Western Number Theory Problems, 16 & 18 Dec 2013

for distribution prior to 2014 (Monterey) meeting

Edited by Gerry Myerson

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	2011 Asilomar	011.01–011.16
2012 Asilomar	012:01–012:17	2013 Asilomar	013.01–013.13

[With comments on 99:08]

COMMENTS ON ANY PROBLEM WELCOME AT ANY TIME

Department of Mathematics,
Macquarie University,
NSW 2109 Australia
gerry.myerson@mq.edu.au
Australia-2-9850-8952 fax 9850-8114

99:08 (Greg Martin) Define a multiplicative function $\tilde{\sigma}$ by

$$\tilde{\sigma}(p^r) = p^r - p^{r-1} + p^{r-2} - \ldots + (-1)^r$$

Note that $\tilde{\sigma}(n) \le n$ with equality only for $n = 1$. Call n $\tilde{\sigma}$-perfect if $2\tilde{\sigma}(n) = n$; examples are $n = 2, 12, 40, 252, 880, 10880$, and 75852. Call n $\tilde{\sigma}$-k-perfect (or, more generally, $\tilde{\sigma}$-multiply perfect) if $k\tilde{\sigma}(n) = n$ for a positive integer k. Two examples of $\tilde{\sigma}$-3-perfects are $n = 30240$ and $n = 2^{10}3^4 5^4 11 \cdot 13^2 \cdot 31 \cdot 61 \cdot 157 \cdot 521 \cdot 683$—there are at least 40 $\tilde{\sigma}$-3-perfects.

1. Are there any $\tilde{\sigma}$-k-perfect numbers with $k \ge 4$?
2. Are there infinitely many $\tilde{\sigma}$-k-perfect numbers?
3. Are there any odd $\tilde{\sigma}$-3-perfect numbers? Any such number must be a square.

Remarks: Paraphrasing email from Greg: let $\tau(n) = n/\tilde{\sigma}(n)$, so $\tau(n) = k$ means n is a $\tilde{\sigma}$-k-perfect number. Suppose $n = p^{2k-1}m$, p prime, and $\tilde{\sigma}(p^{2k}) = q$ is prime, and $(m, pq) = 1$. Then it's not hard to prove that $\tau(n) = \tau(npq)$. In particular, if n is $\tilde{\sigma}$-k-perfect, so is npq.

Some examples of prime powers p^{2k-1} such that $\tilde{\sigma}(p^{2k})$ is prime are

$$2^1, 2^3, 2^5, 2^9, 3^1, 3^3, 3^5, 5^3, 7^1, 13^1.$$

This makes it possible to find 40 $\tilde{\sigma}$-3-perfects from the four examples $2^3 3^3 5^2 7$, $2^5 3^3 5 \cdot 7$, $2^5 3^5 5^2 7^3 13$, and $2^9 3^3 5^3 11 \cdot 13 \cdot 31$.

Jeff Lagarias suggested looking at the Dirichlet series generating function for $\tilde{\sigma}$, in analogy with

$$\sum_{n=1}^{\infty} \frac{\sigma(n)}{n} n^{-s} = \zeta(s+1)\zeta(s).$$

Greg finds that

$$\sum_{n=1}^{\infty} \frac{1}{\tau(n)} n^{-s} = \zeta(2s+2)\zeta(s)/\zeta(s+1),$$

but no such tidy form for $\sum_{n=1}^{\infty} \tau(n) n^{-s}$.

Remark: (2000) Doug Iannucci reports that if there is an odd $\tilde{\sigma}$-3-perfect number it has at least 18 prime factors, and its largest prime factor exceeds 10^8.

Remarks: (2013) 1. Greg's questions appear toward the end of Problem B1 of UPINT, 3rd edition.

2. Iannucci's work is published as On a variation on perfect numbers, Integers: Electronic Journal of Combinatorial Number Theory 6 (2006) #A41, MR2280357 (2007i:11006), available from http://www.integers-ejcnt.org/vol6.html.

3. There are lower bounds on odd $\tilde{\sigma}$-k-perfect numbers in Zhou and Zhu, On k-imperfect numbers, Integers 9 (2009), A01, MR2475629 (2009k:11008).

4. The $\tilde{\sigma}$-function is studied in László Tóth, A survey of the alternating sum-of-divisors function, Acta Univ. Sapientiae, Math 5 (2013) 93–107; the emphasis is on questions other than those raised in 99:08.

5. Andreas Weingartner answers Greg Martin's first question in the affirmative:

We found 192 $\tilde{\sigma}$-4-perfect numbers. The smallest of these is

$$2^{13} \cdot 3^8 \cdot 5 \cdot 7^2 \cdot 11 \cdot 13 \cdot 19 \cdot 23 \cdot 37 \cdot 43^2 \cdot 127 \cdot 139 = 993803899780063855042560 \approx 9.9 \times 10^{23}$$

The largest of these is

$$\begin{aligned}
&2^{50} \cdot 3^{18} \cdot 5^{14} \cdot 7^{7} \cdot 11 \cdot 13^{2} \cdot 17^{4} \cdot 19^{2} \cdot 37 \cdot 61 \cdot 71 \cdot 101 \cdot 127 \cdot 149 \cdot 157 \cdot 257 \cdot \\
&\quad \cdot 307 \cdot 521 \cdot 1201 \cdot 2851 \cdot 2857 \cdot 6529 \cdot 7621 \cdot 43691 \cdot 101917 \\
&\qquad = 526488444119076287810942809851369796232282693025280543888735235 \\
&\qquad\quad 0837451795403609477302400000000000000 \approx 5.3 \times 10^{98}
\end{aligned}$$

Problems proposed 16 and 18 December 2013

013.01 (Bart Goddard). For natural n, define $D(n)$ by

$$D(n) = \#\{\, k \le n : \sigma(k) < 2k \,\}$$

We say n is a Goddard number if $\sigma(n) < 2k$ and $\sigma(D(n)) > 2D(n)$. Do there exist Goddard triplets (that is, n such that n, $n+1$, and $n+2$ are all Goddard)? quadruplets? quintuplets?

Remark: Goddard and Florian Luca have shown that there exist infinitely many Goddard twins, and no Goddard sextuplets.

013.02 (Bart Goddard). Let k be a natural number. What conditions on k cause $-1, -2, \ldots, -2k$ all to be quadratic nonresidues modulo k^n for some n? What is the relation between numbers k and r, $1 \le r \le 2k$, such that $-r$ is a quadratic residue modulo k^n for all n?

Remarks: 1. As an example illustrating the first question, $-1, -2, \ldots, -20$ are all quadratic nonresidues modulo 10^n for all $n \ge 6$.

2. [Incorporating remarks of Kjell and Amy Wooding] Let $k = 2m$, with m odd. Then in any reduced set of residues mod m, half will be quadratic residues modulo m. For n large enough, the numbers r such that $-r$ is a quadratic residue modulo 2^n will be the numbers $4^i(8s+7)$. The condition on the number k is that the quadratic residues modulo m be disjoint from those modulo 2^n. For example, for $k = 10$, the quadratic residues modulo high powers of 5 are the negatives of $1, 4, 6, 9, 11, 14, 16, 19, 21, 24, 25, 26, 29, 31, \ldots$, the quadratic residues modulo high powers of 2 are the negatives of $7, 15, 23, 28, 31, \ldots$, and the first number in both lists is 31, so $-1, -2, \ldots, -30$ are all quadratic nonresidues modulo 10^n for n large. The same is true for $k = 14$. For $k = 22$, we find 7 is on both lists (-7 is a quadratic residue modulo 11, and also modulo 2^n for all n). $k = 2p$ does not work for any other $p < 100$.

013.03 (Carl Pomerance). Let

$$D = \left\{ n : n \mid \binom{2n}{n} \right\}$$

Is the lower asymptotic density of D positive? Does D have an asymptotic density?

Remarks: Carl notes that D is infinite; if p and q are prime with $(3/2)p < q < 2p$, then pq is in D. He also notes that the upper asymptotic density is at most $1 - \log 2$, based on the observation that if $n = mp$ where $p > 2m$ is prime, then n is not in D. Further, for each fixed positive integer k,

$$\left\{ n : (n+k) \mid \binom{2n}{n} \right\}$$

has asymptotic density 1.

013.04 (Sebastian Wedeniwski, via Kjell Wooding). Let $f(x)$ be a polynomial. Find x in polynomial time such that $f(x)$ is a sum of two squares.

Remark: It was pointed out that there may be no such x, e.g., if $f(x) = 4g(x) + 3$ for some polynomial g. Carl Pomerance noted that there is no polytime algorithm to find a prime $p \equiv 1 \pmod 4$, so if $f(x)$ is $x + n$ with n large, and we require $x > 0$, there is no polytime algorithm even though we know there are solutions. Kjell suggests asking for a randomized polytime algorithm, instead. In case f is quadratic (a case of particular interest for Wedeniwski), Dave Rusin suggests looking at J. B. Friedlander, H. Iwaniec, Small representations by indefinite ternary quadratic forms, Number Theory and Related Fields, Springer Proceedings in Mathematics & Statistics Volume 43 (2013) 157–164.

013.05 (David Thomson). Let p be a prime, let $r = tn + 1$ be a different prime, let $q = p^e$. Let

$$K = \{ 1, \omega, \dots, \omega^{t-1} \}$$

with ω a primitive t-th root of unity in the field of r elements. Let $K_i = q^i K$. Define the cyclotomic constants t_{ij} by

$$t_{ij} = \#\big(K_i \cap (1 + K_j)\big)$$

Under what conditions does p divide t_{ij}?

Remark: David awards bonus points if the K_i are all disjoint; an easy condition for this is if $\mathbf{Z}_r^*$ is generated by q and K.

013.06 (Colin Weir). Fix $f(x)$ monic, squarefree, nonconstant in $\mathbf{F}_q[x]$. For p irreducible in $\mathbf{F}_q[x]$, let $N_p = q^{\deg p}$. Does the product

$$\prod \left(1 - \frac{\left(\frac{f}{p}\right) + 1}{N_p(N_p + 1)} \right)$$

over p not dividing $f(x)$ converge to a rational function in q?

013.07 (Stefan Erickson). 1. Let d_k be the number of irreducible polynomials of degree k over $\mathbf{F}_q$. Find, if possible, a closed form for the product,

$$\prod_{k=1}^{\infty} \left(\frac{1 + \frac{(-1)^k}{q^k+1}}{1 + \frac{(-1)^k}{q^k}} \right)^{d_k}$$

2. What if we replace d_k with $d_k/2$?

3. What if we restrict k to just even values?

Stefan reports that computer calculations suggest the first product is approximately $1 + (1/q)$.

013.08 (Christelle Vincent). Fix a positive integer, N. Consider the set of all elliptic curves over the rationals of conductor N. What is the smallest prime $p > 2$ such that all of these elliptic curves are *not* supersingular at p?

013.09 (Marc Brown, via Gerry Myerson). Is it true that for each rational r there is a set S of positive asymptotic density and a positive integer N such that for all rational α and β, $\alpha\beta^n + r$ is in S for at most N positive integers n?

Source: MathOverflow question 147431 from 9 November 2013.

Remark: For $r = 0$, we can take S to be the squarefree integers, and $N = 2$.

Solution: (Carl Pomerance) If r is an integer, we can take S to be the squarefree integers, shifted by r, and $N = 2$. If r is not an integer, then if β is not an integer there is at most one value of n such that $\alpha\beta^n + r$ is an integer, and we can take S to be the set of all integers, with $N = 1$. Finally, if r is not an integer, and β is an integer, then we can write $\alpha\beta^n + r$ as $(st^n + p)/q$ for some integers p, q, s, t, with $\gcd(p, q) = 1$. Let U be the set of numbers that are squarefree and congruent to $-p$ modulo q; this is a set of positive asymptotic density. Let S be the set of numbers of the form $(u + p)/q$, with u in U. Then S has positive asymptotic density, and if $(st^n + p)/q$ is in S, then st^n is squarefree, so we can use this set S, with $N = 2$.

013.10 (John Friedlander). Let K be a number field of degree n, with discriminant $\pm D$, $D > 0$. Let $\omega = (\omega_1, \ldots, \omega_n)$ be an integral basis. Let

$$\omega_i\omega_j = \sum_{k=1}^{n} a_{ijk}\omega_k$$

for $1 \le i, j \le n$. Let $A(\omega) = \max_{i,j,k} |a_{ijk}|$. Let $A = \min A(\omega)$ over all integral bases ω.

1. Give a good upper bound for A,

(a) for fixed n (but varying K),

(b) uniformly in n.

2. The same for $B(\omega) = \max_{i,j,k} |a_{ijk}\omega_k|$.

Remark: Renate Scheidler suggested one could probably get D^n.

013.11 (Kjell Wooding). A DBNS (Double Base Number System) representation for an integer n is given by

$$n = \sum b_{ij} 2^i 3^j$$

with b_{ij} in $\{0, 1\}$ or in $\{0, \pm 1\}$. It is hard to find a shortest (fewest non-zero coefficients) representation for an integer. The greedy algorithm, where you find the largest 2^i3^j not exceeding N, and then proceed iteratively on $N - 2^i3^j$, finds a near-shortest representation.

Is there an efficient algorithm that consistently finds representations shorter than those found by the greedy algorithm?

Remark: Michael R. Avidon, On primitive 3-smooth partitions of n, Electron. J. Combin. 4 (1997) no. 1, Research Paper 2, MR1435128 (98a:11136) discusses these representations (in the b_{ij}-in-$\{0, 1\}$ case), but is more concerned with the number of representations than with their lengths. The paper is available at
http://www.combinatorics.org/ojs/index.php/eljc/article/view/v4i1r2/pdf.

013.12 (Kate Stange, via Stefan Erickson). An Apollonian Super-Packing (ASP, for short) is an orbit of a single Descartes configuration under the super-Apollonian group; see Graham et al., Apollonian Circle Packings: Geometry and Group Theory I, II, in Discrete and Computational Geometry. Is there a number-theoretic interpretation when two circles in an ASP intersect?

013.13 (Reese Scott and Rob Styer). 1. Can we find distinct pairs of integers

$$(a_1, b_1), (a_2, b_2), (a_3, b_3), (a_4, b_4)$$

and positive real numbers x and y, $x \neq 1$, $y \neq 1$, such that

$$x^{a_1} - y^{b_1} = x^{a_2} - y^{b_2} = x^{a_3} - y^{b_3} = x^{a_4} - y^{b_4} \tag{1}$$

The a_i and b_i are not required to be positive.

2. Can we show that (1) is satisfied by at most a finite number of choices of $a_1, b_1, a_2, b_2, a_3, b_3, a_4, b_4, x, y$?

Remarks: 1. It is easy to find $(a_1, b_1), (a_2, b_2), (a_3, b_3)$ such that

$$x^{a_1} - y^{b_1} = x^{a_2} - y^{b_2} = x^{a_3} - y^{b_3} \tag{2}$$

has a solution in positive real numbers x and y, since there are many ways to choose $a_1, b_1, a_2, b_2, a_3, b_3$ so that the curve $x^{a_1} - y^{b_1} = x^{a_2} - y^{b_2}$ intersects the curve $x^{a_1} - y^{b_1} = x^{a_3} - y^{b_3}$.

2. It is not hard to show that (1) requires that both x and y be irrational. (2) also requires both x and y be irrational except for two specific cases.