Western Number Theory Problems, 17 & 19 Dec 2001

Edited by Gerry Myerson

for distribution prior to 2002 (San Francisco) meeting

Summary of earlier meetings & problem sets with old (pre 1984) & new numbering.

1967 Berkeley	1968 Berkeley		1969 Asilomar	
1970 Tucson	1971 Asilomar		1972 Claremont	72:01–72:05
1973 Los Angeles	73:01–73:16		1974 Los Angeles	74:01–74:08
1975 Asilomar	75:01–75:23			
1976 San Diego	1–65	i.e., 76:01–76:65		
1977 Los Angeles	101–148	i.e., 77:01–77:48		
1978 Santa Barbara	151–187	i.e., 78:01–78:37		
1979 Asilomar	201–231	i.e., 79:01–79:31		
1980 Tucson	251–268	i.e., 80:01–80:18		
1981 Santa Barbara	301–328	i.e., 81:01–81:28		
1982 San Diego	351–375	i.e., 82:01–82:25		
1983 Asilomar	401–418	i.e., 83:01–83:18		
1984 Asilomar	84:01–84:27		1985 Asilomar	85:01–85:23
1986 Tucson	86:01–86:31		1987 Asilomar	87:01–87:15
1988 Las Vegas	88:01–88:22		1989 Asilomar	89:01–89:32
1990 Asilomar	90:01–90:19		1991 Asilomar	91:01–91:25
1992 Corvallis	92:01–92:19		1993 Asilomar	93:01–93:32
1994 San Diego	94:01–94:27		1995 Asilomar	95:01–95:19
1996 Las Vegas	96:01–96:18		1997 Asilomar	97:01–97:22
1998 San Francisco	98:01–98:14		1999 Asilomar	99:01–99:12
2000 San Diego	000:01–000:15		2001 Asilomar (current set)	001:01–001:23

[With comments on 98:12, 99:06, and 99:07]

COMMENTS ON ANY PROBLEM WELCOME AT ANY TIME

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

17 August 2002

Comments on earlier problems

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

Remark: See Remark 2 on Problem 001:05, below.

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

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

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

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

Remark: (new) That 22/47 should be 27/47.

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

1. Given f, which numbers have finite expansions? periodic expansions? Is it true that if $f(x) = x^{-2/3}$ then $(\sqrt[3]{3})_f = (\dot{1}, 1, 1, \dot{2})$?

2. Is there an f such that $(\alpha)_f$ is periodic for all algebraic α of degree 3?

3. Find f such that $(\pi)_f$ has a recognizable pattern.

4. Find f such that $(e)_f$ is periodic.

5. Find conditions on f and α for $\lim_{n\to\infty} c_n = \alpha$.

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

Remark: Jeff Lagarias refers to

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

Remark: (new) Some of these questions are answered in

Greg Martin, The unreasonable effectualness of continued fraction expansions, preprint.

Following

B. H. Bissinger, A generalization of continued fractions, Bull. Amer. Math. Soc. 50 (1944) 868–876, MR 6, 150h,

Greg calls the construction of 99:07 an f-expansion. Among other things, he proves that there is a function f such that the f-expansion of a real number x is periodic if and only

if x is a cubic irrational number. He notes that if $f(x) = x^{-2/3}$ then $(\sqrt[3]{3})_f \neq (\dot{1}, 1, 1, \dot{2})$. Indeed, the expansion of $\sqrt[3]{3} = 1.44224957\ldots$ is

$$(\sqrt[3]{3})_f = (1, 1, 1, 2, 1, 1, 1, 2, 1, 1, 1, 2, 1, 1, 1, 3, 1, 1, 1, 1, 1, 3, 1, 2, 1, 1, 7, 23, 1, \ldots),$$

while the number $x = 1.44225029\ldots$ whose expansion is $(\dot{1}, 1, 1, \dot{2})$ is an algebraic number of degree 93.

Problems Proposed 17 & 19 Dec 2001

001:01 (David H. Bailey) Let $x_0 = 0$, and for $n = 1, 2, \ldots$ let

$$x_n = 16x_{n-1} + \frac{120n^2 - 89n + 16}{512n^4 - 1024n^3 + 712n^2 - 206n + 21} \pmod 1.$$

1. Is the sequence $x_0, x_1, \ldots$ uniformly distributed in $[0, 1)$? If so, then π is normal to base 16 (and thus to base 2).

2. Let $y_n = [16x_n]$, $n = 0, 1, \ldots$. Prove that y_n gives the hexadecimal expansion of π, that is, $y_1 = 2$, $y_2 = 4$, $y_3 = 3$, etc., matching $\pi = 3.243f6a8\ldots$ (base 16).

Remark: This has been checked out to $n = 100{,}000$.

001:02 (David H. Bailey) Let $x_0 = 0$, and for $n = 1, 2, \ldots$ let

$$x_n = 2x_{n-1} + \frac{1}{n} \pmod 1.$$

Is the sequence $x_0, x_1, \ldots$ uniformly distributed in $[0, 1)$? If so, then $\log 2$ is normal to base 2.

001:03 (Neville Robbins) Let $s(h, k)$ be the Dedekind sum,

$$s(h, k) = \sum_{\nu=1}^{k-1} ((\nu/k))((h\nu/k)),$$

where $((x)) = 0$ if x is an integer, $((x)) = \{x\} - \frac{1}{2}$ otherwise, and h and k are integers with $0 < h < k$ and $\gcd(h, k) = 1$. Find all solutions of $s(h, k) = h/k$.

Remark: With Nick Phillips, an undergraduate at Macquarie, your editor has found that there are infinitely many. It appears unlikely that any simple formula will capture all of them. One infinite family is given by $h = 11m^3$, $k = 121m^4 + 11m^2 + 1$, $m = 1, 2, \ldots$.

001:04 (David Petrie Moulton) Given a set of numbers P, let

$$\text{rank}(P) = \min\{\, \#B : \text{every element of } P \text{ is a sum of distinct elements of } B \,\}.$$

1. Is $\text{rank}(\{\, 1!, 2!, \ldots, n! \,\})$ ever less than n?

2. Index the Fibonacci numbers by $f_1 = 1$, $f_2 = 2$, $f_{n+1} = f_n + f_{n-1}$. Do we ever have $\text{rank}(\{\, f_1, f_2, \ldots, f_n \,\}) \le n/2$?

3. For r algebraic is it true that $\lim_{n\to\infty} \frac{1}{n}\text{rank}(\{\, 1, r, \ldots, r^{n-1} \,\}) = 0$?

Remark: The last equation is true when r is rational. For many algebraic numbers r, there are values of n for which $\text{rank}(\{\, 1, r, \ldots, r^{n-1}\}) < n$, which implies that the limit above is strictly less than 1. The existence of such an n is often obvious, e.g., when r is the golden ratio, but there is also such an n for r a zero of $x^2 - 2x - 1$ or $x^2 - 3x + 1$. Notice also that if the third question is answered in the affirmative when r is the golden ratio, then the second question is answered in the affirmative as well.

001:05 (Brian Conrey, via Carl Pomerance) Is the number of solutions of $n = xyz + x + y$ in positive integers bounded by n^ϵ?

Remarks: 1. This equation can be written as $zn + 1 = (zx + 1)(zy + 1)$.

2. Ognian Trifonov writes, "There is a connection between Problems 001:05 and 98:12 (see above for statement of 98:12 — Ed.). Also, Carl Pomerance mentioned that there are $\ll_\epsilon n^{1/3+\epsilon}$ solutions of the equation in Problem 001:05. I include a short proof of that, too.

"Let $T(n)$ be the number of solutions of $n = xyz + x + y$ in positive integers. We want to prove $T(n) \ll_\epsilon n^\epsilon$.

"Let $T'(n)$ be the number of solutions of $n = xyz + x + y$ in positive integers with $\gcd(x, y) = 1$. We have $T(n) = \sum_{d|n} T'(n/d)$. Thus, to obtain the desired inequality it suffices to prove $T'(n) \ll_\epsilon n^\epsilon$.

"Let x and y be coprime positive integers. Then $n = xyz + x + y$ for some positive integer $z \Leftrightarrow xy|n - x - y \Leftrightarrow x|n - y$ and $y|n - x$.

"The number of pairs of positive integers (x, y) with the above property is at most the quantity $s(-1, n)$ from Kevin Ford's Problem 98:12. His conjecture is $s(A, B) \ll_\epsilon |AB|^\epsilon$. (It is true that he requires A and B to be positive but probably the conjecture holds for any integers A and B.)

"So, if the extended version of Kevin Ford's conjecture is true then $T'(n) \ll_\epsilon n^\epsilon$ and Brian Conrey's conjecture is true.

"Thus, in a sense Problem 001:05 is a special case of Problem 98:12.

"One easy proof that $T'(n) \ll_\epsilon n^{1/3+\epsilon}$ and thus $T(n) \ll_\epsilon n^{1/3+\epsilon}$ is the following: First, we count solutions with $x \le n^{1/3}$. Fix x. Since $y|n - x$ there are $\ll_\epsilon n^{1/3+\epsilon}$ such solutions. Similarly, there are $\ll_\epsilon n^{1/3+\epsilon}$ solutions with $y \le n^{1/3}$. If $x > n^{1/3}$ and $y > n^{1/3}$ then $z < n^{1/3}$. Fix z in this case and use Remark 1, and we get $\ll_\epsilon n^{1/3+\epsilon}$ solutions in this case as well."

001:06 (Carl Pomerance) Is it true that $n > n_0$ implies the largest prime factor p of $2^n - 1$ exceeds $2n + 1$?

Remarks: 1. Schinzel proves $p \geq 2n+1$ for $n > 12$. Equality obtains for $n = 20$. See

A. Schinzel, On primitive prime factors of $a^n - b^n$, Proc. Cambridge Philos. Soc. 58 1962, 555–562, MR 26 #1280.

2. Noam Elkies writes, "If this fails then the value at 2 of the n-th cyclotomic polynomial is of the form $(2n + 1)^{a_2}(4n + 1)^{a_4}$, with a_k integers that may not be positive unless the corresponding $kn+1$ is prime. This seems most unlikely for large n, for various reasons including the ABC-conjecture."

001:07 (Andrew Granville and Carl Pomerance) Let $N_3(x)$ be the number of triples $a < b < c$ with $abc \leq x$, $a \mid bc + b + c$, $b \mid ac + a + c$, and $c \mid ab + a + b$. Is it true that $N_3(x) \leq x^{\frac{1}{3}+\epsilon}$?

Remark: This is related to the number of Carmichael numbers with three prime factors.

001:08 (Peter Borwein and Chris Smyth) Let $p(x_1, \ldots, x_n)$ be a polynomial in n variables with integer coefficients in which every variable occurs. Show that

$$\sup_{(x_1,\ldots,x_n) \text{ in } [-2,2]^n} |p(x_1, \ldots, x_n)| \geq 2n.$$

Remark: A lower bound of $\sqrt{2n}$ is easy to obtain. The bound $2n$ is attained by $p(x_1, \ldots, x_n) = x_1 + \ldots + x_n$ and many other polynomials.

001:09 (Greg Martin) Let $f(x)$ be an integer-valued polynomial of degree d, not identically zero (mod p) for any p. Let $M = \max(|f(0)|, |f(1)|, \ldots, |f(d + 1)|)$, let R be the radical, $R = \prod_{p|f(0)f(1)\cdots f(d+1)} p$. Is it true that $M \ll dR^{1+\epsilon}$?

Remarks: 1. In the case $d = 1$ we have $f(0) + f(2) = 2f(1)$ and the question reduces to the *abc*-conjecture. Thus, it can be seen as a generalization of the *abc*-problem.

2. The dependence on d is illustrated by the example $f(0) = f(1) = 2$, $f(2) = \ldots = f(d) = 1$. Then $f(d+1) = 1 - (-1)^d d$. Take $d = 2^k - 1$. Then $f(d+1) = 2^k$ so $R = 2$, but M is roughly d.

3. In response to various counterexamples to the formulation above, let T_d be the set of vectors $(f(0), \ldots, f(d+1))$ with f integer-valued, degree d, not identically zero (mod p) for any p; call $(v_0, \ldots, v_{d+1})$ in T_d decomposable if there is a proper non-empty set of entries such that if those entries are changed to zero the resulting vector is a non-zero multiple of an element of T_d. There are counterexamples for decomposable elements of T_d, e.g., $(3 \times 5^k, -2 \times 7^k, -1 \times 5^k, 6 \times 7^k)$ is in T_2 with $M = 6 \times 7^k$ and $R = 210$, but this is decomposable since $(3 \times 5^k, 0, -1 \times 5^k, 0) = 5^k \times (3, 0, -1, 0)$ and $(3, 0, -1, 0)$ is in T_2. So, the question is whether $M \ll dR^{1+\epsilon}$ when $(f(0), \ldots, f(d + 1))$ is indecomposable. This reformulation is due to Nils Bruin and Bjorn Poonen.

4. Peter Montgomery notes that if $f(x) = c_1\binom{x-1}{d} + c_2$ then $f(0) = c_2 + (-1)^d c_1$, $f(1) = \ldots = f(d) = c_2$, $f(d+1) = c_1 + c_2$. Taking c_1 and c_2 large such that few primes divide $(c_2 + (-1)^d c_1)c_2(c_1 + c_2)$ refutes $M \ll dR^{1+\epsilon}$. However, if d is even then these examples are decomposable, while if d is odd then we're back to the *abc*-problem.

5. Andrew Granville writes, "In Remark 3, Greg has attempted to patch up the conjecture using some ideas about vanishing subsums borrowed from the subspace theorem literature. However the following example shows that this is also way wrong:

$$f(x) = \big((2^{6k-1}+1)/3 + 2^{4k-1} - 2^{2k-1}\big)x^2 - \big((2^{6k-1}+4)/3 + 3\times 2^{4k-1} - 3\times 2^{2k-1}\big)x + 1$$

which has

$$f(0) = 1; \qquad f(1) = -2^{2k}(2^{2k}-1); \qquad f(2) = (2^{2k}-1)^3/3; \qquad f(3) = 2^{6k}.$$

"This example is far less adhoc than it may look. Let me explain:

"For degree 2 polynomials one has $f(3) - 3f(2) + 3f(1) - f(0) = 0$ so one is looking at the *abcd* conjecture with some side conditions like $3|b$ and $3|c$. For degree d polynomials one has a similar relation (the coefficients are binomial coefficients), leading to a question about the $abc\ldots z$-conjecture with some minor divisibility properties.

"It is a fact that if you have a deg d polynomial with $f(0), .., f(d)$ all integers, then f is integer-valued (proof: use the above linear recurrence involving binomial coefficients). Also $f(n)$ is always divisible by p if $f(0), .., f(d)$ are. So Greg's conjecture follows from the conjecture if $a_1 + .. + a_d = 0$ with $(a_1, ..., a_d) = 1$ and $m_i|a_i$ for some given $m_i > 0$ then $\max\ a_i \ll d\ \text{radical}(a_1...a_d)^{1+o(1)}$.

"This is well-known to be very wrong. The easiest way to get counterexamples is to take an example of $a + b = c$ with $c = \ \text{radical}(abc)^{1+o(1)}$, and then consider the identity

$$a^3 + 3abc + b^3 - c^3 = 0$$

The side condition can be satisfied by taking $3|b$. Thus we get a much more general counterexample than what I just gave above. To get the above I specialized $a + b = c$ to $1 + (2^{2k} - 1) = 2^{2k}$.

"So what is the "latest" on the $abc\ldots z$-conjecture? That

$$\max a_i \ll d\ \text{radical}(a_1...a_d)^{1+\epsilon}$$

except for "finitely many subvarieties" (notice this is more general, and far more esoteric, than the vanishing subsums criterion); I have heard this conjecture by Mazur and Birch. Thus we might guess that the correct way to repair Greg's conjecture is this: for each given integer d, and $\epsilon > 0$, there exist finitely many "families" of polynomials f, such that if f has degree d and is not in one of these families then

$$\max_{0\le i\le d+1} |f(i)| \ll_{d,\epsilon} \text{radical}(f(0)...f(d+1))^{1+\epsilon}.$$

"The great thing about this conjecture is that any clever trick that goes into disproving it can almost certainly be dismissed as giving rise to part of one of those exceptional families!"

001:10 (Ron Bruck via Gerry Myerson) If you know the minimal polynomial of an algebraic number α, when can you write α as a sum of algebraic numbers of lower degree?

Remarks: 1. "Sum" can be interpreted as "sum of two" or as "sum of an arbitrary finite number." Both interpretations seem to be interesting.

2. I take this to be both an existence question and a construction question. Given α, how to decide whether it can be written as required? If it can be so written, how to find such an expression for it?

3. Certainly if $\deg(\alpha, \mathbf{Q})$ is prime then α can't be written as a sum of any finite number of algebraic numbers of lower degree.

4. A simple example is $\sqrt{2}+\sqrt{3}$, an algebraic number of degree 4 written as a sum of algebraic numbers of degree 2. A more interesting example is $\alpha = \beta + \gamma$, where β and γ are any two distinct roots of an S_4-quartic; α has degree 6.

5. The Galois group of the normal closure of $\mathbf{Q}(\alpha)$ seems to be a key to the problem.

001:11 (Neville Robbins) Is it true that every prime $p \equiv 11 \pmod{24}$ is represented by the quadratic form $8a^2 + 3b^2$?

Solution: Florian Luca supplies this proof. Let $\mathbf{K} = \mathbf{Q}[i\sqrt{6}]$. The field $\mathbf{K}$ has degree $d = 2$, discriminant $D = -24$, integral base for the ring of its algebraic integers $\{1, i\sqrt{6}\}$ and class number $h = 2$. Let p be a prime, $p \equiv 11 \pmod{24}$. Since the Legendre symbol $(D/p) = 1$, we know that in $\mathbf{K}$ we have $(p) = PP_1$, where P and P_1 are two different prime ideals. Clearly, P is not principal, because if P were principal generated by, say $a + ib\sqrt{6}$, then by taking norms we would get an equation of the form $p = a^2 + 6b^2$ which mod 3 gives $2 \equiv a^2 \pmod{3}$, which is impossible. So, P is non-principal. Now since 2 divides D, we get that $(2) = I^2$, and it is easy to see that I is also non-principal, for if I were principal generated by, say $a_1 + ib_1\sqrt{6}$ then by taking norms we would get $2 = a_1^2 + 6b_1^2$, which is obviously impossible. So, both I and P are non-principal, and since $h = 2$, we get that they represent the same class in the ideal class group of order 2. In particular, IP is principal, say generated by $x + iy\sqrt{6}$. Taking norms we get $2p = x^2 + 6y^2$, and now $x = 2x_1$ is even and $p = 2x_1^2 + 3y^2$. Clearly, y is odd, hence $y^2 \equiv 1 \pmod{8}$, therefore $3y^2 \equiv 3 \pmod{24}$, and the above equation for p modulo 24 implies that $11 \equiv 2x_1^2 + 3 \pmod{24}$, leading to the conclusion that x_1 is even, which finishes the argument.

David Leep notes that a more elementary proof can be found in Nagell, Introduction to Number Theory, on pages 188–190. It goes like this. Let $p \equiv 11 \pmod{24}$ be prime. Legendre symbol considerations show that $2z^2 + 3 \equiv 0 \pmod{p}$ is solvable. By Thue's remainder theorem there exist x and y, $1 \le x, y < \sqrt{p}$, $\gcd(x, y) = 1$, such that $2(x/y)^2 + 3 \equiv 0 \pmod{p}$, that is, $2x^2 + 3y^2 = dp$ for some d, $1 \le d \le 4$. We rule out the cases $d = 2, 3, 4$;

If $2x^2 + 3y^2 = 2p$ then $y = 2y_1$, $x^2 + 6y_1^2 = p$, x is odd, $p \equiv \pm 1 \pmod{8}$, contradiction.

If $2x^2 + 3y^2 = 3p$ then $x = 3x_1$, $6x_1^2 + y^2 = p$, and again $p \equiv \pm 1 \pmod 8$.

If $2x^2 + 3y^2 = 4p$ then x and y are both even, contradiction.

Thus, $2x^2 + 3y^2 = p$. Now y is odd and $p \equiv 3 \pmod 8$ so x is even, $x = 2x_1$, and $8x_1^2 + 3y^2 = p$.

001:12 (Chris Smyth) Let L be a sublattice of $\mathbf{Z}^n$ such that every non-zero member of L has at least three non-zero components, and $(1, 1, 1, 0, \ldots, 0)$ is in L, and all components of L look the same—that is, there is a group G acting transitively on $\{ 1, \ldots, n \}$ such that if σ is in G and $(x_1, \ldots, x_n)$ is in L then $(x_{\sigma(1)}, \ldots, x_{\sigma(n)})$ is in L. Must n be a multiple of 3?

Remark: If so, then if α is an algebraic number with three conjugates adding to zero, and if $-\alpha$ is not a conjugate of α, then the degree of α is a multiple of 3. There is an algebraic number β of degree 20 with three conjugates that add to zero, but $-\beta$ is a conjugate of β.

001:13 (Chris Smyth) What is the greatest degree of an algebraic number whose conjugates span a 4-dimensional vector space over the rationals? It is known that the degree cannot exceed 1152, and an example of degree 384 is known.

Solution: Noam Elkies writes, "The upper bound of 1152 is attained. Let G be the 1152-element subgroup of $\mathrm{GL}_4(\mathbf{Q})$ generated by the signed coordinate permutations and the scaled Hadamard matrix $[1, 1, 1, 1; 1, 1, -1, -1; 1, -1, 1, -1; 1, -1, -1, 1]/2$. This group is also known as the Weyl group of F_4. Let G act by linear transformations on x_1, x_2, x_3, x_4 and thus on the polynomial ring $\mathbf{Q}[x_1, x_2, x_3, x_4]$. Then it is known that the G-invariant subring of $\mathbf{Q}[x_1, x_2, x_3, x_4]$ is a polynomial ring with generators of degrees 2, 6, 8, 12, call them A_2, A_6, A_8, A_{12}. Then $\mathbf{Q}(x_1, x_2, x_3, x_4)$ is a normal extension of $\mathbf{Q}(A_2, A_6, A_8, A_{12})$ with Galois group G. For (c_1, c_2, c_3, c_4) outside the union of finitely many hyperplanes in $\mathbf{Q}^4$, this extension is generated by $X := c_1x_1 + c_2x_2 + c_3x_3 + c_4x_4$, and X has 1152 conjugates all in a four-dimensional space over $\mathbf{Q}$. By the Hilbert irreducibility theorem there exist rational a_2, a_6, a_8, a_{12} such that when we substitute a_i for the corresponding A_i we obtain an extension of $\mathbf{Q}$ with the same Galois group G. The resulting algebraic number X satisfies the criterion of the problem.

"Indeed it is known that of the N smallest choices for (a_2, a_6, a_8, a_{12}) all but $o(N)$ work as $N \to \infty$; see for instance Chapter 3 of Serre's Topics in Galois Theory for Hilbert irreducibility and its applications to this kind of inverse Galois problem."

Remark: Much can be said about the analogous question for dimensions other than 4. The interested reader is referred to Chris Smyth for details.

001:14 (Hugh Edgar) If $\epsilon - 1$, ϵ, and $\epsilon + 1$ are all units, must they be real?

Solution: (Kiran Kedlaya) No. Let ϵ be a non-real root of $x^3 - x + 1$. Then the product $(\epsilon - 1)\epsilon(\epsilon + 1) = -1$, so all three numbers are units.

001:15 (Hugh Edgar) Are there infinitely many pairs of primes whose difference is perfect?

Remark: Presumably there are infinitely many pairs of primes whose difference is 6, but maybe it's easier to prove something about perfection.

001:16 (Hugh Edgar) Does $1 + q + \ldots + q^{x-1} = p^y$ have any solutions with p and q odd primes, $x > 3$ and $y > 1$ other than $(p, q, x, y) = (11, 3, 5, 2)$?

Remarks: 1. Hugh offers \$50 (U.S.) for the solution to this problem.

2. This problem appears, without the monetary offer, as D10 in UPINT.

3. Florian Luca notes that there are several recent papers on the equation $1 + q + \ldots + q^{x-1} = p^y$ by Bugeaud, Mignotte and others, e.g.,

Y. Bugeaud, G. Hanrot, M. Mignotte, Sur l'équation diophantienne $(x^{n-1})/(x-1) = y^q$, III, Proc. London Math. Soc. (3) 84 (2002) 59–78.

I have not checked to see whether these papers deal with the particular restrictions on the variables contemplated here.

4. Noam Elkies writes, "The equation $(q-1)p^y+1 = q^x$ has a discriminant of $p(q-1)q$ which is less than the $2/x + 1/y$ power of q^x. So under the ABC-conjecture there should be finitely many solutions with $x > 3$ and $y > 1$ except for $(x, y) = (4, 2)$, even without the primality hypothesis. But $(4, 2)$ yields $1 + q + q^2 + q^3 = p^2$ which is known to have no integer solutions other than $(1, 2)$ and $(7, 20)$, neither of which meets the primality requirement. So the ABC-conjecture implies that there are only finitely many solutions, and suggests that $(p, q, x, y) = (11, 3, 5, 2)$ is the unique solution assuming that a search over a reasonable region found no others."

001:17 (Filip Saidak) Is it true that if $n > 11$ then $n = a + b$ with $\Omega(a) = \Omega(b)$ and $\gcd(a, b) = 1$? Recall that $\Omega(n) = a_1 + \ldots + a_r$, where $n = p_1^{a_1} \times \ldots \times p_r^{a_r}$ is the prime factorization of n.

Remark: Florian Luca writes: Recall that a theorem of Chen says that every large enough even number can be written in the form $n = p + m$ where $m = q$ or $m = qr$, with p, q, r primes and in fact, in

H. Halberstam, H. E. Richert, Sieve Methods, Academic Press, London, 1975

there is a more general theorem of this type. Presumably, using the same techinque one might be able to prove that every large enough positive integer is of the form $a + b$ with a and b coprime and $\Omega(a) = \Omega(b) = 2$ (if n is odd, then it will be of the form $2p + b$ with $\Omega(b) = 2$).

001:18 (Tim Redmond) Let $Q(m,n) = 3m^2 + 2mn + 6n^2$, let

$$\theta_1(q) = \sum q^{Q(m,n)}, \qquad \theta_2(q) = \sum q^{Q(m+\frac{1}{2},n+\frac{1}{2})}, \qquad \theta_3(q) = \sum (-1)^{m+n} q^{Q(m,n)}.$$

Are $k_1 = \theta_2^2/\theta_1^2$ and $k_2 = \theta_3^2/\theta_1^2$ algebraically related?

Solution: Noam Elkies writes, "Yes. k_1 and k_2 are modular functions for some congruence subgroup of $\mathrm{PSL}_2(\mathbf{Z})$, and are thus algebrically related. Actually exhibiting the relation might be more trouble than it's worth unless there is a good reason for working out this special case."

001:19 (Peter Montgomery) Are there infinitely many primitive solutions to $a^3 = 2b^4 + c^4$? One solution is $(a,b,c) = (11,5,3)$. An infinity of solutions would contradict the *abc*-conjecture.

Solution: As Florian Luca points out in email of 11 March 02,

H. Darmon, A. Granville, On the equations $z^m = F(x,y)$ and $Ax^p + By^q = Cz^r$, Bull. London Math. Soc. 27 (1995) 513-543, MR 96e:11042

contains a proof that $Ax^p + By^q = Cz^r$ has only finitely many proper (i.e., $\gcd(x,y,z) = 1$) integer solutions in x, y, z when $1/p + 1/q + 1/r < 1$. Noam Elkies suggests that the methods of the paper may allow for the complete solution of the equation.

001:20 (Doug Bowman) Is it true that for all rational a, $b > 1$

$$f(a,b) = \sum_{n=1}^{\infty} \frac{\phi(n)}{(a^n - 1)(b^n - 1)}$$

is rational?

Remarks: 1. Even one counterexample would disprove a geometrical conjecture of Atiyah.

2. $f(a,b)$ is a transcendental function which satisfies the identities $f(a,b) = \frac{ab}{(ab-1)^2} + f(ab,b) + f(a,ab)$ and $f(a,b) = \sum_{j,k} \gcd(j,k) a^{-j} b^{-k} = \sum_{(k,m)=1} \frac{a^k b^m}{(a^k b^m - 1)^2}$.

3. Filip Saidak says that if there are infinitely many Mersenne primes then $f(2,2)$ is irrational.

001:21 (Arthur Baragar) Every number α constructible with compass and twice-notched straightedge is in a 2-3-5-6 tower, that is, there are fields $E_1, \ldots, E_n$ such that the numbers $[\mathbf{Q}(\alpha) : E_1], [E_1 : E_2], \ldots, [E_n : \mathbf{Q}]$ are all in $\{\, 2,3,5,6 \,\}$. Is it true that every number that is in such a tower is constructible with compass and twice-notched straightedge?

001:22 (Gary Walsh) Is there a heuristic that suggests that $(x^3-1)(y^3-1)=z^2$ has infinitely many solutions with integers x, y, and 1 distinct?

Remark: Noam Elkies writes, "The usual heuristics suggest that there should be only finitely many solutions, but this seems quite hard to prove. There are a few solutions that are perhaps surprisingly large, such as $(x,y,z)=(3,313,28236)$ and $(x,y,z)=(-20,-362,616077)$. It seems likely that the complete list of solutions consists of these two, the three positive solutions $(2,4,21),(2,22,273),(4,22,819)$ and the three negative solutions $(0,-2,3),(-1,-23,156),(-6,-26,1953)$, and the images of those $2+3+3=8$ solutions under the obvious involutions that switch x with y or z with $-z$, for a total of $4\times 8=32$ solutions. At any rate an exhaustive search shows that these are the only solutions with both $|x|$ and $|y|$ in $[0,10^6]$. (Naturally this search was not over all 10^{12} or so (x,y) pairs: I had gp list, for each m in this range, the smallest integer d such that m^3-1 is d times a square, and then sort the list of d-values and look for duplicates.)"

001:23 (Aaron Meyerowitz) Consider sets of integers $n_1<n_2<n_3\ldots<n_k$ with square product. Let $t(n,k)$ be minimal so that there is a solution with $n_1=n$ and $n_k=n+t(n,k)$. Let $T(n,k)$ be the smallest value of $t(n,j)$ with $j\geq k$. Is there a C with $t(n,3)<Cn^{1/5}$ infinitely often? Is there a C' with $T(n,4)<C'n^{1/4}$ infitely often?

Remarks: 1. If $n=rs^2$ with r square-free then $t(n,2)=r(2s+1)>n^{1/2}$.

2. There is a parametric family with $t(n,3)<5n^{1/4}$.