Western Number Theory Problems, 17 & 20 Dec 1998

Edited by Gerry Myerson

for mailing prior to 1999 (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 (present set) 98:01–98:14			

[With comments on 95:18, 97:10, 97:15, 97:16, and 97:22]

COMMENTS ON ANY PROBLEM WELCOME AT ANY TIME

Centre for Number Theory Research,
MPCE Building E7A,
Macquarie University,
NSW 2109 Australia
gerry@mpce.mq.edu.au
Australia-2-9850-8952 fax 9850-8114

3 August 99

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

Remark: Duncan Buell carried out a search for a "magic hourglass," a configuration

$$\begin{array}{ccc} a-b & a+b+c & a-c \\ & a & \\ a+c & a-b-c & a+b \end{array}$$

all of whose entries are squares, and reports that there is no magic hourglass for which a is less than $25 \cdot 10^{24}$.

97:10 (Bob Silverman) The question concerns representations $N = \sum_{j=1}^{L} p_j^{\alpha_j}$ where p_j is the jth prime and $\alpha_j \geq 1$, e.g., $23 = 2 + 3^2 + 5 + 7$.

1. Is 33 the largest N not so representable?
2. How many different representations are there as $N \to \infty$?
3. How do α_j and L behave as $N \to \infty$?

Solution: Ernie Croot answers the first question in the affirmative. Here is a sketch of his solution. Further details can be obtained directly from Croot.

First, establish directly that if $33 < N < 4124$ then N is representable (Croot shows how to do this with minimal computational effort). From here on, we assume $N \geq 4124$.

Find the smallest prime q such that $\sum_{p \leq q} p \geq N/4$ and $\sum_{p \leq q} p \equiv N \pmod 2$. Write $N = \sum_{p \leq q} p + \delta$. It follows from standard estimates on primes (i.e., Rosser-Schoenfeld) that $\delta \geq 2062$. Note that δ is even. We claim that there are distinct primes $p_1, \ldots, p_k$ not exceeding q such that $\delta = (p_1^2 - p_1) + \cdots + (p_k^2 - p_k)$. The result follows immediately from this claim.

To prove the claim, first establish it directly for $2062 \leq \delta \leq 8248$ (again, Croot shows how to do this with minimal computational effort). The proof now proceeds by induction: assume $\delta \geq 8250$, and assume that if δ' is even and $2062 \leq \delta' < \delta$ then the claim is true for δ'. Let p be the largest prime not exceeding $\sqrt{3\delta}/2$. Write $\delta = p^2 - p + \delta'$. Another appeal to Rosser-Schoenfeld yields $2062 < \delta' < \delta$, so $\delta' = (p_1^2 - p_1) + \cdots + (p_k^2 - p_k)$ for some distinct primes $p_1, \ldots, p_k$, and it is easily checked that each of these primes is smaller than p. Thus $\delta = (p^2 - p) + (p_1^2 - p_1) + \cdots + (p_k^2 - p_k)$, establishing the claim.

97:15 (Peter Montgomery) Given a positive integer n, let $f(n)$ be the number of ways for two people to exchange n dollars, using the minimum number of bills of standard U.S. denominations (1, 5, 10, 20, 50, 100). For example, $f(13) = 3$ because there are three ways to make \$13 with 4 bills ($10+1+1+1$, $10+5-1-1$, and $20-5-1-1$), and no way using fewer bills.

What is the range of f? What ranges are possible, using other currency systems?

Solution: Bjorn Poonen writes, Let m be such that $100m < n \leq 100(m+1)$. At most $m+5$ bills are needed to exchange n dollars, since m \$100 bills can be used to get up to $100m$, then at most two more of \$10, \$20, \$50, \$100 are needed to get to the multiple of 10 nearest n, and finally at most 3 more bills of value \$1 or \$5 are needed to nail n exactly. If $n > 500$, then any minimal representation of n involves at least one \$100 bill, else the total value of bills exchanged would be at most $(m+5)50 \leq (2m)50 = 100m < n$. In other words, the minimal representations for n are obtained by appending a \$100 bill to each minimal representation for $n - 100$. Hence $f(n) = f(n-100)$ for $n > 500$. A simple computer program computes $f(n)$ for n up to 500, and shows that the range of f is $\{1, 2, 3, 4, 6\}$.

Poonen remarks:

1) In fact, $f(n + 100) = f(n)$ for all $n \geq 1$.

2) $f(n) = 6$ if and only if n is 33 or 37 mod 100.

3) A similar argument will reduce the question for any other finite set of denominations to a finite computation. The range is always finite.

97:16 (Gerry Myerson) Do there exist integers, $a_1, \ldots, a_n$, not necessarily distinct, such that each of the $n+1$ integers $1, 2, 4, \ldots, 2^n$ can be obtained as $\sum_{j \in J} a_j$ for some subset J of $\{1, \ldots, n\}$? The answer is no for $n \leq 3$.

Remarks: Building on examples of Peter Montgomery and David Moulton, the editor suggested letting $f(n)$ be the smallest number of integers needed to express $1, 2, 4, \ldots, 2^{n-1}$ as subsums. Moulton noted $f(7) \leq 5$, using -20, -15, 17, 19, 28. These remarks were included in the 1997 problem set.

Moulton now defines the rank of a set P as the least k for which there exist $a_1, \ldots, a_k$ such that every element of P is a subset sum from $a_1, \ldots, a_k$. He lets

$$\rho(2) = \lim_{n \to \infty} \mathrm{Rank}(\{1, 2, 4, \ldots, 2^{n-1}\})/n$$

(more generally; $\rho(r) = \lim_{n\to\infty} \mathrm{Rank}(\{1, r, r^2, \ldots, r^{n-1}\})/n$) and shows that $\rho(2)$ exists and that $\rho(2) < 15/22$.

Moulton proves $\rho(r) \leq (2r-2)/(2r-1)$; also, $\mathrm{Rank}(\{1, 2, 4, \ldots, 2^{n-1}\}) \geq n/\log_2 n$, and $\mathrm{Rank}(\{1, r, r^2, \ldots, r^{n-1}\}) > n/(1 + \log_r n)$. Further details available from Moulton.

Peter Montgomery asks whether there are results on the rank of an initial segment of a (linear, constant coefficient) recurrence sequence.

Problems Proposed 17 & 20 Dec 98

98:01 (Sam Wagstaff) Let integers a and d be given, with a fairly large, and let the Legendre symbols $(\frac{a+1}{p}), (\frac{a+2}{p}), \ldots, (\frac{a+k}{p})$ be given for some unknown prime $p > a$ of d digits and some $k \gg \log_2 p$.

1. Can you find p quickly (in time polynomial in $\log p$, say, or at least in time $O(p^\epsilon)$)?
2. Is there an easier way to find $(\frac{a+k+1}{p})$ than by finding p first?

98:02 (Gary Walsh) Ankeny-Artin-Chowla conjectured that if $p \equiv 1 \pmod 4$ is prime and $\epsilon_p = (T + U\sqrt{p})/2$ is the fundamental unit in $\mathbf{Q}(\sqrt{p})$ then p does not divide U. For $d = 46$,

$d = 430$, $d = 1817$ and a few other composite numbers under 10^7, if $x = T$, $y = U$ is the minimal solution to $x^2 - dy^2 = 1$, then $d \mid U$. Is there any reason to believe that there are only finitely many such composite d? that there are infinitely many?

98:03 (Neville Robbins) Let p be an odd prime, let g be the least positive primitive root (mod p). Is g always a primitive root (mod p^2)?

Solution: See

E. L. Litver, G. E. Judina, Primitive roots for the first million primes and their powers (Russian), Mathematical analysis and its applications, Vol. III (1971) 106–109.

The review by J. B. Roberts (MR 49 #4915) says,

. . .the authors have shown that with the single exception of 40487 all primes up to 1001321 have a least positive primitive root that is also a primitive root of the square of the prime. . . However 5, which is a primitive root of 40487, satisfies $5^{40486} \equiv 1 \pmod{40487^2}$.

This example was also found, at the meeting, independently, by Bjorn Poonen, Kevin Ford, and Peter Montgomery; it was also found that there are no further prime counterexamples below 4000000. One may ask whether there are infinitely many counterexamples.

98:04 (Sergei Konyagin, via Kevin Ford) Write $A + A$ for $\{ a + b : a, b \text{ in } A \}$, $A \cdot A$ for $\{ ab : a, b \text{ in } A \}$, and $|A|$ for the cardinality of A. Erdős-Szemeredi prove that if A is a finite set of real numbers then $|A + A| + |A \cdot A| \gg |A|^{1+\delta}$ for some positive δ, and Elekes (1997) showed one can take $\delta = 1/4$. It is conjectured that δ can be taken as $1 - \epsilon$, and known that δ cannot be taken as 1. Is there an analogous result for subsets of $\mathbf{F}_p$? We need a restriction on $|A|$, say $|A| \leq \sqrt{p}$.

98:05 (Kevin Ford) Using explicit zero density bounds (or otherwise), obtain explicit (lower) bounds for primes in short intervals superior to Rosser-Schoenfeld type bounds, especially in the range $100 \leq \log x \leq 10000$.

Remark: Carl Pomerance notes that Fred Chang is working on this and has some results.

98:06 (Paulo Ribenboim) Find integers P and Q such that each of the two numbers $P^2 - Q$ and $P^2(P^2 - 3Q^3)^2 - Q^3$ is three times a square, subject to the following restrictions: $P > 0$, $Q \neq 0$, $\gcd(P, Q) = 1$, $P^2 - 4Q > 0$, P even, and $Q \equiv 1 \pmod 4$.

The motivation for this problem is that if you find such P and Q, and if the sequence U_n is given by $U_n = PU_{n-1} - QU_{n-2}$, $U_0 = 1$, $U_1 = 1$, then U_9 is a perfect square.

There is a similar, but lengthier, set of conditions on P and Q which entail that U_{12} is a square—contact Ribenboim for the details.

98:07 (Paulo Ribenboim) Show that $x^n + y^n + z^n = 0$ with n prime and $n \geq 13$ has no non-trivial solution in any quadratic field.

Remark: The statement would be false for $n = 3$, and has been proved true for $n = 5$, 7, and 11 by Gross and Rohrlich.

98:08 (Bjorn Poonen) If $f(x, y, z) = x(2x-1) + y(2y-1) + z(2z-1)$, then the image under f of $\mathbf{Z} \times \mathbf{Z} \times \mathbf{Z}$ is $W = \{0, 1, 2, \dots\}$. Is there an f in $\mathbf{Z}[x, y]$ such that $f(\mathbf{Z} \times \mathbf{Z}) = W$?

98:09 (John Brillhart) Let the Jacobi function $\mathrm{sn}(t, k) = \sum_{m=0}^{\infty} a_m(k^2) \frac{t^{2m+1}}{(2m+1)!}$. For $n \geq 0$ we know $k^2 + 1 \| a_{2n+1}(k^2)$ and $k^4 + 14k^2 + 1 \| a_{3n+2}(k^2)$. For a given n, when these factors are removed, is the resulting polynomial irreducible?

There are analogous questions for $\mathrm{sc}(t, k)$ and $\mathrm{sd}(t, k)$.

98:10 (Robin Pemantle, via David Moulton) Find a two-parameter triple of rational functions α, β, γ with $\alpha + \alpha^{-1}, \beta + \beta^{-1}, \gamma + \gamma^{-1}$ in arithmetic progression.

Moulton reports $\alpha = \frac{2r^3 - 4r^2 + 4r}{r^4 - 4}$, $\beta = \frac{2r^3 - 4r}{r^4 + 4}$, $\gamma = \frac{2r^3 + 4r^2 + 4r}{r^4 - 4}$ is a one-parameter solution. He notes the relation to the problem of finding three integer-sided right triangles with a common base and hypotenuses in arithmetic progression; use hypotenuses $\alpha + \alpha^{-1}$, $\beta + \beta^{-1}$, $\gamma + \gamma^{-1}$ and common base 2, and clear fractions.

The editor asks whether there are sets of four (or more) integer-sided right triangles with a common base and hypotenuses in arithmetic progression.

98:11 (Jean-Marie De Koninck) Let $\beta(n) = \sum_{p \mid n} p$, let $B(n) = \sum_{p^\alpha \| n} \alpha p$. Prove that each of the equations

$$\beta(n) = \beta(n+1) = \dots = \beta(n+k) \qquad \text{and} \tag{1}$$

$$B(n) = B(n+1) = \dots = B(n+k) \tag{2}$$

has infinitely many solutions for each positive integer k. Obtain asymptotic estimates for $R_k(x) = \#\{n \leq x : (1) \text{ holds}\}$ and $S_k(x) = \#\{n \leq x : (2) \text{ holds}\}$.

Remarks: In the case $k = 1$, note that if p is a prime number such that $r = 6p - 1$, $s = 10p - 1$, and $q = 15p - 4$ are also primes, then clearly $n = 4pq = rs - 1$ is a solution of (1). According to the famous Hypothesis H of Schinzel, the 4 numbers x, $6x - 1$, $10x - 1$, and $15x - 4$ are simultaneously primes for infinitely many x; therefore, if Schinzel's conjecture is true, then $\beta(n) = \beta(n+1)$ has infinitely many solutions.

When $k = 2$, the smallest solution of (1) is $n = 89460294$, and the only solution $n < 10^8$ of (2) is $n = 417162$. Carl Pomerance provides a heuristic argument which suggests $R_k(x) > x^{1/3}$ and $S_k(x) > x^{1/3}$ for x large enough.

98:12 (Kevin Ford) For positive integers A, B, let $s(A, B)$ be the number of pairs of positive integers x, y, such that $x \mid Ay + B$ and $y \mid Ax + B$. Show that $s(A, B) \ll_\epsilon (AB)^\epsilon$.

Remark: If this is true then $C_3(x)$, the number of Carmichael numbers up to x with exactly three prime factors, satisfies $C_3(x) \ll_\epsilon x^{\frac{1}{3} + \epsilon}$.

98:13 (Ernie Croot) Let $\rho(\epsilon) = \lim_{N \to \infty} \Psi(N, N^\epsilon)/N$, where Ψ is the smooth-number counting function. Show that for any integer $k \geq 1$,

$$\#\{n \leq x - k : n, n+k \text{ both } x^\epsilon\text{–smooth}\} < 4\big(\rho(\epsilon)\big)^2 x$$

for x sufficiently large.

98:14 (Jeff Lagarias) We say $p = \sum_{j=0}^{m} a_j r^j$, $1 \le a_j \le r-1$, is highly prime in base r if $\sum_{j=0}^{k} a_j r^j$ is prime for $k = 0, 1, 2, \ldots, m$; we adopt the convention that 1 is prime. Conjecture: there are only finitely many highly prime numbers for each base. If so, estimate the number of highly prime numbers in base r and the size of the largest highly prime number in base r as $r \to \infty$.

Remarks: Adopting the convention that 1 is <u>not</u> prime,

I. O. Angell, H. J. Godwin, On truncatable primes, *Math. Comp.* 31 (1977) 265–267, MR 55 #248

find the largest highly prime number P_r for each base $3 \le r \le 11$ and conjecture an estimate for general r. They find that $P_{10} = 357686312646216567629137$.

A thread on this topic broke out on the Usenet newsgroup sci.math in January 1999. It can be found by searching dejanews for the subject, "Interesting primes." Dik Winter posted a simple Maple program for listing highly prime numbers. Modifying it to consider 1 a prime, your editor found (modulo any mistakes in Winter's program, my modification, my computer, or Maple) that the largest highly prime number in base 10 ending in 1 is 89726156799336363541, four digits shorter than the Angell-Godwin number.