two squares up to x. (John Selfridge) Arbitrarily large gaps can be constructed by the Chinese remainder theorem: e.g. if $n \equiv 3 \bmod 9$, $n + 1 \equiv 7 \bmod 49$, $n + 2 \equiv 11 \bmod 121$, ..., where the moduli are the squares of distinct primes $\equiv 3 \bmod 4$, then none of n, $n + 1$, $n + 2$, ... can be a sum of 2 squares.

90:06 (Neville Robbins) Are there infinitely many n such that $4n$, $4n+1$, and $4n+2$ are all sums of two squares?

Solution: (Peter Montgomery) Yes, there are infinitely many solutions to the Pell equation $8x^2+1=y^2$, and $8x^2=(2x)^2+(2x)^2$, $8x^2+1=y^2+0^2$, $8x^2+2=(2x+1)^2+(2x-1)^2$ (or y^2+1^2). Also, if $a-1$, a, $a+1$ is a solution, so is a^2-1, a^2, a^2+1, since $a^2-1=(a-1)(a+1)$ and 8, 9, 10 generates an infinity of solutions. Again, let $u=4n^4+4n^2$, so that u, $u+1$, $u+2$ are all sums of two squares.

90:07 (Internet via Bob Silverman) Consider the set of areas of integer-sided right triangles, $ab(a^2-b^2)$, $a>b>0$, arranged in increasing order $A_1=6$, $A_2=24$, $\ldots$, $A_9=A_{10}=210$, $\ldots$. Is $n^{-2}A_n$ bounded?

Partial result: a counting argument shows

$$\#\{\text{pairs } (a,b) : ab(a^2-b^2)<n^2\} \geq Cn^{4/3}$$

for some constant C (on the other hand, it has been suggested that there are only Cn such pairs), so $n^{-2}A_n$ would be bounded if all the $ab(a^2-b^2)$ were distinct. However, many are duplicates.

90:08 (Keith Dennis via Andy Odlyzko; also Claudia Spiro) Let P be the smallest set of pairs of positive integers such that

1. (1,1) is in P,
2. if (x,y) is in P, then so is $(y,x+y)$,
3. if (x,y) and (x',y') are in P, then so is (xx',yy').

Let $S=\{x:(x,y)$ is in P for some $y\}$. Conjecture: S contains all positive integers with exactly 508 exceptions, the largest of which is about 55000. It is known that there are no other exceptions up to 5×10^7.

90:09 (Gene Smith) Let $p(x)$ be a polynomial with integer coefficients. Given a finite set S_i of primes such that $p(x)\equiv 0 \bmod q$ has a solution for every q in S_i, let n be the product of the elements of S_i, let S_i' be the primes that divide $p(n)$, and let $S_{i+1}=S_i\cup S_i'$. Given that S_1 is nonempty and that l is a prime such that $p(x)\equiv 0 \bmod l$ has a solution, must l be in S_i for some i ?

Remarks: Smith noted that one should not consider $p(x)=x^j$. Peter Montgomery pointed out that if $p(x)=x+2$ and $l=2$ is not in S_1, then l is not in any S_i. There was discussion of other polynomials to be avoided.

90:10 (Richard McIntosh) For x and y in [0,1], let L satisfy

1. $L(x) + L(1-x) = L(1)$,
2. $L(x) + L(y) = L(xy) + L(\frac{x(1-y)}{1-xy}) + L(\frac{y(1-x)}{1-xy})$

Is it true that $L(\beta) - L(\beta^3) = \frac{L(1)}{5}$, where $\beta = \frac{1}{2}(\sqrt{3+2\sqrt{5}} - 1)$ is a root of $\beta^4 + 2\beta^3 - \beta - 1$?

1. and 2. are satisfied by the Rogers L-function

$$L(x) = \sum_{n=1}^{\infty} \frac{x^n}{n^2} + \frac{1}{2} \ln x \ln(1-x), \ L(1) = \frac{\pi^2}{6}, \ L(0) = 0$$

Remark: For this function $L(\beta) - L(\beta^3)$ and $\pi^2/30$ agree to over 100 decimal places. It is rumored that McIntosh later proved the identity.

90:11 (Hugh Edgar) Let p and q be odd primes such that

$$1 + q + q^2 + \ \ldots \ + q^{x-1} = p^y$$

has a solution in integers x, y. Then $x = \mathrm{ord}_p q$ and $y = u\mathrm{ord}_q p$ for some u.

1. Must u be 1 ?
2. If $u = 1$, then $p^{\mathrm{ord}_q p} \equiv 1 + q \bmod q^2$. Is the converse true?

Reference: *UPINT* D10.

90:12 (Charles Nicol via John Selfridge) Let N_n be the concatenation of the first n positive integers. E.g. $N_{13} = 12345678910111213$. Are any of these numbers prime? Are infinitely many prime? Robert Baillie has found that there are no primes out to $n = 1000$.

90:13 (John Selfridge) Are there any odd perfect numbers of the form $n^3 + 1$? Or $n^n + 1$? [There is an even one, $3^3 + 1 = 28$.]

Solution: Peter Montgomery showed that $n^n + 1$ is not perfect if n is even. Submitted to the MONTHLY as an elementary problem, Jan. 1991.

90:14 (D.H. and Emma Lehmer) Let $p = n^2 + 108 = 6f + 1 = 109, 157, 229, 277, 397, \ldots$ be a prime, and

$$\eta_j = \sum_{i=0}^{f-1} \zeta_p^{g^{6i+j}}$$

(ζ_p is a primitive p-th root of unity) be the Gaussian periods of degree 6. Let

$$\delta_j = \eta_j - \eta_{j+k} \qquad\qquad k \perp 6$$

(i.e., k is prime to 6) Then the δ_j satisfy the sextic

$$G(x) = x^6 - p(x-1)^2(x-2)^2 = 0$$

so that

$$G(1) = \prod_{j=0}^{5}(\eta_j - \eta_{j+k} - 1) = 1$$

and hence $\rho_j = \eta_j - \eta_{j+k} - 1$ is a unit. Is ρ_j a fundamental unit? [These primes do not have translation units.]

For $e = 5$ there is only one prime, $p = 211$, known to have this property.

90:15 (Dick Bumby) The set of primes for which 2 has odd order is known to have density 7/24. Find a good estimate for the error.

Remarks: Basil Gordon gave two references of Hasse (see especially p. 23 of the latter) and said that the error term is the same as in the Čebotarev density theorem.

H. Hasse, Über die Dichte der Primzahlen p, für die eine vorgegebene ganzrationale Zahl $a \neq 0$ von durch eine vorgegebene Primzahl $l \neq 2$ teilbarer bzw. unteilbarer Ordnung mod p ist, *Math. Annalen*, **162**(1965) 74–76.

H. Hasse, Über die Dichte der Primzahlen p, für die eine vorgegebene ganzrationale Zahl $a \neq 0$ von gerade bzw. ungerader Ordnung mod p ist, *Math. Annalen*, **166**(1966) 19–23.

Lagarias mentioned a paper of Odoni:

A conjecture of Krishnamurthy on decimal periods and some allied problems, *J. Number Theory*, **93**(1981) 303–319; *MR* **83a**:10098.

90:16 (Jim Propp via Robby Robson & Jeff Lagarias) For m even, let $k(m)$ be the number of ways of tiling an $m \times m$ checkerboard with dominoes. It is known that $k(m)$ is a square if 4 divides m, otherwise twice a square. Find a combinatorial proof. Note that tilings related by symmetries of the square are counted separately.

Kasteleyn, Statistics of dimers on a lattice, *Physica*, (1961) 1209–1225.

M. Fisher, *Phys. Rev.*, **124**(1961) #6

90:17 (Bob Silverman) Find an upper bound, in terms of n and k, for the number of doubly stochastic $n \times n$ matrices with k distinct entries. The entries are to be rationals in [0,1], and are to include both 0 and 1. Also, for a given n, find the set of k numbers which achieves the maximum.

Remark: You can make more doubly stochastic matrices from $\{0, \frac{1}{2}, 1\}$ than from $\{0, \alpha, 1\}$ for any $\alpha \neq \frac{1}{2}$, but it is not known how many such $n \times n$ matrices can be made from $\{0, \frac{1}{2}, 1\}$.

Solution: Jeff Lagarias lets $S(a)$ denote the number of $n \times n$ doubly stochastic matrices having all entries either 0 or drawn from $a = \{a_1, \ldots, a_r\}$, where all $a_i > 0$. He also lets $S_n(r)$ denote the maximum of $S(a)$ over all sets **a** of cardinality r and proves that

$$(r+1)^{n^2} \geq S_n(r) \geq (r+1)^{n^2 - O(n^{3/2} \ln n)}$$

as $n \to \infty$. He notes that the set **a** achieving the maximum changes with n.

For even n Andrew Odlyzko obtains the better lower bound

$$(r+1)^{n^2 - O(n \ln n)}$$

.

90:18 (Hugh Edgar) Among all n with the property that there is no odd number k with $\phi(k) = \phi(n)$, find one divisible by as small a power of 2 as possible.

Remark: This is essentially MONTHLY problem E 3361, **97**(1990) 63. Lorraine Foster gave the minimal counterexample, $2^9 \cdot 257^2$ (**98**(1991) 443); this was also found by Selfridge. For the minimal power of 2, Gerry Myerson gives $2^2 \cdot 3 \cdot 5 \cdot 17 \cdot 257 \cdot 65537$. Non-minimal counterexamples were given by Edgar, the proposer of the MONTHLY problem, 64 other readers, and in Sierpiński's *Elementary Theory of Numbers.* Basil Gordon said the problem was proposed in the 1920's by Gassmann (?)

90:19 (Bart Stoddard) Can you reconstruct an $n \times n$ 0–1 matrix from its row, column and diagonal sums? The diagonals intended are the (broken) diagonals parallel to the principal diagonal. If not, how many different matrices can have the same data?

Solution: Peter Montgomery gave

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix} \qquad \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

and noted that larger matrices can be built up therefrom, yielding as many as $2^{(n/3)^2}$ different matrices, depending on how nonsparse the matrices are allowed to be.