Western Number Theory Problems, 17 & 19 Dec 2007

Edited by Gerry Myerson

for distribution prior to 2008 (Colorado) 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	005:01–005:12
2006 Ensenada	006:01–006:15	2007 Asilomar (current set)	007:01–007:15

[With comments on 001:22, 004:06, 006:03 and 006:11]

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

Comments on earlier problems

001:22 (Gary Walsh) Is there a heuristic that suggests that $(x^3-1)(y^3-1)=z^2$ has infinitely many solutions with integers x, y, and 1 distinct?

Remark: (2002) Noam Elkies writes, "The usual heuristics suggest that there should be only finitely many solutions, but this seems quite hard to prove. There are a few solutions that are perhaps surprisingly large, such as $(x,y,z)=(3,313,28236)$ and $(x,y,z)=(-20,-362,616077)$. It seems likely that the complete list of solutions consists of these two, the three positive solutions $(2,4,21),(2,22,273),(4,22,819)$ and the three negative solutions $(0,-2,3),(-1,-23,156),(-6,-26,1953)$, and the images of those $2+3+3=8$ solutions under the obvious involutions that switch x with y or z with $-z$, for a total of $4\times 8=32$ solutions. At any rate an exhaustive search shows that these are the only solutions with both $|x|$ and $|y|$ in $[0,10^6]$. (Naturally this search was not over all 10^{12} or so (x,y) pairs: I had gp list, for each m in this range, the smallest integer d such that m^3-1 is d times a square, and then sort the list of d-values and look for duplicates.)"

Remark: (2008) Peter Montgomery writes, "I searched $|x|,|y|<4294*10^6$ and found another solution, $(x,y)=(1173,110187925)$.

"The program chose 100 primes p_j around 2000. Define a quadratic character χ_j on the non-zero integers by $\chi_j(np_j^e)=\text{jacobi}(n,p_j)$ if $\gcd(n,p_j)=1$. The candidate values of x were put in an array. Those x with $\chi_1(x^3-1)=+1$ were moved to one end of the array and those with $\chi_1(x^3-1)=-1$ to the other end. Each subarray was further split according to $\chi_j(x^3-1)$ for $j=2,3,\ldots$. If, at some point in the recursion, a subarray had only one x, that x was discarded."

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 $n\ge s$ then $n-s$ is in P, also if n is in P and $n\ge t$ then $n-t$ is in P. Prove that

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

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

Remarks: (2005) 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.

Remark: (2008) The statement about partitions is proved in B. Olsson and D. Stanton, Block inclusions and cores of partitions, Aequat. Math. 74 (2007) 90-110. No mention is made of the Kane-Sze formulation of the problem. In a preprint, Amitabha Tripathi proves the Kane-Sze inequality, and deduces the Olsson-Stanton result from it.

006:03 (Mel Nathanson, via Carl Pomerance) For p prime, and for $\mathbf{a} = (a_1, \ldots, a_d)$ with non-zero entries modulo p, let

$$h(\mathbf{a}) = \min_{1 \le k \le p-1} \sum_{i=1}^{d} (ka_i \bmod p)$$

where "u mod p" means the integer in $[0, p-1]$ congruent to u modulo p. Suppose none of the quantities $a_i \pm a_j$, $a_i + a_j + a_k$ vanish modulo p for distinct i, j, and k. Must it be true that $h(\mathbf{a}) \le p(p-1-2d)/4$?

Remark: For more information, see Mel Nathanson, Heights on the finite projective line, available at http://arxiv.org/abs/math.NT/0703646, and Joshua Batson, Nathanson heights in finite vector spaces, http://arxiv.org/abs/0710.4605.

006:11 (John Brillhart) What is the probability that a polynomial chosen uniformly at random from the polynomials of a given degree n over a given field of p elements has a multiple root in some extension field?

Solution: Let $P_{q,n}$ be the probability that a random univariate polynomial over F_q of degree n has a multiple root in some extension field. Jeff Achter noted that results of Bjorn Poonen, Bertini theorems over finite fields, Ann. Math. 160 (2004) 1099–1127, imply that $\lim_{n\to\infty} P_{q,n} = 1/q$. Poonen writes,

In fact, $P_{q,n} = 1/q$ exactly for all $n \ge 2$. Equivalently, for $n \ge 2$, the number of monic squarefree polynomials in $F_q[x]$ of degree n is $q^n - q^{n-1}$. This is a very old result: see the formula for $Q(nu)$ on the first page of Leonard Carlitz, The arithmetic of polynomials in a galois field, Amer. J. Math. 54 (1932), no. 1, 39–50.

Problems Proposed 17 & 19 Dec 2007

007:01 (Sam Wagstaff) Let $r_s(n)$ be the number of ways to write n as a sum of s squares. Various congruences for $r_s(n)$ are known, e.g., if $s = 2^k$ then for all n, $r_s(n) \equiv 0 \pmod{2s}$. Either find h, not a divisor of $2s$, with a proof of a congruence for $r_s(n) \pmod{h}$ for infinitely many s and n, or prove that there is no such h.

Remark: Known results can be found in S. Wagstaff, Congruences for $r_s(n)$ modulo $2s$, Journal of Number Theory 127 (2007) 326–329.

007:02 (Doug Iannucci) Call n a *year number* if $\varphi(n)/\varphi(\sigma(n)) = 2$ (note that 365 is a year number, whence the terminology). Are there any even year numbers? Are there any odd year numbers that are not squarefree?

Remark: If $n = q_1 q_2 \ldots q_k$ is a product of odd primes such that $(q_j + 1)/2$ is prime for all j, then n is a year number.

Solution: $n = 5491 = 17^2 \cdot 19$ is the smallest non-squarefree year number. The next few non-squarefree year numbers are $8075 = 5^2 \cdot 17 \cdot 19$, $25317 = 3^2 \cdot 29 \cdot 97$, $27455 = 5 \cdot 17^2 \cdot 19$, $71383 = 13 \cdot 17^2 \cdot 19$, $72283 = 41^2 \cdot 43$, $76131 = 3^2 \cdot 11 \cdot 769$, $104975 = 5^2 \cdot 13 \cdot 17 \cdot 19$, $138575 = 5^2 \cdot 23 \cdot 241$, and $193041 = 3^2 \cdot 89 \cdot 241$.

The smallest non-cubefree (and non-4th-powerfree) year number is $295569 = 3^4 \cdot 41 \cdot 89$. The smallest year number divisible by 5^3 is $1964375 = 5^4 \cdot 7 \cdot 449$. The smallest year number divisible by 31 (which is the smallest prime not appearing in the previous paragraph) is $595975 = 5^2 \cdot 31 \cdot 769$.

Eric Landquist found year numbers divisible by 7^2, 7^3, and 7^4, as well as $120781449 = 3^8 \cdot 41 \cdot 449$. The existence of even year numbers is still open, but Eric checked all 200-smooth even integers with a single large prime up to 100,000,000 and found no year numbers among them. Perhaps for every odd n there is a year number divisible by n.

007:03 (Bob Styer and Reese Scott, via Gerry Myerson) Find all solutions to $a^x \pm a^y = b^r \pm b^s$, the signs being chosen independently.

Remarks: We assume $a, b > 1$, $a \neq b$, a and b not perfect powers, $x > y > 0$, $r > s > 0$, and $x/y \neq r/s$, to eliminate infinite families. Below is a list of 23 solutions from which all other known solutions can be derived, either by combining two solutions to create a third (e.g., $2^5 - 2 = 3^3 + 3 = 5^2 + 5$, $2^8 - 2^2 = 3^5 + 3^2 = 6^3 + 6^2$), or by noting that from any solution with $x = 2y$ we can derive another solution from $a^{2y} \pm a^y = (a^y \pm 1)^2 \mp (a^y \pm 1)$.

The 23 solutions are:

$2^3 - 2 = 3^2 - 3$
$2^7 - 2^3 = 5^3 - 5$
$2^5 - 2 = 3^3 + 3$
$2^5 + 2^2 = 3^3 + 3^2$
$3^3 + 3 = 5^2 + 5$
$5^7 - 5 = 279^2 + 279$
$6^3 - 6 = 15^2 - 15$
$21^3 + 21^2 = 98^2 + 98$

$2^5 - 2^3 = 3^3 - 3$
$2^4 + 2^3 = 3^3 - 3$
$2^8 - 2^2 = 3^5 + 3^2$
$2^7 + 2 = 5^3 + 5$
$3^7 - 3 = 13^3 - 13$
$3^5 + 3^2 = 6^3 + 6^2$
$5^5 + 5^2 = 15^3 - 15^2$
$30^5 - 30 = 4929^2 + 4929$

$2^8 - 2^4 = 3^5 - 3$
$2^4 + 2 = 3^3 - 3^2$
$2^3 + 2^2 = 3^2 + 3$
$2^7 + 2^2 = 11^2 + 11$
$2^{13} - 2 = 91^2 - 91$
$3^8 - 3^4 = 6^5 - 6^4$
$2^{16} + 2^6 = 40^3 + 40^2$

Are there other solutions? There are no others with terms less than 10^{20} when $a, b < 53000$.

Some references are Michael Bennett, On some exponential equations of S. S. Pillai, Canad. J. Math. 53 (2001) 897–922; Yann Bugeuad and Florian Luca, On Pillai's Diophantine equation, New York J. Math. 12 (2006) 193–217; Reese Scott and Robert Styer, On the generalized Pillai equation $\pm a^x \pm b^y = c$, J. Number Theory 118 (2006) 236–265.

007:04 (Andrew Shallue) Given a finite group G, and an element g of G, let $n_g(G)$ be the length of the longest sequence of (not necessarily distinct) elements of G for which no nonempty subsequence has product g, if such a maximum exists. Find conditions under which $n_g(G)$ exists, and find upper bounds for it in terms of invariants of G.

Remark: P. van Emde Boas and D. Kruyswijk, A combinatorial problem on finite abelian groups, III, Rep. No. ZW 1969-008, Math. Centrum, Amsterdam, 1969 proved that if G is a finite abelian group of order n and exponent m, then in any product of at least $m \log(en/m)$ group elements, there is a non-empty subproduct whose value is the identity. The result also appears in R. Meshulam, An uncertainty inequality and zero subsums, Discrete Math. 84 (1990) 197–200, and it was applied in W. R. Alford, Andrew Granville, Carl Pomerance, There are infinitely many Carmichael numbers, Ann. Math. 139 (1994) 703–722.

Note that picking appropriate conditions so that $n_g(G)$ even exists is already a challenging problem. If we allow subsequences for which all elements fall in a subgroup that g does not belong to, then $n_g(G)$ does not exist.

Motivation: Let a "double Carmichael" number be a composite square-free positive integer n such that for all prime $p \mid n$, $(p-1) \mid (n-1)$ and $(p+1) \mid (n+1)$. None have been found, but the following heuristic argument of Erdős gives a construction.

Choose smooth L and M such that $\gcd(L, M) = 2$. Find the set P of primes p such that $(p-1) \mid L$ and $(p+1) \mid M$. Find a subset of P whose elements multiply to the element

$(1, -1)$ in $\mathbf{Z}/L\mathbf{Z} \times \mathbf{Z}/M\mathbf{Z}$. It should be possible to choose L and M large enough so that $2^{|P|} > LM$, so then there should be an appropriate subset. Solving the problem would be one step towards proving that double Carmichael numbers exist.

007:05 (Geoffrey Apel) Let $F(k_1, k_2, \ell_1, \ell_2, \alpha) = \sum_{s,t \text{ in } \mathbf{Z}} q^{k_1 s^2 + k_2 t^2 + \ell_1 s + \ell_2 t + \alpha}$ with k_1, k_2 positive integers, ℓ_1, ℓ_2, and α integers. Let $I(k_1, k_2, \ell_1, \ell_2, \alpha) = \ell_1^2 k_2 + \ell_2^2 k_1 - 4k_1 k_2 \alpha$. Conjecture: If $\sum_{i=1}^{n} \pm F(k_1, k_2, \ell_{1i}, \ell_{2i}, \alpha_i)$ is identically zero, and no proper subsum is identically zero, then $I(k_1, k_2, \ell_1, \ell_2, \alpha)$ takes on the same value for $i = 1, \ldots, n$.

007:06 (David Moulton) Is there any n other than 1, 2, 5, 14, and 714 such that $n(n+1)$ is the product of the first k primes for some k?

Remark: This is equivalent to problem 93:08; If p_i is the ith prime, for which n is

$$4\prod_{i=1}^{n} p_i + 1$$

a square? David Bailey showed that if $P(x)$ is the product of the primes not exceeding x (so, e.g., $P(10) = 210$), then $4P(x) + 1$ is not a square for any x between 19 and 23000. Later, Peter Montgomery extended the search to $p_n < 50000$, finding no more examples.

The problem was also stated much earlier, in the original paper on Ruth-Aaron pairs; C. Nelson, D. E. Penney, C. Pomerance, 714 and 715, J. Recreational Math. 7 (1974) 87–89.

007:07 (Adrian Tang) Let $n > 1$ be an integer, let $S \subseteq \{1, 2, \ldots, n-1\}$ be such that n doesn't divide $\sum_{x \text{ in } S} x$. Prove that you can order the elements of S in such a way that n doesn't divide the sum of any consecutive block.

Remark: Equivalently, prove that you can order the elements of S in such a way that no two initial segments have the same sum, modulo n (where we include the empty initial segment, with sum zero).

The question can be asked in a wider context. Let G be any group, let S be any finite or countably infinite subset of G, not containing the identity element of G; if S is finite, we require in addition that there be at least one ordering of S such that the product of the elements of S, in this order, is not the identity of G. Then prove that you can order the elements of S in such a way that no two initial segments have the same product.

A related question which has an extensive literature is that of sequencing a group. Sequencing a finite group is ordering it in such a way that no two initial segments have the same product (this time, we don't include the empty initial segment). The abelian case was settled by Basil Gordon, Sequences in groups with distinct partial products, Pac. J. Math. 11 (1961) 1309–1313. A paper that deals with subsets of groups, and may thus be closer to the problem at hand, is David Bedford, A partial solution to a question raised by R. L. Graham, Ars Combin. 36 (1993) 289–295.

007:08 (Florian Luca and V. Janitzio Huguet Mejia) Let A be the set of even integers not expressible as $\pm 2^m \pm \varphi(k)$ for integers $m \geq 0$, $k \geq 1$ (where φ is the Euler phi-function). Show that A is infinite. Show that $\#(A \cap [1, x]) \gg x$.

Remark: It is known that there are infinitely many even integers not expressible as $2^m + \varphi(k)$; similarly for $2^m - \varphi(k)$, and for $\varphi(k) - 2^m$.

007:09 (Florian Luca and V. Janitzio Huguet Mejia) An odd number k is a Sierpinski number if $2^n k + 1$ is composite for all $n \geq 0$. Are there infinitely many primes p for which $2^p - 1$ is Sierpinski? Are there infinitely many n for which $2^{2^n} + 1$ is Sierpinski?

007:10 (Qingquan Wu) Let $D = pqr$ with p, q, and r distinct primes, $p \equiv q \equiv 3 \pmod 4$, $r \equiv 1 \pmod 4$. Let $x + y\sqrt{D}$ be the fundamental unit of $Q(\sqrt{D})$ with $x > 0$. Are there infinitely many D such that $x \equiv 5 \pmod 8$?

Solution: Gary Walsh shows that there aren't any such D. Rewrite $x^2 - Dy^2 = 1$ as $Dy^2 = (x+1)(x-1)$. The power of 2 dividing the left side is even, but if $x \equiv 5 \pmod 8$ (or if $x \equiv 3 \pmod 8$) then the power of 2 dividing the right side is 3. Note that the only fact used about D is that it is odd.

Qingquan Wu now asks whether there are infinitely many $D = pqr$ as above such that each of the congruences $x \equiv 1 \pmod 8$ and $x \equiv 7 \pmod 8$ holds; similarly, and independently, each of the congruences $y \equiv 0 \pmod 8$ and $y \equiv 4 \pmod 8$.

007:11 (Gerry Myerson) Find useful conditions on a function f which guarantee

$$\sum_{n \leq x, n \text{ squarefree}} f(n) = \left(6\pi^{-2} + O(1)\right) \sum_{n \leq x} f(n)$$

Remark: We assume $\sum_{n \leq x} f(n)$ goes to infinity with x. The equation holds for power functions $f(n) = n^r$ for any $r \geq -1$. The set of all f for which the equation holds forms a vector space, and it is closed under small perturbations, that is, if the equation holds for f, and g is small compared to f, then it holds for $f + g$.

David Moulton points out that it can't hold if f grows too fast (say, exponentially), for then the sums are dominated by their biggest summand.

007:12 (John Brillhart) Find interesting functions f such that $f(f(x)) = -x$.

Remarks: 1. A long list of references to this sort of problem is Lars Kindermann's webpage on Iterative Roots and Fractional Iteration, http://reglos.de/lars/ffx.html

2. John amends his problem to ask for interesting solutions to $f\big(af(x/a)\big) = x$. He notes that the Gudermanian, $\text{gd}(x) = \arctan \sinh x$, satisfies this functional equation when $a = -i$.

007:13 (Gary Walsh) Prove that F_n and L_n are both prime for $n = 148091$.

Remark: F_n are the Fibonacci numbers with $F_0 = 0$, $F_1 = 1$, and L_n are the Lucas numbers with $L_0 = 2$, $L_1 = 1$. They are both prime for $n = 4, 5, 7, 11, 13, 17$, and 47. No other value of N is known for which both have been proved prime, but both are probable primes for $n = 148091$.

007:14 (Gary Walsh) A polynomial $f(x)$ with integer coefficients is "primitive reducible" if it is reducible but $f(x^{1/e})$ is not reducible for any $e > 1$. For example, $x^4 + 4$ is primitive reducible. Is there a primitive reducible polynomial of the form $x^i + x^j + x^k + 4$ with $0 < k < j < i$ and $i > 17$? Aside from

$$x^7 + x^5 + x^3 + 8 = (x^3 - x^2 - x + 2)(x^4 + x^3 + 3x^2 + 2x + 4)$$

is there a primitive reducible polynomial of the form $x^i + x^j + x^k + n$ with $0 < k < j < i$ and $n > 4$, and not divisible by a linear or quadratic polynomial?

007:15 (Leon McCulloh) Let G be a finite abelian group. Let $\hat{G} = \mathrm{Hom}(G, \mathbf{C}^\times)$. Define a $\mathbf{Q}$-bilinear map: $\mathbf{Q}\hat{G} \times \mathbf{Q}G \to \mathbf{Q}$, $(\chi, s) \mapsto \langle \chi, s \rangle$ where $\chi(s) = e^{2\pi i \langle \chi, s \rangle}$ and $0 \leq \langle \chi, s \rangle < 1$. Define a $\mathbf{Q}$-linear map $\theta : \mathbf{Q}\hat{G} \to \mathbf{Q}G$ by $\theta(\chi) = \sum_{s \text{ in } G} \langle \chi, s \rangle s$. Let $S_G = \theta(\mathbf{Z}\hat{G}) \cap \mathbf{Z}G$.

(i) Conjecture: If ℓ is an odd prime, and G an abelian ℓ-group, then $\#\big(\mathrm{Cl}(\mathbf{Z}G)^-\big) = [\mathbf{Z}G^- : S_G^-]$, where $\mathrm{Cl}(\mathbf{Z}G)$ is the (locally free) class group of $\mathbf{Z}G$ and $()^-$ refers to the skew-symmetric part with respect to the canonical involution $s \mapsto s^{-1}$ of G.

(ii) Find appropriate generalizations if G is abelian but not an ℓ-group; if G is not abelian.

Remark: For reference, see the two papers by McCulloh, A class number formula for elementary abelian group rings, J. Alg. 68 (1981) 443–452, and Galois module structure of abelian extensions, Crelle 375/376 (1987) 259–306.

Supplement to the problem set — John Brillhart tells a Paul Erdős story

During the first 30 years of the Western Number Theory conference the problem sessions were run by John Selfridge. Paul Erdős always attended if he didn't have more pressing plans to be elsewhere.

At the problem session, as at the meeting itself, Paul always sat in the first row, often apparently nodding off during the proceedings.

There always came a point in the problem session when John asked for another problem, and no one replied. He then turned to Paul, who always had a problem to contribute.

This happened at one meeting and John turned to Paul, who was apparently deep in sleep. He asked, "Paul, do you have a problem?" Paul roused himself, gesturing weakly with his hand, and said, "I'll be all right in a minute." Everyone laughed.