Western Number Theory Problems, 16 & 19 Dec 1999

Edited by Gerry Myerson

for mailing prior to 2000 (San Diego) 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 (current set)	99:01–99:12

[With comments on 76:60, 86:05, 88:06, 93:20, 95:18, and 97:22]

COMMENTS ON ANY PROBLEM WELCOME AT ANY TIME

Centre for Number Theory Research,
Department of Mathematics,
Macquarie University,
NSW 2109 Australia
gerry@mpce.mq.edu.au
Australia-2-9850-8952 fax 9850-8114

9 Aug 2000

Comments on Earlier Problems

76:60 (Peter Weinberger) Let $|f|$ denote the number of non-zero coefficients of a polynomial f. Is there a function A such that $|(f,g)| \leq A(|f|,|g|)$? Can such an A be a polynomial? The example $f = (x^{ab}+1)(x^b+1)/(x+1)$, $g = (x^{ab}+1)(x^b+1)/(x^a+1)$ with $a > b-1$, a even, b odd shows that if such an A exists then $A(n,n) \gg n^2$.

Solution: Andrzej Schinzel writes that the answer to this problem is negative, and a simple counterexample is $f = x^{ab} - 1$, $g = (x^a - 1)(x^b - 1)$, where $|f| = 2$, $|g| = 4$ and $|(f,g)|$ can be arbitrarily large. The only difficult case in characteristic 0 is $|f| = |g| = 3$.

86:05 (Michael Filaseta) Is $f_n(x) = \frac{d}{dx}(x^n + x^{n-1} + \cdots + x + 1)$ irreducible for all positive integers n? For almost all n?

Solution: The "almost all" question is answered in the affirmative in

A. Borisov, M. Filaseta, T. Y. Lam, O. Trifonov, Classes of polynomials having only one non-cyclotomic irreducible factor, Acta Arith. 90 (1999) 121–153,

where Theorem 1 states that "if $\epsilon > 0$ then for all but $O(t^{1/3+\epsilon})$ positive integers $n \leq t$ the derivative of the polynomial $f(x) = 1 + x + x^2 + \cdots + x^n$ is irreducible."

88:06 (Emil Grosswald) Mike Filaseta proved that almost all Bessel polynomials [polynomial solutions of $x^2y'' + xy' - n(n+1)y = 0$ with $y(0) = 1$] are irreducible over $\mathbf{Q}$. Get rid of "almost all".

Solution: In work submitted for publication, Filaseta and Trifonov write the Bessel polynomials as

$$y_n(x) = \sum_{j=0}^{n} \frac{(n+j)!}{2^j(n-j)!j!} x^j$$

and prove that if n is a positive integer and $a_0, a_1, \ldots, a_n$ are arbitrary integers with $|a_0| = |a_n| = 1$ then

$$\sum_{j=0}^{n} a_j \frac{(n+j)!}{2^j(n-j)!j!} x^j$$

is irreducible.

The techniques are similar to those used in

M. Filaseta, The irreducibility of all but finitely many Bessel polynomials, Acta Math. 174 (1995) 383–397.

93:20 (Eugene Gutkin via Jeff Lagarias) [...] consider the polynomials

$$p_n(x) = \frac{(n-1)(x^{n+1}-1) - (n+1)(x^n - x)}{(x-1)^3}$$

[which arise in the solution of $\tan n\theta = n \tan \theta$] for $n \geq 1$.

Conjecture. $p_n(x)$ is irreducible if n is even, and is $x+1$ times an irreducible if n is odd.

Solution: This is true for almost all n. Theorem 4 of the four-author paper cited above states that if $\epsilon > 0$ then for all but $O(t^{4/5+\epsilon})$ positive integers $n \le t$ the polynomial $p(x) = (n-1)(x^{n+1}-1) - (n+1)(x^n - x)$ is $(x-1)^3$ times an irreducible polynomial if n is even and $(x-1)^3(x+1)$ times an irreducible polynomial if n is odd.

95:18 (Martin LaBar, via Richard Guy) Is there a 3×3 magic square with distinct square entries?

Remark: Comments on this problem have appeared in each problem set since it was first proposed.

Andrew Bremner, On squares of squares, Acta Arith. 88 (1999) 289–297

constructs parametrized families of 3×3 matrices with distinct square entries and with all sums equal except that along the non-principal diagonal.

97:22 (John Selfridge) Let $n = rs^2$, r square-free, $r > 1$. It is conjectured that for all such n except $n = 8$ and $n = 392$ there exist integers a, b with $n < a < b < r(s+1)^2$ such that nab is a square.

Remark: See the paper,

Paul Erdős, Janice L. Malouf, J. L. Selfridge, Esther Szekeres, Subsets of an interval whose product is a power, Discrete Math. 200 (1999) 137–147.

Selfridge reports that he and Aaron Meyerowitz have proved that if there is a counterexample $n > 392$ then n is at least on the order of 10^{30000}.

Problems Proposed 16 & 19 Dec 99

99:01 (John Wolfskill) Let $d \equiv 3 \pmod 4$ be positive and squarefree. Let a fundamental unit in $\mathbf{Z}[\sqrt{d}]$ be given by $\epsilon = a + b\sqrt{d} > 1$. Characterize those d for which $\sqrt{2}$ is in $\mathbf{Q}(\sqrt{\epsilon})$.

Remarks: $\sqrt{2}$ is in $\mathbf{Q}(\sqrt{\epsilon})$ for all prime d and for some but not all composite d.

Gary Walsh shows that the following are equivalent:

a) $\sqrt{2}$ is in $\mathbf{Q}(\sqrt{\epsilon})$;

b) at least one of the equations $x^2 - dy^2 = \pm 2$ is solvable in integers x and y;

c) the prime over 2 in $\mathbf{Q}(\sqrt{d})$ is principal.

Characterizing d such that $x^2 - dy^2 = -1$ has a solution is a notorious open question, which suggests that there may be no simple solution to the current problem.

Walsh's argument, as presented by Wolfskill, runs as follows. Let $K = \mathbf{Q}(\sqrt{\epsilon})$, let α in K be such that $\alpha^2 = \epsilon$. Note that the norm of ϵ is 1, whence $K/\mathbf{Q}$ is Galois and non-cyclic. Since α is in K we have $\alpha = r + s\sqrt{d} + t\sqrt{d'} + u\sqrt{dd'}$ for some rational r, s, t and u and some d' with $\sqrt{d'}$ in K. Let σ be the element of the Galois group of $K/\mathbf{Q}$ fixing $\sqrt{d}$ but not fixing $\sqrt{d'}$. Then $\big(\sigma(\alpha)\big)^2 = \sigma(\alpha^2) = \sigma(\epsilon) = \epsilon = \alpha^2$, so $\sigma(\alpha) = \alpha$ or $\sigma(\alpha) = -\alpha$. If $\sigma(\alpha) = \alpha$ then α is in $\mathbf{Q}(\sqrt{d})$ but then $\alpha^2 = \epsilon$ contradicts the hypothesis that ϵ is a fundamental unit in $\mathbf{Q}(\sqrt{d})$, so $\sigma(\alpha) = -\alpha$, so $\alpha = t\sqrt{d'} + u\sqrt{dd'}$.

Now assume $\sqrt{2}$ is in K, so $\alpha = t\sqrt{2} + u\sqrt{2d}$, t and u rational. From $\alpha^2 = \epsilon$ we get that $2(t^2 + du^2) = a$ and $4tu = b$ are both integers, from which it is easy to deduce that $2t = x$ (say) and $2u = y$ (say) are integers. Then $(x^2 - dy^2)^2 = 4(a^2 - db^2) = 4$, so $x^2 - dy^2 = \pm 2$.

Conversely, suppose x and y are positive integers such that $x^2 - dy^2 = \pm 2$. Note that x and y are odd. Let $a = (x^2 + dy^2)/2$, $b = xy$. Then $a^2 - db^2 = 1$, so $a + b\sqrt{d}$ is a unit in $\mathbf{Q}(\sqrt{d})$. Also, $\left(\frac{x}{2}\sqrt{2} + \frac{y}{2}\sqrt{2d}\right)^2 = a + b\sqrt{d}$, so $a + b\sqrt{d}$ must be an odd power of the fundamental unit in $\mathbf{Q}(\sqrt{d})$—otherwise, $\frac{x}{2}\sqrt{2} + \frac{y}{2}\sqrt{2d}$ would be in $\mathbf{Q}(\sqrt{d})$. So, $\sqrt{2}$ is in $\mathbf{Q}(\sqrt{\epsilon})$.

99:02 (Greg Martin) Consider the following "proof" that 4680 is perfect: $4680 = 2^3 \cdot 3^2 \cdot (-5) \cdot (-13)$, so $\sigma(4680) = (1+2+2^2+2^3)(1+3+3^2)(1+(-5))(1+(-13)) = 9360 = 2 \times 4680$. Allowing the use of $\sigma(-p^n) = \sum_{j=0}^{n}(-p)^j$, is there a "spoof perfect number" with exactly 3 distinct prime factors?

Remark: If so, it must be negative.

Solution: Dennis Eichhorn found that $-84 = 2^2(3)(-7)$ is spoof-perfect, and Eichhorn and Peter Montgomery independently found that $-120 = 2^3(3)(-5)$ is spoof-perfect. Montgomery also found that $-672 = (-2)^5(3)(7)$ leads to

$$\sigma(-672) = (1 - 2 + 4 - 8 + 16 - 32)(1 + 3)(1 + 7) = -672.$$

Alf van der Poorten asked whether there are any odd spoof-perfects.

John Selfridge asked whether 4680 is the smallest positive spoof-perfect.

See also 99:08, below.

99:03 (Mike Filaseta) Find m_0 such that if $m \geq m_0$ and $m(m-1) = 2^a 3^b m'$ and $(m', 6) = 1$ then $m' > \sqrt{m}$.

Remark: See

M. Filaseta, A generalization of an irreducibility theorem of I. Schur, Analytic number theory, Vol. 1 (Allerton Park, IL, 1995), 371–396, Progr. Math. 138, Birkhauser, Boston 1996

for a similar but ineffective result derived from work of Mahler.

99:04 (Mike Filaseta) Show that every $n \times n$ integer matrix, $n \geq 2$, is a sum of 3 squares of $n \times n$ integer matrices.

Remark: What is wanted is an argument more transparent than that in

Leonid N. Vaserstein, Every integral matrix is the sum of three squares, Linear and Multilinear Algebra 20 (1986) 1–4.

99:05 (Zachary Franco) Call n equidigital if each digit occurs equally often in the repeating block in the decimal expansion of $1/n$. It is easy to see that if p is prime and 10 is a primitive root (mod p) then p is equidigital. Are there any equidigital primes p for which 10 is not a primitive root?

Remarks: The answer to the corresponding question in base 2 is yes; 2 is not a primitive root (mod 17) but the binary expansion of 1/17 is $.\dot{0}000111\dot{1}$.

There are equidigital composites, e.g., $n = 1349 = 19 \times 71$.

Mike Filaseta notes that if $p \equiv 11 \pmod{20}$ is prime and 10 is of order $(p-1)/2 \pmod{p}$ then 10^k runs through the quadratic residues (mod p), and since there are more quadratic residues in $[1, (p-1)/2]$ than in $[(p+1)/2, p-1]$ for such p ($p \equiv 3 \pmod{4}$) p can't be equidigital. For example, $1/31 = .\dot{0}3225806451612\dot{9}$ has 9 small digits and 6 large ones. Perhaps there are similar results for 10 of order $(p-1)/k$ for $k = 3, 4, \ldots$.

99:06 (Kevin O'Bryant) Write $\sqrt{\ } a_1, a_2, \ldots]$ for the continued square root

$$\cfrac{1}{\sqrt{a_1 + \frac{1}{\sqrt{a_2 + \ldots}}}}$$

where $a_1, a_2, \ldots$ are positive integers. Every real number r, $0 < r < 1$, has such an expression, and the expression is unique in the same sense as for simple continued fractions. Does $3/4$ have a finite continued root?

Remark: $2/3 = \sqrt{\ } 2, 16]$, $22/47 = \sqrt{\ } 3, 1098, 2892, 410, 256]$.

99:07 (Bart Goddard) Let $f : (0, \infty) \to (0, \infty)$ be strictly decreasing and onto with $f(1) = 1$. Let g be the functional inverse f^{-1} of f. For α_0 real and positive, define integers $a_0, a_1, \ldots$ and reals $\alpha_1, \alpha_2, \ldots$ by $a_j = [\alpha_j]$, $\alpha_j = g(\alpha_{j-1} - a_{j-1})$. Write $(\alpha_0)_f$ for the sequence $a_0, a_1, \ldots$. Let $c_0 = a_0$, $c_1 = a_0 + f(a_1)$, $c_2 = a_0 + f\big(a_1 + f(a_2)\big)$, etc. Note that $f(x) = 1/x$ gives the usual continued fraction expansion of α_0, and $f(x) = 1/\sqrt{x}$ gives the expansion of 99:06.

Some interesting examples are

$f(x) = x^{-5}$, $(\sqrt[5]{7})_f = (1, 1, 1, \ldots)$

$f(x) = 1/\Omega(ex)$, where Ω is the Lambert Ω-function,

$$(\pi)_f = (3, 3033, 23766810023426903113005, 2279, 2, 864, \ldots)$$

1. Given f, which numbers have finite expansions? periodic expansions? Is it true that if $f(x) = x^{-2/3}$ then $(\sqrt[3]{3})_f = (\dot{1}, 1, 1, \dot{2})$?
2. Is there an f such that $(\alpha)_f$ is periodic for all algebraic α of degree 3?
3. Find f such that $(\pi)_f$ has a recognizable pattern.
4. Find f such that $(e)_f$ is periodic.
5. Find conditions on f and α for $\lim_{n\to\infty} c_n = \alpha$.

Solution: (to question 4) Greg Martin notes that if $f(x) = x^{\log(e-2)/\log(e-1)}$ then $(e)_f = (2, 1, 1, 1, \ldots)$.

Remark: Jeff Lagarias refers to

A. Rényi, Representations for real numbers and their ergodic properties, Acta Math. Acad. Sci. Hungar. 8 (1957) 477–493, MR 20 #3843.

Many later papers refer to this one, as may be seen from the listing on MathSciNet.

99:08 (Greg Martin) Define a multiplicative function $\tilde\sigma$ (or $\utilde{\sigma}$ if you are left-handed) by $\tilde\sigma(p^r) = p^r - p^{r-1} + p^{r-2} - \cdots + (-1)^r$. 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.

Remark: 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 $\sum_{n=1}^{\infty} \tau(n) n^{-s}$.

99:09 (Jean-Marie De Koninck) Given an integer k, $k \ge 2$, not a multiple of 3,

1. prove that there is a prime whose digits sum to k,
2. prove that if $k \ge 4$ then there are infinitely many primes whose digits sum to k.

Remarks: Jean-Marie provided a table of values of $\rho(k)$, the smallest prime whose digits add up to k, for $2 \le k \le 83$, k not a multiple of 3. Your editor notes that $\rho(56) - \rho(55) = 2999999 - 2998999 = 1000$ and asks whether there are infinitely many k with $\rho(k+1) - \rho(k) = 1000$, or with $\rho(k+1) - \rho(k) = 10^m$ for some m, or whether there is an integer r with $\rho(k+1) - \rho(k) = r$ for infinitely many r.

Your editor further notes that $\rho(34)/\rho(32) = 17989/6899 = 2.61$ (to two decimals), $\rho(37)/\rho(35) = 29989/8999 = 3.33$, $\rho(70)/\rho(68) = 189997999/59999999 = 3.17$, and $\rho(73)/\rho(71) = 289999999/89999999 = 3.22$, and asks whether $\rho(3k+1)/\rho(3k-1)$ is unbounded. Moreover, your editor also notes that $\rho(34)/\rho(35) = 17989/8999 = 2.00$ and $\rho(70)/\rho(71) = 189997899/89999999 = 2.11$ and asks whether $\rho(k) > \rho(k+1)$ infinitely often.

Further questions: is it true that $k > 25$ implies $\rho(k) \equiv 9 \pmod{10}$? that $k > 38$ implies $\rho(k) \equiv 99 \pmod{100}$? that $k > 59$ implies $\rho(k) \equiv 999 \pmod{1000}$?

Jean-Marie also notes that it is trivial that $\rho(k) \geq (a+1)10^b - 1$, where $b = [k/9]$ and $a = k - 9b$; and asks whether equality holds infinitely often. For instance, it is the case when $k = 5, 7, 10, 11, 14, 16, 17, 19, 22, 23, 28, 29, 31, 35, 40$.

99:10 (Jeff Lagarias) Is there a field with Galois group S_n, $n \geq 5$, whose ring of integers has a power basis?

99:11 (Sinai Robins) Let q be real, $|q| < 1$. Is the function given by $f(x) = \sum_{n=1}^{\infty} [nx] q^n$ real analytic in x?

Remark: A starting place for the analytic properties of this and related series is

Wolfgang Schwarz, Über Potenzreihen, die irrationale Funktionen darstellen, I and II, Überblicke Mathematik, Band 6, 179–196 and 7, 7–32, MR 51 #8382-3.

See also

J. H. Loxton, A. J. van der Poorten, Arithmetic properties of certain functions in several variables. III, Bull. Austral. Math. Soc. 16 (1977) 15–47, MR 81g:10046.

99:12 (Jeff Lagarias) Given $n > 3$, find upper and lower bounds for the number of solutions $1 < q_1 < \cdots < q_n$ of the system $q_j^{-1} \prod_1^n q_j \equiv 1 \pmod{q_j}$, $j = 1, \ldots, n$.

Remark: It is known that there are only finitely many solutions for each n, in fact there is an upper bound for q_n, but it does not give a good estimate for the number of solutions. $(2, 3, 5)$ is the only solution for $n = 3$. The problem is discussed in

Lawrence Brenton, Mi-Kyung Joo, On the system of congruences $\prod_{j \neq i} n_j \equiv 1 \pmod{n_i}$, Fib. Q. 33 (1995) 258–267.

The review, MR 96k:11039, is also worth reading.