Western Number Theory Problems, 17 & 19 Dec 2004

Edited by Gerry Myerson

for distribution prior to 2005 (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	92:01–92:19	1993 Asilomar	93:01–93:32
1994 San Diego	94:01–94:27	1995 Asilomar	95:01–95:19
1996 Las Vegas	96:01–96:18	1997 Asilomar	97:01–97:22
1998 San Francisco	98:01–98:14	1999 Asilomar	99:01–99:12
2000 San Diego	000:01–000:15	2001 Asilomar	001:01–001:23
2002 San Francisco	002:01–002:24	2003 Asilomar	003:01–003:08
2004 Las Vegas (current set)	004:01–004:17		

[With comments on 001:23, 002:12, 002:18, and 002:22]

COMMENTS ON ANY PROBLEM WELCOME AT ANY TIME

Department of Mathematics,
Macquarie University,
NSW 2109 Australia
gerry@math.mq.edu.au
Australia-2-9850-8952 fax 9850-8114

001:23 (Aaron Meyerowitz) Consider sets of integers $n_1 < n_2 < n_3 \ldots < n_k$ with square product. Let $t(n,k)$ be minimal so that there is a solution with $n_1 = n$ and $n_k = n + t(n,k)$. Let $T(n,k)$ be the smallest value of $t(n,j)$ with $j \geq k$. Is there a C with $t(n,3) < Cn^{1/5}$ infinitely often? Is there a C' with $T(n,4) < C'n^{1/4}$ infitely often?

Remarks: 1. If $n = rs^2$ with r square-free then $t(n,2) = r(2s+1) > n^{1/2}$.

2. There is a parametric family with $t(n,3) < 5n^{1/4}$.

Remark: (new) Sam Wagstaff spoke on joint work with Chaogui Zhang in which they established $\liminf T(n,3)/n^{\alpha} \leq 1$ for all positive α, and the stronger result

$$\liminf \frac{T(n,3)}{\exp\big((\log 2n)^{1/6} + (\log 2n)^{5/6+\epsilon}\big)} \leq 1$$

for any positive ϵ.

002:12 (Doug Iannucci) Let D be the multiplicative function on the positive integers satisfying $D(p^a) = ap^{a-1}$ for all primes p.

1. Is the sequence $n, D(n), D(D(n)), \ldots$ bounded for all n?
2. Does any such sequence of iterates lead to a cycle of length 7?

Remarks: The sequence beginning with $n = 31^{124}$ has been pursued to 48 million iterations without the appearance of a cycle. Also, no cycle has been found for $n = 23^{92}$. Cycles of length k are known only for $k = 8$ and $1 \leq k \leq 6$.

Solution: (Kevin G. Hare and Soroosh Yazdani) The second question is settled in

Kevin G. Hare, Soroosh Yazdani, Further results on derived sequences, J. Integer Seq. 6 (2003) #2, article 03.2.7, 7pp. (electronic), MR 1988646 (2004g:11015).

The authors describe explicitly how to construct cycles of arbitrary length.

002:18 (Neville Robbins) For p prime, let $f(p) = \frac{p-1}{2} - \phi(p-1)$, so $f(p)$ is the number of quadratic non-residues that aren't primitive roots. Are there infinitely many positive integers r such that $f(p) = r$ has no solution?

Solution: (Florian Luca and Gary Walsh) The solution, reported in last year's problem set, has now appeared as

Florian Luca, P. G. Walsh, On the number of nonquadratic residues which are not primitive roots, Colloq. Math. 100 (2004), #1, 91–93, MR2079349.

002:22 (John Selfridge) The number 82818079 . . . 1110987654321 (obtained by concatenating the numbers $82, 81, \ldots, 1$) is prime. Is there any other n for which the number obtained by concatenating $n, n-1, \ldots, 1$ is prime? Is there any n for which concatenating the numbers $1, 2, \ldots, n$ gives a prime?

Remark: In

Ralf Stephan, Factors and primes in two Smarandache sequences, Smarandache Notions J. 9 (1998) 4–10,

available at http://me.in-berlin.de/~rws, it is claimed that the given prime is the only one for n up to 750, and that there are no primes in the other sequence for n up to 840.

Remarks: (new) At http://www.primepuzzles.net/puzzles/puzz_008.htm it says that as of 20 June 1998 Yves Gallot had found that in the forward sequence there is no prime up to $n = 8000$.

At MathWorld (http://mathworld.wolfram.com/ConsecutiveNumberSequences.html) it is reported that Fleuren (1999) verified that the absence of primes in the forward sequence up to $n = 200$, a result extended to the first 19700 terms by Weisstein on 8 June 2004. "This is roughly consistent with simple arguments based on the distribution of primes which suggest that only a single prime is expected in the first 15000 or so terms."

It also reports that as of the same date Weisstein has found that the 82nd term is the only prime in the first 19100 terms of the backward concatenation. The problem is also mentioned in UPINT, A3.

Problems Proposed 17 & 19 Dec 2004

004:01 (James Buddenhagen, via Gerry Myerson) Can a square be expressed as a sum of cubes of two primes in two different ways? That is, does $n^2 = a^3 + b^3 = c^3 + d^3$ have any solutions in positive integers, a, b, c and d all prime, $\{a, b\} \neq \{c, d\}$?

Remarks: It's easy to see that if there is a solution then the primes are all odd and distinct. If the conditions are weakened at all then moderate-sized solutions exist, e.g.,

$$228^2 = 11^3 + 37^3$$

shows that a square can be the sum of cubes of two primes,

$$31^3 + 1867^3 = 397^3 + 1861^3$$

shows that a number can be the sum of cubes of two primes in two different ways, and

$$77976^2 = 1026^3 + 1710^3 = 228^3 + 1824^3$$

shows that a square can be the sum of two cubes in two different ways.

Peter Montgomery notes that if p and q are odd primes with $p + q \equiv 0 \pmod 3$ and $p^3 + q^3$ is a square then p and q are $6A^2B^2 \pm (A^4 - 3B^4)$ for some integers A, B, and $p^3 + q^3 = 36A^2B^2(A^4 + 3B^4)^2$.

004:02 (David Terr) A superior highly composite number is a positive integer N that maximizes $N^{-e}d(N)$ for some $e > 0$; here, $d(N)$ is the number of divisors of N. Let N_n be the nth such number. Then $N_n = \pi_n N_{n-1}$ for some prime π_n. Let $D_n = d(N_n) = \prod_{m=1}^{n}(1 + k_m^{-1})$ where k_m is the π_m-adic valuation of N_m. π_n and k_n are chosen so that $e_n = \log(1 + k_n^{-1})/\log \pi_n$ is monotonically decreasing. Let $u_n = D_{n-1}/N_{n-1}^{e_n} = D_n/N_n^{e_n}$. Find asymptotic formulas for N_n, D_n, e_n and u_n.

Remarks: A reference is

S. Ramanujan, Highly composite numbers, Proc. London Math. Soc. (2) 14 (1915), 347–409.

Further work of Ramanujan on this problem was first published many years later;

S. Ramanujan, Highly composite numbers, Ramanujan J. 1 (1997), no. 2, 119–153, MR1606180 (99b:11112).

Jeff Lagarias also suggests his paper,

J. Lagarias, An elementary problem equivalent to the Riemann hypothesis, Amer. Math. Monthly 109 (2002), no. 6, 534–543, MR1908008 (2003d:11129),

which is also available on the preprint server at math.NT/0008177.

The superior highly composite numbers form sequence A002201 in the On-Line Encyclopedia of Integer Sequences. The first few terms are given there as 2, 6, 12, 60, 120, 360, 2520, 5040, 55440, 720720, 1441440, 4324320, 21621600, 367567200, 6983776800, 13967553600, 321253732800, 2248776129600, 65214507758400, 195643523275200.

004:03 (Carl Pomerance and Greg Martin) Carmichael's function $\lambda(n)$ is the maximal order of an element of $(\mathbf{Z}/n\mathbf{Z})^*$. Let $\ell(n)$ be the number of iterations of λ required to take n to 1 (e.g., $\lambda(100) = 20$, $\lambda(20) = 4$, $\lambda(4) = 2$, $\lambda(2) = 1$, so $\ell(100) = 4$). Is it true that $\ell(n)$ is of order of magnitude $\log\log n$ for almost all n?

Do powers of 3 maximize $\ell(n)$? It's easy to see that $\ell(3^n) = n$, so the question is whether $\ell(m) > n$ implies $m > 3^n$.

Remark: This isn't true for small n, e.g., $47 < 3^5$ but $\ell(47) = 6$. Note that 47 is at the end of the Cunningham chain 2, 5, 11, 23, 47 of primes, each of which is one greater than twice its predecessor. Similarly, $\ell(2879) = 10$ and $2879 < 3^9$.

004:04 (Ron Graham and Kevin O'Bryant) Suppose $1 \le u_1 < u_2 < \ldots < u_n < q$ are integers with $\gcd(u_j, q) = 1$ for all j. Let $v_1, v_2, \ldots, v_n$ be arbitrary integers, and let $f(x) = \sum_{j=1}^{n} x^{v_j}/(1 - x^{u_j})$. Prove that if $f(e^{2\pi i/q}) = 0$ then $\sum_{k=1}^{n} u_k \ge q$.

A stronger conjecture is that if no subset of the u_j sums to a multiple of q then $f(e^{2\pi i/q}) = 0$ implies $f(e^{2\pi ij/q}) = 0$ for $1 \le j \le q - 1$.

Remarks: The cases $n = 1$ and $n = 2$ have been settled, but $n \ge 3$ remains open. Also, if q is prime then vanishing at $e^{2\pi i/q}$ implies vanishing at $e^{2\pi ij/q}$ for $1 \le j \le q - 1$, so only composite values of q are of interest. Joe Buhler has found that

$$\frac{1}{1-x} + \frac{x^5}{1-x^2} + \frac{x^{10}}{1-x^4} + \frac{x^{10}}{1-x^{11}} + \frac{x^5}{1-x^{13}} + \frac{1}{1-x^{14}}$$

vanishes at $e^{2\pi i/15}$ but not at $e^{2\pi i\cdot 3/15}$, but there is no contradiction here since there are subsets of the u_j that sum to 15.

References on vanishing sums of roots of unity include

J. H. Conway, A. J. Jones, Trigonometric Diophantine equations (On vanishing sums of roots of unity), Acta Arith. 30 (1976), no. 3, 229–240, MR0422149 (54 #10141),

T. Y. Lam, K. H. Leung, On vanishing sums of roots of unity, J. Algebra 224 (2000), no. 1, 91–109, MR1736695 (2001f:11135),

Bjorn Poonen, Michael Rubinstein, The number of intersection points made by the diagonals of a regular polygon, SIAM J. Discrete Math. 11 (1998), no. 1, 135–156 MR1612877 (98k:52027).

004:05 (Syrous Marivani) Let $f(n)$ be the nth Fibonacci number (with $f(0) = 0$, $f(1) = 1$). For p prime, let p_0 be the least positive n such that $f(n) \equiv 0 \pmod{p}$. Characterize the primes for which $p_0 = p + 1$; $p_0 = p - 1$; p_0 divides $(p + 1)/3$; p_0 divides $(p - 1)/4$; p_0 divides $(p - 1)/3$.

Remarks: Neville Robbins points out that p_0 is often written $\omega(p)$ and is called an entry point. Moreover, there is considerable literature on $\omega(p)$. Asking for primes p with $\omega(p) = p \pm 1$ is much like asking for primes p with a given number (say, 2) as a primitive root, and most likely it is very difficult to say anything about it.

004:06 (Ben Kane and Lawrence Sze) Let s and t be relatively prime positive integers. Let P be a set of positive integers with the property that if n is in P and $n \geq s$ then $n - s$ is in P, also if n is in P and $n \geq t$ then $n - t$ is in P. Prove that

$$\sum_{n \text{ in } P} n - \#(P)(\#(P) - 1)/2 \leq (s^2 - 1)(t^2 - 1)/24$$

with equality if $P = \{ n > 0 : n = as + bt \rightarrow ab < 0 \}$.

Remarks: Note that P is not allowed to contain zero, so it cannot contain any integer $as + bt$ with a and b both non-negative, so it is in any event a subset of the set that yields equality. There is an equivalent statement of the conjecture in the language of partitions; the maximal partition that is both an s-core and a t-core is of size $(s^2 - 1)(t^2 - 1)/24$.

If P is closed under subtraction of three relatively prime integers s, t, u, no conjecture concerning $\sum_{n \text{ in } P} n$ is offered.

004:07 (Bart Goddard) Let $\nu = (-1 + \sqrt{-d})/2$ with d positive, squarefree, and $d \equiv 3 \pmod 4$, so that $\mathcal{O}_d = \{ a + b\nu : a, b \text{ in } \mathbf{Z} \}$ is the ring of integers of $\mathbf{Q}(\sqrt{-d})$. Let N be the usual norm on $\mathbf{Q}(\sqrt{-d})$. Find a, b such that $N(a + b\nu) = 10a + b$.

Remarks: If $d = 3$ then $N(\underline{3} + \underline{7}\nu) = \underline{37}$ and $N(\underline{4} + \underline{8}\nu) = \underline{48}$; it was these digital coincidences that suggested the problem. If, as in these examples, it is assumed that a and b are digits, then it is not difficult to find all solutions; presenting the solutions in the form $(d, N(a+b\nu))$, they are $(3, 37)$, $(3, 48)$, $(19, 63)$, $(19, 73)$, $(43, 11)$, $(115, 41)$, $(115, 71)$, $(123, 51)$, and $(123, 61)$.

It is also not hard to find the solutions of $N(a + b\sqrt{-d}) = 10a + b$ in digits a, b with d positive, squarefree, and $d \not\equiv 3 \pmod 4$. In the form (d, N) they are $(10, 11)$, $(10, 91)$, $(17, 21)$, $(17, 81)$, $(22, 31)$, $(22, 71)$, and $(26, 51)$. Allowing $d \equiv 3 \pmod 4$ permits $N(4 + 3\sqrt{-3}) = 43$ and $N(6 + 3\sqrt{-3}) = 63$. The real quadratic fields yield no solutions in digits.

One suggested extension to the problem is to ask for solutions of $N(a + b\nu) = 10^k a + b$ with $0 < b < 10^k$ and $a > 0$. For example, with $d = 3$, this permits $N(14 + 7\nu) = 147$. Another suggestion is to look for solutions of $N(\sum_{i=1}^n a_i \nu_i) = \sum_{i=1}^n a_i 10^{n-i}$ with $\nu_1, \ldots, \nu_n$ an integral basis for a number field of degree n, and $a_1, \ldots, a_n$ digits.

004:08 (Carrie Finch and Carl Pomerance) Let $\mathcal{S}_k$ be the collection of sets of k distinct positive integers. For S in $\mathcal{S}_k$ let $n(S)$ be the number of subsets U of S such that the polynomial $1 + \sum_{e \text{ in } U} x^e$ is reducible. Find $f(k)$, the maximum of $n(S)$ over all S in $\mathcal{S}_k$.

Remarks: $f(2) = 3$, since $1 + x^3$, $1 + x^{15}$ and $1 + x^3 + x^{15}$ are all reducible. For $k \geq 3$, $f(k) < 2^k - 1$ since at least one of $1 + x^a + x^b$, $1 + x^a + x^c$ and $1 + x^b + x^c$ is irreducible.

004:09 (Lenny Fukshansky) A piece of paper with N creases in it corresponds to a binary word of length N by writing 0 for each valley and 1 for each hill. Can we define a set of folding protocols in such a way that the resulting collection of binary words forms a code, that is, a subspace of the $\mathbf{F}_2$-vector space of all binary words of length N? Can we define a set of folding protocols in such a way that the resulting collection of binary words forms a code of large minimal distance, that is, one in which each non-zero word has many 1s?

004:10 (Gennady Bachman) Let $f_n(z)$, $n = 1, 2, \ldots$, be defined by

$$f_1(z) = z(e^{-z} - 1), \qquad f_{n+1}(z) = z(e^{f_n(z)} - 1).$$

Define $a_k(n)$, $k = 1, 2, \ldots$, $n = 1, 2, \ldots$, by $f_n(z) = z^n \sum_{k=1}^{\infty} a_k(n) z^k$. Define a_k for $k = 1, 2, \ldots$, by $a_k = \lim_{n\to\infty} a_k(n)$. Let $A(q, b) = \sum_{k \equiv b \pmod q} a_k$. Is it true that $A(q, b) = 0$ for all b and q?

Remark: There are non-trivial sequences $b_1, b_2, \ldots$ such that $\sum_{k\equiv b \pmod q} b_k = 0$ for all b and q.

004:11 (Matthias Beck and Eric Mortenson) Let P be the convex polytope defined by

$$P := \{x \in \mathbf{R}^d_{\geq 0} : Ax = b\}$$

where

$$A := (c_1 \ldots c_d) \in \mathbf{Z}^{m\times d}, \quad b \in \mathbf{Z}^m.$$

Define the following generating functions for the number of integer points in dilates of the closed and open polytope, respectively, as

$$H(q) := \sum_{t\geq 0} \#\left(tP \cap \mathbf{Z}^d\right) q^t = \Omega \frac{1}{(1 - q\lambda^b)\prod_{k=1}^d (1 - \frac{1}{\lambda^{c_k}})}$$

and

$$H^*(q) := \sum_{t>0} \#\left(t \operatorname{int}(P) \cap \mathbf{Z}^d\right) q^t = \Omega \frac{q\lambda^{b-1}}{(1 - q\lambda^b)\prod_{k=1}^d (1 - \frac{1}{\lambda^{c_k}})\lambda^{c_k}}.$$

Here Ω denotes MacMahon's Ω-operator (see MacMahon's *Combinatory Analysis* and the *MacMahon's Partition Analysis* series of papers by Andrews & co-authors), which computes the constant term of a multivariate Laurent series in the components of λ, $\lambda = (\lambda_1, \ldots, \lambda_m)$. We use the vector notation $\lambda^v = \lambda_1^{v_1} \cdots \lambda_m^{v_m}$. (The Omega identities follow quickly from setting up an Euler-style generating function.)

The fundamental Ehrhart-Macdonald Reciprocity Theorem says that

$$H\left(\frac{1}{q}\right) = (-1)^{d-\operatorname{rank}(A)+1} H^*(q)$$

In terms of the Omega operator...

$$\Omega \frac{(-1)^{d-\operatorname{rank}(A)+1}}{(1 - \frac{\lambda^b}{q})\prod_{k=1}^d (1 - \frac{1}{\lambda^{c_k}})} = \Omega \frac{q\lambda^{b-1}}{(1 - q\lambda^b)\prod_{k=1}^d (1 - \frac{1}{\lambda^{c_k}})\lambda^{c_k}}$$

Can this identity be proved from scratch, i.e., through Omega calculus?

004:12 (Martin Juráš) For $n \geq 3$ and $3 \leq t \leq 6n-6$ let

$$B_t = \{\, (i,j,k) : 0 \leq i < j < k \leq 2n-1 \text{ and } i+j+k = t \,\}.$$

Let V_t be the real vector space with basis B_t. Define the linear map $D^{(t)} : V_t \to V_{t+1}$ by $D^{(t)}\big((i,j,k)\big) = (i+1,j,k) + (i,j+1,k) + (i,j,k+1)$, taking $(i,i,k) = (i,j,j) = (i,j,2n) = 0$ in V_{t+1}. Prove that $D^{(t)}$ is injective for $3 \leq t \leq 3n-1$.

Remarks: This is simple to prove for $3 \leq t \leq 2n-1$, and has been verified by computer for $n \leq 100$.

004:13 (Gary Walsh) (The diophantine n-tuples problem) There are many known examples of sets of 6 (distinct, positive) rational numbers for which the product of any two, increased by 1, is a square (of a rational). Is there such a set with more than 6 elements? What is the upper bound for the size of such a set?

Andrej Dujella's website, http://www.math.hr/~duje/dtuples.html, is an important resource for this problem, which is Problem D29 in UPINT.

004:14 (Pante Stanica) Let f be a rotation-symmetric function from $\mathbf{F}_2^n$ to $\mathbf{F}_2$, that is, $f(x_1, \ldots, x_n) = f(x_2, \ldots, x_n, x_1)$. There are functions g such that $fg = 0$. Given f, how do you find such a non-zero g of minimal degree? Of course for any given f this is a finite problem; the goal is to find an efficient algorithm.

004:15 (John Baldwin, Abe Kunin, Lawrence Sze) Show that

$$1^2 + 2^2 + 3^2 + 4^2 + 9n = a_1^2 + a_2^2 + a_3^2 + a_4^2$$

is solvable in integers a_1, a_2, a_3, a_4 with $a_i^2 \equiv i^2 \pmod 9$, $i = 1,2,3,4$, only for n not of the form $(4^k - 10)/3$, $k \geq 2$—equivalently, only when $30 + 9n$ is not of the form $3 \cdot 4^k$, $k \geq 2$.

Solution: (Peter Montgomery) If the left side, N, is a multiple of 8 then each a_i must be even. Division by 4 yields an expression for $N/4$ as a sum of four squares, still satisfying the congruences modulo 9. But there is no solution for $N = 48$, hence, none for $N = 3 \cdot 4^k$, $k \geq 2$.

Peter also supplies a proof that there is a solution when $30 + 9n$ is not of the form $3 \cdot 4^k$. The proof is elementary but a bit too long for inclusion here.

004:16 (Kevin O"Bryant, Dennis Eichhorn, Josh Cooper) Let A and B be sets of nonnegative integers, both containing 0, and satisfying the formal power series identity,

$$\Big(\sum_{a \text{ in } A} q^a\Big)\Big(\sum_{b \text{ in } B} q^b\Big) \equiv 1 \pmod 2.$$

Is it true that if A is uniformly distributed modulo every power of 2 and its indicator function is not eventually periodic, then B has positive density?

Remark: If so, then the open question of whether the set of n for which the partition function $p(n)$ is odd has positive density would be settled in the affirmative, since the sets

$$A = \{\, n(3n+1)/2 : n \text{ in } \mathbf{Z} \,\}, \qquad B = \{\, n : p(n) \text{ is odd} \,\}$$

satisfy the hypotheses by Euler's Pentagonal Number Theorem.

004:17 (Helen Grundman and E. A. Teeple) For $b \geq 2$, and $0 \leq a_i < b$, define $S_{3,b} : \mathbf{Z}^+ \to \mathbf{Z}^+$ by

$$S_{3,b}\left(\sum_{i=0}^{n} a_i b^i\right) = \sum_{i=0}^{n} a_i^3.$$

If $S_{3,b}^m(a) = 1$ for some $m \geq 0$, then a is a cubic b-happy number.

A d-consecutive sequence is an arithmetic sequence with constant difference d.

We conjecture that, in general, if $d = \gcd(6, b-1)$, there exist arbitrarily long finite sequences of d-consecutive cubic b-happy numbers.

The conjecture is known to be true for small d (certainly up to $d = 12$), but the question is how to prove it in general, for all b (if, indeed, it is true).