Western Number Theory Problems, 18 & 20 Dec 2003

Edited by Gerry Myerson

for distribution prior to 2004 (Las Vegas) 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 (current set)	003:01–003:08

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

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) Yes. In fact, for all $k \geq 0$, $t_k = 3 \times 2^{4k+3}$ is not of the form $f(p) = (p-1)/2 - \phi(p-1)$ for any odd prime p.

Proof: Let p be any odd prime, and write p as $p = 1 + (2^a)m$, with m odd and $a > 0$. Assume that $t_k = f(p)$. It follows that $t_k = 2^{a-1}(m - \phi(m))$. Since $f(p) = t_k > 0$, it follows that $m > 1$, and so $m - \phi(m)$ must be odd. This forces $a = 4k+4$ and $m - \phi(m) = 3$. But $m - \phi(m) = 3$ implies that $m = 9$, and therefore $p = 1 + 9 \times 2^{4k+4}$, which is always divisible by 5, contradicting the assumption that p is prime. Therefore $t_k = f(p)$ is not possible.

More generally, Luca and Walsh can prove that for each odd $w > 1$, there are infinitely many t for which $(2^t)w$ is not of the form $f(p)$ for any prime p.

Problems Proposed 18 & 20 Dec 2003

003:01 (Neville Robbins) Let $p(n)$ be the partition function. Is it true that for $n \geq 2$ the number of distinct degree sequences of trees with n nodes is $p(n-2)$?

Solution: (Greg Martin) Yes. A tree with n nodes has $n-1$ edges, so the degrees of the nodes add up to $2n-2$. Thus if the degree sequence is $d_1 \geq d_2 \geq \ldots \geq d_n$, then $(d_1 - 1) + (d_2 - 1) + \ldots + (d_n - 1) = n - 2$ is a partition of $n-2$.

Going the other way, let $a_1 + a_2 + \ldots + a_r = n - 2$ be a partition of $n-2$, with $a_1 \geq a_2 \geq \ldots \geq a_r \geq 1$. Then we construct a tree with degree sequence $a_1 + 1$, $a_2 + 1$, $\ldots$, $a_r + 1, 1, 1, \ldots, 1$, where the number of 1s is $n - r$, as follows. First draw a path with r nodes, labeling them $v_1, v_2, \ldots, v_r$. Draw $n - r$ isolated nodes. For i from 1 to r draw an edge from v_i to enough of the (formerly) isolated nodes to raise the degree of v_i to $a_i + 1$; don't connect any isolated node to more than one path node. There are just enough isolated nodes to go around, and the result is a tree on n nodes with the given degree sequence.

The two maps between degree sequences and partitions are inverse to each other, so the cardinalities are equal.

Solution: (David Moulton) The degree sequence $d_1 \geq d_2 \geq \ldots \geq d_n$ of a tree with n nodes gives a partition $d_1 + d_2 + \ldots + d_n = 2n - 2$ of $2n - 2$ with n parts. Conversely, we prove by induction on n that every partition of $2n-2$ into n parts is a degree sequence. The case $n = 2$ is trivial. Suppose then $a_1 + a_2 + \ldots + a_n = 2n - 2$ with $a_1 \geq a_2 \geq \ldots \geq a_n$ and $n \geq 3$. Then $a_1 > 1$ and $a_n = 1$. Then $(a_1 - 1) + a_2 + \ldots + a_{n-1} = 2n - 4$ is a partition of $2n - 4$ into $n - 1$ parts. By the induction hypothesis, there is a tree with degree sequence $a_1 - 1, a_2, \ldots, a_{n-1}$. Add a leaf to the node of degree $a_1 - 1$, and you have a tree on n nodes with degree sequence $a_1, a_2, \ldots, a_n$.

Thus the number of degree sequences is the number of partitions of $2n-2$ into n parts. By subtracting 1 from each part we see this is $p(n-2)$.

003:02 (Peter Montgomery) Let k be an integer, $k \geq 2$. Let $S = \{1, 2, \ldots, k\}$. Select random subsets $S_1, S_2, \ldots$, of S. Let $p_{n,k}$ be the probability that $S_1, \ldots, S_n$ generate all the subsets of S under union, intersection, and complementation, but $S_1, \ldots, S_{n-1}$ don't. Find the generating function $f_k(x) = \sum_{n=0}^{\infty} p_{n,k} x^n$.

Remarks: 1. If N has k distinct prime factors then $p_{n,k}$ is the probability that the General Number Field Sieve will need exactly n dependencies to factor N.

2. $f_2(x) = x/(2-x)$, $f_3(x) = 3x^2/(4-x)(2-x)$.

003:03 (Jim Hafner) Let q be a prime power. Let β be an element of order n in $\mathrm{GF}(q)$, $\beta \neq 0$. Let $V(\beta)$ be the matrix with entries $v_{ij} = \beta^{ij}$, $i = 0, \ldots, n-1$, $j = 0, \ldots, n-1$. For $m = 1, \ldots, n$ let W_m be the set of $n \times m$ submatrices of $V(\beta)$, that is, matrices formed from m columns of $V(\beta)$. For W in W_m let $r(\beta, W)$ be the smallest integer r such that every $n \times (n+r)$ submatrix of $(I_n|W)$ has rank n (here $(I_n|W)$ is the matrix obtained by augmenting the $n \times n$ identity matrix by W). Find $r(\beta, m) = \max_W r(\beta, W)$, and characterize those W for which $r(\beta, W) = r(\beta, m)$.

Remark: If $q = 2^3$, $n = 7$, and β is any non-zero element of $\mathrm{GF}(q)$ then $r(\beta, m) = 0$ if $1 \leq m \leq 3$, $r(\beta, m) = 1$ if $4 \leq m \leq 7$, and W can be chosen as the first m columns of $V(\beta)$.

003:04 (Tsz Ho Chan) Is it true that $\left|\sum_{n \leq x} \left(\frac{n(n+1)}{p}\right)\right| \gg \sqrt{p}$ for some x? More generally, is it true that if $f(x)$ is in $\mathbf{Z}[x]$ then $\left|\sum_{n \leq x} \left(\frac{f(n)}{p}\right)\right| \gg \sqrt{p}$ for some x? Here p is a prime and $\left(\frac{a}{p}\right)$ is the Legendre symbol.

Remark: It is known that $\left|\sum_{n \leq x} \left(\frac{n}{p}\right)\right| \gg \sqrt{p}$ for some x.

003:05 (Kevin O'Bryant) Given integers x and q write $|x|_q$ for the distance from x to the nearest multiple of q, that is, $|x|_q = \min\{\, |x - qn| : n \text{ in } \mathbf{Z} \,\}$. For x relatively prime to q write x' for the inverse of $x \pmod q$. Conjecture: if $x_1, \ldots, x_m$ are relatively prime to q and $|x_r|_q \neq |x_s|_q$ for $r \neq s$, and if $q > q_0(m)$, then there is a j in $\{x'_1, \ldots, x'_m\}$ such that $\sum_{k=1}^{m} \frac{1}{|jx_k|_q} < 2$.

Solution: (Greg Martin) It suffices to show that under the hypotheses there exists k, $1 \leq k \leq m$, such that $|x'_k x_i|_q \geq (q-1)^{1/m}$ for all i, $1 \leq i \leq m$, $i \neq k$. For if this is true then choosing $j = x'_k$ gives $\sum_{i=1}^{m} \frac{1}{|jx_i|_q} < 1 + (m-1)/(q-1)^{1/m} \leq 2$ for $q > (m-1)^m$.

So suppose to the contrary for each k, $1 \leq k \leq m$, there exists i, $1 \leq i \leq m$, $i \neq k$, with $|x'_k x_i|_q < (q-1)^{1/m}$. Form the directed graph on vertices $\{1, 2, \ldots, m\}$ with an arc from k to i if $i \neq k$ and $|x'_k x_i|_q < (q-1)^{1/m}$. Then each vertex has outdegree at least 1, so the graph has a cycle. Relabeling, if necessary, we may assume the cycle joins 1 to 2, 2 to 3, …, $r-1$ to r, and r to 1, for some r.

Now let $x'_1 x_2 \equiv b_1 \pmod q$, $x'_2 x_3 \equiv b_2 \pmod q$, …, $x'_r x_1 \equiv b_r \pmod q$, with $1 < |b_i| < (q-1)^{1/m}$ for $1 \leq i \leq r$. Then $b_1 \times \ldots \times b_r \equiv x'_1 x_2 x'_2 x_3 \ldots x'_r x_1 \equiv 1 \pmod q$, so $|b_1 \times \ldots \times b_r| \equiv \pm 1 \pmod q$. But $1 < |b_1| \times \ldots \times |b_r| < \left((q-1)^{1/m}\right)^r \leq q-1$, contradiction.

003:06 (David Bailey) Find an analytic evaluation of $\alpha = \int_0^\infty \cos 2x \left(\prod_{n=1}^\infty \cos \frac{x}{n}\right) dx$.

Remark: α agrees with $\pi/8$ to 43 decimals, but $\alpha \neq \pi/8$.

003:07 (Peter Borwein) Suppose that n is even, $n > 12$. Let

$$p_n(z) = n + 1 + (-1)^{n/2} \sum_{k=-n/2, k\neq 0}^{n/2} z^{2k}.$$

Show that $z^n p_n(z)$ is irreducible over the rationals.

003:08 (David Angell via Gerry Myerson) Find a closed form for $\sum_{n=1}^\infty \frac{\phi(n)}{2^n}$, where ϕ is Euler's function.