Comments on Earlier Problems

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

Remarks: (1998) Building on examples of Peter Montgomery and David Moulton, the editor suggested letting $f(n)$ be the smallest number of integers needed to express $1, 2, 4, \ldots, 2^{n-1}$ as subsums. Moulton noted $f(7) \le 5$, using -20, -15, 17, 19, 28. These remarks were included in the 1997 problem set.

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

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

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

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

(2000) Moulton's work will appear in J. Number Theory, as will a follow-up by Michael Develin. In email of 25 October 2000, Moulton writes that he can now prove that $\rho(r) = 0$ for any rational number r. He also reports, via Kiran Kedlaya, that he can show that for fixed r,

$$\frac{n}{\log_r n}\big(1+o(1)\big) \le \mathrm{Rank}(\{\,1, r, r^2, \ldots, r^{n-1}\,\}) \le \frac{2n}{\log_r n}\big(1+o(1)\big),$$

and also $\liminf_{n\to\infty} \frac{\mathrm{Rank}(\{\,1,r,r^2,\ldots,r^{n-1}\,\})}{n/\log_r n} = 1$.

99:08 (Greg Martin) Define a multiplicative function $\tilde\sigma$ (or $\check\sigma$ if you are left-handed) by $\tilde\sigma(p^r) = p^r - p^{r-1} + p^{r-2} - \cdots + (-1)^r$. Note that $\tilde\sigma(n) \le n$ with equality only for $n = 1$. Call n $\tilde\sigma$-perfect if $2\tilde\sigma(n) = n$; examples are $n = 2, 12, 40, 252, 880, 10880$, and 75852. Call n $\tilde\sigma$-k-perfect (or, more generally, $\tilde\sigma$-multiply perfect) if $k\tilde\sigma(n) = n$ for a positive integer k. Two examples of $\tilde\sigma$-3-perfects are $n = 30240$ and $n = 2^{10}3^45^411\cdot13^2\cdot31\cdot61\cdot157\cdot521\cdot683$—there are at least 40 $\tilde\sigma$-3-perfects.

1. Are there any $\tilde\sigma$-k-perfect numbers with $k \ge 4$?
2. Are there infinitely many $\tilde\sigma$-k-perfect numbers?
3. Are there any odd $\tilde\sigma$-3-perfect numbers? Any such number must be a square.

Remarks: Doug Iannucci reports that if there is an odd $\tilde\sigma$-3-perfect number it has at least 18 prime factors, and its largest prime factor exceeds 10^8.

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

Solution: In email of 17 October 2000, Jeff notes that Dan Bernstein has found that the splitting field of $x^5 - x^2 - 2x - 3$ has Galois group A_5 and its ring of integers has a power basis. Examples with S_n were given by Kiran Kedlaya in his talk. See also **000:09**, below.

Problems Proposed 17 & 20 Dec 2000

000:01 (Bjorn Poonen via David Boyd) Classify tetrahedra whose dihedral angles are all rational multiples of π.

Remarks: 1. Let α_{ij} be the angle between faces i and j, with $\alpha_{ii} = 0$; then setting $\det\big(\cos(\alpha_{ij})\big)$ to 0 leads to an equation in roots of unity. There are at least two parametric families of solutions and 44 sporadic examples, discovered jointly with Michael Rubinstein in 1995, although many were known previously.

2. Your editor was directed to this problem by John Conway in 1974, but had no success with it. The problem is connected to that of space-filling tetrahedra, for which see

Michael Goldberg, Three infinite families of tetrahedral space-fillers, J. Combinatorial Theory Ser. A 16 (1974) 348–354, MR 49 #7900.

Marjorie Senechal, Which tetrahedra fill space? Math. Mag. 54 (1981), no. 5, 227–243, MR 83h:52020.

000:02 (M. I. Mostafa) Does the identity

$$\begin{aligned}(x^5+y^5)(z+t)^5 - (x+y)^5(z^5+t^5)& \\ = 5(x+y)(z+t)(xz-yt)(xt-zy)\big((x^2+xy+y^2)(z^2+zt+t^2)-xyzt\big)&\end{aligned}$$

help to determine whether $x^5 + y^5 = z^5 + t^5$ has any solutions in positive integers with $\{\,x,y\,\} \neq \{\,z,t\,\}$?

Remarks: In UPINT, F30, Erdős asks for a polynomial $P(x)$ such that all the sums $P(a) + P(b)$, $0 \le a < b$, are distinct, and Guy notes that x^5 is a likely answer.

000:03 (Kiran Kedlaya) Given a positive integer m is there a finite set S_m such that if z is in $\mathbf{Z}[\zeta_n]$ and $|z|^2 = m$ then $z = \alpha\zeta$ for some α in S_m and some root of unity ζ? If so, how big is S_m?

Remarks: If z is in $\mathbf{Z}[\zeta_n]$ and $|z| = \sqrt{m}$ then every conjugate of z has modulus $\sqrt{m}$, for if z^σ is a conjugate of z then $|z^\sigma|^2 = z^\sigma\overline{z^\sigma} = z^\sigma(\overline{z})^\sigma = (z\overline{z})^\sigma = m^\sigma = m$. In the case $m = 1$ Kronecker's theorem states that if z is an algebraic integer with all conjugates of modulus 1 then z is a root of unity.

On 19 April, Kiran writes, "I proved that for m fixed and p ranging over primes, the set of m-Weil numbers [that is, the set of z in $\mathbf{Z}[\zeta_p]$ with $|z|^2 = m$] in the union of the p-th cyclotomic fields is finite. (That's the union, not the compositum, which would be a stronger result.) There's a preprint on my web page about this: *Weil numbers in prime cyclotomic fields*."

000:04 (no name supplied) Let $p_1, p_2, \ldots$ be the primes, in order, in base 10. Are there infinitely many n for which the concatenation $p_{n+1}p_np_{n+2}$ is prime? Note that 312937 is the first such prime, as the numbers 325, 537, ..., 292331 are all composite.

000:05 (Ron Evans and Marvin Minei) Starting with the b-by-b circulant matrix with first row $(2, 1, 0, 0, \ldots, 0, 1)$, replace the twos on the diagonal by $2\cos(2\pi x)$, $2\cos(4\pi x)$, $2\cos(6\pi x)$,..., $2\cos(2b\pi x)$, in that order, beginning from the upper left. Call the resulting matrix $H(b, x)$. For example,

$$H(4,x) = \begin{pmatrix} 2\cos 2\pi x & 1 & 0 & 1 \\ 1 & 2\cos 4\pi x & 1 & 0 \\ 0 & 1 & 2\cos 6\pi x & 1 \\ 1 & 0 & 1 & 2\cos 8\pi x \end{pmatrix}$$

Suppose that a and b are positive integers such that a/b is close (but not equal) to $1/3$. Representing each of the b (real) eigenvalues of $H(b, a/b)$ by a red dot and plotting these red dots, we end up with a picture that looks very much like the union of three red intervals: $[-1-\sqrt{3}, -2]$, $[1-\sqrt{3}, \sqrt{3}-1]$, $[2, 1+\sqrt{3}]$. The closer a/b gets to $1/3$, the more the picture looks like these three intervals. Explain why!

Remarks: 1. Some might wonder if for large b, the spectrum of $H(b, 1/3)$ also looks like the three intervals above. The answer is no.

2. If one uses c/d in place of $1/3$ in the problem above, where c, d are coprime integers with $0 < c < d$, then instead of 3 intervals, one gets d intervals (which depend on c).

3. For each fraction c/d in Remark 2 with $d < 50$, plot the corresponding d intervals at a height $y = c/d$ on the xy-plane. The resulting picture, which lies in the rectangular region $[-4, 4] \times [0, 1]$, is the famous Hofstadter butterfly (see p. 2241 of Physical Review B, vol. 14, no. 6, September 15, 1976)

000:06 (Greg Martin) Call a rational number r *equidigital base* b if the repeating part of the b-ary expansion of r has all "digits" $\{0, \ldots, b-1\}$ equally often—e.g., $19/24 = .110\overline{01}$ is equidigital base 2. Note that this is not the same definition as given in **99:05**.

1. Are there infinitely many m such that $\frac{a}{2^r m}$ is equidigital base 2 for all a? Such m include 3, 5, 9, 11, 13, 17, and 19. Are there infinitely many m such that $\frac{a}{3^r m}$ is equidigital base 3 for all a? Such m include 7, 14, 19, and 31.

Call r *absolutely simply abnormal* (ASA, for short) if there is no base $b \geq 2$ to which it is equidigital.

2. Characterize the ASA rationals.

Remarks: 1. If q is prime and g is a primitive root (mod q) dividing $q-1$ then a/q is equidigital base g (and thus not ASA).

2. If a/q is equidigital base b, then b divides the multiplicative order of b modulo q^*, where $q^* = \prod_{\substack{p^r \| q \\ p \nmid b}} p^r$. This implies a/q is ASA if $q = 2^r$, $r \geq 1$, also if $q = 15$ or 28.

000:07 (Greg Martin) Is there a symmetric polynomial $h(x, y)$ that gives a bijection between $\{(m, n) \text{ in } \mathbf{N} \times \mathbf{N} : m \geq n\}$ (or $\{(m, n) \text{ in } \mathbf{N} \times \mathbf{N} : m > n\}$) and $\mathbf{N}$?

Remark: It is well-known that $g(x, y) = \frac{(x+y)(x+y+1)}{2} + y$ gives a bijection between $\mathbf{N} \times \mathbf{N}$ and $\mathbf{N}$.

000:08 (Jean-Marie De Koninck) Let $\gamma(n) = \prod_{p|n} p$. Are there any solutions to $\sigma(n) = \big(\gamma(n)\big)^2$ other than $n = 1$ and $n = 1782$?

Remarks: 1. There is no other solution with $n < 10^8$.

2. If there are other solutions they must be even, not squarefree, and not powerful.

3. There are infinitely many n such that $\big(\gamma(n)\big)^2 \mid \sigma(n)$, even restricting n to the form $n = 2^\alpha 3^\beta$, but only three known n such that $\sigma(n) \mid \big(\gamma(n)\big)^2$, namely, $n = 1$, $n = 6$, $n = 1782$.

4. It is easily seen that $\phi(n) = \big(\gamma(n)\big)^2$ has exactly 6 solutions.

000:09 (David Boyd) Is $n^n - (n-1)^{n-1}$ squarefree for infinitely many n? Is it squarefree whenever n is prime?

Remarks: 1. This relates to problem **99:10**. The polynomial $f_n(x) = x^n - x - 1$ has Galois group S_n for $n \geq 2$ (H. Osada, J. Number Theory 25 (1987) 230–238) and its discriminant Δ_n satisfies $|\Delta_n| = n^n + (-1)^n(n-1)^{n-1}$. If $|\Delta_n|$ is squarefree and α is a root of $f_n(x)$ then the ring of integers in $\mathbf{Q}(\alpha)$ has a power basis.

2. In email of 16 March 2001, Boyd notes that $n^n - (n-1)^{n-1}$ is the absolute value of the discriminant of $x^n - x + 1$, which is reducible when $n = 6k + 2$. This explains the factor $(12k^2 + 6k + 1)^2$ which he had earlier found to appear in this case. For $n \leq 100$ and not of the form $6k + 2$ Maple finds no small square factors.

3. Greg Martin points out that if p is prime and $4^{p-1} \equiv 1 (\mathrm{mod}\ p^2)$ (e.g., if $p = 1093$ or 3511) and $n = p^2 - 3p + 2$ then $p^2 \mid \Delta_n$. Note that any such n is necessarily a multiple of 6.

4. In email of 20 February 2001, Greg writes, "if p^2 divides $n^n - (n-1)^{n-1}$, then p^2 will divide $m^m - (m-1)^{m-1}$ for every m congruent to n modulo $p(p-1)$. I've computationally found about 250 examples of such divisibilities for n not of the form $6k+2$ (not counting the repetitions generated by the previous remark); the smallest found is $59^2 \mid 257^{257} - 256^{256}$. In particular, these last two statements imply that there are infinitely many primes p for which $p^p - (p-1)^{p-1}$ is not squarefree, by Dirichlet's theorem on primes in AP."

000:10 (Jeff Lagarias via Kiran Kedlaya) What is the minimum of the absolute value of the discriminant of a monic irreducible polynomial of degree n with integer coefficients? It is at least c^n, with c taken from Odlyzko's discriminant bounds; is it $\Omega(n^{cn})$?

Remark: David Boyd refers to

Denis Simon, Construction de polynômes de petits discriminants, C. R. Acad. Sci. Paris 239 (1999) 465–468.

000:11 (Jeff Lagarias) Let $\|x\|$ be the distance from x to the nearest integer. Is it true that $S = \{\, (\alpha, \beta) \text{ in } (0,1) \times (0,1) : \liminf_{q \to \infty} q\|q\alpha\|\|q\beta\| > 0 \,\}$ has Hausdorff dimension zero?

Remarks: Littlewood's conjecture is that S is empty. It is not known that the Hausdorff dimension of S is less than 2. Jeff mentions

Andrew D. Pollington, Sanju L. Velani, On a problem in simultaneous Diophantine approximation: Littlewood's conjecture, Acta Math. 185 (2000) 287–306

as a pointer to what is currently knnown about Littlewood's conjecture.

000:12 (Kevin O'Bryant) Given a sequence $a_1, a_2, \ldots$ of integers, with bounded gaps ($M_1 < a_{i+1} - a_i < M_2$), must there be distinct indices i_1, i_2, i_3 in arithmetic progression with $a_{i_1}, a_{i_2}, a_{i_3}$ also in arithmetic progression? Given a sequence $\mathbf{a}_1, \mathbf{a}_2, \ldots$ of elements in $\mathbf{Z}^d$ with $\|\mathbf{a}_{i+1} - \mathbf{a}_i\|$ bounded (where $\|\mathbf{a}\|$ is any reasonable norm on $\mathbf{Z}^d$), and given an integer $k \geq 3$, must there be indices $i_1, \ldots, i_k$ with $\mathbf{a}_{i_1}, \ldots, \mathbf{a}_{i_k}$ in arithmetic progression (that is, with $\mathbf{a}_{i_{j+1}} - \mathbf{a}_{i_j} = \mathbf{a}_{i_2} - \mathbf{a}_{i_1}$ for $1 \leq j \leq k-1$)?

Remarks: 1. Greg Martin asks whether $M_1 < a_{i+1} - a_i < M_2$ is enough to ensure that there are three distinct collinear points of the form (i, a_i).

2. One can inductively define sequences of integers which have no three terms in A.P. and which furthermore satisfy various greedy conditions. For example, the sequence $(a_i) = 1, 2, 4, 5, 8, 9, 11, 12, 16, 18, 19, 21, 26, 28, 29, 32, 33, 35, 36, 39, 43, 44, 46, \ldots$ is obtained by insisting the sequence be increasing with each new term chosen as small as possible. For the sequence $(b_i) = 1, 1, 2, 1, 1, 2, 2, 4, 4, 1, 1, 2, 1, 1, 2, 2, 4, 4, 2, 4, 4, 5, \ldots$ we drop the insistence that the sequence be increasing. In the sequence $(c_i) = 0, 0, 1, 1, 0, 0, 1, 1, 3, 3, 4, 4, 3, 3, 4, 4, 1, 1, 2, 2, 1, 1, 2, 2, 4, 4, 5, 5, 4, 4, 5, 5, 10, \ldots$ each term c_{n+1} is the first permissible term among $c_n, c_n + 1, c_n - 1, c_n + 2, c_n - 2, \ldots$. What is the rate of growth of a_n? Is $a_{n+1} - a_n$ bounded? What are the rates of growth of $\sum^n b_k$ and $\sum^n c_k$? Are b_k, $|b_{k+1} - b_k|$, c_k, $|c_{k+1} - c_k|$ bounded? Is $c_k \geq 0$ for all k?

In email of 13 Feb 01, Carl Pomerance supplies some relevant references, one of which answers Greg Martin's query in the affirmative. The annotations are Carl's.

T. C. Brown, Is there a sequence on four symbols in which no two adjacent segments are permutations of one another, Amer. Math. Monthly 78 (1971) 886–888.

From Brown's work it follows that in O'Bryant's problem, if the gap size is bounded by 3, then in any 9 consecutive terms, three of the points (i, a_i) will be collinear. Here, 9 is best possible, as can be seen by the sequence $0, 1, 3, 4, 7, 8, 10, 11$.

F. M. Dekking, Strongly nonrepetitive sequences and progression-free sets, JCT-A 27 (1979) 181–185, MR 81b:05027.

Dekking shows that there is an infinite sequence of plane lattice points where each gap is $(0, 1)$ or $(1, 0)$ such that no 5 points are in AP.

J. L. Gerver and L. T. Ramsey, On certain sequences of lattice points, Pacific J. Math. 83 (1979) 357–363, MR 80k:10053.

Gerver and Ramsey show that in an infinite sequence of plane lattice points with bounded gaps, there are arbitrarily many that are collinear, thus answering Martin's question.

C. Pomerance, Collinear subsets of lattice point sequences—an analog of Szemerédi's theorem, JCT-A (1980) 140–149 MR 81m:10104.

I generalize the Gerver-Ramsey theorem, so that now it is only assumed that the gaps are bounded on average: that is, it is assumed there is a constant B such that the sum of the lengths of the first n gaps in the sequence is at most Bn, and this is true for each n. In such a sequence of plane lattice points, there must be arbitrarily many that are collinear.

000:13 (Gerry Myerson) Is there an irredundant set of covering congruences with exactly two odd moduli? exactly three?

Remark: A set of covering congruences (for short: a cover) is a finite set of congruences $x \equiv a_1 (\mathrm{mod}\ m_1), \ldots, x \equiv a_r (\mathrm{mod}\ m_r)$ with $1 < m_1 < \cdots < m_r$ such that every integer satisfies at least one of the congruences. A cover is irredundant if no proper subset is a cover. An example is given by the (a_i, m_i) pairs $(0,2), (0,3), (1,4), (1,6), (11,12)$. A notorious problem is to decide the existence of a cover with no even modulus. It is known that an irredundant cover cannot have exactly one even modulus, and the example given above has exactly four even moduli.

000:14 (Gerry Myerson) Is it true that for all integers a with $|a| \geq 2$ and all non-zero integers b there is an integer k relatively prime to b such that $ka^n + b$ is composite for all n? Variation: let $u_n = u_n(a,b,k) = ka^n + b$, let $d = d(a,b,k) = \gcd(u_0, u_1, \ldots)$. Given a and b as above, must there be an integer k such that $d^{-1}u_n$ is composite for all k?

Remark: The case $a = 2$, $b = 1$ was settled (in the affirmative) by Sierpiński. His second proof relied on a result of Erdős to the effect that there exist odd numbers k such that $2^n + k$ is composite for all n. Erdős' proof relied on covering congruences. The general case could be settled if we knew that covering congruences with certain specified properties exist, but these existence questions are very difficult.

W. Sierpiński, Sur un problème concernant les nombres $k \cdot 2^n + 1$, Elem. Math. 15 (1960) 73–74, MR 22 #7983.

P. Erdős, On integers of the form $2^k + p$ and some related problems, Summa Brasil. Math. 2 (1950) 113–123, MR 13, 437i

000:15 (Alexander Schwartz via Gerry Myerson) Can $\mathbf{Z} \oplus \mathbf{Z}$ be partitioned into cosets $C_1, \ldots, C_n$ of distinct proper subgroups for some n?

Remarks: It is known that $\mathbf{Z}$ cannot be so partitioned, that is, $\mathbf{Z}$ is not the finite disjoint union of arithmetic progressions with distinct common differences exceeding 1. There are such partitions for $\mathbf{Z} \oplus \mathbf{Z} \oplus \mathbf{Z}$ (in fact, for $\mathbf{Z}^n$ for any $n \geq 3$), e.g., $\mathbf{Z}^3$ is the disjoint union of $\{\,(x,y,z) : x \text{ is odd and } y \text{ is even}\,\}$, $\{\,(x,y,z) : y \text{ is odd and } z \text{ is even}\,\}$, $\{\,(x,y,z) : z \text{ is odd and } x \text{ is even}\,\}$, $\{\,(x,y,z) : x, y, z \text{ all odd or all even}\,\}$.

The question can also be asked at the level of finite abelian groups. No cyclic group is a disjoint union of cosets of distinct proper subgroups. $(\mathbf{Z}/2\mathbf{Z})^3$ is the disjoint union of $(1,0,0) + \langle (0,0,1) \rangle$, $(0,1,0) + \langle (1,0,0) \rangle$, $(0,0,1) + \langle (0,1,0) \rangle$, and $\langle (1,1,1) \rangle$, and similar constructions apply to $(\mathbf{Z}/2\mathbf{Z})^m$, $m > 3$. Do there exist m and n such that $\mathbf{Z}/m\mathbf{Z} \oplus \mathbf{Z}/mn\mathbf{Z}$ can be partitioned this way?

Is there such a partition for $(\mathbf{Z}/m\mathbf{Z})^3$ for all $m \geq 2$?

Solution: Schwartz answers this last question in the affirmative. Let p be an odd prime, let n be a quadratic non-residue (mod p), let $G_{a,b}$ be the subgroup of $(\mathbf{Z}/p\mathbf{Z})^3$ generated by $(a,b,1)$, $0 \leq a \leq p-1$, $0 \leq b \leq p-1$, and let $C_{a,b}$ be the coset of $G_{a,b}$ containing $(nb, a, 0)$. It is routine to show that the cosets partition $(\mathbf{Z}/p\mathbf{Z})^3$, and then routine to extend the result to $(\mathbf{Z}/m\mathbf{Z})^3$, or, indeed, to $\mathbf{Z}/r\mathbf{Z} \oplus \mathbf{Z}/rs\mathbf{Z} \oplus \mathbf{Z}/rst\mathbf{Z}$ for any positive integers r, s, t, $r > 1$.

Schwartz also shows that $\mathbf{Z}/m\mathbf{Z} \oplus \mathbf{Z}/mn\mathbf{Z}$ has no partition when m and n are both powers of some prime p, but the general case remains unsolved.