Western Number Theory Problems, 16 & 18 Dec 2010

Edited by Gerry Myerson

for distribution prior to 2011 (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	008:01–008:15	2009 Asilomar	009:01–009:20
2010 Orem	010:01–010:12		

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

010:01 (Bart Goddard). Given a positive integer k, estimate $n = n(k)$, the smallest modulus to which there are k consecutive quadratic non-residues.

Remarks: Bart notes that a weak upper bound for $n(k)$ can be given by letting b_i be a quadratic non-residue modulo p_i such that b_i+1 is also a non-residue, where p_i are consecutive primes, $1 \le i \le \ell$, starting with $p_1 = 5$ (there are always pairs of consecutive non-residues modulo any prime $p \ge 5$). Let x satisfy $x + 2i - 1 \equiv b_i \pmod{p_i}$, $1 \le i \le \ell$. Then $x, x+1, \ldots, x+2\ell-1$ are quadratic non-residues modulo $p_1 p_2 \ldots p_\ell$, so $n(2\ell) \le p_1 p_2 \ldots p_\ell$, which is roughly ℓ^ℓ.

For k odd, one can adjoin the congruence $x - 1 \equiv 2 \pmod 3$ to get $n(2\ell+1) \le 3p_1 p_2 \ldots p_\ell$.

There is a considerable literature on the greatest possible number of consecutive quadratic non-residues for a prime modulus. A good reference is Patrick Hummel, On consecutive quadratic non-residues: a conjecture of Issai Schur, J. Number Theory 103 (2003) 257–266, MR 2004k:11157. Hummel gives an elementary proof that $p = 13$ is the only prime number for which the greatest number of consecutive quadratic non-residues modulo p exceeds $p^{1/2}$. Hummel also summarizes earlier work which gives sharper bounds on the order of $p^{1/4}\log p$, but those bounds involve constants which are not explicit. It is not immediately clear how to relate these results to the problem for arbitrary modulus.

010:02 (Bart Goddard). Prove that $12^2 = 111+33$, $38^2 = 1111+333$, and $211^2 = 44444+77$ are the only examples of two repdigit numbers summing to a square, excluding cases where one number is a single digit, or where each number is two digits long.

Remarks: Bart explains, write $(10^m - 1)a/9 + (10^n - 1)b/9 = k^2$ with a, b non-zero digits. Rewrite as $10^m a + 10^n b - c = (3k)^2$ where $2 \le c = a + b \le 18$. If $m \ge 6$ and $n \ge 6$ then this is $-c \equiv (3k)^2 \pmod{10^6}$, and it happens that all the integers $-2, -3, \ldots, -18$ are quadratic non-residues modulo 10^6, so there are no solutions with $m \ge 6$ and $n \ge 6$. Many of the cases with smaller values of m and n can be ruled out by congruences modulo smaller powers of 10, reducing the problem to 7 cases. Writing a_m for $(10^m - 1)a/9$, these cases are $2_m + 22, 3_m + 111, 8_m + 33, 6_m + 55, 4_m + 77, 2_m + 99, 7_m + 99999$; the problem is now to show that these forms yield no squares other than the known cases.

Solution: Jeremy Rouse writes each of the remaining cases as $(10^m - 1)a/9 + d = k^2$, or $10^m a + e = 9k^2$, with $e = 9d - a$. Considering m modulo 3, any solution to these equations will be an integer point on one of the elliptic curves $ay^3 + e = x^2, 10ay^3 + e = x^2, 100ay^3 + e = x^2$ with y a power of 10. By Siegel's Theorem, each of the resulting 21 elliptic curves has only finitely many integer points, so there are in any event only finitely many solutions. Magma has software to find all the solutions. Running this software reveals that there are no solutions other than those already known.

010:03 (Gerry Myerson). How small can

$$\left|\frac{1}{a} + \frac{1}{b} + \frac{1}{c} - \frac{1}{d}\right|$$

be, as a function of n, if it isn't zero, and if a, b, c, d are taken from $\{1, 2, \ldots, n\}$?

Remarks: 1. This question grew out of question 40819 on mathoverflow.net, "The difference of two sums of unit fractions," posted by Anadim.

2. The quantity is a rational number with numerator at least 1 and denominator at most n^4, so a trivial lower bound is n^{-4}. The question is to what extent can one improve on this bound.

3. The more general question is, for fixed r and s, how small can

$$\left|\frac{1}{a_1}+\cdots+\frac{1}{a_r}-\frac{1}{b_1}-\cdots-\frac{1}{b_s}\right|$$

be, as a function of n, if it isn't zero, and if $a_1,\ldots,a_r,b_1,\ldots,b_s$ are taken from $\{1,2,\ldots,n\}$? For $r=s=1$ it is easily seen that $|(n-1)^{-1}-n^{-1}|\approx n^{-2}$ is best possible. For $r=2, s=1$, $|(2m+1)^{-1}+(2m-1)^{-1}-m^{-1}|\approx 2n^{-3}$ for $n=2m+1$ is best possible. For $r=s=2$ there are formulas to show that we can asymptotically achieve n^{-4}. Here we ask about the case $r=3, s=1$.

4. Macquarie undergraduate Charles Walker has been looking at this problem. He points out that by a simple argument we can improve the lower bound to $3n^{-4}$ (and in the general case, the trivial lower bound of $n^{-(r+s)}$ can be improved, for $r\ge s$, to $(r-s+1)n^{-(r+s)}$). He has also found the identity

$$\left|\frac{1}{6x^2-1}+\frac{1}{6x^2+12x+5}+\frac{1}{6x^2+6x-1}-\frac{1}{2x^2+2x-1}\right|=\frac{4}{P}$$

where $P=(6x^2-1)(6x^2+12x+5)(6x^2+6x-1)(2x^2+2x-1)$, and the right side is asymptotic to $12n^{-4}$ for $n=6x^2+12x+5$. Charles has also found

$$\frac{1}{1583}+\frac{1}{1541}+\frac{1}{1530}-\frac{1}{517}=\frac{1}{(1583)(1541)(1530)(517)}=\frac{3.25}{(1583)^4}$$

010:04 (Gerry Myerson). Let $h(n)$ be the sum, over all partitions of n into at most three parts, of the largest part:

$$h(n)=\sum_{\substack{a\ge b\ge c\ge 0\\ a+b+c=n}} a$$

Is it true that

$$\sum_{n=1}^{\infty} h(n)x^n=\frac{x+3x^2+4x^3+3x^4}{(1-x^2)^2(1-x^3)^2}$$

Remarks. 1. This question grew out of Math Overflow question 30716, "Inequality constraints, probability distributions, and integer partitions," posted by Jonathan Fischoff.

2. For $n=1,\ldots,12$ we get $h(n)=1,3,6,11,17,27,37,52,69,90,113,144$, a sequence not yet appearing in the Online Encyclopedia of Integer Sequences.

3. A consequence of equality would be the estimate $h(n)=(11/216)n^3+O(n^2)$.

4. The problem generalizes in several directions. For positive integers j,k,n we let $f_{j,k}(n)$ be the sum, over all partitions of n into at most k parts, of the jth largest part:

$$f_{j,k}(n)=\sum_{\substack{a_1\ge\ldots\ge a_k\ge 0\\ a_1+\cdots+a_k=n}} a_j$$

In this notation, $h(n)$ is $f_{1,3}(n)$. We can ask for the behavior of $f_{j,k}(n)$ as n goes to infinity, subject to various conditions on j and k.

Solution: George Andrews notes that if we let $H(q) = \sum h(n)q^n$, and let $c = t$, $b = s+t$, $a = r + s + t$, then

$$H(q) = \sum_{n=0}^{\infty} \sum_{\substack{r,s,t \geq 0 \\ r+2s+3t=n}} (r + s + t)q^{r+2s+3t}$$

Now let $J(z, q) = \sum_{r,s,t\geq 0} z^{r+s+t}q^{r+2s+3t}$. Then $J_z(1, q) = H(q)$, but also

$$J(z, q) = \sum_r (zq)^r \sum_s (zq^2)^s \sum_t (zq^3)^t = \frac{1}{(1 - zq)(1 - zq^2)(1 - zq^3)}$$

from which one easily calculates $J_z(1, q) = (q + 3q^2 + 4q^3 + 3q^4)(1 - q^2)^{-2}(1 - q^3)^{-2}$, as desired.

Undoubtedly, this approach can be used in regard to the generalizations in Remark 4.

010:05 (Gerry Myerson) Let G be an abelian group with subgroups H_1, H_2, H_3 of index 3. Let g_1, g_2, g_3 be elements of G such that if $i \neq j$ then $(g_i + H_i) \cap (g_j + H_j) = \phi$. Does this imply $H_1 = H_2 = H_3$?

Solution: Pace Nielsen proves that much more is true. Let G be a group with normal subgroups H_1 and H_2 of prime index (not necessarily the same prime index). Let g_1 and g_2 be elements of G such that $g_1H_1 \cap g_2H_2 = \phi$. Then $H_1 = H_2$. Clearly this settles the question in the affirmative.

Proof. On the hypotheses, let $g = g_1^{-1}g_2$, so $H_1 \cap gH_2 = \phi$. Also, $gH_2 \neq H_2$ since $H_1 \cap H_2$ contains the identity. G/H_2 is a group of prime order, hence it is cyclic and gH_2 is a generator. Thus G is the disjoint union of the cosets g^iH_2, $i = 0, \dots, q - 1$, where $q = (G : H_2)$. If $H_1 \cap g^iH_2 \neq \phi$ for some i, $1 \leq i \leq q - 1$, say $h_1 \in H_1 \cap g^iH_2$, let $ij \equiv 1 \pmod q$; then $h_1^j \in H_1 \cap g^{ij}H_2 = H_1 \cap gH_2$, contradiction. Hence, $H_1 \cap g^iH_2 = \phi$ for $i \neq 0$. Hence, $H_1 \subseteq H_2$. But H_1 and H_2 are of prime index, so $H_1 = H_2$.

Remark: See **010:10**.

010:06 (Gerry Myerson) Assume every x in $\mathbf{Z}$ satisfies at least one of the congruences $x \equiv a_i \pmod{m_i}$, $i = 1, \dots, t$. Let G be an abelian group of order $n = \mathrm{lcm}(m_1, \dots, m_t)$. Must G have subgroups $H_1, \dots, H_t$ with $(G : H_i) = m_i$ and elements $g_1, \dots, g_t$ such that $G = \cup_{i=1}^t (g_i + H_i)$?

Conversely, let G be an abelian group of order n. Suppose $G = \cup_{i=1}^t (g_i + H_i)$ for some subgroups $H_1, \dots, H_t$ and elements $g_1, \dots, g_t$. Must there exist integers $a_1, \dots, a_t$ such that every x in $\mathbf{Z}$ satisfies at least one of $x \equiv a_i \pmod{m_i}$, $i = 1, \dots, t$, where $m_i = (G : H_i)$?

010:07 (Andreas Weingartner). Let g_1, g_2 be polynomials with no common zero in $\mathbf{C}$. Let $K \subset \mathbf{C}$ be compact. Must there exist polynomials f_1, f_2 such that $g_1f_1 + g_2f_2 = 1$ and for all z in K, $f_1(z)f_2(z) \neq 0$?

Remark: There are unique polynomials F_1, F_2 with $g_1F_1 + g_2F_2 = 1$ and $\deg F_1 < \deg g_2, \deg F_2 < \deg g_1$, and all solutions are given by $f_1 = F_1 + kg_2, f_2 = F_2 - kg_1$ for some polynomial k, so the question is whether we can choose k in such a way that f_1 and f_2 are both zero-free in K.

Solution: Andreas writes that Pierre Mazet from Paris has answered this question in the negative, using Picard's Theorem.

010:08 (Andreas Weingartner). Let $f(s) = \sum_{n=1}^{N} \frac{a_n}{n^s}$, a_n in $\mathbf{C}$, be a Dirichlet polynomial with no repeated factors in the ring of Dirichlet polynomials. Let $M(T)$ be the number of multiple zeros s of f with |Imaginary part of $s| \le T$. Is it true that $M(T) = \mathrm{o}(T)$?

010:09 (Victor Miller). An Erdős-Woods number is a positive integer b for which there exists a positive integer a such that $\gcd(n, a(a+b)) > 1$ for all n, $a \le n \le a+b$. Do the Erdős-Woods numbers have a positive density in the integers?

Remarks: 1. The first non-trivial Erdős-Woods number is $b = 16$, corresponding to $a = 2184$. It is known that there are infinitely many, but known constructions yield a set of zero density. Computation of all Erdős-Woods numbers $b \le 500,000$ suggests a density near 0.16.

2. The On-Line Encyclopedia of Integer Sequences reference for the Erdős-Woods numbers is http://oeis.org/A059756.

010:10 (Gerry Myerson). Let m be composite and square-free. Let G be a group with m normal subgroups $H_1, \ldots, H_m$ of index m and elements $g_1, \ldots, g_m$ such that $i \ne j$ implies $(g_i + H_i) \cap (g_j + H_j) = \phi$. Does this imply that the subgroups are not all distinct?

Remarks: This problem grows out of Pace Nielsen's solution to **010:05**. That solution yields a positive answer if m is prime, but does not apply if m is composite. If m is not square-free then there is an r such that $\mathbf{Z}_r \oplus \mathbf{Z}_r \oplus \mathbf{Z}_r$ can be partitioned into cosets of m distinct subgroups each of index m.

010:11 (Hilarie Orman). Find a closed form solution to the general Josephus problem. In this problem there are n objects on a circle; you remove every kth object, repeatedly, until only one object remains; the question is, where is that last object, in terms of n, k, and its location relative to the start of counting. E.g., if $n = 7$ and $k = 2$, and we name the objects $1, 2, \ldots, 7$ in order around the circle, and we start the count at object 1, then we remove $2, 4, 6, 1, 5, 3$, leaving 7, so we may say $f(7, 2, 1) = 7$.

Remark: References to the Josephus problem in the literature can be found in Gregory L. Wilson and Christopher L. Morgan, An application of Fourier transforms on finite Abelian groups to an enumeration arising from the Josephus problem, J. Number Theory 130 (2010) 815–827, MR 2600404.

010:12 (Rich Schroeppel). The decimal expansion of e has a repeated portion that comes fairly early in terms of its length: $2.718281828\ldots$. Are there other "naturally occurring" real irrationals with this property? Part of the problem is determining how long and how early the repetition has to be to qualify. Do we accept $\gamma = .577\ldots$?