Western Number Theory Problems, 1993–12–18 & 21

Edited by Richard K. Guy

for mailing prior to 1994 (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 (present set)	93:01–93:32

[With comments on earlier problems: 82:16, 84:01, 85:13, 91:24, 92:12.]

UPINT(2) = Richard K. Guy, Unsolved Problems in Number Theory, Springer, 1981. Second edition 1994.

COMMENTS ON ANY PROBLEM WELCOME AT ANY TIME

Department of Mathematics and Statistics,
The University of Calgary,
Calgary, Alberta, Canada, T2N 1N4.
rkg@cpsc.ucalgary.ca 403-220-6314 fax 282-5150

94-03-03.

COMMENTS ON EARLIER PROBLEMS

82:16 (= **366**) (J. Martin Borden, via Kevin McCurley) Given positive integers d, n_1, n_2 with $n_1 \perp n_2$, can one always find non-negative integers d_1, d_2 with $d_1 + d_2 = d$ and $d_1 \perp n_1$, $d_2 \perp n_2$?

1983 Comments: Peter Montgomery gave the counter-example $d = 16$, $n_1 = 273$, $n_2 = 110$. Mike Filaseta gave a list of d yielding counterexamples and suggested that there were infinitely many. Lagarias suggested it may be true if $n_i < d$. In a 83-10-26 letter Sitarama Chandra Rao, denoted the number of representations of $d = d_1 + d_2$ by $R(d)$ and proved

THEOREM 1. For all d, $|R(d) - d\phi(K)/K| \leq 1 + \sigma(K)$ where $K = n_1n_2$, ϕ is Euler's totient formula and $\sigma(K)$ is the sum of the positive divisors of K.

COROLLARY. Given n_1, n_2 with $n_1 \perp n_2$, then $R(d) > 0$ for all $d > K(1 + \sigma(K))/\phi(K)$.

THEOREM 2.

$$R(d) = \sum_{\substack{a|n_1 \\ b|n_2}} \mu(a)\mu(b) \left\{ \frac{d}{ab} - \frac{1}{2a} - \frac{1}{2b} - \frac{1}{a}\sum_{r=2}^{a} \frac{1}{\alpha_r^d(1-\alpha_r^{-b})} - \frac{1}{b}\sum_{s=2}^{b} \frac{1}{\beta_s^d(1-\beta_s^{-a})} \right\}$$

where $\alpha_r = e^{2\pi i r/a}$, $\beta_s = e^{2\pi i s/b}$ and μ is the Möbius function.

1984 Comments: Mike Filaseta corrected his list of counterexamples to (16) 22, 34, 36, 46, 56, 64, 66, 70, ... It was again suggested that there are infinitely many counterexamples, but none with $n_i < d$. Erdős noted that the first part of the statement is a result in

P. Erdős & W. T. Trotter, When the cartesian product of directed cycles is hamiltonian, *J. Graph Theory*, **2**(1978) 137–142; *MR* **80e**:05063

and that the sieve of Eratosthenes suffices to prove the second part when d is sufficiently large. In fact the Brun sieve shows that for some constant $1 > c > 0$ and for d sufficiently large, there are no counterexamples for which $n_1n_2 < e^{d^c}$. Mike Filaseta noted that the second part can be settled for all d in a rather simple way: indeed there are no counterexamples with $\min(n_1, n_2) < d$. To see this, suppose $n_2 < d$ and that n_2 is squarefree. Let $d_1 = n_2/(d, n_2)$ and $d_2 = d - d_1$. Then it can be shown that $d_1 \perp n_1$ and $d_2 \perp n_2$. He also noted that if the question is asked for *any* integers, possibly negative, then there are no counterexamples. Related open questions are:

84:01 (Paul Erdős & Mike Filaseta) In the previous problem, what is the density of the d which provide counterexampls? Are there infinitely many such odd d? [$d = 15395$ may be the least; see the Erdős-Trotter paper quoted above.

1985 Comments: Mike Filaseta notes that the original problem is equivalent to: are there positive integers a, b with $b > a + 1$ such that every integer between a and b has a factor in common with either a or b? Thai is, a counterexample to one problem gives rise to counterexamples to the other. For example, Peter Montgomery's original example with $d = 16$, $n_1 = 273$, $n_2 = 110$ corresponds to the example $(a, b) = (2184, 2200)$ in the present question ($b - a = 16$). Compare

P. Erdős & J. L. Selfridge, Complete prime subsets of consecutive integers, *Proc. Manitoba Conf. Numer. Math.*, 1971, *Congressus Numerantium* V, pp. 1–14. *MR* **49** #2597.

1993 Comments: Selfridge supplies a piece of paper with $d = 15493$ and $d = 903$ on it; I will get him to interpret. Should 15493 be 15395? Evidently $d = 903$ is a smaller odd counterexample. He refers to

David L. Dowe, On the existence of sequences of co-prime pairs of integers, *J. Autral. Math. Soc. Ser. A*, **47**(1989) 84–89; *MR* **90e**:11005

85:13 (J. R. Buchi) Let $n \geq 5$ and let $x_1^2 < \ldots < x_n^2$ be squares of positive integers. If the $n-2$ second differences $x_{i+2}^2 - 2x_{i+1}^2 + x_i^2$ are all equal to 2, must the x_i be *consecutive* integers?

Remark (1986) There is a paper,

Duncan A. Buell, Integer squares with constant second difference, *Math. Comput.*, **49**(1987) 635–644.

and John Leech quotes

D. Allison, On square values of quadratics, *Math. Proc. Cambridge Philos. Soc.*, **99**(1986) 381–383.

who rediscovers [Leech, The location of four squares in an arithmetic progression, with some applications, in *Computers in Number Theory* (Atlas Sympos. 1969), 83–98; *MR* **47** #4913] an infinity of symmetrical sets of eight squares with constant second differences; fails to find symmetrical sets of seven (proved impossible by Pocklington); and does some "interesting work on unsymmetrical sets."

Remark (1987) Leech writes (87-07-17): consider 4, $1+2a^2$, $4a^2$, $1+6a^2$, $4+8a^2$. We want $1+2a^2 = \square$, i.e., $a_n = 2, 12, 70, 408, \ldots, 6a_{n-1} - a_{n-2}$. Can we also make $1+6a^2 = \square$? This requires $a_n = 2, 20, 198, 1960, \ldots, 10a_{n-1} - a_{n-2}$. These sequences probably have no common term other than 2. But there are infinitely many *rational* a with $1+2a^2 = \square$, $1+6a^2 = \square$, since x^2+2y^2, x^2+6y^2 are concordant forms (Dickson's *History*, Vol. 2, pp. 472ff).

Richard Pinch observes that the general technique given in his paper,

Simultaneous Pellian equations, *Math. Proc. Cambridge Philos. Soc.*, **103**(1988) 35–46,

will answer Leech's question, and that he should be able to do this quite quickly when he is next within reach of a computer.

Remark (1993): It evaded his reach until

Richard G. E. Pinch, Squares in quadratic progression, *Math. Comput.*, **60**(1993) 841–845

where he finds the 72 nontrivial 4-term progressions with a term less than 1000^2, but no 5-term ones.

91:24 (Dick Katz) Inscribe an equilateral triangle in a circle of unit radius. Inscribe a circle in the triangle. Inscribe a square in the second circle, and inscribe a circle in the square. Inscribe a regular pentagon in the third circle, and continue indefinitely. The radii of the circles converge to

$$\prod_{k=3}^{\infty} \cos \frac{\pi}{k}.$$

What is this number?

1992 Comments (Richard McIntosh): (a) Abramowitz & Stegun, p. 75, give

$$\prod_{k=3}^{\infty} \cos \frac{\pi}{k} = \prod_{k=3}^{\infty} \prod_{n=1}^{\infty} \left(1 - \frac{4}{k^2(2n-1)^2}\right).$$

(b) Since $\frac{d}{dx} \ln \cos x = -\tan x$ can be expanded as a power series involving Bernoulli numbers, it follows that

$$\begin{aligned}
\ln \prod_{k=3}^{\infty} \cos \frac{\pi}{k} &= \sum_{k=3}^{\infty} \ln \cos \frac{\pi}{k} \\
&= -\sum_{n=1}^{\infty} \frac{(2^{2n}-1)(2\pi)^{2n} B_{2n}}{2n(2n)!} \left(\frac{(2\pi)^{2n} B_{2n}}{2(2n)!} + \frac{(-1)^n (2^{2n}+1)}{2^{2n}} \right) \\
&= -\sum_{n=1}^{\infty} \frac{(2^{2n}-1)}{n} \zeta(2n) \left(\zeta(2n) - 1 - \frac{1}{2^{2n}} \right)
\end{aligned}$$

where B_m is defined by

$$\frac{x}{e^x - 1} = \sum_{m=0}^{\infty} B_m \frac{x^m}{m!} \quad \text{and} \quad \zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$$

Using MAPLE we get $\prod_{k=3}^{\infty} \cos \frac{\pi}{k} =$

0.11494 20448 53296 20070 10401 57469 59874 28307 95337 20086 35168 44023 39651 89660 12825 35305 11779...

(c) Since $\prod_{n=1}^{\infty} \cos \frac{x}{2^n} = \frac{\sin x}{x}$, it follows that if we use only 2^n-gons ($n = 2, 3, 4, \ldots$), then the radii converge to $\frac{2}{\pi}$.

1993 Comment: (Patrick Wahl) The problem goes back to Kepler (1595).

92:12 (Andrew Granville) Find examples of

$$x^p + y^q = z^r \quad \text{with} \quad \frac{1}{p} + \frac{1}{q} + \frac{1}{r} < 1$$

other than $2^3 + 1^7 = 3^2$ and $7^3 + 13^2 = 2^9$. [Blair Kelly III gave $2^5 + 7^2 = 3^4$ and Reese Scott $17^3 + 2^7 = 71^2$.]

Find examples of coprime triples (A, B, C) for which there are at least 3 solutions of

$$Ax^p + By^q + Cz^r = 0 \text{ with } \frac{1}{p} + \frac{1}{q} + \frac{1}{r} < 1 \text{ and } |x|,\ |y|,\ |z| \geq 2$$

Find a solution to

$$Ax^2 + By^3 = Cz^5 \text{ in polynomials } x(A, B, C),\ y(A, B, C),\ z(A, B, C)$$

such that Ax, By, Cz have no common factors.

Remark: Gerry Myerson suggests that it was intended that x, y, z be relatively prime in order to avoid $x^3 + y^7 = z^2$ with $x = (n^2 - 1)^2$, $y = n^2 - 1$, $z = n(n^2 - 1)^3$ and, more generally, $x = b^r - 1$, s any multiple of r, $p = s + 1$, q any divisor of s, $y = x^{s/q}$, $z = bx^{s/r}$ gives $x^p + y^q = z^r$. Also $2^5 + 88^2 = 6^5$; $22^5 + 33^5 = 6655^2$. [The proposer concurs.]

Andrew Granville also gave $3^5 + 11^4 = 122^2$. Peter Montgomery reports that extraordinarily large solutions have been found recently by Beukers and Zagier: $17^7 + 76271^3 = 21063928^2$, $1414^3 + 2213459^2 = 65^7$, $9262^3 + 15312283^2 = 113^7$, $43^8 + 96222^3 = 30042907^2$, $33^8 + 1549034^2 = 15613^3$.

PROBLEMS PROPOSED 93–12–18 & 21

93:01 (Mike Filaseta) $p(n)$ is the usual unrestricted partition function. Is the set $\{q : q \text{ prime}, \exists n \in \mathbb{Z}^+ \ni q|p(n)\}$ of primes which divides the values of the partition function infinite? Does it include all primes?

Remark: Odlyzko and the proposer later supply the following references:

A. Schinzel & E. Wirsing, Multiplicative properties of the partition function, *Proc. Indian Acad. Sci. (Math. Sci.)* **97**(1987) 297–303.

P. Erdős & A. Ivić, The distribution of values of a certain class of arithmetic functions at consecutive integers, in Papers from the conference held in Budapest, July 20–25, 1987, edited K. Győry & G. Halász, North-Holland, Amsterdam, *Colloq. Math. Soc. János Bolyai*, **51**(1990) 45–91.

93:02 (Mike Filaseta) Is

$$\frac{(x+1)^{2n} - x^{2n} - 1}{x}$$

irreducible over the rationals for every positive integer n?

Remarks: Yes, when n is prime. Checked for $n \le 90$ by *Mathematica*©. Connected to a conjecture of Mirimanoff.

93:03 (John Conway & Andrew Odlyzko) Call d a **high-jumper** if d occurs most frequently as the difference of consective primes $\le x$ for some x (there may be several high-jumpers for a given x).

Example: $x = 11$: 2, 3, 5, 7, 11 gives 1, 2, 2, 4, so $C(11) = \{2\}$.

Conjecture: the only high-jumpers are 4 and the prime factorials 2, 6, 30, 210, 2310, ... Can one prove that high-jumpers tend to infinity? That any prime p divides all high-jumpers for $x \ge x_0(p)$?

Remarks: A paragraph of UPINT2 reads as follows:

Victor Meally used the phrase **prime deserts**. He notes that below 373 the commonest gap is 2; below 467 there are 24 gaps of each of 2, 4 and 6; below 563 the commonest gap is 6, as it is between 10^{14} and $10^{14} + 10^8$ and probably also from 2 to 10^{14}. He asks: when does 30 take over as the commonest gap?

Dan Goldston provides the references:

Harry Nelson, Problem 654, *J. Recreational Math.*, **10**(1977-78) 212.

P. Erdős & E. G. Straus, Remarks on the difference between consecutive primes, *Elem. Math.*, **35**(1980) 115-118.

Erdős & Straus assumed a version of the Hardy-Littlewood prime k-tuple conjecture to show that high-jumpers go to infinity. The proposers can almost certainly show that the conjecture is true if they assume a uniform version of the k-tuple conjecture. This has not been written down yet, though.

93:04 (Neville Robbins) Find a formula for the number of self-conjugate partitions.

Remark: It is easy to see via the Ferrers's diagram that this is the same as the number of partitions into distinct odd parts, so that the generating function is $\prod_{k=0}^{\infty}(1+q^{2k+1})$.

On removing the Durfee square, the largest square that can be drawn in the top left corner of the diagram, it is seen that the number of self-conjugate partitions of n is

$$\sum_{d\equiv n \bmod 2}^{\lfloor\sqrt{n}\rfloor} p\left(\frac{1}{2}(n-d^2)\right)$$

where $p(n)$ is the unrestricted partition function, so that formulas will be of the same type as for that function, i.e., good asymptotic ones.

93:05 (Graeme Cohen via Hugh Edgar) Prove that if $n(2n-1)$ is perfect, then n is even.

Remark: Graeme Cohen has proved that if the odd perfect number $N = p^a L^2 = n(2n-1)$ where the prime $p \nmid L$ and $p \equiv a \equiv 1 \bmod 4$ then if q is a prime divisor of N and $q \equiv 3 \bmod 8$, then $\left(\frac{p}{q}\right) = -1$. Also $p \notin \{73, 89, 129, 233, 257, 281\}$.

93:06 (David, Jonathan & Peter Borwein & Roland Girgensohn, via Hugh Edgar – two problems from a manuscript "On a Conjecture of Giuga") (a) Investigate the set of positive integers (generalized Carmichael numbers) $n = \prod p^e$ for which $(p^e-1)|(n-1)$ for each component, p^e, of n. Examples are 12025, 13833, 35425, 54145. Are there infinitely many? It seems that the methods of Alford, Granville & Pomerance probably won't help.

(b) Characterize those positive integers n such that

$$\sum_{p^e\|n}\frac{1}{p^e} - \prod_{p^e\|n}\frac{1}{p^e}$$

is a nonnegative integer. Examples of composite **Kirchhoff numbers** are 30, 858, 1722, 66198. Is there an odd composite Kirchhoff number? If so, it has at least 9 prime factors.

93:07 (Denis Hanson via Richard McIntosh) Give an elementary proof of

$$\sum_{k=0}^{n}\frac{\binom{n}{k}\binom{n+1}{k}}{\binom{2n}{2k}} = 2n+1$$

What about

$$\sum_{k=0}^{n}\frac{\binom{n}{k}\binom{n+r}{k}}{\binom{2n}{2k}}?$$

Remark: A proof was given by Peter Montgomery using the generating function for the Catalan numbers. He also notes that it can be shown by induction on m that for $0 \le m \le n$, the partial sums

$$\sum_{k=0}^{m}\frac{\binom{n}{k}\binom{n+1}{k}}{\binom{2n}{2k}} = 2m+1\frac{\binom{n}{m}^2}{\binom{2n}{2m}}$$

Now set $m = n$. But neither method seems to work if $r \neq 1$.

It would be nice to see a purely combinatorial (counting) proof.

93:08 (Gerry Myerson) If p_i is the ith prime, for which n is

$$4\prod_{i=1}^{n} p_i + 1$$

a square?

NOTE: $n = 1 \quad 4 \cdot 2 + 1 = 3^2$; $n = 2 \quad 4 \cdot 2 \cdot 3 + 1 = 5^2$; $n = 3 \quad 4 \cdot 2 \cdot 3 \cdot 5 + 1 = 11^2$; $n = 4 \quad 4 \cdot 2 \cdot 3 \cdot 5 \cdot 7 + 1 = 29^2$; $n = 7 \quad 4 \cdot 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 + 1 = 1429^2$.

The proposer found no others up to $n = 25$, the editor extended this to $n = 35$ and on 94-01-17 the proposer quoted David Bailey: if $P(x)$ is the product of the primes not exceeding x (so, e.g., $P(10) = 210$), then $4P(x) + 1$ is not a square for any x between 19 and 23000. This may be a good place to quote Andrew Granville who in turn quotes Fermat:

> In the 17th century there were, as we view it today, two meanings to induction. Due to a lack of good notation, and even a clear notion of what a proof was, many "proofs" actually were 'doing' the first few cases and then extrapolating that all cases would follow in similar fashion. Thus, what was known (by Descartes) as "complete" induction was one where you could clearly see how to deduce the $(n+1)$st case from the nth (given, say, the deduction of the 3rd case from the 2nd case as an example). Whereas "incomplete" induction was where there was no clear procedure – just wishful thinking from the first few cases (i.e. 'the law of small numbers').
>
> In 1656 Wallis used such incomplete 'induction' in his "Arithmetica Infinitorum". In 1657 Fermat, while praising some of Wallis's work, wrote (translating from the French):
>
> > "One might use this method if the proof of some proposition were deeply concealed and if, before looking for it, one wished first to convince oneself more or less of its truth; but one should place only limited confidence in it and apply proper caution. Indeed, one could propose such a statement, and seek to verify it in such a way, that it would be valid in several special cases but nonetheless false and not universally true, so that one has to be most circumspect in using it; no doubt it can still be of value if applied prudently, but it cannot serve to lay the foundations of some branch of science, as Mr. Wallis seeks to do, since for such a purpose nothing short of a demonstration is admissible."
>
> Nicely put, don't you think!

93:09 (Gerry Myerson) Is it true that for $n \geq 1$ there exist disjoint sets A, B such that $A \cup B = \{2, 3, \ldots, p_n\}$ and $\prod_{p\in A} + \prod_{p\in B}$ is prime? What about $\prod_{p\in A} - \prod_{p\in B}$? What about both being prime?

E.g., $2 \cdot 3 + 1 = 7$ & $2 \cdot 3 - 1 = 5$ are prime, $2 \cdot 5 + 3 = 13$ & $2 \cdot 5 - 3 = 7$ are prime, $5 \cdot 7 + 2 \cdot 3 = 41$ & $5 \cdot 7 - 2 \cdot 3 = 29$ are prime, $7 \cdot 11 + 2 \cdot 3 \cdot 5 = 107$ & $7 \cdot 11 - 2 \cdot 3 \cdot 5 = 47$ are prime, $7 \cdot 11 \cdot 13 + 2 \cdot 3 \cdot 5 = 1031$ & $7 \cdot 11 \cdot 13 - 2 \cdot 3 \cdot 5 = 971$ are prime.

93:10 (Gerry Myerson) Given k, let $n = n(k)$ be the smallest integer $> k$ such that $k!$ divides $\binom{n}{k}$. How does $n(k)$ grow?

Notes: 1. It is easy to show that $n(k) \le k \cdot k!$ **2.** $n(k)$ is not monotone, $n(1) = 1$, $n(2) = 4$, $n(3) = 9$, $n(4) = 33$, $n(5) = 28$, $n(6) = 165$, $n(7) = 54$, $n(8) = 1029$, $n(9) = 40832$.

93:11 (Gerry Myerson) Given a non-constant polynomial $f : \mathbb{Z} \to \mathbb{Z}$ and an integer a_1, define a sequence $\{a_n\}$ by $a_{n+1} = f(a_n)$, $n = 1, 2, \ldots$. Assume that this sequence is unbounded.

(a) Do there exist f and a_1 such that every a_n is prime?

(b) Do there exist f and a_1 for which you can prove that infinitely many of the a_n are prime?

Note: Among the sequences that can be obtained in this way are the Fermat numbers $F_n = 2^{2^n} + 1$ and the Mersenne numbers $M_n = 2^n - 1$.

Remark: (Peter Montgomery) If $k > 0$, then we can use $f(x) = x + k$ and $\gcd(a_1, k) = 1$ in (b). If f exists (in (a) or (b)), then there are infinitely many integers k such that $f(k)$ is prime. The only known polynomials with this property are linear polynomials.

93:12 (Richard Guy) The elliptic curve $y^2 + y = x^3 - x$ has the smallest conductor, 37, among rank 1 curves. The fraction

$$\int_0^\infty \frac{dx}{y} \bigg/ \int_{-\infty}^\infty \frac{dx}{y}$$

(if I've got the equation in the right form) of the branch between the generator (0,0) and the point at infinity is

$$\frac{1}{3+}\,\frac{1}{4+}\,\frac{1}{1+}\,\frac{1}{1+}\,\frac{1}{5+}\,\frac{1}{2+}\,\frac{1}{168+}\,\frac{1}{46793+}\,\frac{1}{1+}\,\frac{1}{7+}\,\cdots$$

Explain the large partial quotients.

Remark: This is a specific instance of Problem **92:14**.

93:13 (Reese Scott via Andrew Granville) The cardinality of the set

$$\{(x, y, z) \ : \ x^2 + y^2 = z^2, \gcd(x, y, z) = 1, \ \# \text{ of prime factors of } xyz \text{ is } \le 5\}$$

is finite. Can 5 be replaced by 6 or 7?

Remark: (Peter Montgomery) If $k \ge 7$ is of the form $2^r 3^s 5^t p$ where p is 1 or prime and $30k \pm 1$ and $900k^2 + 1$ are simultaneously prime, then $x = 60k$, $y = 900k^2 - 1$, $z = 900k^2 + 1$ contain just seven distinct prime factors. E.g., $k = 6$, $k = 19$.

Remark: (Kevin Ford) There are just 30 such triples with $k \le 5$, the largest being $(375, 7808, 7817)$.

We consider the general form of a primitive pythagorean triple $(2pq, p^2 - q^2, p^2 + q^2)$ where p and q are coprime positive integers of opposite parity.

Using Theorem 10.4 from *Sieve Methods* by Halberstam & Richert, I can prove that there are infinitely many triples with $k \le 19$. This is accomplished by setting $q = 1$ and sieving the polynomial $p(p+1)(p-1)(p^2+1)$. The primes 2, 3 and 5 always divide this polynomial, so they must be excluded from the sieve.

The following heuristic shows that there are probably infinitely many such triples with $k = 6$. Let $p = 2^a$, $q = 3^b 5^c < p/2$. The probability that $p+q$, $p-q$ and p^2+q^2 are simultaneously prime is $\gg 1/a^3$. Summing over b, c, a yields a divergent series. A computer search using PARI yielded 49 triples with $p = 2^a$, $q = 3^b$, 5^c (without the condition $q < p/2$) and $p, q < 10^{18}$. The one with largest z corresponded to $(a,b,c) = (40,24,9)$. The triple is $x = 6065128113051669626880000000000$, $y = 3042848322927688492328794198975594449$, $z = 304284832295186700872108678246971801$.

93:14 (Andrew Granville) Are there addition chains with $l(4n) = l(2n) = l(n)$? And if so, then with $l(8n) = l(4n) = l(2n) = l(n)$ etc.?

[For background to this and problem **93:15** we quote from **C6** of UPINT2:

An **addition chain** for n is a sequence $1 = a_0 < a_1 < \ldots < a_r = n$ with each member after the zeroth the sum of two earlier, not necessarily distinct, members. For example

1, 1+1, 2+2, 4+2, 6+2, 8+6 and 1, 1+1, 2+2, 4+2, 4+4, 8+6

are addition chains for 14 of **length** $r = 5$. The minimal length of an addition chain for n is denoted by $l(n)$.

The main unsolved problem is the Scholz conjecture

$$¿ \quad l(2^n - 1) \le n - 1 + l(n) \quad ?$$

It has been proved for $n = 2^a$, $2^a + 2^b$, $2^a + 2^b + 2^c$, $2^a + 2^b + 2^c + 2^d$ by Utz, Gioia et al, and Knuth, and demonstrated for $1 \le n \le 18$ by Knuth and Thurber. Brauer proved the conjecture for those n for which a shortest chain exists which is a **Brauer chain**, that is one in which each member uses the previous member as a summand. The second of the examples is not a Brauer chain, because the term 4+4 does not use the summand 6. Such an n is called a **Brauer number**. Hansen proved that there are infinitely many non-Brauer numbers, but also that the Scholz conjecture still holds if n has a shortest chain which is a **Hansen chain**, that is one for which there is a subset H of the members such that each member of the chain uses the largest element of H which is less than the member. The second example is a Hansen chain, with $H = \{1, 2, 4, 8\}$. Knuth gives the example

$$1, 2, 4, 8, 16, 17, 32, 64, 128, 256, 512, 1024, 1041, 2082, 4164, 8328, 8345, 12509$$

of a Hansen chain (H={1, 2, 4, 8, 16, 32, 64, 128, 256, 512, 1024, 1041, 2082, 4164, 8328, 8345}) for $n = 12509$ which is not a Brauer chain (32 does not use 17) and no such short Brauer chain exists for $n = 12509$.

Are there non-Hansen numbers?

It is clear that $l(2n) \le l(n) + 1$. That strict inequality is possible was shown by Knuth with $l(382) = l(191) = 11$. The smallest even n with $l(2n) = l(n)$ is 13818, given by Thurber, who also noticed the odd adjacent pair 22453, 22455.

Walter Aiello & M. V. Subbarao, A conjecture in addition chains related to Scholz's conjecture. *Math. Comput.*, **61**(1993) 17–23; *MR* **93k**:11015.

A. T. Brauer, On addition chains, *Bull. Amer. Math. Soc.*, **45**(1939) 736–739.

A. Cottrell, A lower bound for the Scholz-Brauer problem, Abstract 73T-A200, *Notices Amer. Math. Soc.*, **20**(1973) A-476.

Paul Erdős, Remarks on number theory III. On addition chains, *Acta Arith.*, **6**(1960) 77–81.

R. P. Giese, PhD thesis, University of Houston, 1972.

R. P. Giese, A sequence of counterexamples of Knuth's modification of Utz's conjecture, Abstract 72T-A257, *Notices Amer. Math. Soc.*, **19**(1972) A-688.

A. A. Gioia & M. V. Subbarao, The Scholz-Brauer problem in addition chains II, *Congr. Numer. XXII*, Proc. 8th Manitoba Conf. Numer. Math. Comput. 1978, 251–274; *MR* **80i**: 10078; *Zbl.* 408.10037.

A. A. Gioia, M. V. Subbarao & M. Sugunamma, The Scholz-Brauer problem in addition chains. *Duke Math. J.*, **29**(1962) 481–487; *MR* **25** #3898.

W. Hansen, Zum Scholz-Brauerschen Problem, *J. reine angew. Math.*, **202** (1959) 129–136; *MR*25 #2027.

Kevin Hebb, Some problems on addition chains, thesis, Univ. of Alberta, 1974.

A. M. Il'in, On additive number chains (Russian), *Problemy Kibernet.*, **13** (1965) 245–248.

H. Kato, On addition chains. PhD dissertation, Univ. Southern California, June 1970.

Donald Knuth, *The Art of Computer Programming*, Vol. 2, Addison-Wesley, Reading MA, 1969, 398–422.

D. J. Newman, Computing when multiplications cost nothing, *Math. Comput.*, **46**(1986) 255–257.

Arnold Scholz, Aufgabe 253. *Jber. Deutsch. Math.-Verein. II*, **47**(1937) 41–42 (supplement).

Rolf Sonntag, Theorie der Addition Sketten, PhD Technische Universität Hannover, 1975.

K. B. Stolarsky, A lower bound for the Scholz-Brauer problem, *Canad. J. Math.*, **21**(1969) 675–683; *MR* **40** #114.

M. V. Subbarao, Addition chains – some results and problems, in R. A. Mollin (ed.) Number Theory and Applications, NATO ASI Series. Kluwer, Boston, 1989, pp. 555–574; *MR* **93a**:11105.

E. G. Straus, Addition chains of vectors, *Amer. Math. Monthly*, **71**(1964) 806–808.

E. G. Thurber, The Scholz-Brauer problem on addition chains, *Pacific J. Math.*, **49**(1973) 229–242; *MR* **49** #7233.

E. G. Thurber, On addition chains $l(mn) \leq l(n) - b$ and lower bounds for $c(r)$, *Duke Math. J.*, **40**(1973) 907–913.

E. G. Thurber, Addition chains and solutions of $l(2n) = l(n)$ and $l(2^n - 1) = n + l(n) - 1$, *Discrete Math.*, **16**(1976) 279–289; *MR* **55** #5570; *Zbl.* **346**.10032.

W. R. Utz, A note on the Scholz-Brauer problem in addition chains, *Proc. Amer. Math. Soc.*, 4(1953) 462–463; *MR* **14**, 949.

C. T. Wyburn, A note on addition chains, *Proc. Amer. Math. Soc.*, **16**(1965) 1134.]

93:15 (Edward Thurber) Is $l(2n) \geq l(n)$ for all n? Some related questions are:

(a) For all positive integers t, does there exist an odd positive integer m such that $l(2^{t+1}m) = l(2^t m)$? Examples with $t = 1$ are 13818 and 27578.

(b) Is there an adjacent pair n, $n+1$ satisfying $l(2n) = l(n)$ and $l(2(n+1)) = l(n+1)$?

(c) If $h(x)$ denotes the number of integers $n \leq x$ such that $l(2n) = l(n)$, then is $h(x) = \Omega(x)$?

(d) If $c(r)$ is the least integer requiring r steps in a minimal addition chain, is $c(r+1) \le 2c(r)$? If $c(r+1) > c(r)$, then if $n = c(r)$ it follows that $l(2n) = l(n)$. $c(11) = 191$ and $c(19) = 18287$ satisfy $l(2n) = l(n)$.

(e) Is $c(r)$ odd for all r ? $l(281) = 10$ and $l(282) = 11$; thus, there do exist odd integers n for which $l(n) < l(n+1)$. Does this happen when $n = c(r) - 1$?

93:16 (Melvyn Knight) When $p \equiv 1 \bmod 4$

$$\left[\left(\frac{p-1}{2}\right)!\right]^2 \equiv -1 \bmod p \quad \text{and} \quad \left(\frac{p-1}{2}\right)! \equiv i \bmod p$$

When is $0 < i < p/2$?

Remark: (Andrew Granville) In

L. J. Mordell, The congruence $(\frac{p-1}{2})! \equiv \pm 1 \bmod p$, *Amer. Math. Monthly*, **68**(1961) 145–146; *MR* **23** #A837; rNT R14-41

it is shown that if $p \equiv 3 \bmod 4$ and $p > 3$, then $(\frac{p-1}{2})! \equiv (-1)^a \bmod p$ where $a \equiv \frac{1}{2}\{1 + h(-p)\} \bmod 2$ and $h(-p)$ is the class number of the quadratic field $k(\sqrt{-p})$. Mordell notes that this follows from a result of Dirichlet and that Jacobi had conjectured an equivalent result before the class number formula was known. In

S. Chowla, On the class number of real quadratic fields, *Proc. Nat. Acad. Sci. U.S.A.*, **47**(1961), 878; *MR* **23** #A2413; rNT R14-42

if $p \equiv 1 \bmod 4$, h is the class number of the real quadratic field $R(\sqrt{p})$ and $\epsilon = (t + u\sqrt{p})/2 > 1$ is its fundamental unit, then $((p-1)/2)! \equiv (-1)^{(h+1)/2} t/2 \bmod p$.

93:17 (Andrew Granville) Find a non-homogeneous irreducible polynomial $F(x,y) \in \mathbb{Z}[x,y]$ of degree $d \ge 5$ with a lot of rational solutions x, y to $F(x,y) = 0$.

Remark: The best examples known are $y^2 - A(x-1)(x-2)\cdots(x-d) - 1$ with solutions $(1, \pm 1)$, $(2, \pm 1)$, $\ldots$, $(d, \pm 1)$, $(0, \pm B)$ where $B^2 = A(-1)^d d! + 1$. Can one get an infinite sequence of $F_i(x,y)$ of degree d_i with at least cd_i^2 rational points for some constant c? You are not allowed to cheat by using factorable polynomials such as $(x-y)(x-2y)$.

Andrew Bremner notes that if d is even there are also the solutions $(d+1, \pm B)$.

Remarks by Gene Smith, Peter Montgomery and the proposer imply that one is not allowed to have examples where x and y may be parametrized in terms of polynomials or points on some elliptic curve. The curves should be of genus ≥ 2.

93:18 (David Gove) If ω is a string of zeros and ones such that for any block B the string BBB does not appear (e.g., the Morse-Hedlund sequence 01101001100101101001...) does

$$\lim_{n \to \infty} \frac{s(n)}{n} = \frac{1}{2}$$

where $s(n)$ is the number of ones in the first n positions of ω?

93:19 (Jeff Lagarias) Prove or disprove that the lengths of the blocks of consecutive zeros and ones in the binary expansion of

$$\sqrt{2} = 1.011010100000100111100110011001111111001110111100110010010000100\ldots$$

are unbounded. I.e., are there values of n such that the fractional parts, $\{\ \ \}$, satisfy $0 < \{2^n\sqrt{2}\} < \epsilon$ (for a long block of zeros) and $1 - \epsilon < \{2^n\sqrt{2}\} < 1$ (for a long block of ones)?

93:20 (Eugene Gutkin via Jeff Lagarias) Let G_n be the solutions of $\tan n\theta = n \tan\theta$ with $0 \le \theta < \pi$. Determine $G_n \cap G_m$. (The question arises in studying orbits of billiards with special properties.)

Remark: (Jeff Lagarias) If we write $x = e^{2i\theta}$ then

$$\tan n\theta = \frac{e^{in\theta} - e^{-in\theta}}{e^{in\theta} + e^{-in\theta}} = \frac{x^n - 1}{x^n + 1} \quad \text{and} \quad \tan\theta = \frac{x-1}{x+1}$$

Hence the equation $\tan n\theta = n\tan\theta$ becomes

$$(n-1)(x^{n+1} - 1) - (n+1)(x^n - x) = 0$$

The left side has a "trivial" factor $(x-1)^3$, so consider the polynomials

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

for $n \ge 1$.

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

Checked by Maple for $n \le 20$. It would imply $G_n \cap G_m = \{0\}$ if $mn \equiv 0 \bmod 2$ and $G_n \cap G_m = \{0, \frac{1}{2}\pi\}$ if $n \equiv m \equiv 1 \bmod 2$.

93:21 (Gerry Myerson) (a) Let n lines divide a disk into the maximum possible number of regions, namely $\binom{n}{0} + \binom{n}{1} + \binom{n}{2}$. How large can the smallest region be? [Solving $n = 3$ is a nontrivial calculus exercise.]

(b) What's the largest number of equal-area regions a disk can be cut into by n lines? A trivial lower bound is $2n$.

93:22 (Arthur Baragar) The Markoff equation $x^2 + y^2 + z^2 = 3xyz$ has a group $\mathcal{G}$ of automorphisms generated by $(x,y,z) \to (x,y,3xy - z)$, $(x,y,z) \to (-x,-y,z)$, and permutations of the variables. Modulo a prime $p \ge 5$ this equation has

$$p^2 + \left(\frac{-1}{p}\right) 3p + 1$$

solutions, where $(-1|p)$ is the quadratic residue of -1 modulo p. Is this set of solutions precisely $\{(0,0,0)\} \cup \mathcal{G}(1,1,1)$? I.e., does every modulo p solution lift to an integer solution? Can this at least be shown for $p \equiv 1 \bmod 4$?

93:23 (Peter Montgomery) Given a large integer n, find a geometric progression

$$\mathcal{C} = [c_4, c_3, c_2, c_1, c_0] \bmod n,$$

where each c_i is $O(n^{2/3})$. We also require that $\mathcal{C}$ not be a second-order linear recurrence over $\mathbb{Q}$. This latter condition means that the determinant

$$\begin{vmatrix} c_4 & c_3 & c_2 \\ c_3 & c_2 & c_1 \\ c_2 & c_1 & c_0 \end{vmatrix}$$

is nonzero (indeed, it is a nonzero multiple of n^2).

More generally, given n and $d > 1$, find a geometric progression modulo n of length $2d-1$ with all terms $O(n^{1-1/d})$ and which is not a linear recurrence of order $d-1$ over $\mathbb{Q}$. We are primarily interested in the case where n is composite with no known prime factors, but even a solution for prime n would be of interest.

Example: If $n = 1993$, then $[57, -33, 124, 138, 25]$ has ratio 419 and largest term 138, compared to $n^{2/3} \approx 158.36$. From this one can derive the cubics $X^3 - X - 3$ and $3X^3 - 3X^2 + 3X + 1$ which have root 419 modulo 1993. The vector $[43, 12, -43, -12, 43]$ has ratio $1159 = \sqrt{-1}$ modulo 1993, but satisfies a second-order linear recurrence and is ineligible. [The background, factoring n with the general number field sieve, is available from the proposer. The address `pmontgom@cwi.nl` is valid only through August 1994.]

93:24 (Richard Guy) Is every sufficiently large number $24n + 3$ expressible as the sum of three squares of shape $(6r-1)^2$ with $r \geq 0$? [E.g., $291 = 17^2 + (-1)^2 + (-1)^2$ is acceptable, but not $11^2 + 11^2 + (-7)^2$. Perhaps $r > 0$ is possible.]

93:25 (Richard Guy) Are all multiples of 3, other than those of shape $4^k(24l+15)$, expressible as the sum of three squares, none of them multiples of 3?

Solution: (Peter Montgomery) Yes. Let n be a multiple of 3 not of the shape $4^k(24l+15)$. Select a representation $n = x^2 + y^2 + z^2$ in which the power of 3 dividing $\gcd(x, y, z)$ is as small as possible. If $\gcd(x, y, z, 3) = 1$, then at least one square is not divisible by 3. Since $n \equiv 0 \bmod 3$, one easily checks that none of x, y, z can be divisible by 3. Suppose $\gcd(x, y, z)$ is divisible by 3, say $x = 3a$, $y = 3b$, $z = 3c$. Then

$$n = x^2 + y^2 + z^2 = 9a^2 + 9b^2 + 9c^2 = (2a + 2b - c)^2 + (2a - b + 2c)^2 + (-a + 2b + 2c)^2.$$

We can get other representations for n as a sum of three squares by changing the signs of a, b, c. The gcd of the 12 quantities $2a \pm 2b \pm c$, $2a \pm b \pm 2c$, $a \pm 2b \pm 2c$ will divide $\gcd(a, b, c)$ since, for example, $2a = (a - 2b - 2c) + (a + 2b + 2c)$, $2b = (b - 2a - 2c) + (b + 2a + 2c)$, $2c = (c - 2a - 2b) + (c + 2a + 2b)$, $a = (a - 2b - 2c) + 2b + 2c$, $b = (b - 2a - 2c) + 2a + 2c$, $c = (c - 2a - 2b) + 2a + 2b$. Therefore some value among the 12 is divisible by a lesser power of 3 than is $3\gcd(a, b, c) = \gcd(x, y, z)$. This contradicts the minimality assumption.

93:26 (Richard Guy) Are all sufficiently large numbers $40n + 27$ expressible as the sum of three squares of shape $(10r \pm 3)^2$? [427, 667, 3067 are not. Are there other exceptions?

Remark: Problems **93:24–26** stem from attempting to express (sufficiently large) numbers as the sum of three pentagonal, octagonal or heptagonal numbers (of positive rank). Patrick Wahl may have answers to these questions by 1994, 1997 and 1996 respectively.]

93:27 (Paul Feit) Let $\mathcal{S}(n) = \{\text{all subsets of } \mathbb{Z}^n\}$. By a **density** δ for $\mathbb{Z}^n$ we mean a function $\delta : \mathcal{S}(n) \to [0, 1]$ such that

1. $\delta(\mathbb{Z}^n) = 1, \quad \delta(\{0\}) = 0$
2. for $S, T \subseteq \mathbb{Z}^n$, $\delta(S \cup T) \leq \delta(S) + \delta(T)$
3. for $S \subseteq \mathbb{Z}^n, v \in \mathbb{Z}^n$, $\delta(S + v) = \delta(S)$
4. if $S \subseteq \mathbb{Z}$ such that $\delta(S) > 0$ and $v \in \mathbb{Z}^n$, then there is $k \in \mathbb{N}$ for which $\delta(S \cap S + kv) > 0$

Example: Suppose $\{F_n\}_{n=1}^{\infty}$ is a sequence of finite non-empty subsets of $\mathbb{Z}^n$ such that for each $v \in \mathbb{Z}^n$

$$\lim_{n\to\infty} \frac{|F_n \cap (F_n + v)|}{|F_n|} = 1$$

then $\delta(S) = \sup |F_n \cap S|/|F_n|$ is a density.

Question: Let f, g be coprime nonzero polynomials in $\mathbb{Z}[x_1, \ldots, x_n]$ and $S = \{b \in \mathbb{Z}^n \mid g(b) \neq 0 \text{ and } \frac{f(b)}{g(b)} \in \mathbb{Z}\}$. If $\delta(S) > 0$, must $g(x) \in \mathbb{Z}$?

Remark: Known: Consider $\mathbb{Z}^n$ as the integer points of the n-dimensional affine variety $\mathbb{A}^n$. Imbed $\mathbb{A}^n \in \mathbb{P}^n$ and let $\infty = \mathbb{P}^n - \mathbb{A}^n$. The affine variety $g(x) = 0$ corresponds to a projective variety W_0. Let $W = W_0 \cap \infty$. Now consider the real manifold $\mathbb{P}^n(\mathbb{R})$. If, for each $\epsilon > 0$ there is an open neighborhood $\mathcal{U}$ of $W(\mathbb{R})$ such that $\delta(\mathcal{U} \cap \mathbb{A}^n(\mathbb{Z})) < \epsilon$, then the answer to the question is 'yes'.

93:28 (Paul Feit) Let $\lambda_1, \ldots, \lambda_n$ be indeterminates and for each $k \in \mathbb{N}$ define a symmetric polynomial $\nu_k = \lambda_1^k + \cdots + \lambda_n^k$. Is the ring $\mathbb{Z}[\{\nu_k \mid k \in \mathbb{N}\}]$ integrally closed?

Remark: True, and easily proved, when $n = 2$.

93:29 (Gerry Myerson) Given a positive integer k, let $n = n(k)$ be the smallest integer such that none of the numbers is relatively prime to all the others. It is known that $n(k)$ exists just if $k \geq 17$. How does $n(k)$ grow?

Note: $n(17) = 2184$. Richard Duffy and others have shown that $n(18) = 27829$, $n(19) = 27828$, $n(20) = n(21) = 87890$, $n(22) = n(23) = 171054$, $n(24) > 200000$. It's not obvious to the proposer, who doesn't count the little kink at 19, that $n(k)$ is monotone.

93:30 (John Wolfskill) What is the 5-dimensional volume of the convex polyhedron whose 12 vertices are (0,0,0,0,0), (1,0,0,0,0), (0,1,0,0,0), (0,0,1,0,0), (0,0,0,1,0), (0,0,0,0,1), (1,1,0,0,0), (0,0,1,1,1), (0,0,1,1,0), (1,0,0,1,1), (0,0,1,0,1), (0,1,0,1,1). Is this the smallest convex polyhedron, with vertices on the unit cube, which contains the 'half-cube' spanned by (0,0,0,0,0), ($\frac{1}{2}$,0,0,0,0), (0,$\frac{1}{2}$,0,0,0), (0,0,$\frac{1}{2}$,0,0), (0,0,0,$\frac{1}{2}$,0), (0,0,0,0,$\frac{1}{2}$)?

93:31 (Richard Guy) Which integers can be represented by $(x+y+z)^3/xyz$ with x, y, z integers, preferably positive ones?

Remarks: Peter Montgomery found 539 solutions with $1 \le x \le y \le z \le 46300$, involving 501 values of n: $(1,1,1) \to 27$, $(1,1,2) \to 32$, $(968,1125,2197) \to 33$, $(1,2,3) \to 36$, $(125,162,343) \to 36$, $(8,25,27) \to 40$, $(36,49,125) \to 42$, $(7,8,27) \to 49$, $(1,4,5) \to 50$, 54, 56, 62, 66, 68, 72, 75, 81, 86, 90, 91, 96, 104, ... Write

$$\frac{x, y}{z} = \frac{\pm Y - nX - 4}{8}$$

and solutions correspond to rational points on the elliptic curves $Y^2 = n^2X^3 + (nX+4)^2$ with discriminant $2^{12}n^8(n-27)$, which are singular just if $n = 0$ or 27. The points of inflexion $(0, \pm 4n^2)$ are rational (and of order 3) and the torsion group is $\mathbb{Z}/3\mathbb{Z}$ except when the cubic has a rational root, i.e. when $n = -1$, 2, (27), 32, 54 and 125 and the torsion group is $\mathbb{Z}/6\mathbb{Z}$.

Necessary & sufficient conditions for positive solutions are $n > 0$ (indeed ≥ 27) and $X < 0$.

L-series calculations by Andrew Bremner suggest that the rank is odd if $n = \ldots$, -16, -13, -11, -9, -7, -6, -4, 7, 10, 12, 14, 15, 19, 22 (so far solutions *must* involve negative x, y or z), 31, 33, 36, 37, 40, 41, 42, 43, 44, 49, 50, 51, 53, 56, 61, 62, 65, 66, 67, 68, 72, 73, 75, 76, 78, 80, 81, 82, 83, 85, 87, 88, 89, 90, 91, 96, ... Presumably 32, 54, 86 give curves of rank 2 and solutions for 31, 37, 41, 43, 44, 51, 53, 61, 65, 67, 73, 76, 78, 80, 82, 83, 85, 87, 88, 89 involve negative x, y or z.

Examples, also due to Andrew Bremner, are $(1,27,-49) \to 7$, $(108,-343,25) \to 10$, $(1,2,-9) \to 12$, $(1,125,-196) \to 14$, $(1,9,-25) \to 15$, $(1442897,-7762392,793117) \to 19$, $(19652,-68921,3267) \to 22$.

93:32 (W. Moran) Are the numbers $\sqrt{9+\frac{4}{m^2}}$ where $m \in \mathbb{N}$ and $m^2 + m_1^2 + m_2^2 = 3mm_1m_2$, isolated in the Markoff spectrum?

Remark: Arthur Baragar suggested that the sign under the root was meant to be minus and that then the answer is 'yes' as was shown by Markoff. But the problem is as set; Moran has a preprint.