WESTERN NUMBER THEORY PROBLEMS, 1985-12-21 & 23.

Edited by Richard K. Guy, for mailing prior to 1986 Tucson 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	(present set)		85:01 - 85:23

[with comments on earlier problems: 74:04(UPINT F28), 79:15(=215), 81:21(=321), 82:16(=366), 83:15 & 16(=415 & 416), 84:02, 84:16, 84:17, 84:18, 84:19]

UPINT = Richard K. Guy, Unsolved Problems in Number Theory, Springer, 1981.
rNT2 = Reviews in Number Theory, 1973-1983, AMS, Providence RI, 1984.

COMMENTS WELCOME AT ANY TIME

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

86-07-13

G. Szekeres, Determinants of skew type ±1 matrices, *Period. Math. Hungar.* 3 (1973) 229-234.

He writes "Although the method of averaging is the same, the result itself is quite surprising: averaging over skew-symmetric ±1 matrices gives a value much closer to the suspected limiting value corresponding to the suspected existence of Hadamard matrices of any order $4n$. Indeed it makes it very likely that even skew Hadamard matrices exist for all these orders. ... in skillful hands it might turn into a useful method to prove the existence of Hadamard matrices (without constructing a single such matrix)."

81:21 (= 321) (Carl Pomerance). Let $k = k(n)$ be the least non-negative integer

A063377 such that $2^k n - 1$ is composite. Prove that $k/n \longrightarrow 0$. [$k = 0$ unless $n = 1,2$ or one more than a prime. Moreover, if p is a prime, having 2 as a primitive root, which does *not* divide n, then $k \le p - 2$, and there are considerations modulo other primes; so large k are hard to come by. What's the next biggest after $k(90) = 6$?]

A063377, A339579, A339580, ...

Stanley Rabinowitz reports that Peter Gilbert of DEC, Nashua, NH, has found $k(1122660) = 7$, $k(19099920) = 8$ and $k(427827270) = 9$.

82:16 (= 366) (J. Martin Borden via Kevin McCurley). Given positive integers d, n_1, n_2 with $(n_1,n_2) = 1$, can you always find d_1, d_2 with $d_1 + d_2 = d$ and $(d_1,n_1) = 1 = (d_2,n_2)$?

See comments in 1984 set. Mike Filaseta further notes that the original problem is equivalent to the question: are there positive integers a, b with $b > a + 1$ such that every integer between a and b has a factor in common with either a or b? That is, a counterexample to one problem gives rise to counterexamples to the other. For example, Peter Montgomery's original example with $d = 16$ ($n_1 = 273$, $n_2 = 110$) corresponds to the example $(a,b) = (2184,2200)$ in the present question: note that $b - a = 16$. Compare

P. Erdős & J.L. Selfridge, Complete prime subsets of consecutive integers, *Proc. Manitoba Conf. Numer. Math.*, 1971, Congressus Numerantium V, pp. 1-14.

83:01 (= 401; and see 75:02) (Basil Gordon). Find a set in the plane (or prove its non-existence) such that any line in any one of *four* directions meets it either in a set of measure 1, or in *the empty set*. (Not "a set of measure 0" as I said before.)

85:02 (D.H. Lehmer). If $c_{2n}(4)$ is the coefficient of x^{3n} in $(1 + x + x^2 + x^3)^{2n}$, find an expression for the generating function $\Sigma_{n=0}^{\infty} c_{2n}(4)x^{2n}$.

[1,4,44,580,8092,... is not in Sloane's Handbook.] A005721

85:03 (D.H. Lehmer). If $c_n(3)$ is the coefficient of x^n in $(1 + x + x^2)^n$, show that the determinant of the matrix $\begin{bmatrix} c_0 & c_1 & \cdots & c_k \\ c_1 & c_2 & \cdots & c_{k+1} \\ \vdots & & & \\ c_k & c_{k+1} & & c_{2k} \end{bmatrix}$ is 2^k.

[It was noted that the generating function for c_n is $(1 - 2x - 3x^2)^{-1/2}$. The sequence is #1070 in N.J.A. Sloane, A Handbook of Integer Sequences: there is a reference to Euler, *Opera Omnia*, v.15, p.50.] A002426

[Lehmer solves this using generating functions and continued fractions, but believes that there should be a more direct proof.]

85:04 (Charles Small). Is every rational number a sum of five fifth powers of rational numbers?

85:05 (Martin Davis). Consider the k polynomials $p_i(x_1,\ldots,x_n)$, $1 \le i \le k$, with coefficients in $\mathbb{Z}$, as defining a map of $\mathbb{Z}^n$ into $\mathbb{Z}^k$. Is it possible that the map is *onto* for $n < k$? If so, what is the least n?

Peter Montgomery and David Cantor each showed that the map cannot be onto.

85:06 (Peter Waksman, via John Wolfskill). Let A be a finite set of integers and D be the set of differences $a_i - a_j$, $a_i > a_j$, with multiplicity. If A is translated or reflected, D is preserved. Apart from this, does D determine A?

David Cantor and Peter Montgomery each gave counterexamples. E.g. $A_1 = (0,1,2,3,5,6,7,9,12\}$, $A_2 = \{0,1,3,4,5,6,7,10,12\}$ both give $D=\{1,1,1,1,1,2,2,2,2,2,3,3,3,3,3,4,4,4,4,5,5,5,5,6,6,6,6,7,7,7,8,9,9,10,11,12\}$.

85:07 (Neville Robbins). If P_n is the nth Pell number, $P_0 = 0$, $P_1 = 1$, $P_{n+2} = 2P_{n+1} + P_n$, do the simultaneous diophantine equations $2P_n + 1 = 3x^2$, $2P_n - 1 = y^2$ imply that $n = x^2 = y^2 = 1$?

85:08 (Ron Graham, via Neville Robbins). Show that the only positive integer solutions of $2(x^4 - x^2) = 3(y^2 - 1)$ are $x = 1,2,3,6,91$; possibly by linking the equation to $2^n - 1 = t(t - 1)/2$, whose only solutions are known to be $t = 1,2,3,6,91$. A180445

D. Allison, On square values of quadratics, *Math. Proc. Cambridge Philos. Soc.* 99 (1986) 381-383 finds infinitely many quadratics $f(x)$ such that $f(t)$ is square for t an integer, $-1 \le t \le 6$. The simplest is $f(x) = -420x^2 + 2100x + 2809$, which yields Peter Montgomery's second example. All of these quadratics have the same symmetry as this example. In the asymmetric case, Allison finds two quadratics $f(t)$ square for $0 \le t \le 6$. The smaller is $-4980t^2 + 32100t + 2809$ which yields 53^2, 173^2, 217^2, 233^2, 227^2, 197^2, 127^2 with common second difference -9960.

85:14 (Leonard Lipshitz). If $\{n_k\}$ is an increasing sequence of positive integers such that $n_{k+1}/n_k > r > 1$ for all k, then most of the sums $n_{k_1} + n_{k_2} + \ldots + n_{k_\alpha}$ are distinct (the number of different sums with $k_1 \le k_2 \le \ldots \le k_\alpha \le K$ is asymptotic to $K^\alpha/\alpha!$). What can be said under the weaker assumption that $n_{k+1}/n_k > ((k+1)/k)^\beta$ for any $\beta > 0$ and all large enough k?

Andy Odlyzko takes $n_k \sim k^{\ell n k}$ with the n_k divisible by large powers of 2. Then the sums $n_{k_1} + \ldots + n_{k_\alpha}$, divided by large powers of 2, display a good deal of duplication.

85:15 (Hugh Williams, via John Selfridge). Are there infinitely many primes $p = 8r - 1$ such that whenever a prime q divides r, then $q \equiv 7 \pmod{12}$?

A339582 151, 631, 823, 1063, 1303, 1783, 2647, 2887, 3511, ...

85:16 (Gerry Myerson). Among all non-polynomial functions $f\colon \mathbf{Z} \longrightarrow \mathbf{Z}$ satisfying "$x \equiv y \pmod{n}$ implies $f(x) \equiv f(y) \pmod{n}$ for all x, y, n", are there any with subexponential growth? With polynomial growth?

Raphael Robinson asked if there are polynomials with non-integer coefficients.

The proposer now notes that the answers are already known (see references below). Let f be a function of the type described. Then

1. $(\ell n|f(n)|)/\ell nn$ tends to infinity with n.
2. If $w(n)$ is any positive, unbounded function, then there are f with $\lim\inf(\ell n|f(n)|)/w(n)\ell nn < \infty$.
3. $\operatorname{Lim\,sup}(\ell n|f(n)|)/n \ge \ell n(e-1)$.
4. It is conjectured that $\ell n(e-1)$ in 3. can be replaced by 1; if so this is best possible.