Western Number Theory Problems, 12, 16 & 18 Dec 2008

Edited by Gerry Myerson

for distribution prior to 2009 (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	004:01–004:17		2005 Asilomar	005:01–005:12
2006 Ensenada	006:01–006:15		2007 Asilomar	007:01–007:15
2008 Fort Collins (current set)	008:01–008:15			

[With comments on 006:01]

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

006:01 (Claude Anderson, via Carl Pomerance) Is it true that if n is even and m is odd then $\sigma(n)/n \neq \sigma(m)/m$?

Remark: If so, then there are no odd perfect numbers.

Solution: Walter Nissen points out that Anderson and Dean Hickerson discuss pairs m and n such that $\sigma(n)/n = \sigma(m)/m$ in problem 6020, Amer. Math. Monthly 84 (1977) 65–66. They give two examples of such pairs of opposite parity, $n = 42$, $m = 544635 = 3^2 \cdot 5 \cdot 7^2 \cdot 13 \cdot 19$, and $n = 2 \cdot 3^6 \cdot 23 \cdot 137 \cdot 547 \cdot 1093$, $m = 3^4 \cdot 5 \cdot 7 \cdot 11^2 \cdot 19$. Many more examples can be extracted from http://upforthecount.com/math/ffp8.html.

Problems proposed 12, 16, and 18 December 2008

There was a Number Theory problem session at the 7th Joint Australia-New Zealand Mathematics Convention at the University of Canterbury in Christchurch, New Zealand. The first seven problems below were presented at that session.

008:01 (John Friedlander) Let f be an irreducible integer-valued polynomial in two variables with no fixed prime divisor. Make a plausible conjecture as to $\pi_f(x)$, the number of primes not exceeding x in the range of f. Similarly, let f and g be integer-valued polynomials in three variables such that there is no trivial reason why they can't be simultaneously prime infinitely often, and with infinitely many different prime values. Make a plausible conjecture as to the number of pairs of primes, neither exceeding x, in the range of the ordered pair (f, g).

Remark: Let $f_1, \ldots, f_m$ be distinct irreducible polynomials in one variable with integer coefficients. Let f be their product, and suppose there is no prime p which divides $f(n)$ for all n. Let $P(x)$ be the number of integer arguments not exceeding x at which all the polynomials are prime. Then Bateman and Horn, "A heuristic asymptotic formula concerning the distribution of prime numbers," Math. Comp. 16 (1962) 363–367, MR 26 #6139, conjecture that

$$P(x) \sim (C/D) \int_2^x (\log t)^{-m}\, dt, \qquad C = \prod_p \frac{1 - N(p)/p}{(1 - 1/p)^m}$$

where $N(p)$ is the number of solutions of $f(x) \equiv 0 \pmod p$, and D is the product of the degrees of the polynomials. What is wanted here is analogous conjectures for polynomials in two variables, and for pairs of polynomials in three variables.

008:02 (Mike Bennett) Let $f(x, y) = x^4 + y^4$, $G(u, v) = u^4 + 12u^2v^2 + 4v^4$. Let P_F (resp., P_G) be the set of primes represented by F (resp., G).

(i) Give plausible asymptotic formulas for $\#\{\, p \leq N : p \text{ is in } P_F \,\}$ and for $\#\{\, p \leq N : p \text{ is in } P_G \,\}$.

(ii) What is $P_F \cap P_G$?

Remarks: The first question is a special case of 008:01, above. The particular polynomials F and G are of interest in connection with congruent numbers. Concerning the second question, among the first 300,000 primes in P_F, the only one in P_G is 17. John Friedlander suggests checking to see how many numbers up to N (not restricting to primes) are represented by both F and G (other than numbers of the forms s^4 and $17s^4$). There are such numbers, e.g.,

$$23137 = (17)(1361) = F(7,12) = G(9,4)$$
$$50881 = (17)(41)(73) = F(4,15) = G(3,10)$$
$$72097 = (17)(4241) = F(9,16) = G(11,6)$$
$$32300017 = (17)(257)(7393) = F(39,74) = G(57,23)$$
$$38241857 = (17)(257)(8753) = F(47,76) = G(31,44)$$

Solution: Jing Long Hoelscher has a proof that $P_F \cap P_G = \{\,17\,\}$. Here is an outline.

$f(x,y) = N(x+y\zeta_8)$, and $g(u,v) = N\big(u+(2+\sqrt{2})iv\big)$, where ζ_8 is a primitive complex 8th root of unity and N is the norm from $\mathbf{Q}(\zeta_8)$ to $\mathbf{Q}$. If p is in $P_F \cap P_G$ then this yields two factorizations of (p) into products of four prime ideals. We may assume $(x+y\zeta_8) = \big(u+(2+\sqrt{2})iv\big)$ as ideals (there are other cases which can be dealt with by the same methods). This can be shown to imply that $\big(u+(2+\sqrt{2})iv\big)/(x+y\zeta_8)$ is a unit. Then by Dirichlet's Unit Theorem, $\big(u+(2+\sqrt{2})iv\big)/(x+y\zeta_8) = (1+\sqrt{2})^a\zeta_8^b$. Analyzing the eight possibilities for b leads to $p = 17$ in one case and to contradictions in all other cases.

Mike Bennett was also able to solve this part of the problem.

008:03 (Kevin Broughan) The odd part of a natural number n is the largest odd number dividing n. Prove that there are infinitely many primes p such that the odd part of $p+1$ is prime.

Remark: Of course for each fixed $e \geq 1$ it is conjectured that there are infinitely many primes p such that $(p+1)/2^e$ is prime. The question is whether letting e vary makes it any easier to get a proof.

008:04 (Andrew Bremner, via Gary Walsh) Find all rational points on $y^2 = x^6 + k$ for $k = -39$, $k = -47$.

008:05 (Mike Bennett, via Gary Walsh) Let $\alpha = 3 + 2\sqrt{2}$, and $\alpha^8 = 665857 + 470832\sqrt{2} = v + u\sqrt{2}$. Then v is prime. Let $\alpha^{8v} = v' + u'\sqrt{2}$. Then $v^2 \mid v'$. Let $N = v'/v^2$. Is N composite? Is N a prime times a square?

008:06 (Gary Walsh) Let d and k be relatively prime squarefree positive integers. Let $N(d,k)$ be the number of solutions of $x^2 - dy^4 = k$ in relatively prime positive integers x and y. Prove that $N(d,k)$ is bounded independent of d.

Remark: (Patrick Rault) Homogenize the equation to $z^2x^2 - dy^4 = kz^4$. Then consider the related equation $xz - dy^2 - kz^2 = 0$ This equation can be parametrized by $\phi : \mathbf{P}^1 \to \mathbf{P}^2$ given by $(u:v) \mapsto (dku^2 + k^2v^2 : kuv : du^2)$. So it suffices to count $(u:v)$ in $\mathbf{P}^1(\mathbf{Q})$ such that the representation of $(dku^2 + k^2v^2 : kuv : du^2)$ as coprime integers is a triple of square integers.

008:07 (Florian Luca) Let $\begin{bmatrix} n \\ k \end{bmatrix}_F = \dfrac{F_nF_{n-1}\cdots F_{n-k+1}}{F_1F_2\cdots F_k}$ where F_j are the Fibonacci numbers, and let $\begin{bmatrix} n \\ k \end{bmatrix}_q = \dfrac{(q^n-1)(q^{n-1}-1)\cdots(q^{n-k+1}-1)}{(q-1)(q^2-1)\cdots(q^k-1)}$, q an integer.

(i) Find all solutions of $\begin{bmatrix} n \\ k \end{bmatrix}_F = y^\ell$ with $n \geq 2k \geq 2$, $\ell \geq 2$, y an integer.

(ii) Find all solutions of $\begin{bmatrix} n \\ k \end{bmatrix}_q = y^\ell$ with $n \geq 2k \geq 2$, $\ell \geq 2$, y an integer, $q > 1$.

008:08 (Maurizio Monge, via Bart Goddard) Is there a polynomial in two variables which is a bijection from $\mathbf{Z} \times \mathbf{Z}$ to $\mathbf{Z}$?

Remarks: The question appeared on the NMBRTHRY list on 4 December 2008. It was also sent to the Usenet newsgroup sci.math by Carlo Mantegazza on 29 November 2008, with the subject header, Map problem. It is trivial to find a surjection, and not too hard to find an injection. The problem of finding a polynomial injection from $\mathbf{Z}^4$ to $\mathbf{Z}$ was studied by Zachary Abel, My favorite problem: Bert and Ernie, Harvard Coll. Math. Rev. 1 (2007) 78–83.

It is well-known that $f(x,y) = (1/2)(x+y)(x+y-1)-y+1$ gives a bijection from $\mathbf{N}\times\mathbf{N}$ to $\mathbf{N}$.

008:09 (Stefan Erickson) Given a finite set $S = \{ x_1, \ldots, x_n \}$ of positive real numbers, find a closed formula — or, failing that, good asymptotics — for $F(x)$, the number of n-tuples $(a_1, \ldots, a_n)$ of non-negative integers such that $a_1x_1 + \ldots + a_nx_n \le X$.

Remarks: This has applications to the number of compounds of bounded molecular weight. It can also be interpreted as the number of lattice points in the region in the positive orthant cut off by a hyperplane. A reference is Beck and Robins, Computing The Continuous Discretely, Springer 2007.

008:10 (Ming-Hsuan Kang) Given a finite field $\mathbf{F}_q$, we are interested in the set S of all polynomials Φ in an indeterminate u with coefficients in $\mathbf{F}_q(t)$ such that $\Phi(f)$ is in $\mathbf{F}_q[t]$ for all f in $\mathbf{F}_q[t]$. If $N = a_0 + a_1q + \ldots + a_mq^m$ for some non-negative integers $a_0, \ldots, a_m$, then the polynomial

$$\Phi_N(u) = u^{a_0} \prod_{k=1}^{m} \left(\frac{u^{q^k} - u}{t^{q^k} - t} \right)^{a_k}$$

has degree N, and $\Phi_N(u)$ is in S. Do the polynomials $\Phi_N(u)$ generate S (in the sense that every member of S is a linear combination of such polynomials, with coefficients in $\mathbf{F}_q[t]$)?

Remark: It is well-known that the integer-valued polynomials with rational coefficients are precisely the integer linear combinations of the polynomials $\binom{x}{k}$, $k = 0, 1, \ldots$. The question is an attempt to find for $\mathbf{F}_q[t]$ the polynomials analogous to $\binom{x}{k}$ for $\mathbf{Z}$.

Solution: Jianqiang Zhao, after consulting with David Goss, writes that the required generators are the Carlitz polynomials. He recommends Keith Conrad, "The digit principle," J. Number Theory 84 (2000) 230–257, MR 2001i:11143.

008:11 (Patrick Rault) Let f and g be integral binary forms of degree $d \ge 2$. An invariant of weight k on pairs (f, g) of forms is a $\mathbf{Q}$-valued function I such that

$$I(f \circ \gamma, g \circ \gamma) = (\det \gamma)^k I(f, g)$$

for all γ in $\mathrm{GL}_2(\mathbf{Z})$. Find the dimension of the algebra of invariants (or bounds for this dimension) as a function of d. Better yet, find a basis for each d.

Remarks: A reference is Olver, Classical Invariant Theory. The Hilbert Basis Theorem guarantees that these algebras are all finite-dimensional, but its proof is not constructive.

008:12 (Mike Knapp) Given a finite sequence $a_1, \ldots, a_n$ of positive integers with largest term b, we define a_j, $j > n$, to be the smallest integer exceeding b and not representable as the sum of a subset of $\{ a_1, \ldots, a_{j-1} \}$. For example, the sequence 1, 5 generates the sequence $1, 5, 7, 9, 11, 29, 31, 89, 91, 269, 271, \ldots$ where the pattern $10 \times 3^k - 1, 10 \times 3^k + 1$ that begins with 9, 11 continues forever. Is it the case that no matter what the given initial terms the sequence always develops some sort of pattern?

Remarks: A student of Mike's has settled the cases $n = 2$ with $a_1 = 1$, also with $a_2 - a_1 = 1$. Sunil Chetty asks whether one can always find $a_1, \ldots, a_n$ so that the continuation of the sequence will contain a given pair of terms; also whether two different sequences can be equal from some point on.

David Terr offered a reformulation of the problem. Given $B = \{ s_1, \ldots, s_k \}$, an increasing finite sequence of positive integers, define s_j for $j \geq k$ by letting s_{i+1} be the least integer exceeding s_i and not the sum of a subset of $\{ s_1, \ldots, s_i \}$. Let $S(B)$ be the infinite sequence $s_1, s_2, \ldots$. Then the conjecture is that every $S(B)$ is of the form $B, P, F_0, F_1, \ldots$ where $F_k = \Phi + ab^k$, $a = (1/\#F_0) \sum_{s \text{ in } F_0} s$, $\Phi = F_0 - a$, and $b = \#\Phi + 1$. Here $\#$ refers to the number of terms in a finite sequence, and $F_0 - a$ means subtract a from each term in the sequence F_0 ($\Phi + ab^k$ is interpreted similarly). In the example above, P (the "pre-period") is $\{ 7 \}$, $F_0 = \{ 9, 11 \}$, $\#F_0 = 2$, $a = 10$, $\Phi = \{ -1, 1 \}$, and $b = 3$.

Now let $k = \#(B)$, and for $i \geq k$ let $\sigma_i = \sum_{j \leq i} s_j$, and define G_i by

$$G_i = \{ g : 0 < g < \sigma_i, g \text{ is not the sum of any subset of } \{ s_1, \ldots, s_i \} \}$$

It is claimed that G_i is symmetric about its midpoint. Further it is claimed that the following conjecture implies an affirmative answer to the original question, and may be easier to settle: There exist i and j with $j > i \geq k$ such that $G_i = \Gamma \cup (\sigma_i - \Gamma)$ and $G_j = \Gamma \cup (\sigma_j - \Gamma)$ where $\Gamma = G_k \cap \{ 1, \ldots, \sigma_k \}$.

008:13 (Bart Goddard) Find all interesting functions $f : \Omega \to \mathbf{C}$ such that for all z in some domain Ω symmetric with respect to the real line we have $|f(z)| = |f(\overline{z})|$. "Interesting" means meromorphic in Ω and having a Taylor expansion at some real z_0 with at least one non-real coefficient.

Remark: The conditions permit $f(z) = \alpha g(z)$, where α is in $\mathbf{C}$ and $g(z)$ has a Taylor expansion at some real z_0 with all coefficients real, but presumably we want something more interesting.

Solution: I posted this problem to the Usenet newsgroup sci.math, and received several helpful replies. This comes from Robert Israel.

$\overline{f(\overline{z})}/f(z)$ is analytic in Ω (except at zeros of f) and has absolute value 1 everywhere, therefore is constant (and the zeros of f are removable singularities). Say this constant is e^{ir} where r is real, and let $g(z) = e^{ir/2} f(z)$. For x in $\Omega \cap \mathbf{R}$, we have $\overline{g(x)} = e^{-ir/2} \overline{f(x)} = e^{ir/2} f(x) = g(x)$, i.e., $g(x)$ is real. Thus the Taylor series of $g(z)$ about any point of $\Omega \cap \mathbf{R}$ has all real coefficients.

008:14 (Mike Knapp) Let p be a prime, let $k > 2$ be a divisor of $p - 1$. Find upper bounds in terms of p and k for the smallest m such that $\{ 1^k, 2^k, \ldots, m^k \}$ is the set of all k-th powers modulo p.

Remark: For $k = 2$ it's easy to see that $m = (p - 1)/2$.

008:15 (Lenny Fukshansky) A plank in $\mathbf{R}^n$ is the region between two parallel hyperplanes. The width of a plank is the distance between the two hyperplanes. The width $w(M)$ of a compact set M in $\mathbf{R}^n$ is the minimal width of a plank containing M.

Let M_1 be a convex set of least width containing M, and let M_2 be a convex set of greatest width contained in M. Suppose that M is covered by a finite set of planks of widths $h_1, \ldots, h_k$. Find conditions on M for which one can prove an inequality of the form $h_1 + \ldots + h_k \geq f\big(w(M_1), w(M_2)\big)$ with $f\big(w(M_1), w(M_2)\big) > w(M_2)$.

Remark: A conjecture of Tarski, proved by Thøger Bang (A solution of the "plank problem", Proc. Amer. Math. Soc. 2 (1951) 990–993, MR 13, 769a), asserts that if M is convex then $h_1 + \ldots + h_k \geq w(M)$. In the problem at hand, this implies $h_1 + \ldots + h_k \geq w(M_2)$.