Western Number Theory Problems, 17 & 20 Dec 2005

Edited by Gerry Myerson

for distribution prior to 2006 (Ensenada) 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	004:01–004:17	2005 Asilomar (current set)	005:01–005:12

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

Problems Proposed 17 & 20 Dec 2005

005:01 (Jim Hafner) What is the next number in the sequence 9, 27, 33, 63, 87, 117, 123, 153, 207, 243, 297? These are all the numbers under 300 that are multiples of 3, not multiples of 5, and satisfy some property too complicated to detail here—see Theorem 5 in IBM Technical Report RJ10352 at http://domino.watson.ibm.com/library/CyberDig.nsf/home. The sequence appears on page 19 (and does not appear in the On-Line Encyclopedia of Integer Sequences).

005:02 (Peter Montgomery) Given n, find a 5-term geometric progression (mod n), c_1, c_2, c_3, c_4, c_5, in which each term is $O(n^{2/3})$ and

$$\det \begin{pmatrix} c_0 & c_1 & c_2 \\ c_1 & c_2 & c_3 \\ c_2 & c_3 & c_4 \end{pmatrix} \neq 0$$

E.g., for $n = 1993$ we can take 57, -33, 124, 138, 25 with common ratio 419 and $[n^{2/3}] = 158$. A preprint available from Peter explains the relation to the general number field sieve factorization method.

005:03 (Gary Walsh) Let α be the quaternion $a + bi + cj + dk$ with integer coefficients and $\gcd(a, b, c, d) = 1$. Let $\alpha^n = a_n + b_n i + c_n j + d_n k$, and let $g_n = \gcd(b_n, c_n, d_n)$. Does g_n contain a primitive divisor for all sufficiently large n? A primitive divisor is a prime divisor of g_n which doesn't divide any g_k, $1 \le k \le n - 1$.

Remarks: 1. It is intended to exclude trivial cases such as $\alpha = 1$ and $\alpha = 1 + i$.

2. Nils Bruin and Gary Walsh note that all powers of α are in the submodule generated by 1 and α, which is isomorphic to an order of a quadratic field. The isomorphism is given by $\psi(a + bi + cj + dk) = a + i\sqrt{b^2 + c^2 + d^2}$. Then g_n is given by $(a + i\sqrt{b^2 + c^2 + d^2})^n = a_n + ig_n\sqrt{b^2 + c^2 + d^2}$. It is known from linear forms in logarithms that $|g_n| \to \infty$ with n.

Solution: Bilu has pointed out to Gary that results in

Yu. Bilu, G. Hanriot, P. M. Voutier, Existence of primitive divisors of Lucas and Lehmer numbers, J. Reine Angew. Math. 539 (2000) 75–122, MR 2002j:11027

guarantee a primitive prime divisor for $n > 30$.

005:04 (Gary Walsh) Let $\alpha = (1+\sqrt{-7})/2$ and define A_n and B_n by $\alpha^n = (B_n + A_n\sqrt{-7})/2$. Show that if p is prime then $A_{p^2} \neq \pm A_p$.

Remark: In

I. A. Sakmar, General Ramanujan-type Diophantine equations and their complete solution, J. Number Theory 55 (1995) 160–169, MR 96h:11024

all solutions are found to $A_n = \pm A_m$, but there is a gap in the proof, concerning the sentence at the bottom of page 165.

Solution: The problem is solved in the Bilu, Hanriot, Voutier paper referenced above.

005:05 (David Moulton) Let the rank of S be the size of the smallest set B such that every element of S is the sum of distinct elements of B. What are the aymptotics for the rank of $\{ 1, \|\pi\|, \|\pi^2\|, \ldots, \|\pi^{n-1}\| \}$, where $\|x\|$ is the integer nearest x?

005:06 (David Moulton) Given a positive integer n, let $p(n)$ be the number of partitions of n. A partition of n can be visualized as a Ferrers diagram, which can then be turned into a tableau by replacing the dots with the numbers $1, 2, \ldots, n$ in such a way that the numbers increase going down and going right. E.g., the partition $5 = 2 + 2 + 1$ has the diagram $\begin{array}{cc} \cdot & \cdot \\ \cdot & \cdot \\ \cdot & \end{array}$ and tableaux

$$\begin{array}{cc} 1 & 2 \\ 3 & 4 \\ 5 & \end{array} \quad \begin{array}{cc} 1 & 2 \\ 3 & 5 \\ 4 & \end{array} \quad \begin{array}{cc} 1 & 3 \\ 2 & 4 \\ 5 & \end{array} \quad \begin{array}{cc} 1 & 3 \\ 2 & 5 \\ 4 & \end{array} \quad \begin{array}{cc} 1 & 4 \\ 2 & 5 \\ 3 & \end{array}$$

For fixed n, let $a_i = a_i^{(n)}$, $i = 1, \ldots, p(n)$, be the number of tableaux associated to the ith partition of n (the ordering of the partitions of n is arbitrary). Thus $\sum_i a_i^0 = p(n)$. It is known that $\sum_i a_i$ is the number of involutions in S_n, the symmetric group on n symbols, and $\sum_i a_i^2 = n!$. Find interpretations and/or formulas for $\sum_i a_i^3$ and $\sum_i a_i^4$.

This table may be helpful:

n	0	1	2	3	4	5	6
Tableaux	1	1	1^2	$2, 1^2$	$3^2, 2, 1^2$	$6, 5^2, 4^2, 1$	$16, 10^2, 9^2, 5^4, 1^2$
$\sum_i a_i^3$	1	1	2	10	64	596	8056
$\sum_i a_i^4$	1	1	2	18	180	3060	101160

The entry 5^2 under $n = 5$ (for example) means there are two partitions of 5 (namely, $2+2+1$ and $3+2$) which give rise to 5 tableaux. The sequences do not appear in the On-Line Encyclopedia of Integer Sequences.

005:07 (David Moulton) A positive integer n is an Erdős-Woods number if there exists a positive integer a such that each integer between a and $a + n$ has a common factor with a or $a + n$. Do they have a positive density?

Remark: The smallest Erdős-Woods number is 16; take $a = 2184$. All Erdős-Woods numbers up to 100,000 are known. The first few appear as A059756 in the On-Line Encyclopedia of Integer Sequences. A reference is

Patrick Cégielski, François Heroult, Denis Richard, On the amplitude of intervals of natural numbers whose every element has a common prime divisor with at least an extremity, Theoret. Comput. Sci. 303 (2003) 53–62, MR 2004g:11001.

005:08 (Richard Stauduhar via John Brillhart) For p prime let F_p be the number of distinct residues (mod p) of $n!$, $n = 1, 2, \ldots, p - 1$. Conjecture: $\lim_{p\to\infty} \frac{1}{p} F_p$ exists and is $1 - e^{-1}$.

Remark: As John noted, this is an old problem. It is F11 in UPINT, which cites the Proceedings of the Number Theory conference in Boulder in 1963.

005:09 (Risto Kauppila via Gerry Myerson) For p prime let $f(p)$ be the smallest prime congruent to 1 (mod p). Prove that f is one-one.

Remark: If p and q are prime, $p < q$, and $f(p) = f(q) = n$, then $p \mid (n - 1)$ and $q \mid (n - 1)$ so $pq \mid (n - 1)$, so $n \geq 2pq + 1 > 2p^2$. Thus it suffices to show that $f(p) < 2p^2$. While numerical evidence and heuristic arguments agree that $f(p)$ is much less than p^2, no such result has been proved. Even on ERH the best known result is $f(p) < 2p^2 \log^2 p$.

More generally, for non-zero integer a with $|a| < p$, let $f(a, p)$ be the smallest prime exceeding p and congruent to a (mod p). Is it true that for each a $f(a, p)$ is one-one?

005:10 (Tomohiro Yamada) Let $\omega(m)$ be the number of distinct prime divisors of m. Given k, are there only finitely many odd integers n such that $\omega(\sigma(n)) = k$ and n divides $\sigma(\sigma(n))$?

Remark: The only solutions for $k = 1$ are $n = 21$ and $n = 2^m$ with $2^{m+1} - 1$ prime, according to

G. G. Dandapat, J. L. Hunsucker, Carl Pomerance, Some new results on odd perfect numbers, Pac. J. Math. 57 (1975) 359–364, MR 52 #5554

Other solutions are $n = 15$ and $n = 1023$.

005:11 (Lenny Jones) Is it true that if $1 < r < s$ then $\gcd(10^{2^r} + 1, 3^{2^s} + 1) = 1$? It is not true if $r = s$ is allowed, e.g., the gcd is 17 if $r = s = 3$.

005:12 (David Bailey) Define the n-fold iterated integrals C_n as

$$C_n = \frac{4}{n!} \int_0^\infty \cdots \int_0^\infty \frac{1}{\left(\sum_{j=1}^n (u_j + u_j^{-1})\right)^2} \frac{du_1}{u_1} \cdots \frac{du_n}{u_n}$$

It has been established that $C_1 = 2$, $C_2 = 1$,

$$C_3 = L_{-3}(2) = \sum_{n \geq 0} \left((3n+1)^{-2} - (3n+2)^{-2}\right)$$

and $C_4 = (7/12)\zeta(3)$. Are there closed-form evaluations for C_n for $n > 4$?