Western Number Theory Problems, 1994–12–19 & 21

Edited by Richard K. Guy

for mailing prior to 1995 (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 (present set) 94:01–94:27			

[With comments on: 70:XY, 76:02, 76:28, 125(=77:25), 126(=77:26), 147(=77:47), 148(=77:48) 167(=78:17), 324(=81:24), 90:12, 93:03, 93:06, 93:08, 93:(14 &)15, 93:17, 93:20, 93:30, 93:31]

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

95-03-30

COMMENTS ON EARLIER PROBLEMS

The following appeared in the 1989 problem set:

An interesting historical item has been supplied by John Brillhart. It was hoped that Mordell would attend the 1970 Western Number Theory conference in Tucson, and he submitted a problem for presentation. My records are not complete as far back as that, but it may be worth repeating, if this is in fact a repetition. It was solved by another distinguished participant in our conferences, but before giving the solution, others may like to see if they can find an even more general one.

70:XY (Louis Joel Mordell) Let p be an odd prime. Write $f(x) = x^2$, $g(x) = ax^2$, where a is a quadratic non-residue of p. It is trivial that if n is any integer, then either the congruence $f(x) \equiv n$ or $g(x) \equiv n$ is solvable mod p. Find other functions with this property. Prove that, if d is any integer, the functions $f(x) = 2x + dx^4$, $g(x) = x - 1/4dx^2$ have this property.

Solution John Brillhart has supplied a solution, but it is largely superseded by the following

Generalization (Emma Lehmer): Mordell's problem is a special case of the following theorem (replace the d in the problem statement by a).

Theorem. Every integer n modulo a prime p is representable by at least one of the two forms

$$f(x) = ax^4 + 4bx^3 + 6cx^2 + 4dx$$

$$g(y) = -a^2 + \frac{A}{a^2y} \quad \text{where } A \equiv 2ad^2 - c^3 \bmod p$$

under the conditions

$$b^2 \equiv ac \bmod p, \quad 3c^2 \equiv 4bd \bmod p$$

Remark: To obtain Mordell's theorem, let $b \equiv c \equiv 0 \bmod p$, $d \equiv \frac{1}{2} \bmod p$ and $y \equiv \frac{1}{2ax} \bmod p$.

Proof: If $g(y) \equiv n \bmod p$, then the theorem holds for n. Therefore assume that n is not represented by $g(y)$. In other words, the congruence

$$a^3y^3 + a^2yn - A \equiv 0 \bmod p$$

has no rational root. Hence, by Stickelberger's Theorem, its discriminant Δ satisfies $(\Delta|p) = 1$, where $(\Delta|p)$ is the Legendre symbol. [**Stickelberger's Theorem:** Let $P_n(x) \in \mathbf{Z}[x]$, $\deg P_n = n \geq 1$, and p be an odd prime such that $p \nmid \Delta(P_n(x))$, the discriminant of $P_n(x)$. If $P_n(x) \equiv \prod_{i=1}^{s} Q_i(x) \bmod p$, where each $Q_i(x)$ is irreducible mod p, then $(-1)^{n+s} = (\Delta|p)$.]

But $a^3y^3 + a^2yn - A$ is the Lagrange resolvant of $f(x) - n$ and therefore has the same discriminant as $f(x) - n$. Using Stickelberger's Theorem once more this shows that $f(x) - n$ has an even number of factors, namely 2 or 4. It is well known, however, that if a quartic equation is a product of two irreducible quadratics, then the resolvant cubic must have rational roots, contrary to our assumption. Therefore $f(x) - n$ contains a linear factor and the congruence $f(x) \equiv n \bmod p$ is solvable in case $g(y) \equiv n \bmod p$ is not. This proves the theorem.

The corresponding theorem, where $f(x)$ is a cubic, holds only for primes of the form $6m + 1$ and is as follows.

Theorem 2. Every integer n modulo a prime $p \equiv 1 \bmod 6$ is representable by at least one of the two forms

$$f(x) = x^3 - 3hx, \qquad g(y) = y + \frac{h^3}{y}$$

Proof: If n is represented by $g(y)$, the theorem is true for n. Therefore suppose that $g(y) \equiv n \bmod p$ has no solution. Then

$$y^2 - ny + h^3 \not\equiv 0 \bmod p$$

and the discriminant $\Delta = n^2 - 4h^3$ is such that $(\Delta|p) = -1$. But the discriminant D of the cubic $f(x) - n$ is $D = 27(4h^3 - n^2) = -3\Delta$ and therefore $(D|p) = -1$ for $p \equiv 1 \bmod 6$. Hence by Stickelberger's Theorem the cubic $f(x) - n$ has an even number of factors and therefore $f(x) \equiv n \bmod p$ has a solution if $g(y)$ does not and the theorem follows.

76:02 (Jerry Bergum) For what integers n are there positive integers x, y with x even and $x \perp y$, such that $x^2 + y^2 = b^2$ and $x^2 + (y - nx)^2 = c^2$ are both perfect squares? It was noted that
(a) if $n = 2m(2m^2 + 1)$ [$n = \pm 6, \pm 36, \pm 114, \ldots$], then $x = 4m(4m^2 + 1)$, $y = 16m^4 + 4m^2 + 1$ is a solution [$b = 16m^4 + 12m^2 + 1$, $c = 64m^6 + 32m^4 + 4m^2 + 1$].
(b) for $n = 8$, the smallest x is 2996760 [$y = 19306049$, $nx - y = 4668031$, $b = 19537249$, $c = 5547169$].
(c) there are no solutions for $n = \pm 1, \pm 2, \pm 4$.

1986 remark: (Andrew Bremner) The equations represent an elliptic curve, which, in more standard form, is

$$Y^2 = X[X^2 + (n^2 + 2)X + 1]$$

with 2-isogenous curve

$$\mathcal{Y}^2 = \mathcal{X}(\mathcal{X} - n^2)(\mathcal{X} - (n^2 + 4))$$

[The same equations arise from the 'ν-configurations' in tiling the square with rational triangles. See **76:28** below.] For any particular n, one can hope to calculate the rank; it seems certain that there is no simple characterization of those n for which the rank is zero. That it is zero for $n = \pm 1, \pm 2, \pm 3, \pm 4$ follows from H.C. Pocklington, Some diophantine impossibilities, *Proc. Cambridge Philos. Soc.*, 17(1914) 110–121, who, in effect, calculates the rank of $Y^2 = X[X^2 + NX + 1]$ for $|N| \le 30$. If x is not constrained to be even, then for $n = 8$ there is the solution $x = 15$, $y = 8$. [See comments on **77:48** below.]

76:28 (D19 in *UPINT*) Does there exist a point in $\mathbf{R}^2$ whose four distances from the corners of a unit square are all rational?

1986 remark: Problems **76:02** and **76:28** were repeated in 1977, noting the connexion that the former asks for the coordinates (x, y) of a point distance b from $(0,0)$ and distance c from an adjacent corner $(0, nx)$ of a square of side nx with n an integer. For comparison with **77:47** and **77:48** below, we can also state the problem as 'find integer sided triangles whose base is n times their height'. For the purposes of **76:28** it suffices to take n rational.

Peter Montgomery used a computer to find 50 pairs of squares whose corners had integer coordinates and integer distances between corners of mates. But all 100 squares had irrational sides. E.g., (101, 120) is distance 41, 229, 289, 181 from (60, 120), (−120, 60), (−60, −120), (120, −60). He formulated the related questions

77:25 (= **125**) Are there infinitely many pairs of coprime Gaussian integers z_1, z_2, with z_1/z_2 neither real nor purely imaginary, such that $|z_1 - i^k z_2|$ is an integer for $k = 0, 1, 2, 3$?
Examples: $(36 + 84i, 15 + 56i)$, $(409 + 840i, 396 + 924i)$ [and $(60 + 120i, 101 + 120i)$].

77:26 (= **126**) Are there infinitely many pairs of distinct acute angles x, y with $\tan x/2$, $\tan y/2$ rational and $\cos 2x \cos 2y$ a rational square?
Examples: $(\tan x/2, \tan y/2) = (\frac{1}{4}, \frac{8}{25})$, $(\frac{2}{5}, \frac{10}{37})$, $(\frac{3}{8}, \frac{60}{149})$.

John Leech lets $\tan x/2 = a/b$ so that $\cos 2x = (a^4 - 6a^2b^2 + b^4)/(a^2 + b^2)^2$. A nontrivial solution of $a^4 - 6a^2b^2 + b^4 = kn^2$ for a fixed k implies an infinity of them for this k, so for any value of x he expects an infinity of y with $\cos 2x \cos 2y$ a square.

Peter Montgomery himself used elliptic curves to find two half-angles with tangents t and $(t^9 - 6t^5 + 24t^3 - 3t)/(-3t^8 + 247^6 - 6t^4 + 1)$. The cosines of the whole angles have equal squarefree parts. He uses these and lets $z_1 = b(a^4 - b^4 + 2ia^4)$, $z_2 = a(2b^4 + i(a^4 - b^4))$ with $a^2 + b^2$ a perfect square, and has a solution of **77:25**: e.g., $a = 4$, $b = 3$ gives $(525 + 1536i, 648 + 700i)$.

77:47 (=**147**) (Ron Evans) Find every integer sided triangle whose base divides its height [a sort of dual to **76:02**].

77:48 (=**148**) (Ron Evans) Let k, s, t be natural numbers. For which k is $(st)^2 + k^2(s^2 + t^2)^2$ never a square? [$k = 1$ is such, but $k = 3$ $(s = 7,\ t = 4)$ and $k = 5$ $(s = 399,\ t = 188)$ are not.]

1986 remark: In connexion with **76:02**, Hansraj Gupta noted that if you can find $x_1, \ldots, x_4$, coprime in pairs, just one even; x_1, x_4 with no divisors of shape $4r + 3$, and
$2n = (x_1^2 - x_4^2)(x_2^2 + x_3^2)/x_1x_2x_3x_4$, then $x = 2x_1x_2x_3x_4$, $y = x_1^2x_2^2 - x_3^2x_4^2$, $nx - y = x_1^2x_3^2 - x_2^2x_4^2$ is a solution. [E.g., $n = 8$, $x_1 = 113$, $x_2 = 39$, $x_3 = 20$, $x_4 = 17$ gives the solution already mentioned.]

In 1978 it was stated that $n = -3$ can occur, and $x = 201608$, $y = 1905$ was given as a solution! However, although $b = 201617$, $nx - y = 606729$, we have $201608^2 + 606729^2 = 639348^2 + 1$; someone must have used floating point, rather than integer arithmetic! Most amateur number-theorists would note that $64 + 41 \equiv 05$ was not a square mod100.

[Can anyone improve on the following in testing if n is a perfect square: $n - \lfloor(\sqrt{n} + 0.5)\rfloor^2$ and test for zero?]

Andrew Bremner confirms the duality mentioned above by noting that **77:48** is equivalent to 'for which k is the rank of the elliptic curve $y^2 = x[x^2 + (1/k^2 + 2)x + 1]$ equal to zero?' Compare his comment on **76:02** with $n \leftrightarrow 1/k$. He again believes that there is no straightforward characterization of such k.

In the *Amer. Math. Monthly*, 84(1977) 820, Ron Evans asked the special case of **77:47**:
E2687. Is there a triangle with rational sides whose base equals its altitude?

This is also a special case of **76:28**, and goes back to Pocklington (*loc. cit.*). J. G. Mauldon, **86**(1979) 785–786, gave a proof of nonexistence which didn't get into the annual index (p. 904) and is not easy to trace. So late solutions were submitted by Selfridge, who used a classical Fermat descent, as Mauldon did, and by Richard Guy, who used an elliptic curve. The primes 2 and 5 are both essential to any proof.

In 1979 Jerry Bergum spoke to the W#θ meeting at Asilomar about **76:02** and asked the question again in the specific cases n a prime of shape $4m + 3$ with $n^2 + 4$ not prime: $n = \ldots, -41, -29, 11, 19, 23, 31, 43, 59, \ldots$ [In 1980 the question was renewed with no restriction on n]. The erroneous example was replaced by $n = -29$, $x = 120$, $y = 119$, $b = 169$, $y - nx = 3599$, $c = 3601$. The cases $n = \pm 3$ were not considered. Jerry Bergum gave the least (x, y) for $n = 19$ as $(2410442371920, 32189022936649)$.

1994 remark: The following reference appears to be relevant:

Charles K. Cook & Gerald E. Bergum, Integer sided triangles whose ratio of altitude to base is an integer, *Applications of Fibonacci numbers, Vol.* 5 (*St. Andrews,* 1992), 137–142, Kluwer Acad. Publ., Dordrecht, 1993.

1995 remark: On 95-01-17 Noam Elkies wrote:

> Several of these problems (e.g. **76:02**) amount to a family of elliptic curves $E(n)$ over $\mathbb{Q}$ and the question of characterizing those n for which $E(n)$ has positive rank. While such problems are still intractable in general, there is now a heuristic that should give most such n: compute the sign of the elliptic curve (which should be the sign of its functional equation if enough standard conjectures are proved). For most families, including presumably those in this problem list, that sign is -1 half the time. The sign is supposed to be -1 just if the curve has odd rank. Thus all the -1 curves should have positive rank, while many of the $+1$'s have rank zero. (I say "many" rather than "most" because it is no longer believed that a random elliptic curve of even rank has rank zero with probability 1. Still the probability seems to be quite large, maybe 70% to 80%, so the -1 curves will give the majority of those with positive rank.) Warning: computing the arithmetic sign of a curve with additive reduction at 2 is not pleasant; it has not yet been implemented on GP/PARI.
>
> Also, it is now possible to compute large generators of elliptic curves of rank 1 over $\mathbb{Q}$; see for instance my paper on "Heegner point computations" in the proceedings of ANTS-I (Lect. Notes in Comp. Sci. #877).

and, on 95-02-01:

> Likewise in **77:25** we can prove that there are infinitely many squares with coordinates in the Gaussian integers all four of whose vertices have integer absolute value, with no two collinear with the origin. (NB: the square may be arbitrarily tilted relative to the real/imaginary axes in this problem.) Indeed let the vertices be $z_1 - i^k z_2$ $(k = 0, 1, 2, 3)$. The key is that given for each k the class of $z_1 - i^k z_2$ modulo squares in $K = \mathbb{Q}(i)$ we get a curve of genus 1 over K. It suffices to find one choice of four classes in $K*/K*^2$ with norm 1 for which that curve has a non-torsion rational point, and this has already been done by the searches which found specific small values of z_1, z_2 that work.
>
> But we don't even need those initial pairs, thanks to the observation that the elliptic curves are all twists of the complex multiplication curve $Y^2 = X^3 - X$. [A 'twist' is $tY^2 = X^3 - X$.] This lets us start with one of the trivial solutions like $(z_1, z_2) = (4, 3)$ and take a multiple of it by some Gaussian integer to get a nontrivial solution. Indeed for $z_1 = 4$, $z_2 = 3$ we find that $z_1^2 + z_2^2$ is square, $z_1^2 - z_2^2 = 7$ times a square. Taking $x = (z_1/z_2)^2$ for a generic z_1, z_2 satisfying these conditions gives $7y^2 = x^3 - x$ with initial solution $x = 16/9$. Multiplying this by odd integers gives further solutions. Multiplying by odd Gaussian integers yields solutions satisfying the nontriviality condition. For instance the $2 - i$ multiple gives $z_1 = 648 + 700i$, $z_2 = 525 + 1536i$; the $3 + 2i$ multiple yields (sauf erreur) $z_1 = 189714312 + 113054900i$, $z_2 = -87350784 + 208638675i$; "etc.".

78:17 (=167) (D. H. Lehmer. This was also asked in Raphael M. Robinson, Mersenne and Fermat numbers, *Proc. Amer. Math. Soc.*, 5(1954) 842–846; *MR* 16, 335.) Let $S_1 = 4$, $S_{k+1} = S_k^2 - 2$; if $M_p = 2^p - 1$ is prime, then $S_{p-2} \equiv \pm 2^{(p+1)/2} \bmod M_p$: which sign?

The edited version of a 94-06-22 email letter from Franz Lemmermeier that appeared in earlier drafts is now superseded by the following [proofs can be found in

Franz Lemmermeyer, *Reciprocity Laws: Their History from Euler to Artin*, monograph, in preparation].

Proposition 1.1 Let $q = 4a^2 + 27b^2$ be prime; then

$$(2+\sqrt{3})^{(q+1)/2} \equiv (-1)^a \bmod q.$$

Moreover,

$$(2+\sqrt{3})^{(q+1)/4} \equiv \begin{cases} +1 & \bmod q \quad \text{if } a \equiv 2 \bmod 4, \\ -1 & \bmod q \quad \text{if } a \equiv 0 \bmod 4, \\ (-1|ab)\frac{b}{a}\sqrt{3} & \bmod q \quad \text{if } a \equiv 1 \bmod 2. \end{cases}$$

Conjecture 1 Let $q = 4a^2 + 27b^2 = c^2 + 6d^2 = e^2 - 2f^2 \equiv 7 \bmod 24$ be prime, where $a \equiv b \equiv 1 \bmod 2$, and a, b, c, d, e, $f > 0$. Then

$$(2+\sqrt{3})^{(q+1)/8} \equiv \left(\frac{2}{ae}\right)\left(\frac{-1}{f}\right)\frac{e}{2f} + \left(\frac{6}{a}\right)\left(\frac{-6}{c}\right)\left(\frac{-1}{d}\right)\frac{c}{d}\sqrt{3} \bmod p.$$

Corollary 1.2 Let $q = M_p = 2^p - 1$ be prime, and assume that $p \geq 5$; then $M_p = e^2 - 2f^2$ for $e = 2^{(p+1)/2} - 1$ and $f = 2^{(p-1)/2} - 1$, and

$$\begin{aligned} S_{p-2} &= (2+\sqrt{3}\,)^{(q+1)/8} + (2-\sqrt{3}\,)^{(q+1)/8} \\ &\equiv (\tfrac{2}{a})(\tfrac{2}{e})(\tfrac{-1}{f})\tfrac{e}{f} \\ &\equiv (\tfrac{2}{a})2^{(p+1)/2} \bmod q. \end{aligned}$$

For a proof, just observe that $e \equiv 7 \bmod 8$ and $f \equiv -1 \bmod 4$, hence $(2|e) = 1$, $(-1|f) = -1$.

81:24 (=**324**) (Julia Robinson) See **94:27** below.

90:12 (Charles Nicol via John Selfridge) Let N_n be the concatenation of the first n positive integers. E.g. $N_{13} = 12345678910111213$. Are any of these numbers prime? Are infinitely many prime? Robert Baillie has found that there are no primes out to $n = 1000$.

Remark: In a 95-02-14 email, Nicol enquires if further progress has been made, and asks the same question with the concatenation reversed: 1, 21, 321, 4321, 54321, 654321, ..., 13121110987654321, ... He and Mike Filaseta find that 8281807978 ... 54321 is the only prime starting with 100 or less. Selfridge conjectures that there are infinitely many such primes.

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

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 $x \geq x_0(p)$?

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.

Remarks: A 94-12-20 preprint
Rob Harley, Some estimates due to Richard Brent applied to the "high jumpers" problem,
and the following 94-11-15 email message have been received.

"Using the Hardy-Littlewood prime k-tuple conjecture and inclusion-exclusion you can estimate the number of occurrences, up to some bound, of prime gaps of some fixed size. In [RB] Richard Brent showed how to calculate some of the constants that occur in the estimates and noted that the estimates agree well with actual counts at least in the range $10^6 \dots 10^9$.

"Concerning Victor Meally's question: one can compute where the estimated count of gaps of size 30 overtakes that for 6. However even if the conjectured estimates are good, the crossover point of the estimates, X, could be far from the true crossover due to the functions being relatively flat for instance. Nevertheless X would be somewhat useful as a "ball-park" figure. I'm currently computing X." [The preprint gives $X \approx 1.7 \cdot 10^{35}$ which gives a 'guesstimate' for the true crossover point.]

[RB] Richard Brent, The distribution of small gaps between successive primes, *Math. Comput.*, 28 (1974) 315–324.

Michael Rubinstein has worked with Andrew Odlyzko on this problem.

93:06 (David, Jonathan & Peter Borwein & Roland Girgensohn, via Hugh Edgar – two problems from their paper, "On a Conjecture of Giuga", which will appear in the *Amer. Math. Monthly* and which concludes with 10 open problems.) (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.

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

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

a square?

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

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. On 94-02-16 Peter Montgomery reports having extended the search to $p_n < 50000$ and notes that it should be easy to extend this much further by computing the partial products modulo several huge primes and testing the quadratic characters.

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.?

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 $2^t m = 13818$ 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 $c(r+1) \leq 2c(r)$? If $c(r+1) > 2c(r)$, 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 $n = c(r) - 1$?

Remarks: Misprint in **93:15**(d) corrected. **93:14** also quoted to put things in context, but for definition of $l(n)$ and what is known, see **C6** in *UPINT2* (quoted in the 1993 Problems set). A recent paper is

E. G. Thurber, Addition chains – an erratic sequence, *Discrete Math.*, **122**(1993) 287-305.

In a 95-02-10 email message, Thurber says "that if in the addition chain problem $c(r)$ represents the first integer that requires r steps in a minimal addition chain, then $c(21) = 65131$. This turned up in December shortly after the conference. Knuth determined these numbers up to $c(18)$. We now have $c(19) = 18287$, $c(20) = 34303$ and $c(21)$."

93:17 (Andrew Granville) Find a non-homogeneous irreducible polynomial $F(x,y) \in \mathbf{Z}[x,y]$ of degree $d \geq 5$ 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.

Solution: (Ed Schaeffer, 94-12-19)

$$F_d(x,y) = x(x-1)(x-2)\cdots(x-(d-1)) - y(y-1)(y-2)\cdots(y-(d-2))$$

has genus $(d-1)(d-2)/2$ and solutions (d, d); $(d, -2)$ or $(-1, d)$ according as d is odd or even; and (i, j) with $i \in \{0, 1, \ldots, d-1\}$, $j \in \{0, 1, \ldots, d-2\}$; a total of $d^2 - d + 2$ solutions. If $d = n^2$ there is also the solution $(n^2 + n - 1, n^2 + n)$ and for $d = 9$ we have (13,15) and for $d = 36$ we have (54,57). In **94:01** below, Schaefer asks if there are any other positive integer solutions.

Further remarks: (Noam Elkies) This is related to questions suggested by recent work of Caporaso, Harris and Mazur on uniform bounds of the number of rational points of curves of genus g over number fields. For curves of given large genus over **Q** the best approach is probably Mestre's trick: pick "random" rational $x_1, x_2, \ldots, x_d$ with d even, and write $(x - x_1) \cdots (x - x_d)$ as a square minus a remainder polynomial $R(x)$ of degree $\frac{1}{2}d - 1$. Then there are at least d pairs of rational points on the hyperelliptic curve $y^2 = R(x)$, with x-coordinates $x_1, \ldots, x_d$. [Variations of this will be my topic at the March 1995 meeting in Chicago.]

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

Remark: (Jeff Lagarias, 1993) 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, for $n \geq 1$, the polynomials

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

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

Checked by Maple for $n \leq 20$. 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 $n \equiv m \equiv 1 \bmod 2$.

Remark: (Gene Ward Smith, 94-07-03) We can use Jeff's polynomial to analyze this, but it seems easier to work with the $\tan(\theta)$ directly. To do this, set $f_n(z) = (1 + iz)^n - (1 - iz)^n$, where $i = \sqrt{-1}$. Then

$$T_n(z) = i[(n-1)f_{n+1}(z) - (n+1)(z^2+1)f_{n-1}(z)]/8z^3$$

is a polynomial of degree $n-2$ if n is even, and $n-3$ if n is odd. It is a polynomial in z^2: that is, with only even terms. The roots of it correspond to the non-trivial solutions of $\tan(n\theta) = n\tan(\theta)$, with $z = \tan(\theta)$.

We can obtain a partial solution to the problem for the case when $n+1$ is a prime by noting that in this case, the above polynomial is Eisenstein at $n+1$ and hence irreducible.

To see this, note that the constant term is $\binom{n+1}{3}$; and the $n-2$th term is $(-1)^{(n+1)/2}n/2$ when n is even, or $(-1)^{(n+1)/2}4\binom{(n+1)/2}{2}$ when n is odd. Hence the highest degree term is not divisible by the prime $n+1$, and the lowest degree term is divisible exactly once. The other terms can be seen to be divisible by $n+1$ from the general form of $T_n(z)$ above.

If we could show that $T_n(z)$ was irreducible in general, it would solve the problem.

It it worth noting that $T_n(\sqrt{z})$ seems to be irreducible, with Galois group the symmetric group for the corresponding degree, and that the field extension obtained from it appears to ramify only at primes less than or equal to $n+1$.

Remark: (Jeff Lagarias, 94-07-05) Eugene Gutkin, egutkin@math.usc.edu, has a preprint: "Billiard tables of constant width and dynamical characterization of the circle."

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,$\frac{1}{2}$)?

Remark: (Andrew Mayer, 94-07-11) I entered the given points, and found that the 5-dimensional volume of the polytope is 23/120 (about 0.19). Just to make sure, I verified the number by Monte Carlo runs, and it checked out. This, I believe, answers the first question.

The second question is more interesting. If the vertices of the cube are identified with subsets of $\{a,b,c,d,e\}$ in the obvious way, and the V_i are the selected vertices (a subset of the power set of $\{a,b,c,d,e\}$), then a sufficient condition for the "half-cube" to be contained in the convex hull of the V_i is the following:

Every subset of $\{a,b,c,d,e\}$ is the disjoint union of two of the sets corresponding to the V_i.

This is because $(V_i+V_j)/2$ is a vertex of the half-cube when V_i and V_j are disjoint. It may not be necessary, though, because it requires the extra condition that each vertex of the half-cube be the midpoint of a line connecting just two of the vertices. It may be possible that the use of less trivial combinations will give rise to a smaller polytope.

So I fiddled around and found the following set of V_i satisfying the above condition:

$\{\emptyset\} = 00000$, $\{a\} = 10000$, $\{b\} = 01000$, $\{c\} = 00100$, $\{d\} = 00010$, $\{e\} = 00001$, $\{a,b\} = 11000$, $\{a,c\} = 10100$, $\{b,c\} = 01100$, $\{d,e\} = 00011$, $\{a,b,c\} = 11100$,

There are only 11 of these, as opposed to the 12 given, and my program gives the volume of the convex hull to be 1/10, which is almost half the size of the one given (answering the second question in the negative). Sadly, (as explained above) I don't know if this is the optimal value.

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

Remark: This is essentially solved, by relating it to the family of elliptic curves $Y^2 = n^2X^3 + (nX+4)^2$, in

Andrew Bremner & Richard K. Guy, Two more representation problems, (submitted to) *Proc. Edinburgh Math. Soc.*

PROBLEMS PROPOSED 94–12–19 & 21

94:01 (Ed Schaefer) (Compare **93:17** above.) Let

$$F_d = x(x-1)(x-2)\cdots(x-(d-1)) - y(y-1)\cdots(y-(d-2))$$

where d is an integer at least 5. Then $F_d(x,y) = 0$ has solutions (d,d) and (i,j) where $i \in \{0,1,2,\ldots,d-1\}$, $j \in \{0,1,2,\ldots,d-2\}$. If $d = n^2$, there's (n^2+n-1, n^2+n) and for $d = 9$ we have (13,15) and for $d = 36$ we have (54,57). Are there any other positive integer solutions?

94:02 (Erdős Pál) A system of congruences a_i mod n_i $(1 \le i \le k)$ is a **covering system** if every integer y satisfies $y \equiv a_i$ mod n_i for at least one value of i. For example 0 mod 2; 0 mod 3; 1 mod 4; 5 mod 6; 7 mod 12. If $c = n_1 < n_2 < \cdots < n_k$, then Erdős now offers \$1000.00 for a proof or disproof of the existence of covering congruences with c arbitrarily large.

Remark: See **F13** in *UPINT*2. Choi has a system with $c = 20$ and a Japanese is reputed to have achieved $c = 24$.

94:03 (Erdős Pál) Crocker proved that there are infinitely many odd integers not of the form $2^k + 2^l + p$, where p is prime. There may be cx of them less than x, but can $> x^\epsilon$ be proved?

Remark: See **A19** in *UPINT*2.

94:04 (Erdős Pál) Is it true that for large r every integer is the sum of a prime and r powers of 2 ? At least prove that the density of such numbers is $1 - \epsilon_r$.

94:05 (Neville Robbins) Given a prime p, find a prime q such that $q \equiv 2p-1$ mod $4p$ [by Dirichlet's Theorem there are infinitely many such], so that $q+1 = kp$, $q = a^2+b^2$ and $a^2+b^2+1^2+0^2 = kp$. This leads to a representation of p as the sum of 4 squares. By taking sufficiently many q, can we obtain all representations of p as the sum of 4 squares?

94:06 (Sam Wagstaff) Find a (small) function $B(n,t)$ where n is an integer > 1 and $0 < t < 1$ so that if $A \subseteq$ a reduced system of residues, mod n, and $|A| \ge t\phi(n)$, then

$$\min_{a \in A}(\text{least prime } \equiv a \bmod n) \le B(n,t)$$

Notes:

1. When t is near 0, $B(n,t)$ may be only Linnik's bound, n^c, on
$$\max_{\gcd(a,n)=1}(\text{least } p \equiv a \bmod n).$$
2. When t is near 1, $B(n,t)$ should be small, say $O(n \ln n)$.
3. Can you solve the problem just for $t = \frac{1}{2}$?
4. $B(n,t)$ should be monotonically increasing in n and monotonically decreasing in t.

Remarks: (Carl Pomerance) For $(a,n)=1$, let $p(n,a)$ be the least prime $\equiv a \bmod n$. Let $a_1,\dots,a_{\phi(n)}$ be a reduced residue system mod n organized so that $p(n,a_1) > p(n,a_2) > \cdots > p(n,a_{\phi(n)})$. For $t \in (0,1)$, Wagstaff asks for an upper bound for $p(n,a_i)$ for $i \geq t\phi(n)$.

Using sieve methods I can prove that there is some $t_0 \in (0,1)$ such that $p(n,a_i) < 2(\phi(n)+1-i)\ln n$ for $i \geq t_0\phi(n)$. (I've shown in

Carl Pomerance, A note on the least prime in an arithmetic progression, *J. Number Theory*, **12**(1980) 218–223; *MR* **81m**:10081

that this inequality fails for $i=1$ for most n.) Sketch of proof: Say $i \geq t_0\phi(n)$ and write $\phi(n)-i=\epsilon\phi(n)$. Suppose $\epsilon < 1/\ln n$. Then $p(n,a_i)$ is the $(\phi(n)+1-i)$-th prime that does not divide n and the result follows. Say $\epsilon > 1/\ln n$ Then consider the primes up to $2\epsilon\phi(n)\ln n$. There are about $2\epsilon\phi(n)$ such primes that do not divide n and we wish to show that they cover at least $\epsilon\phi(n)$ residue classes mod n. The number of classes they cover is $\geq$ (# primes $\leq 2\epsilon\phi(n)\ln n$ not dividing n) $-$ (# pairs of primes $\leq 2\epsilon\phi(n)\ln n$ that are congruent mod n). That is we have to show the second term is $< \epsilon\phi(n)$. For each $k < 2\epsilon\frac{\phi(n)}{n}\ln n$, consider N_k, the number of primes $p < 2\epsilon\phi(n)\ln n$ with $p+kn$ prime. Then the second term above is $\leq \sum N_k$ for $k < 2\epsilon\frac{\phi(n)}{n}\ln n$. By the sieve,

$$N_k \ll \frac{k}{\phi(k)}\frac{n}{\phi(n)}\frac{2\epsilon\phi(n)\ln n}{(\ln n)^2} \ll \frac{k}{\phi(k)}\frac{\epsilon n}{\ln n}.$$

Thus

$$\sum N_k \ll \epsilon\frac{\phi(n)}{n}\ln n \cdot \frac{\epsilon n}{\ln n} = \epsilon^2\phi(n).$$

Thus for t_0 sufficiently close to 1, we have $\epsilon \leq 1-t_0$ and so $\sum N_k < \epsilon\phi(n)$, and we're done.

94:07 (Bart Goddard) Let

$$f_n(x) = (n-1)!x^n + (n-2)!x^{n-1} + \cdots + 2x^3 + x^2 - x + \frac{n}{n+1}$$

and $f_n(a_n) = \inf_{[0,1]} f_n(x)$

(a) Find an upper bound for $f_n(a_n)$.

(b) Find $\lim_{n\to\infty} a_n$

Remark: Possible answers: (a) $< \sqrt{n}$, (b) $\frac{1}{2}$.

(Paul Feit) $f'(x) = n!x^{n-1} + \cdots + 2x - 1$. The root is being pushed to 0 rapidly as n gets large.

94:08 (Gene Ward Smith) Show that for $n > 2$, the polynomial

$$P_n(x) = x^n + \left(\frac{n}{n-1}\right)^{n-1} x^{n-1} + \left(\frac{n}{n-2}\right)^{n-2} x^{n-2} + \cdots + nx + 1$$

has precisely one real root $r > -1$.

Remarks: I use the function

$$f(x) = \sum_{n=0}^{\infty} \frac{x^n}{n^n}$$

when teaching power series and the n-th root test. It has a real root around $-1.40376\cdots$ and seems to have no other real roots, but many complex ones. The truncated series seems to have only one root between $-n$ and 0, which gives this problem on making a substitution, and would establish the presumptive theorem about the root of $f(x)$.

For $x = -1$ the polynomial *almost* gets back up to a zero, but not quite. For odd-degree polynomials it then proceeds downward again; for even degree it quickly heads up to what seems to be the only other real root. This can be confirmed for particular n with a Sturm sequence.

94:09 (Morris Newman) Let

$$g(n) = \sum_{d|n} d\phi(d) = \prod_{p^e\|n} \frac{p^{2e+1}+1}{p+1}$$

Is $g(n)$ ever $\equiv 0 \bmod n$?

Remarks: Yes if $n = 1$. No if n is even. This is Problem **10410**, *Amer. Math. Monthly*, **101**(1994) 911, proposed by Frank Schmidt.

Solution: (Peter Montgomery) $g(7\cdot 13\cdot 43\cdot 157) = 43\cdot 157\cdot(13\cdot 139)\cdot(7\cdot 3499)$

94:10 (Morris Newman) Are there infinitely many primes p such that $\gcd(2^p-1, 3^p-1) > 1$?

Remark: Suppose that $p = 12n-1$, $q = 2p+1 = 24n-1$ are both primes, then $q|(2^p-1, 3^p-1)$, so if there are infinitely many such prime pairs, the answer is affirmative. Is there another approach?

There are cases besides $p =$ 11, 23, 83, 131, 179, 191, 239, 251, 359, 419, 431, 443, 491, 659, 683, 719, 743, 911, 1019, 1031, 1103, ... for each of which the gcd is $2p+1$. Sam Wagstaff calculates all examples with $p < 10^4$. In addition there are values of $p \not\equiv 11 \bmod 12$, where the gcd $= 2kp+1$:

$p =$	43	463	883	3319	4057	4373	4787	4903	7529	8317	9007
$k =$	5	12	5	5	12	12	12	5	7	23	5

as well as $p = 6947 \equiv 11 \bmod 12$ for which $2p+1$ is not prime, but which gives a gcd $= 26p+1$. In answer to the question: can the gcd ever be a proper multiple of $2p+1$, he gives the spectacular example $p = 1931$ for which the gcd $= 193949641 = 3863\cdot 50207$, where $3863 = 2p+1$, $50207 = 26p+1$, $k = 50220$.

These calculations were also carried out by Robert Harley, who notes that similar considerations hold for $\gcd(2^p-1, 5^p-1)$ when 2 and 5 happen to be k-th powers mod q.

Unless $p = 2$, k is even so $q \equiv \pm 1$ or $\pm 9 \bmod 40$. Respectively, $40|k$ unless $p = 2$ or 5; $2|k$ unless $p = 2$; $8|k$ unless $p = 2$; $10|k$ unless $p = 2$ or 5. Examples are

p	q	k	p	q	k	p	q	k
2	3	1	937	28111	30	4013	120391	30
431	3449	8	1013	6079	6	4273	25639	6
499	20959	42	1223	31799	26	4513	135391	30
547	5471	10	1789	39359	22	4787	114889	24
571	5711	10	2539	25391	10	5393	32359	6
641	49999	78	2593	15559	6	6173	37039	6
761	6089	8	2677	465799	174	6199	61991	10

Likewise for $\gcd(3^p - 1, 5^p - 1)/2$ when 3 and 5 happen to be k-th powers mod q. Unless $p = 2$, k is even so $q \equiv \pm 1$ or $\pm\, 11 \bmod 60$. Respectively, $60|k$ unless $p = 2$, 3 or 5; $2|k$ unless $p = 2$; $10|k$ unless $p = 2$ or 5; $12|k$ unless $p = 2$ or 3. Examples:

p	q	k	p	q	k	p	q	k
109	1091	10	2039	24469	12	4337	104089	24
1009	10091	10	2437	24371	10	4663	214499	46
1607	38569	24	2477	34679	14	4787	114889	24
1999	19991	10	3989	47869	12	5059	50591	10

For $p = 2039$, one can also take $q = 4079$, $k = 2$!

Note that for $p = 2$, $\gcd(3^p - 1, 5^p - 1)/2 = 4$ which is not a product of primes of the form $kp + 1$.

94:11 (Gerry Myerson) Let B_n be the set of all n-tuples with entries taken from $\{-1, 0, 1\}$. For each subset $S \subset B_n$ of size $n - 1$, let W_S be the lattice generated by S, and let $W_n = \bigcup_S W_S$, the union over all such subsets S of B_n. Find a "small" element of $\mathbf{Z}^n$ that's not in W_n.

Remarks: For example, if $n = 3$, (1,2,6) and (2,4,5). After the meeting, the proposer wrote: "I didn't say what I meant by small . . . . It doesn't matter much which norm you use to measure the size of the n-tuple. The sum, Euclidean, and max norms differ by a factor n at most, which I expect is insignificant. Let D_n be the largest possible determinant of an $n \times n$ matrix with entries from $\{-1, 0, 1\}$. Then it is easy to produce an element of W_n with maximal entry roughly D_{n-1}^{n-1}, namely

$$(1, D_{n-1} + 1, (D_{n-1} + 1)^2, \ldots, (D_{n-1} + 1)^{n-1})$$

By the Hadamard bound on determinants (which is, I think, achieved for many n), $D_n \leq n^{n/2}$, so we certainly have an element of W_n of size bounded by $n^{\frac{1}{2}n^2}$. When I asked for a small element, I meant one of size significantly less than n^{cn^2}."

94:12 (Graeme Cohen, via Doug E. Iannucci) For a positive integer n, show that $\sigma(\sigma(n)) = 4n$ only if n is odd.

Remark: The only such numbers less than $5 \cdot 10^8$ are 15, 1023 and 29127. Graeme Cohen has further checked this to 10^9. These numbers were mentioned in

Carl Pomerance, On multiply perfect numbers with a special property, *Pacific J. Math.*, 57(1975) 511-517.

94:13 (Carl Pomerance, via Doug E. Iannucci) For each positive integer n, is there a positive integer k such that $\sigma^k(n)/n$ is an integer?

Remark: $\sigma^k(n) = \sigma(\sigma^{k-1}(n))$, $\sigma^0(n) = n$. The first few (least) values of k are:

n	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37
k	2	4	2	5	1	5	2	7	4	15	3	13	3	2	2	13	4	12	5	2	13	16	2	17	4	9	1	78	7	10	4	17	11	6	5	28

Robert Harley supplies the following 'critical table' of $k(n)$, assuming that 'probable primes' occurring in the computation are actually prime:

n	2	3	5	9	11	23	25	29	59	67	101	131	173	202	239	353	389	401	461	659
k	2	4	5	7	15	16	17	78	97	101	120	174	214	239	261	263	296	380	557	> 718

Find an n which requires a spectacular value of k. It's inconceivable that the conjecture is false. Each (odd part of) n divides $2^{rs} - 1$ for a suitable s and all r. $\sigma(2^{rs-1}) = 2^{rs} - 1$. As k increases, $\sigma^k(n)$ increases quite rapidly, and so does the power of 2 it contains, albeit very erratically. How can the sequence of exponents of 2 avoid all members of the arithmetic progression $rs - 1$? A couple of curiosities: $\sigma^6(36) = \sigma^6(37)$, $\sigma^{26}(37) = 2^{26}3^2 5^2 7^2 13^2$ so that $\sigma^{27}(37)$ is odd.

Much additional information is in a forthcoming paper:

G. L. Cohen & H. J. J. te Riele, Iterating the sum-of-divisors function (1994 preprint).

They call numbers **(m, k)-perfect** if $\sigma^m(n) = kn$; e.g., perfect numbers are $(1, 2)$-perfect, multiperfect numbers are $(1, k)$-perfect, $(2, 2)$-perfect numbers have been called **superperfect** and $(2, k)$-perfect numbers **multiply superperfect**; these last being discussed by Pomerance in the reference at **94:12** above. They tabulate all (m, k)-perfect numbers n for $(m, n) = (2, < 10^9)$, $(3, < 2 \cdot 10^8)$, $(4, < 10^8)$ and prove that the equation $\sigma^2(2n) = 2\sigma^2(n)$ has infinitely many solutions. They ask: for any fixed m, are there infinitely many (m, k)-perfect numbers? and : is every n (m, k)-perfect for some m? (i.e., the present problem.) For $n \in [1, 400]$ they list the least such m. The most 'spectacular value of k' (m in their notation) was 78 for $n = 29$, the only instance in their table with $m > 2n$. Perhaps it is never 'spectacular'?

94:14 (Terry Raines) Find an optimally efficient algorithm for representing a positive integer as the sum of four cubes. For $N = a^3 + b^3 + c^3 + d^3$ a search with four nested loops soon becomes intolerably slow. Much more efficient is to check *three* nested loops for suitable a, b, c and then verify that $N - a^3 - b^3 - c^3$ is a cube. With this I have found representations for all $N \leq 20000$; however, a small number of "bad" N took several hours to break. What are "suitable" a, b, c ? Is an algorithm with only two loops possible? What if we take $N - a^3$ to be small and attempt to represent this difference with three cubes?

Remarks: (editor) Only N of shape $9n \pm 4$ need be tried. Presumably sieving is done, with cubic residues?

(Noam Elkies) Whether a, b, c, d are required to be positive, or not, given N, an exhaustive search for solutions of $N = a^3 + \cdots + d^3$ with a, b, c, d bounded by M [presumably $M \lll N^{1/3}$ is enough] can be done in time $O(M^2 \ln M)$ and space $O(M^2)$ by the standard ruse [see the beginning of Knuth III for instance] of 1) listing all $a^3 + b^3$; 2) sorting the list, keeping track of a, b and deleting duplicates; 3) using this to also create a list of $N - c^3 - d^3$; 4) merging the two lists, sorting, and looking for duplicates. But if you want to catch all N through say 10^6, it is much simpler and quicker to set up a table of length 10^6, run 4 nested loops only once, and each time $a^3 + b^3 + c^3 + d^3$ attains a yet-unseen value of N store a, b, c, d in the N-th place of the table.

(Richard F. Lukes) Extract from 1994 Univ. of Manitoba thesis:

All numbers less than 10 million can be represented as the sum of four cubes

Waring's Problem is to find the least value of $g(k)$ such that every positive integer can be expressed as the sum of at most $g(k)$ kth powers of positive integers. For cubes it is a longstanding result that no more than 9 cubes are required to represent every integer, and thus $g(3) = 9$. The so-called Easier Waring's Problem is that of determining the least value of $v(k)$, such that every integer (positive or negative) can be expressed as the sum of $v(k)$ positive or negative kth powers. In 1894, Oltramare proved that $4 \leq v(3) \leq 5$. In an attempt to find numerical evidence that $v(3) = 5$, we searched for integers which are difficult to represent as the sum of 4 positive or negative integer cubes (4 cubes for short). Instead, we found some numerical evidence to support that $v(3) = 4$ by determining the representations of all integers n, where $|n| \leq 10^7$, as the sum of 4 cubes.

A computer search was undertaken to determine those integers d which are difficult to represent as the sum of 4 cubes. In our algorithm, we first determined all $d_3 = x^3 + y^3 + z^3$ for $0 < d_3 < 10^6$ and $\max(|x|, |y|, |z|) \leq 1300$ and stored these values of d_3 in an array. We then determined all values of d_4, for $0 < d_4 < 10^6$, which can be formed by taking an element d_3 and adding or subtracting integer cubes w^3, where $0 \leq w < 100$. This program took approximately 20 minutes of CPU time on a DEC Alpha 3000-300 workstation. The result of this process was that the only integer d_4 between 0 and 10^6 which could not be represented in this manner was 82,562.

In an attempt to find further examples of integers difficult to represent as the sum of 4 cubes, we extended the search for $0 < d_3, d_4 < 4 \cdot 10^6$ and $\max(|x|, |y|, |z|) \leq 1500$ and $0 \leq w < 150$, and this time found two representations for $d_4 = 82,562$ expressed as the tuples $(x, y, z, w) = (-1498, 1490, 377, 41)$ and $(350, -331, -163, -130)$. This search uncovered no other values of d_4 in the range $0 < d_4 < 4 \cdot 10^6$ which could not be represented as the sum of 4 cubes. As a final test, we ran our algorithm for $0 < d_3, d_4 < 10^7$ and $\max(|x|, |y|, |z|) \leq 1600$ and $0 \leq w < 215$, and again found no values of d_4 in this range which could not be represented as a sum of 4 cubes. To ensure that no errors occurred during our computations, the complete list of representations for $d_4 \equiv \pm 4 \pmod 9$ were stored to a file and double-checked on an Alpha workstation using 64-bit signed integer arithmetic. Only those values of $d_4 \equiv \pm 4 \pmod 9$ need be verified since it is known that all integers $\not\equiv \pm 4 \pmod 9$ can be represented as a sum of 4 cubes.

Because there is heuristic evidence to suggest that it is easier to represent larger integers as the sum of k cubes, the lack of difficult values of d_4 in the range $0 \leq d_4 < 10^7$ suggests that either these difficult values are very rare, or all integers can in fact be represented as a sum of 4 cubes.

[added 95-03-02: Using a modified version of our algorithm we have determined that all integers less than 200 million can be represented as the sum of 4 positive or negative cubes, where $\max(|x|, |y|, |z|) < 1600$, and $0 \leq w < 300$.

94:15 (Paul Bateman) For a positive integer n let Φ_n denote the n-th cyclotomic polynomial,

$$\Phi_n(x) = \prod_{d|n} (1 - x^d)^{\mu(n/d)}$$

Also let A_n be the absolute value of the numerically largest coefficient in Φ_n and let S_n be the set of distinct integers occurring as coefficients in Φ_n. If d and m are odd squarefree integers greater than 1 and if $d|m$,

(a) is it always true that $A_d \leq A_m$?

(b) is it always true that $S_d \subseteq S_m$?

Remark: $S_m = \{1\}$ if m is prime, $S_m = \{0, \pm 1\}$ if m is the product of two primes, $S_m \subseteq [-(p-1), p-1]$ if m is the product of three primes the least of which is p.

Robert Harley provides some counterexamples:

m	S_m	d	S_d
5565	$\{-2,\ldots,3\}$	1855	$\{-3,\ldots,2\}$
8547	$\{-3,\ldots,4\}$	2849	$\{-4,\ldots,3\}$
14235	$\{-2,\ldots,2\}$	4745	$\{-2,\ldots,3\}$
16485	$\{-3,\ldots,2\}$	5495	$\{-2,\ldots,3\}$
22407	$\{-3,\ldots,3\}$	7469	$\{-4,\ldots,2\}$

On 95-03-30 Bateman emails the counterexample

$$S_{12597}=\{-5,\ldots,3\},\quad S_{4199}=\{-3,\ldots,4\}$$

and suggests that it may be more reasonable to consider T_n, the set of absolute values of the coefficients, in place of S_n, and to ask

(c) Is it always true that T_d is a subset of T_m ? [No! See third example above.]

94:16 (Herbert Taylor) Consider an $n \times n$ array of $2n-1$ different letters, each filling a diagonal parallel to the main diagonal.

$$\begin{array}{c} 0 \end{array}\qquad \begin{array}{cc} 0 & a \\ 1 & 0 \end{array}\qquad \begin{array}{ccc} 0 & a & b \\ 1 & 0 & a \\ 2 & 1 & 0 \end{array}\qquad \begin{array}{cccc} 0 & a & b & c \\ 1 & 0 & a & b \\ 2 & 1 & 0 & a \\ 3 & 2 & 1 & 0 \end{array}$$

Try to permute the rows and columns so that one letter still fills the main diagonal, but no letter appears more than once in any other diagonal parallel to the main diagonal.

$$\begin{array}{c} 0 \end{array}\qquad \begin{array}{cc} 0 & a \\ 1 & 0 \end{array}\qquad \begin{array}{ccc} 0 & 1 & a \\ a & 0 & b \\ 1 & 2 & 0 \end{array}\qquad \begin{array}{cccc} 0 & b & c & a \\ 2 & 0 & a & 1 \\ 3 & 1 & 0 & 2 \\ 1 & a & b & 0 \end{array}$$

For which n can it be done?

Remark: The first unknown n is 32. There is a connexion with Costas arrays, e.g.

$$\begin{array}{ccccc} 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 \end{array}$$

Compare Richard K. Guy, Parker's permutation problem involves the Catalan numbers, *Amer. Math. Monthly*, **100**(1993) 287–289, and the references to solutions on pp. 948–949.

94:17 (Sun Hsin-Min via John Brillhart) If p is an odd prime and $2p+1$ is prime (p a Sophie Germain prime), then $2p+1|M_p=2^p-1$ (Euler factor). Is it true that $(2p+1)^2$ never divides M_p ?

Solution: (Franz Lemmermeyer) Let $q \geq 3$ be an odd integer and suppose that $p = 4q + 1$ is prime. Then $S_q = 2^{2q} + 1$ is never prime because of the factorization

$$S_q = A_q \cdot B_q, \quad A_q = 2^q - 2^{\frac{q+1}{2}} + 1, \quad B_q = 2^q + 2^{\frac{q+1}{2}} + 1.$$

Now $p = 4q + 1 \equiv 5 \bmod 8$, hence the quadratic reciprocity law shows that $S_q = 2^{(p-1)/2} \underset{\wedge}{\equiv}$ + 1
$\left(\frac{2}{p}\right) + 1 \equiv 0 \bmod p$. Thus $p \mid A_q B_q$, and the question [first posed by Brillhart in

J. Brillhart, Concerning the numbers $2^{2p} + 1$, p prime, *Math. Comput.*, **16**(1962), 424–430]

is: which? Since quadratic reciprocity has told us that $p \mid A_q B_q$, we might hope that quartic reciprocity will answer this question. We have already seen that quartic reciprocity is somehow related to the presentation $p = a^2 + b^2$ of p as a sum of two squares, hence we let our computer make a small table:

q	p	$*$	a	b
3	13	B	3	2
7	29	B	5	2
9	37	A	1	6
13	53	B	7	2
15	61	A	5	6
25	101	A	1	10
27	109	A	3	10

q	p	$*$	a	b
37	149	A	7	10
39	157	A	11	6
43	173	B	13	2
45	181	A	9	10
49	197	B	1	14
57	229	B	15	2
67	269	A	13	10

This table gives rise to the following

Conjecture. With the above notation, we have

$$p \mid A_q \iff \frac{b}{2} \equiv \pm 3 \bmod 8, \text{ and } p \mid B_q \iff \frac{b}{2} \equiv \pm 1 \bmod 8.$$

In fact, we can prove a somewhat stronger result:

Proposition 3.1 Let q and u be odd integers, and suppose that $p = 4qu + 1 = a^2 + 4b^2$ is prime. Assume moreover that $p \mid S_q = 2^{2q} + 1$ (this is equivalent to $2^{(p-1)/u} \equiv 1 \bmod p$, thus it is always true for $u = 1$). Then

$$S_q = A_q \cdot B_q, \text{ where } A_q = 2^q - 2^{\frac{q+1}{2}} + 1 \text{ and } B_q = 2^q + 2^{\frac{q+1}{2}} + 1,$$

$$\text{and } \begin{cases} b \equiv \pm 3u \bmod 8 & \iff \quad A_q \equiv 0 \bmod p, B_q \equiv 2(1 + 2^q) \bmod p; \\ b \equiv \pm\, u \bmod 8 & \iff \quad B_q \equiv 0 \bmod p, A_q \equiv 2(1 + 2^q) \bmod p. \end{cases}$$

[For proofs of this and the next two propositions, see the Lemmermeyer reference at **78:17** above.]

The octic and sextic analogs are

Proposition 3.2 Let q and u denote odd integers, and let $p = 8qu+1 = a^2+b^2 = c^2+2d^2$ be prime, where $4 \parallel b$. Assume moreover that $p \mid S_q = 2^{2q}+1$ (this is equivalent to $2^{(p-1)/u} \equiv 1 \bmod p$; if $u = 1$, this is trivially true). Then

$$\begin{aligned} p \mid A_q &\iff d + \tfrac{b}{4}u \equiv \pm 1 \bmod 8, \\ p \mid B_q &\iff d + \tfrac{b}{4}u \equiv \pm 3 \bmod 8. \end{aligned}$$

Proposition 3.3 Let $q \equiv 1 \bmod 2$, $u \equiv \pm 1 \bmod 6$, and let $p = \pi\overline{\pi} = 6qu + 1$ be prime, where $\pi = a + b\rho$ is primary. I.e., ρ is a primitive cube root of 1, and $a + b\rho$ is called **primary** if $3|b$ and the following congruences hold:

$$\begin{array}{ll}
a + b \equiv 1 \bmod 4 & \text{if } 2|b, \\
b \equiv 1 \bmod 4 & \text{if } 2|a, \text{ and} \\
a \equiv 3 \bmod 4 & \text{if } ab \text{ is odd.}
\end{array}$$

If $3^{(p-1)/u} \equiv 1 \bmod p$, then $3^{3q} + 1 = K_q L_q M_q \equiv 0 \bmod p$, where

$$K_q = 3^q + 1, \quad L_q = 3^q - 3^{\frac{q+1}{2}} + 1, \quad M_q = 3^q + 3^{\frac{q+1}{2}} + 1,$$

and we have

$$\begin{array}{lcl}
p \mid K_q & \iff & 9 \mid b, \\
p \mid L_q & \iff & (-1)^{\frac{p+1}{4}} \equiv \left(\frac{3}{u}\right) \cdot \frac{b}{3} \bmod 3, \\
p \mid M_q & \iff & (-1)^{\frac{p+1}{4}} \equiv -\left(\frac{3}{u}\right) \cdot \frac{b}{3} \bmod 3.
\end{array}$$

After I had found proofs of the propositions above, I discovered a proof of Conjecture 1 (the special case $u = 1$ of Prop. 3.1.) in

Th. Gosset, On the law of quartic reciprocity, *Messenger Math.*(2), **41**(1911), 65–90.

94:18 (Charles F. Osgood) Do there exist any complex numbers a for which the Riemann zeta function has a positive deficiency in the sense of Nevanlinna theory?

Remark: For those of us without Nevanlinna theory at the tips of our fingers, Noam Elkies kindly explains: is there an $a \in \mathbf{C}$ and $\epsilon > 0$ such that, for an infinite sequence of R approaching infinity, the number of solutions of $\zeta(s) = a$ with $|s| < R$, *not* counting multiplicity, is less than $1 - \epsilon$ times the number of solutions, counting multiplicity, of that equation for generic a? (Presumably $a = 0$ can be taken as a "random" enough a.)

94:19 (Sinai Robins) Evaluate

$$\lim_{s \to 1} \sum_{\substack{(m,n) \in \mathbf{Z}^2 \\ m \neq 0 \\ m - 2n \neq 0}} \frac{1}{m^s (m - 2n)^s}$$

I conjecture that this is a rational number. The meaning of $(-1)^s$ is taken from the counterclockwise direction.

94:20 (Melvyn Knight) Consider the 10-adic number $x = \sum_{n=0}^{\infty} n!$. Is x irrational? Is x transcendental?

Remark: By 'x is rational' is meant that there exist integers a and b such that for every positive integer s there exists $M = M(s)$ such that if $m > M$ then $bx_m \equiv a \bmod 10^s$. For those, if any, as stupid as the editor, Gerry Myerson further explains that $n!$ is divisible by 10^s for all $n \geq n_0(s)$, so, all the m-th partial sums, x_m from some point on are congruent mod10^s. E.g., $x_m \equiv 4 \bmod 10$ for $m \geq 4$, because 5!, 6!, 7!,... are all $\equiv 0 \bmod 10$. And $x_m \equiv 14 \bmod 100$, RKG

see p 20

↓ JPS

for $m \geq 9$, because $x_9 \equiv 14 \bmod 100$ (compute $0! + \cdots + 9!$), and everything from $10!$ on is divisible by 100. So, the last two digits of x are 14. If you want the third from last digit, compute $0! + \cdots + 14!$ modulo 1000.

94:21 (Peter Fletcher, William Lindgren & Carl Pomerance) A pair of different primes p, q form **a symmetric pair** if $\gcd(p-1, q-1) = |p-q|$. For example, twin primes, or $(13, 19)$. Are there infinitely many symmetric pairs?

Remark: The proposers have shown that there exist infinitely many primes that do not belong to a symmetric pair. The first few are 23, 47, 83, 163, 167, 173.

94:22 (James P. Jones) The Pell equation $x^2 - (a^2-4)y^2 = 4$ has solutions $x_a(0) = 2$, $x_a(1) = a$, $x_a(n+2) = ax_a(n+1) - x_a(n)$; $y_a(0) = 0$, $y_a(1) = 1$, $y_a(n+2) = ay_a(n+1) - y_a(n)$. Write the odd prime p in the form $p = 2^t q + \epsilon$, where q is odd and ϵ is the Legendre symbol $((a^2-4)|p)$. Suppose $t \geq 2$, i.e. $p \equiv \epsilon \bmod 4$ and suppose that $p|y_a(q)$. Then it follows that $x_a(q) \equiv \pm 2 \bmod p$. Find the rule for the ± sign.

Remark: Examples: $p = 41$. If $a = 6$ sign is $+$; if $a = 7$ sign is $-$.

$\epsilon_m = \frac{a + \sqrt{m}}{2}$

Solution: (Franz Lemmermeyer) Define $m = a^2 - 4$; then it is easy to see that $x_a(n) + y_a(n)\sqrt{m} = 2\epsilon_m^n$, where $\boxed{\epsilon_m = a + \sqrt{m}}$ is a unit in some order of the quadratic number field $K = \mathbb{Q}(\sqrt{m})$. The problem posed above is equivalent to the evaluation of $\epsilon_m^q \bmod p$, where $q = (p-\epsilon)/2^t$; in fact $x_a(q) = 2\epsilon_m^q \bmod p$.

The case $\epsilon = +1$ has been studied extensively by Scholz, Redei, Aigner, E. Lehmer, Barrucand & Cohn, Brandler, Leonard & K. S. Williams, Halter-Koch, Ishii, and many others. If ϵ_m is the fundamental unit, then $\epsilon_m^{(p-1)/2}$ and $\epsilon_m^{(p-1)/4}$ have been computed for prime m (or more generally for m such that the 2-class group of K has at most one invariant divisible by 4); and if ϵ_m has norm $+1$, similar results for $\epsilon_m^{(p-1)/8}$ are known.

The case $\epsilon = -1$, on the other hand, seems not to have been examined at all. Observe that we have treated some special cases in Sect. 1 (for the unit $2 + \sqrt{3}$); other than that, not much is known:

Proposition 2.1 Let h denote the (odd) class number of $\mathbb{Q}(\sqrt{-q}\,)$, where $q \equiv 3 \bmod 4$ is prime. Let $p \equiv 3 \bmod 4$ be a prime such that $(-q|p) = 1$; then $p^h = 4a^2 + qb^2$ for some $a, b \in \mathbb{N}$. If ϵ_p denotes the fundamental unit of $K = \mathbb{Q}(\sqrt{q}\,)$, then

$$\epsilon_q^{\frac{p+1}{2}} \equiv (-1)^a \bmod p.$$

$$\epsilon_q^{\frac{p+1}{4}} \equiv \begin{cases} +1 & \bmod q \quad \text{if } a \equiv 2 \bmod 4, \\ -1 & \bmod q \quad \text{if } a \equiv 0 \bmod 4, \\ (-1|ab)\frac{b}{a}\sqrt{q} & \bmod q \quad \text{if } a \equiv 1 \bmod 2. \end{cases}$$

[For a proof see Lemmermeyer reference at **78:17** above.]

Back to the example: if $p = 41$, $a = 6$, then $m = 6^2 - 4 = 32$, $\epsilon_m = 3 + 2\sqrt{2} = \epsilon_2^2$, hence $\epsilon_m^{(p-1)/8} = \epsilon_2^{(p-1)/4} = (\epsilon_2|41)_4 = +1$ by Scholz's reciprocitytheorem.

94:23 (Zachary Franco) For which t does $t^a + t^b + 1 = n^2$ have a solution in positive integers a, b, n ? It's clear that if $(3|(t-1)) = -1$, then no solutions exist.

Remarks: It was conjectured that for $t = 2$ the only solutions were $(a, b, n) = (5, 4, 7)$ and $(2k, k + 1, 2^k + 1)$ for $k = 1, 2, 3, \ldots$, but Robert Styer, in a 94-12-30 email, gave $(9, 4, 23)$, and said that there were no other sporadic solutions with $n \le 2^{20}$.

The problem was emailed to Reese Scott and Benne de Weger. Reese Scott shows that if a is even, only the infinite family of solutions exists. If a is odd and $a \le 3b - 3$, then there are only the two sporadic solutions. If a is odd and $a > 3b - 3$, he hadn't solved it at the time of writing, but if a solution exists, $a > 40$.

de Weger notes that the following are relevant:

Frits Beukers, On the generalized Ramanujan-Nagell equation I, II, *Acta Arith.*, **38**(1980/81) 389–410, **39**(1981) 113–123; *MR* **83a**:10028a,b.

namely, for the R-N equation $2^a + D = n^2$, Beukers proves $a \le 435 + 10 \ln |D| / \ln 2$, so for the present equation $a \le 435 + 10b$.

Reese Scott said that the methods he used for $t = 2$ apply for t prime and, for prime p, $p^a + p^b + 1 = n^2$ has no solutions unless $p \equiv 7 \bmod 8$, and there are no solutions unless a is odd and b is even, and no solutions if $a \le 3b$. Hence he shows that $n > 2 \cdot 10^8$.

94:24 (Peter Borwein) Exhibit two Liouville numbers α and β such that $e^\alpha = \beta$.

Remark: It is obvious that two such numbers exist.

94:25 (Peter Borwein) Make the following algorithmic:

Do there exist two distinct sets of integers $\{\alpha_i\}_{i=1}^{11}$, $\{\beta_i\}_{i=1}^{11}$ so that

$$(x-1)^{11} \left| \sum_{i=1}^{11} (x^{\alpha_i} - x^{\beta_i}) \right.$$

Remark: This is the first unresolved case of the Tarry-Escott problem.

94:26 (Mike Zieve) For p prime, let

$$f(x) = x + b_0 + b_1 x + b_2 x^2 + \cdots + b_n x^n \in \mathbf{F}_p[b_0, b_1, \ldots, b_n][x]$$

be a generic polynomial of degree n. Let $g(x) \in F_p[b_0, \ldots, b_n][x]$ be the p-th iterate of f, and write $g(x) - x$ as a sum of monomials $cx^k b_0^{\alpha_0} b_1^{\alpha_1} \cdots b_n^{\alpha_n}$ where $c \in \mathbf{F}_p \backslash \{0\}$, and k, α_0, α_1, $\ldots$, $\alpha_n \ge 0$.

Conjecture: If $k \le p - 1$, then $2\alpha_0 + \alpha_1 \ge p - 1$.

Evidence: For each n and p this is true for the first several thousand terms. For $p \le 5$ this is true for each n. For small n this is true for each p. As an example we give a proof for $n = 1$:

$$\begin{aligned}
f(x) &= b_0 + (1 + b_1)x \\
g(x) &= b_0(1 + (1 + b_1) + \cdots + (1 + b_1)^{p-1}) + (1 + b_1)^p x \\
&= b_0 \frac{(1 + b_1)^p - 1}{(1 + b_1) - 1} + (1 + b_1)^p x \\
&= b_0 \frac{b_1^p}{b_1} + (1 + b_1^p)x \\
&= x + b_0 b_1^{p-1} + b_1^p x
\end{aligned}$$

where the second and third terms have $2\alpha_0 + \alpha_1 = p + 1$ and $2\alpha_0 + \alpha_1 = p$.

94:27 (Dan Shanks & Sam Wagstaff)

Martin Davis, One equation to rule them all, *Trans. New York Acad. Sci. Ser. II*, **30**(1968) 766–773 showed that if the diophantine equation

$$9(u^2 + 7v^2)^2 - 7(r^2 + 7s^2)^2 = 2 \qquad (1)$$

had no solution other than the trivial one $u = 1$, $v = 0$, $r = 1$, $s = 0$, then the Hilbert tenth problem is unsolvable in the sense of recursive number theory. However
Oskar Herrmann, A non-trivial solution of the diophantine equation $9(u^2 + 7v^2)^2 - 7(r^2 + 7s^2)^2 = 2$, *Computers in Number Theory* (ed. A.O.L. Atkin & B.J. Birch, Academic Press, 1971, 207–212.
established that (1) had a non-trivial solution and Shanks computed it.

Does (1) have infinitely many solutions?

We may write (1) in the form $9A_n^2 - 7B_n^2 = 2$, where A_n, B_n are of form $x^2 + 7y^2$.
$A_{n+1} = 8A_n + 7B_n$, $B_{n+1} = 9A_n + 8B_n$, $A_0 = B_0 = 1$. The A_n, B_n are all odd, and an odd z is of the form $x^2 + 7y^2$ just if $p^k \| z$ implies that $p^k \equiv 0, 1, 2, 4 \bmod 7$, i.e. primes $p \equiv 1, 2, 4 \bmod 7$ may divide to any power, but primes $q \equiv 3, 5, 6 \bmod 7$ must divide to an even power. $(A_n, B_n) = (1,1), (\mathbf{3{\cdot}5,17}), (\mathbf{239,271}), (\mathbf{13{\cdot}293},7{\cdot}617), \ldots$, where the **bad** primes q are shown in **bold** and we can rule out as far as $n = 26$. Hermann showed that
$A_{26} = 17\,2314290896\,2461416647\,0862182959$ and $B_{26} = 19\,5386040451\,6750611809\,7869511631$ are prime and lead to a solution. If we continue, $A_{33} = p_4 p_{12} p_{26} \equiv 4 \cdot 1 \cdot 2 \bmod 7$ and
$B_{33} = p_6 p_{14} p'_{26} \equiv 1 \cdot 4 \cdot 1 \bmod 7$ where p_j denotes a prime with j decimal digits. By composition (e.g., $p_4 = 1607 = 40^2 + 7 \cdot 1^2$, $p_{12} = 243402458839 = 179208^2 + 7 \cdot 173735^2$ so that $p_4 p_{12} = (40 \cdot 179208 \pm 7 \cdot 1 \cdot 173735)^2 + 7(40 \cdot 173735 \mp 1 \cdot 179208)^2$) these lead to 16 new solutions of (1). And $A_{35} = p_8 p_{35} \equiv 1 \cdot 1$ and $B_{35} = p_3 p_5 p'_5 p_{13} p_{19} \equiv 2 \cdot 2 \cdot 4 \cdot 4 \cdot 1$ yield 32 more.