Western Number Theory Problems, 1991–12–19 & 22

Edited by Richard K. Guy

for mailing prior to 1992 (Corvallis) 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 (present set)	91:01–91:25
1992 Corvallis			

[With comments on earlier problems:
76:15, 76:44, 86:18, 87:02, 88:09, 88:12, 89:20, 90:07, 90:10, 90:17, 90:18, 90:20.]

UPINT = Richard K. Guy, Unsolved Problems in Number Theory, Springer, 1981. Second edition going to press any minute now.

COMMENTS ON ANY PROBLEM WELCOME AT ANY TIME

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

92-08-20.

Request for copies of correspondence

Dr. Robin Rider at the Bancroft Library on the University of California Berkeley campus has stated that any correspondence that you may have had with D. H. Lehmer would be most welcome at the Bancroft Library. As you may know, Dick Lehmer's papers and journals are to be archived there, and they welcome copies of his correspondence, or the originals if you don't plan to keep them. Please send such material to

Dr. Robin Rider,
Bancroft Library,
University of California,
Berkeley CA 94720, U.S.A.

John Brillhart supplies a list of Dick Lehmer's students:

Donald Marvin Adelman, Some arithmetic properties of sequences of integers satisfying linear recursion sequences, June 1947.

Henry Ludwig Alder, The existence and nonexistence of certain identities in the theory of partitions, June 1947.

Tom Mike Apostol, A study of Dedekind sums and their generalizations, September 1948.

Jayanthi Chidambaraswamy, Divisibility properties of certain factorials, June 1964.

John Brillhart, On the Euler and Bernoulli polynomials, March 1967.

David Friedman, Cubic character sums and congruences, June 1967.

Ronald Lewis Graham, On finite sums of rational numbers, September 1962.

James Brown Herreschoff, A theorem on character sums, December 1968.

Nand Kishore, Arithmetical properties of Bessel functions, September 1961.

William Haddock Simons, Modular functions of stufe 2, September 1947.

David Breyer Singmaster, On means of differences of consecutive integers relatively prime to m, December 1966.

Robert Samuel Spira, Sums of two squares and Bramahgupta's formula, September 1962.

Harold Mead Stark, On the tenth complex quadratic field with class number one, June 1964.

Richard P. Stauduhar, The automatic determination of Galois groups, September 1969.

Donald Dines Wall, Normal numbers, September 1949.

Peter Jay Weinberger, Proof of a conjecture of Gauss on class number two, September 1969.

Mark Brimhall Wells, Simplification of normal form expressions for Boolean functions of many variables, June 1961.

Jonathan David Young, Application of linear programming to the numerical solution of linear differential equations, June 1962.

Alan Zame, On the distribution of the fractional parts of certain sequences, September 1965.

Preprints of

J. Buhler, H. W. Lenstra & C. Pomerance, Factoring integers with the number field sieve.

The sign up sheet at Asilomar was lost. Interested persons may write to

Carl Pomerance,
Department of Mathematics,
Boyd Graduate Studies Research Centre,
Franklin College of Arts and Sciences,
The University of Georgia,
Athens GA 30602, U.S.A.

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 $3^2 - 2^3 = 2^0$; $5^3 - 11^2 = 2^2$; $5^2 - 3^2 = 2^4$.

Reese Scott's paper "On the equations $p^x - q^y = c$ and $|p^x - q^y| = c$" has been accepted for publication by *J. Number Theory*. He proves that, except in a few given cases, there is at most one solution to $p^x - q^y = c$ with the parity of y fixed. In fact $|p^x - q^y| = c$ has 3 solutions only for the choices $(p, q, c) = (2, 3, 1)$, (2,3,5), (2,5,3). See also **91:09** below.

76:44 (Carl Pomerance) For $n = 210$, $n - p$ is prime for all p with $n/2 < p < n$. Are there any larger n with this property?

No! Jean-Marc Deshouillers, Andrew Granville, W. Narkiewicz & Carl Pomerance, An upper bound in Goldbach's problem (preprint) used explicit sieve estimates and explicit versions of Bertrand's postulate in arithmetic progressions.

86:18 (P. Erdős, C. B. Lacampagne & J. L. Selfridge) Define the **deficiency** of the binomial coefficient $\binom{n+k}{k}$, $k \le n$, as the number of i for which $b_i = 1$, where $n + i = a_i b_1$, $1 \le i \le k$, the prime factors of b_i are greater than k, and $\prod a_i = k!$

$$\binom{44}{8}, \quad \binom{74}{10}, \quad \binom{174}{12} \quad \text{and} \quad \binom{239}{14} \quad \text{have deficiency 2;}$$

$$\binom{46}{10}, \quad \binom{47}{10} \quad \text{and} \quad \binom{241}{16} \quad \text{have deficiency 3;}$$

$$\binom{47}{11} \quad \text{has deficiency 4; and} \quad \binom{284}{28} \quad \text{has deficiency 9.}$$

Are there others with deficiency greater than 1? Only finitely many? Are there infinitely many with deficiency 1?

Remark: Additional deficient binomial coefficients include

$$\binom{5179}{27}, \quad \binom{8113}{28}, \quad \binom{8114}{28}, \quad \binom{96022}{42},$$

each of deficiency 2, and

$$\binom{2105}{25}, \quad \binom{1119}{27}, \quad \binom{6459}{33},$$

each of deficiency 3. These are the only binomial coefficients with $k + n < k^3$ and $k \leq 101$ which have deficiencies. Compare **91:03** below.

87:02 (Alvan Beall & Bob Morris, via Blair Kelly) Computer experiments suggest that rows 1, 2, 3, 4, 5, 9, 14, 17, 18, 20, 21, 35 & 41 of Pascal's triangle, and no others, consist entirely of numbers representable as the sum of three squares. Is that true?

Yes. Andrew Granville & Zhu Yiliang, Representing binomial coefficients as sums of squares, *Amer. Math. Monthly*, **97**(1990) 486–493; *MR* **92b**:11009.

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?

Remark: The exact reference to the affirmative solution is:

Roger W. Barnard, W. Dayawansa, K. Pearce & David A. Weinberg, Polynomials with nonnegative coefficients, *Proc. Amer. Math. Soc.*, **113**(1991) 77–85.

88:12 Replace by **91:19** below.

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

$$\alpha + \beta + \gamma = \alpha\beta\gamma = 1$$

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

Remarks. In connexion with the "Solution" Hugh Edgar apologizes that in reporting on Bill McCallum's clever triple, which has the "ESP" (equal sum & product) property, he didn't point out that the ESP was **not** $= 1$, so that the solution was in fact to a slightly different problem. See **91:10** below.

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?

Solution: (Andrew Granville) The number of pairs of integers $a > b > 0$ with $ab(a^2 - b^2) < n^2$ is

$$Cn + O(n^{2/3}) \quad \text{where} \quad C = \frac{1}{2}\int_1^\infty \frac{du}{\sqrt{u^3 - u}}$$

Proof: Let $d = a - b \geq 1$. Evidently

$$bd(d+b)(d+2b) = ab(a^2 - b^2) < n^2$$

so that $b < n^{2/3}$. So we wish to find

$$\sum_{1 \leq b \leq \lfloor n^{2/3} \rfloor} \{x_b + O(1)\}$$

where x_b is the positive real root of $bx(x+b)(x+2b) = n^2$. Now

$$\begin{aligned}
\sum_{1 \leq b \leq \lfloor n^{2/3} \rfloor} x_b &= \int_1^{\lfloor n^{2/3} \rfloor} x_b \, db + O\left(\sum_{b=1}^{\lfloor n^{2/3} \rfloor} (x_{b+1} - x_b)\right) \\
&= \int_1^{n^{2/3}} x_b \, db + O(x_1) \\
&= \int_1^{n^{2/3}} bt_b \, db + O(n^{2/3})
\end{aligned}$$

where $x_b = bt_b$ so that $t = t_b$ satisfies $t(t+1)(t+2) = n^2 b^{-4}$

Now $d\{t(t+1)(t+2)\} = -4n^2 b^{-5} db = \frac{-4n^3 b\, db}{nb^6} = -\frac{4}{n}\{t(t+1)(t+2)\}^{3/2} b\, db$. Therefore

$$\begin{aligned}
\int_1^{n^{2/3}} bt_b \, db &= -\frac{n}{4}\int_{b=1}^{b=n^{2/3}} t \frac{d\{t(t+1)(t+2)\}}{(t(t+1)(t+2))^{3/2}} \\
&= \frac{n}{2}\left\{\left[\frac{t}{\sqrt{t(t+1)(t+2)}}\right]_{b=1}^{b=n^{2/3}} - \int_{b=1}^{b=n^{2/3}} \frac{dt}{\sqrt{t(t+1)(t+2)}}\right\}
\end{aligned}$$

Now if $b = 1$ then $t = n^{2/3} + O(1)$ and if $b = n^{2/3}$ then $t = \frac{1}{2}n^{-2/3}\{1 + O(n^{-2/3})\}$. Therefore

$$\begin{aligned}
\int_1^{n^{2/3}} bt_b \, db &= \frac{n}{2}\left\{O(n^{-1/3}) + \int_{\frac{1}{2}n^{-2/3} + O(n^{-4/3})}^{n^{2/3} + O(1)} \frac{dt}{\sqrt{t(t+1)(t+2)}}\right\} \\
&= \frac{n}{2}\int_0^\infty \frac{dt}{\sqrt{t(t+1)(t+2)}} + O(n^{2/3})
\end{aligned}$$

and the result follows from combining the above results and taking $t + 1 = u$ in the integral.

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. McIntosh later proved the identity.

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 $S(\mathbf{a})$ denote the number of $n \times n$ doubly stochastic matrices having all entries either 0 or drawn from $\mathbf{a} = \{a_1, \ldots, a_r\}$, where all $a_i > 0$. He also lets $S_n(r)$ denote the maximum of $S(\mathbf{a})$ over all sets $\mathbf{a}$ 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 $\mathbf{a}$ which achieves the maximum, changes with n.

For even n Andrew Odlyzko obtains the better lower bound

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

by considering $\mathbf{a} = \{0, \frac{2}{rn}, \frac{4}{rn}, \ldots, \frac{2}{r}\}$ and the set T of $n \times (n/2)$ matrices from $\mathbf{a}$, all of whose column sums are 1. By the multinomial theorem, there are

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

of them, since each column can be chosen independently of the others. Since each row sum must be in $\{0, \frac{2}{rn}, \frac{4}{rn}, \ldots, 1\}$, there are $2n/2+1$ possible row sums, and so for some set of row sums r_1, ..., r_n, the set V of matrices of T with those row sums has cardinality at least of the form $(*)$. But now to each matrix in V associate the matrix in V', obtained by replacing, in matrices of V, each 0 by $2/n$, each $2/rn$ by $2/n - 2/rn$, etc. This gives the desired bound.

[**90:18**] The **Remark:** of Basil Gordon, printed at this point in the 1990 problems set, did not concern **90:18**, but applied to the previously unnumbered problem:

90:20 (W. Narkiewicz via Hugh Edgar) Given two algebraic number fields K and L, does the coincidence of their Dedekind zeta functions, $\zeta_K = \zeta_L$, imply that K and L also share the same number of ideal classes?

about which **Daniel C. Mayer** writes:

Denote by C_K and C_L the ideal class groups of K and L. If $\zeta_K = \zeta_L$ and K is isomorphic (conjugate) to L, then, of course, C_K and C_L are also isomorphic. Hence it remains to investigate so-called **arithmetically equivalent** fields, i.e. non-isomorphic fields K and L with $\zeta_K = \zeta_L$.

The actual existence of a pair of such fields, both of degree 180 over the rationals, with common normal field N having S_6 as Galois group $\mathrm{Gal}(N/\mathbf{Q})$ (and thus of degree 720) was first established in section 3 of

1. Fritz Gaßmann, Bemerkungen zur vorstehenden Arbeit von Hurwitz, *Math. Z.*, **25**(1926) 665–675.

This result of Gaßmann is also discussed in §25 of

2. Helmut Hasse, Bericht über neuere Untersuchengen und Probleme aus der Theorie der algebraischen Zahlkörper, Teil II: Reziprozitätsgesetz, *Jber. DMV* (1930) 1–204

and in Exercises 6.3 and 6.4 of

3. J. W. S. Cassels & A. Fröhlich, Algebraic Number Theory, *Proc. Brighton Conf.*, Academic Press, 1967.

More convenient examples of arithmetically equivalent fields of degree only 7 over $\mathbf{Q}$, and important characterizations have been provided in

4. Robert Perlis, On the equation $\zeta_K(s) = \zeta_{K'}(s)$, *J. Number Theory*, **9**(1977) 342–360,

where he

(a) shows that there are no arithmetically equivalent fields of degree ≤ 6 over $\mathbf{Q}$,

(b) constructs two infinite families of arithmetically equivalent couples, one with the aid of the cohomology of split group extensions, the other by means of permutation representations,

(c) shows that $\zeta_K = \zeta_L$ implies the coincidence of the degree over $\mathbf{Q}$, discriminants, ramified primes, number of real and complex archimedean valuations, normal closure, and normal core of K and L,

(d) proves that $\zeta_K = \zeta_L$ if and only if for all non-ramified primes the decomposition (i.e., the collection of degrees of the factors) is the same in K and L.

5. Robert Perlis, A remark about zeta-functions of number fields of prime degree, *J. reine angew. Math.*, **293/294**(1977) 435–436,

6. Robert Perlis, On the class numbers of arithmetically equivalent fields, *J. Number Theory*, **10**(1978) 489–509,

where it is shown that

(e) $\zeta_K = \zeta_L$ if and only if the permutation representations of the group $\mathrm{Gal}(N|Q)$ of the common normal field N of K and L induced by the unit representations of $\mathrm{Gal}(N|K)$ and $\mathrm{Gal}(N|L)$ are isomorphic linear representations,

(f) $\zeta_K = \zeta_L$ implies that $\#C_K \cdot R_K = \#C_L \cdot R_L$ (R_K, R_L are the regulators), and, moreover, even $\mathrm{Syl}_p C_K \simeq \mathrm{Syl}_p C_L$ (Sylow subgroups) for all primes p which do not divide a certain **invariant** divisible at most by prime factors of the degree $[N : K]$ $(= [N : L])$.

A generalization of arithmetical equivalence for **relative extensions** K and L over an arbitrary ground field $\mathbf{k}$ (not necessarily $\mathbf{k} = \mathbf{Q}$) has been developed in

7. Norbert Klingen, Zahlkörper mit gleicher Primzerlegung, Habilitationsschrift, Univ. Köln, *J. reine angew. Math.*, **299/300**(1977) 342–384.

PROBLEMS PROPOSED 91-12-19 & 22

91:01 (Paul Erdős) Let $1 \leq a_1 < a_2 < \ldots < a_k \leq n$, $k > cn$. Is it true that if $n > n_0(c)$, there are always three a_i which have pairwise the same least common multiple? More generally, are there r of the a_i which have pairwise the same least common multiple?

Pomerance asks: can one prove that there are three a_i so that the least common multiple of every two has the same prime factors?

Perhaps a related combinatorial problem asks: Let $|S| = n$, $A_i \subset S$ for $1 \leq i \leq t_n$. What is the smallest t_n which ensures that there are three A_i which have pairwise the same union?

91:02 (Paul Erdős) Is it true that if $1 \leq a_1 < a_2 < \ldots < a_{n+2} \leq 2n$, 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.

Solution: (Carl Pomerance) We show that this is false for $n = 2k$, where k is odd, $k \geq 5$. Indeed, suppose that $\{a_1, \ldots, a_{n+2}\}$ is

$$\{k-1, k, k+1, \frac{3k-1}{2}, \frac{3k+1}{2}\} \cup \{2k, 2k+1, \ldots, 4k\} \setminus \{2k+1, \frac{5k+1}{2}, 3k, \frac{7k+1}{2}\}.$$

Note that the four numbers deleted are a_2+a_3, a_3+a_4, a_4+a_5 and a_5+a_6. Also $a_1+a_2+a_3 = a_4+a_5$ and $a_2+a_3+a_4 = a_5+a_6$. Further, $a_3+a_4+a_5 > 4k$ and $a_1+a_2+a_3+a_4 > 4k$. Finally note that since $k \geq 5$, we have $k+1 < \frac{3k-1}{2}$ and $\frac{3k+1}{2} < 2k$.

Example: $\underline{k=5}$ {4,5,6,7,8,10,12,14,16,17,19,20}.

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: Compare **86:18** above. Deficient binomial coefficients must have $n+k \geq g(k)$. Carole later wrote that Paul has proved that $g(k) > ck^2/\ln k$ for k large, and that Andrew Granville thinks that he may be able to prove $g(k)$ greater than any power of k for k sufficiently large.

91:04 (Paul Erdős) Let $a_1 < a_2 < \ldots < a_k \leq n$ be a Sidon sequence, i.e., all the sums $a_i + a_j$ are distinct. Is it true that

$$\frac{1}{\ln x} \sum_{a_i+a_j \leq x} \frac{1}{a_i+a_j} \to 0$$

as $x \to \infty$? In fact perhaps

$$\sum_{a_i+a_j<x} \frac{1}{a_i+a_j} < c_1 \ln\ln x.$$

It is known that it can be $> c_2 \ln\ln x$.

91:05 (Paul Erdős) Let $a_1 < a_2 < \ldots < a_k$ be a Sidon sequence (see **91:04**). Can it be prolonged to a **perfect difference set**, i.e.,

$$a_1 < a_2 < \ldots < a_k < a_{k+1} < \ldots < a_{p+1} = p^2 + p + 1$$

so that the differences $a_u - a_v$, $1 \leq u, v \leq p+1$, $u \neq v$, represent every nonzero residue mod $p^2 + p + 1$ exactly once?

I could not even decide if it can be prolonged to

$$a_1 < a_2 < \ldots < a_k < a_{k+1} < \ldots < a_n, \quad a_n < (1 + o(1))n^2,$$

i.e., if it can be made as dense as possible asymptotically.

Is it true that for every $\epsilon > 0$ there is an infinite Sidon sequence $a_n < n^{2+\epsilon}$ for $n > n_0(\epsilon)$? Rényi & I proved [see Halberstam & Roth, Sequences, Oxford, 1966, p. 111, Theorem 2] that there is a sequence satisfying $a_n < n^{2+\epsilon}$ for which the number of solutions of $a_i + a_j = t$ is $\leq k$. Also Ajtai, Komlós & Szemerédi proved that there is a Sidon sequence satisfying $a_n < cn^3/\ln n$.

Let $a_1 < a_2 < \ldots < a_n$ be any sequence of integers. Is it true that it contains a Sidon subsequence $a_{i_1}, \ldots, a_{i_m}$ with $m = (1 + o(1))n^{\frac{1}{2}}$? Komlós, Sulyork & Szemerédi proved this with $m > cn^{\frac{1}{2}}$.

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 $1 + \ln\ln a_n \leq$

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

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.

91:07 (Bruce Berndt via David Boyd) Let $\phi(q) = \sum_{n=-\infty}^{\infty} q^{n^2}$, $\psi(q) = \sum_{n=0}^{\infty} q^{n(n+1)/2}$.

Ramanujan found that

$$\frac{\phi^3(q)}{\phi(q^3)} = 1 + 6\sum_{n=0}^{\infty}\left(\frac{(-1)^n q^{3n+1}}{1+(-q)^{3n+1}} + \frac{(-1)^n q^{3n+2}}{1+(-q)^{3n+2}}\right)$$

$$\frac{\psi^3(q)}{\psi(q^3)} = 1 + 3\sum_{n=0}^{\infty}\left(\frac{q^{6n+1}}{1-q^{6n+1}} - \frac{q^{6n+5}}{1-q^{6n+5}}\right)$$

[See Berndt's Ramanujan's Notebooks, Part III, pp. 226–229 for proofs.]

The right sides have obvious arithmetical interpretations in terms of divisŏr functions. What is being counted on the left side?

Note: The coefficient of q^n in $\phi^3(q)$ is $r_3(n)$, the number of representations of n as a sum of three squares. The coefficient of q^n in $\psi^3(q)$ is the number of ways n can be represented as a sum of three triangular numbers, which, by Gauß, is > 0.

91:08 (Neville Robbins) Is 13 the largest prime p for which $bc \equiv 1 \bmod p$ has no solutions with $1 < b, c < p/2$?

Solution: (Carl Pomerance) We shall show that this is indeed the case. What is needed is to show that for each prime $p > 13$, there are integers a, b, c with $ap + 1 = bc$ and $1 < b, c < p/2$. We consider three ranges: $13 < p \leq 100$, $100 < p \leq 400$ and $p > 400$.

Note that if $(p+1)/2$ is composite, so that it is mn for some m, n with $1 < m \leq n \leq (p+1)/4$, then $p + 1 = (2m)n$ shows we are done for p, namely we let $a = 1$, $b = 2m$ ($\leq p/2$ for $p > 13$), $c = n$. Thus in the range $13 < p \leq 100$ we only have to worry about $p = 37, 61, 73$. But $2 \cdot 37 + 1 = 5 \cdot 15$, $3 \cdot 61 + 1 = 8 \cdot 23$ and $2 \cdot 73 + 1 = 7 \cdot 21$. This completes the first range.

Let q be the least number for which $q \nmid (p - 1)$. I claim that if $p > 100$, then

$$2 < q < \sqrt{\frac{p}{2}}. \tag{1}$$

Indeed, [4,5,6,7]=420, so that if p is in the second range, then not all of 4,5,6,7 can divide $p - 1$. Thus for these p, we have $q \leq 7 < \sqrt{\frac{p}{2}}$ and (1) holds. Now assume $p > 400$. Note that then

$$\left[\left\lfloor\sqrt{\frac{p}{2}}\right\rfloor, \left\lfloor\sqrt{\frac{p}{2}}\right\rfloor - 1, \left\lfloor\sqrt{\frac{p}{2}}\right\rfloor - 2\right] \geq \frac{1}{2}\left(\left\lfloor\sqrt{\frac{p}{2}}\right\rfloor\right)\left(\left\lfloor\sqrt{\frac{p}{2}}\right\rfloor - 1\right)\left(\left\lfloor\sqrt{\frac{p}{2}}\right\rfloor - 2\right) > \frac{1}{2}\left(\sqrt{\frac{p}{2}} - 3\right)^3 > p,$$

so that not all three of $\left\lfloor\sqrt{\frac{p}{2}}\right\rfloor$, $\left\lfloor\sqrt{\frac{p}{2}}\right\rfloor - 1$, $\left\lfloor\sqrt{\frac{p}{2}}\right\rfloor - 2$ can divide $p - 1$. Thus (1) holds if $p > 400$.

Assume now that p is either in the second or third range, so that (1) holds. Let a be the least positive solution to

$$ap + 1 \equiv 0 \bmod q. \tag{2}$$

Then $1 \leq a \leq q - 2$. That is, $q \nmid p - 1$ implies $a \neq q - 1$. Thus $a + 1 < q$, and by the minimality of q, we have $(a + 1) | (p - 1)$. That is,

$$ap + 1 \equiv 0 \bmod (a + 1) \tag{3}$$

holds. Let $b = [a + 1, q]$. From (2) and (3) there is some integer c with $ap + 1 = bc$. Now by (1), $1 < 2a + 2 \leq b \leq (a + 1)q < q^2 < \frac{p}{2}$. Also

$$c = \frac{ap + 1}{b} \leq \frac{ap + 1}{2a + 2} < \frac{ap + p}{2a + 2} = \frac{p}{2},$$

so we are done.

91:09 (Reese Scott, via Hugh Edgar) Assume that p and q are given primes and c a given positive integer; can we show that if $p^x - q^y = c$ has a solution with y even, then it has no solution with y odd?

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

Remarks: "Yes" for $p = 5$, $p = 13$. What about $p = 7$?

Hugh Edgar reports that the question has been solved by Tony Costa, The American University, Washington DC:

$$\left\{1, \epsilon, \frac{\epsilon + 1}{\epsilon - 1}\right\}$$

is an ESP triple in $\mathbb{Z}[\zeta_p + \zeta_p^{-1}]^*$, i.e., the unit group of $\mathbb{Z}[\zeta_p + \zeta_p^{-1}]$, whenever the prime p satisfies $p > 5$ and where $\epsilon = 2\cos\frac{2\pi}{p}$.

91:11 (Gene Smith) It is known that there are triangles with rational sides and area (Heron triangles); are there tetrahedra with rational edges, face-areas and volume?

Remark: This was asked as problem **D22** of *UPINT*. A tentative draft for the second edition currently reads as follows (comments still very welcome):

D22 Are there simplexes in any number of dimensions, all of whose contents (lengths, areas, volumes, hypervolumes) are rational? The answer is "yes" in two dimensions; there are infinitely many **Heron triangles** with rational sides and area. An example is a triangle of sides 13, 14, 15 which has area 84. The answer is also "yes" in three dimensions, but can all tetrahedra be approximated arbitrarily closely by such rational ones?

John Leech notes that four copies of an acute-angled Heron triangle will fit together to form such a tetrahedron, provided that the volume is made rational, and this is not difficult. E.g., three pairs of opposite edges of lengths 148, 195, 203. Is there a smaller example? He also suggests examining references on p. 224 of Vol II of Dickson's *History*:

R. Güntsche, *Sitzungsber. Berlin Math. Gesell.*, **6**(1907) 38–53.

R. Güntsche, *Archiv Math. Phys.*(3), **11**(1907) 371.

E. Haentzschel, *Sitzungsber. Berlin Math. Gesell.*, **12**(1913) 101–108 & **17**(1918) 37–39 (& *cf.* **14**(1915) 371).

O. Schultz, Ueber Tetraeder mit rationalen Masszahlen der Kantenlängen und des Volumen, Halle, 1914, 292 pp.

Dickson appealed for a copy of this last. Did he ever get one? Does anyone know of a copy? Would they be willing to donate it, or offer it for sale, to the Strens Collection?

Leech also notes that this problem is answered positively in three dimensions by solutions to Problem 3 in **D18**. This problem was published as Problem 930 in *Crux Mathematicorum*, **10**(1984) #3, p. 89, and the solution by the COPS (presumably an acronyn for the Carleton (Ottawa) Problem Solvers) is:

Take a tetrahedron with a path of three mutually perpendicular edges, $a = p^2q^2 - r^2s^2$, $b = 2pqrs$, $c = p^2r^2 - q^2s^2$. Then $a^2 + b^2$, $b^2 + c^2$ are squares and $a^2 + b^2 + c^2 = (p^4 + s^4)(q^4 + r^4)$

is a square if

$$p^4 + s^4 = q^4 + r^4.$$

[John Leech notes "but not only if" and gives four casual examples, $(1^4+2^4)(2^4+13^4) = 697^2$; $(1^4+2^4)(38^4+43^4) = 9673^2$; $(1^4+2^4)(314^4+863^4) = 1275643^2$; $(1^4+3^4)(9^4+437^4) = 1729298^2$, which imply further ones of type $(2^4+13^4)(38^4+43^4)$.]

This equation was solved by Euler. The solution mentioned in **D9** is

$$\begin{aligned} p,\ q &= x^7 + x^5y^2 - 2x^3y^4 \pm 3x^2y^5 + xy^6 \\ r,\ s &= x^6y \pm 3x^5y^2 - 2x^4y^3 + x^2y^5 + y^7 \end{aligned}$$

"but this is not in any sense complete". The smallest solution of equal sums of pairs of fourth powers is $x = 1$, $y = 2$, $p = 133$, $q = -59$, $r = 158$, $s = 134$.

Buchholz found that the only rational tetrahedron with edge lengths ≤ 156 was that with edge lengths 117, 80, 53, 52, 51, 84, face areas 1800, 1890, 2016, 1170, and volume 18144. He also shows that a *regular* d-dimensional simplex with rational edge has rational d-dimensional volume just if d is of shape $4k(k+1)$ or $2k^2 - 1$.

Ralph Heiner Buchholz, Perfect pyramids, *Bull. Austral. Math. Soc.*, **45**(1991) 353–368.

Kevin L. Dove & John L. Sumner, Tetrahedra with integer edges and integer volume, *Math. Mag.*, **65**(1992) 104–111.

K. È. Kalyamanova, Rational tetrahedra (Russian), *Izv. Vyssh. Uchebn. Zaved. Mat.*, **1990** 73–75; *MR* **92b**:11014.

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

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

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

91:13 (Kevin O'Bryant via Bart Goddard) $D'(n)$ is the least possible maximum difference between (vertically or horizontally) adjacent entries when the numbers 1, 2, ..., n^2 are placed on an $n \times n$ chessboard. For example,

7	11	14	16
4	8	12	15
2	5	9	13
1	3	6	10

generalizes to show that $D'(n) \leq n$ and we believe that equality has been proved. [Can anyone supply a solution? or a reference?] For the corresponding problem on an $n \times (n-1)$ board, establish equality in $D(n) \leq n - 1$.

91:14 (Hugo Sun) A **magic square** on a group G is an $n \times n$ matrix whose entries are distinct elements of the group G such that the product (or sum depending on the group operation) of each row, column and diagonal all equal the same group element. Thus, the usual magic square of order n is a magic square over the cyclic group of order n^2 if we use 0, 1, 2, ..., $n^2 - 1$ instead of 1, 2, ..., n^2.

Problem: Does there exist a magic square on a nonabelian group of order 16? ... of order n^2?

Solution: (Peter Montgomery) A magic square for two nonabelian groups of order 16. Use quaternions $i^2 = j^2 = k^2 = -1$, $ijk = 1$, with an extra element x commuting with i, j, k and $x^2 = \pm 1$

$$\begin{array}{cccc} ix & -i & i & -ix \\ j & -jx & jx & -j \\ kx & -k & k & -kx \\ 1 & -x & x & -1 \end{array}$$

All row, column and diagonal products are x^2.

91:15 (Paul Erdős & Ron Graham) Is it true that any coloring of the integers with k colors gives a monochromatic solution of

$$\sum \frac{1}{x_i} = 1, \quad x_1 < x_2 < \ldots \quad \text{(finite sum)?}$$

This is open even for $k = 2$. If the answer is affirmative, let $f(k)$ be the smallest integer for which every k-coloring of the integers $1 \le t \le f(k)$ contains a monochromatic solution. Determine or estimate $f(k)$.

91:16 (Paul Erdős) Is it true that if

$$\frac{1}{x_1} + \frac{1}{x_2} + \ldots + \frac{1}{x_n} = 1, \quad x_1 < x_2 < \ldots < x_n$$

then $\liminf \frac{x_n}{x_1} > e$? It is trivial that the limit is $\ge e$. In fact perhaps it is infinite.

91:17 (Paul Erdős) Is it true that for every solution of

$$\frac{1}{x_1} + \frac{1}{x_2} + \ldots + \frac{1}{x_n} = 1,$$

$\max(x_{i+1} - x_i) \ge 3$? {2,3,6} shows that > 3 is not true but perhaps this is the only counterexample. Perhaps $\max(x_{i+1} - x_i) \le k$ has only a finite number of solutions.

91:18 (Paul Erdős & I. Jóó) Let $1 < q < 1 + \epsilon$. Consider all the numbers

$$\sum_{i=0}^{n} \epsilon_i q^i, \quad \epsilon_i = 0 \text{ or } 1, \quad 1 \le n < \infty$$

ordered by size, $1 < x_1 < x_2 < \ldots$. Prove that if ϵ is sufficiently small then $x_{k+1} - x_k \to 0$. Perhaps if $q < q_0$, $q_0^3 = q_0 + 1$ (the smallest Pisot-Vijayaraghavan number) then $x_{k+1} - x_k \to 0$.

91:19 (D. H. & Emma Lehmer) Find the relation between the primitive root g used in generating the cyclotomy of degree e and the sign of M in

$$4p = L^2 + 27M^2, \quad L \equiv 1 \bmod 6 \quad \text{for} \quad e = 3 \quad \text{and} \quad e = 6,$$

the sign of b in

$$p = a^2 + 4b^2, \quad a \equiv 1 \bmod 8 \quad \text{for} \quad e = 4$$

and the signs of x, u, v, w in

$$16p = x^2 + 50u^2 + 50v^2 + 125w^2, \quad xw = v^2 - u^2 - 4uv \quad \text{for} \quad e = 5.$$

Comment: The symmetric functions of the periods are independent of the primitive root. This is no longer the case for semi-symmetric functions. The simplest such function is

$$\sum_{i=0}^{e-1} \eta_i^2 \eta_{i+j} - \sum_{i=0}^{e-1} \eta_i^2 \eta_{i+j+1} = \begin{cases} pM & \text{if } e = 3 \\ pb & \text{if } e = 4 \\ -(3px + 8p + 4) + 25(2v + w)p & \text{if } e = 5 \end{cases}$$

Numerical evidence

$$e = 3, \quad p = L^2 + 27, \quad L \equiv 1 \bmod 3$$

p	7	13	19	37	79	97	139	163	313	349	607	709	877	937
L	1	−5	7	−11	−17	19	−23	25	−35	37	49	−53	−59	61
g	3	2	2	2	3	5	2	3	10	2	3	2	2	5
S_1	−4	−3	−17	41	35	−151	247	−308	765	−543	−1956	1733	3313	−2707
S_2	3	10	2	4	114	−54	108	−145	452	−892	−1349	2442	2436	−3644
$S_1 - S_2$	$-p$	$-p$	$-p$	p	$-p$	$-p$	p	$-p$	p	p	$-p$	$-p$	p	p

$$e = 4, \quad p = a^2 + 16, \quad a \equiv 1 \bmod 4$$

p	17	41	97	137	241	641	977
a	1	5	9	−11	−15	25	−31
g	3	6	5	3	7	3	3
S_1	18	64	6	−60	−708	2604	−4824
S_3	−16	−18	200	−334	−226	1322	−2870
$S_1 - S_3$	$2p$	$2p$	$-2p$	$2p$	$-2p$	$2p$	$-2p$

Within a month, a preprint of

Andrew J. Lazarus, Lehmer's semi-symmetric cyclotomic sums and delta units,

had appeared, it will be published in *Acta Arithmetica.*]

Proposition 1.1 is

$$18S_3(2,j) = p(L + 9(-1)^j M) - 2, \quad j = 1,2.$$

and Proposition 2.1 is

$$16S_4(2,j) = -1 - p(1 - 2a + 4(-1)^{\frac{j-1}{2}} b), \quad j = 1,3$$

$$16S_4(2,2) = 2pa - p - 1$$

$$64S^4(3,j) = 1 - 7p^2 + 6p - 4bp(-1)^{\frac{j-1}{2}}(3 + a), \quad j = 1,3$$

$$64S_4(3,2) = -3p^2 + p(6 - 4a^2) + 1$$

where $p = a^2 + b^2$, $b \equiv 0 \bmod 2$, $b > 0$, $a + b \equiv 1 \bmod 4$.

91:20 (? via John Brillhart, Ron Graham & Andrew Odlyzko) 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.

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

Remark. Bill Blair gives the reference W. R. Scott, Group Theory, p. 314, esp. exer. 11.4.11 for the fact that $S_n \cong \mathcal{A}(S_n)$ for all $n \geq 3$ except $n = 6$, where S_n is the symmetric group on n letters. Hugh Edgar gives the reference Kurosh, Theory of Groups, Chelsea, Vol. 1, p. 92. Later, Bill Blair supplied two more references:

E. Schenkman, *Group Theory*, pp. 94–96; among other things Schenkman shows that $G \cong \mathcal{A}(G)$ if $G = \mathcal{A}(H)$ where H is the direct product of nonabelian simple groups.

M. I. Kargapolov & Ju. I. Merzljakov, *Fundamentals of the Theory of Groups*, pp. 42–44 do not add any new results but offer the opinion that "the fact is that complete groups do not play any major role in group theory. (It is analogous to that played by perfect numbers in number theory.)" Bill's inclined to think they're probably right.

91:22 (Sinai Robbins) Given (non-trivial – what does that mean?) a, b, c and d, are there infinitely many pairs m, n such that

$$a^n + b^n = c^m + d^m \quad ?$$

Remark: Andrew Granville observes that a negative answer follows easily (take S as the set of prime divisors of $abcd$) from the Main Theorem on S-unit equations in

Jan-Hendrik Evertse, On sums of S-units and linear recurrences, *Compositio Math.*, **53**(1984) 225–244; *MR* **86c**:11045,

which states that given any finite set S of primes and an integer $n > 2$, there are only finitely many n-tuples of integers $x_1, \ldots, x_n$ with $x_1 + \ldots + x_n = 0$, $\gcd(x_1, \ldots, x_n) = 1$, prime $p | x_1 \cdots x_n \Rightarrow p \in S$, and no proper subsum of $x_1 + \ldots + x_n$ equal to zero.

91:23 (Hugh Edgar) It has become an almost classical question to ask if there are any integer solutions of $x^3 + y^3 + z^3 = 3$ other than $\{1,1,1\}$ and $\{4,4,-5\}$. Cassels has shown that $x \equiv y \equiv z \bmod 9$. Alf van der Poorten asks if there are any other 3-adic integer solutions.

The plane sections

$$[x^3 + y^3 + z^3 = 3] \cap [x + y + z = 3m]$$

of the surface are elliptic curves

$$(x + y)(x - 3m)(y - 3m) = 9m^3 - 1$$

and m has to be an integer $\equiv 1 \bmod 6$. The only singular curve is given by $m = 1$.

J. W. S. Cassels, A note on the diophantine equation $x^3 + y^3 + z^3 = 3$, *Math. Comput.*, **44**(1985) 265–266.

Manny Scarowsky & Abraham Boyarsky, A note on the diophantine equation $x^n + y^n + z^n = 3$, *Math. Comput.*, **42**(1984) 235–237.

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?

91:25 (Andy Pollington) Write $k\sqrt{10}$ with $k \in \mathbb{Z}$ in base 10 as $\sum \epsilon_i 10^i$. Prove that it is impossible to have $\epsilon_i = 0$ or 1. In fact, are such numbers (with any integer $r > 2$ in place of 10) always either transcendental or rational? Compare

Kurt Mahler, Some suggestions for further research, *Bull. Austral. Math. Soc.*, **29**(1984) 101–108,

and a recent *Acta Arith.* article on the Cantor set. Are the irrational elements of the Cantor set necessarily transcendental?

If $\alpha = \sum \epsilon_i r^{-i}$, $\beta = \sum \epsilon_i s^{-i}$ with r, s integer bases and α is irrational, show that β is not algebraically dependent on α.