SOME HINTS AND ANSWERS (#2)
TO 18.S34 SUPPLEMENTARY PROBLEMS
(FALL 2007)

55. (b) See F. Ardila, The number of halving circles, *Amer. Math. Monthly* **111** (2004), 586–592.

56. (a) Let p be a prime dividing k. Since $n^5-1=(n-1)(n^4+n^3+n^2+n+1)$, we have that p divides n^5-1, i.e., $n^5 \equiv 1 \pmod{p}$. Also

$$(n-1)(n^3+2n^2+3n+4)-(n^4+n^3+n^2+n+1)=-5.$$

Thus either $p=5$ or p doesn't divide $n-1$ [why?]. In other words, $p=5$ or $n \not\equiv 1 \pmod{p}$.

Assume that $p \neq 5$. Let t be the least positive integer for which $n^t \equiv 1 \pmod{p}$. A standard property of congruences states that if $n^m \equiv 1 \pmod{p}$, then t divides m. Since $n^5 \equiv 1 \pmod{p}$ but $n \not\equiv 1 \pmod{p}$, we have $t=5$. Note that n is not divisible by p since $n^5 \equiv 1 \pmod{p}$. Hence by Fermat's theorem we have $n^{p-1} \equiv 1 \pmod{p}$. Thus $p-1$ is divisible by 5, as desired. Since every prime factor of k is congruent to 0 or 1 $\pmod{5}$, the same is true for k, completing the proof.

(b) This is immediate from (a). Essentially the same argument shows that there are infinitely many primes of the form $qn+1$ for any fixed prime q. With a little more work one can show there are infinitely many primes of the form $qn+1$ for any $q>1$. It is in fact true that there are infinitely many primes of the form $qn+r$ for any fixed relatively prime integers q and r, but this is much harder to prove.

60. (c) The surprising answer is that it is *impossible* to reach a point with x-coordinate equal to 5. See R. Honsberger, *Mathematical Gems II*, Mathematical Association of America, 1976, Chapter 3.

68. If n is even, then x^4+4^n is even and greater than 2. If n is odd, say $n=2m+1$, then

$$n^4+4^n=n^4+4(2^m)^4=(n^2+2\cdot 4^m-2^{m+1})(n^2+2\cdot 4^m+2^{m+1}).$$

70. $h(n) = 1+\binom{n}{2}+\binom{n}{4}$. For an elegant proof see R. Honsberger, *Mathematical Morsels*, Mathematical Association of America, 1978, Problem 3.

71. The motion of the fly is not precisely defined by the conditions of the problem. The fly could be anywhere between the man and the point $x = 0$, for if we put the fly in any such position and let time run backwards, then both the man and the fly end up at $x = 0$ after one hour.

72. See J. Borwein and K.-K. S. Choi, On the representations of $xy+yz+xz$, *Experiment. Math.* **9** (2000), 153–158;

    `http://projecteuclid.org/Dienst/UI/1.0/Summarize/euclid.em/1046889597`.

73. Yes. Let w be the *Fibonacci word* that is the unique fixed point of the transformation $0 \to 01$ and $1 \to 0$. Equivalently, we have $w = x_1x_2\cdots$ where $x_1 = 0$, $x_2 = 10$, and $x_{i+1} = x_{i-1}x_i$ for $i \geq 2$. Thus

$$w = 01001010010010100 1010\cdots.$$

    Then w is not eventually periodic, and every prefix of w of length at least 6 ends in a square of length at most 5.

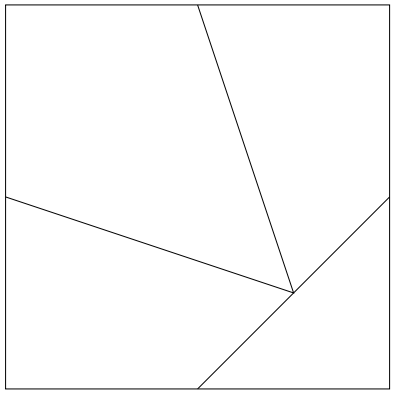
79. In general, if a point p is in the interior of an equilateral triangle of size d and is at distance a, b, c from the vertices, then

$$3(a^4 + b^4 + c^4 + d^4) = (a^2 + b^2 + c^2 + d^2)^2.$$

    Note the curious symmetry between a, b, c, d. The symmetry between a, b, c is obvious, but why also d? (A simple, noncomputational reason can be given.) For the case $a = 3$, $b = 4$, $c = 5$, we have $d = \sqrt{25 + \sqrt{3}}$.

    For some references and generalizations, see R. J. Gregorac, A general 3-4-5 puzzle, *European J. Combinatorics* **17** (1996), 533–541.

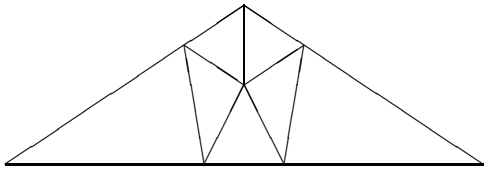
80. Four, as shown in the figure below.



This famous dissection is due to Henry E. Dudeney. A good general reference to problem of this nature is H. Lindgren, *Recreational Problems in Geometric Dissections and How to Solve Them*, revised and enlarged by G. Frederickson, Dover, New York, 1972. See page 25 for the "reason" behind the figure above. Moreover, on page 9 is a dissection of a square into five pieces that can be reassembled into *two* congruent equilateral triangles. A further reference is Chapter 4 of M. Gardner, *The Unexpected Hanging and Other Mathematical Diversions*, Simon and Schuster, New York, 1969.

81. HINT: Consider the largest power of 2 dividing any of $1, 2, \ldots, n$.

83. Two proofs may be found in Solution to Problem 11114, *Amer. Math. Monthly* **113** (2006), pp. 760–761. The first proof is elementary, while the second is an elegant argument based on 2-adic analysis.

92. 

93. ANSWER: $f(p,q) = \dfrac{p(1-q)}{p(1-q)+q(1-p)}$

95. Let $u = (1-xy)^{-1}$ and $v = (1-yx)^{-1}$. Note that $(1-yx)y = y(1-xy)$,

and therefore $yu = vy$. Thus

$$\begin{aligned}(1+x)v(1+y) &= v + xv + yu + xyu \\ &= v + xv + yu + u - (1-xy)u \\ &= u + v + xv + yu - 1.\end{aligned}$$

This last expression is symmetric with respect to the permutation (written in disjoint cycle form) $(x, y)(u, v)$, so an affirmative answer follows. This argument is due to S. Fomin.

A vast generalization is due to D. Krob in *Topics in invariant theory* (M.-P. Malliavin, ed.), Lecture Notes in Math., vol. 1478, Springer-Verlag, Berlin/Heidelberg/New York, 1991, pp. 215–243. (A short discussion also appears in §8 of C. Reutenauer, in *Formal Power Series and Algebraic Combinatorics (New Brunswick, NJ, 1994)*, DIMACS Series Discrete Math. Theoret. Comput. Sci. **24**, American Mathematical Society, Providence, RI, 1996, pp. 159–169.) Namely, *any* identity in noncommutative variables which holds when formally expanded into power series continues to hold in any ring for which the identity is defined.

97. The nth term is the number 16 written in base $17 - n$, so the missing term is 121.

98. These are the positive integers whose spelling begins with the letter t.

100. When we rotate ourselves 180° to compare ourselves with our mirror image, there is a preferred axis of rotation, namely, the up-down axis. Rotation about this axis reverses left and right. We can imagine instead rotating about a line that passes through our two hips, say. In this case, up and down *would* be reversed, but not left and right. It is the earth's gravity that leads to our preferred axis of rotation.

103. See R. Honsberger, *Mathematical Morsels*, problem 12, and Ian Stewart, Pursuing polygonal privacy, *Scientific American*, February 2001, pp. 88–89.

104. In general, if the ladders are of length a and b (with $a \geq b$) and the height of their intersection is c, then their distance x apart is given by

$$x^4 - 2cx^3 + (a^2 - b^2)x^2 - 2c(a^2 - b^2)x + c^2(a^2 - b^2) = 0,$$

Here $a = 119,\ b = 70,\ c = 30,\ x = 56$. See M. Gardner, *Mathematical Circus*, Knopf, New York, 1979, page 62.

105. (a) Let $x = (x_1, x_2, \ldots)$. Since 2^n and 3^n are relatively prime, there are integers a_n and b_n for which $x_n = a_n 2^n + b_n 3^n$. Hence $f(x) = f(y)+f(z)$, where $y = (2a_1, 4a_2, 8a_3, \ldots)$ and $z = (3b_1, 9b_2, 27b_3, \ldots)$. Now for any $k \geq 1$ we have

$$\begin{aligned} f(y) &= f(2a_1, 4a_2, \ldots, 2^{k-1}a_{k-1}, 0, 0, \ldots) \\ &\quad + f(0, 0, \ldots, 0, 2^k a_k, 2^{k+1}a_{k+1}, \ldots) \\ &= 0 + 2^k f(0, 0, \ldots, 0, a_k, 2a_{k+1}, 4a_{k+2}, \ldots). \end{aligned}$$

Hence $f(y)$ is divisible by 2^k for all $k \geq 1$, so $f(y) = 0$. Similarly $f(z)$ is divisible by 3^k for all $k \geq 1$, so $f(z) = 0$. Hence $f(x) = 0$.

(b) Let $a_i = f(e_i)$. Define integers $0 < n_1 < n_2 < \cdots$ such that for all $k \geq 1$,

$$\sum_{i=1}^{k} |a_i| 2^{n_i} < \frac{1}{2} 2^{n_{k+1}}.$$

(Clearly this is possible — once $n_1, \ldots, n_k$ have been chosen, simply choose n_{k+1} sufficiently large.) Consider $x = (2^{n_1}, 2^{n_2}, \ldots)$. Then

$$\begin{aligned} f(x) &= f(a_1 e_1 + \cdots + a_k e_k + 2^{n_{k+1}}(e_{k+1} + 2^{n_{k+2}-n_{k+1}} e_{k+2} + \cdots)) \\ &= \sum_{i=1}^{k} a_i 2^{n_i} + 2^{n_{k+1}} b_k, \end{aligned}$$

where $b_k = f(e_{k+1} + 2^{n_{k+2}-n_{k+1}} e_{k+2} + \cdots)$. Thus by the triangle inequality,

$$\begin{aligned} |2^{n_{k+1}} b_k| &< \left| \sum_{i=1}^{k} a_i 2^{n_i} \right| + |f(x)| \\ &< \frac{1}{2} 2^{n_{k+1}} + |f(x)|. \end{aligned}$$

Thus for sufficiently large k we have $b_k = 0$ [why?]. Since

$$b_j - 2^{n_{j+2}-n_{j+1}} b_{j+1} = f(e_{j+1}) \quad \text{[why?]},$$

we have $f(e_k) = 0$ for k sufficiently large.

106. This identity has been verified to over 20,000 decimal digit accuracy. See J. M. Borwein and D. H. Bailey, *Mathematics by Experiment: Plausible Reasoning in the 21st Century*, A K Peters, Natick, MA, 2004 (pages 90–91).

109. The smallest n such that the solution x to

$$\frac{3}{2}\left(3 \cdot 10^n + x\right) = 10x + 3$$

is an integer is $n = 15$, yielding

$$3 \cdot 10^n + x = 3529411764705882.$$

110. (b) $\alpha = e^{1/e}$

111. For some references and recent work related to this problem (where one has stamps of value $a_1, \ldots, a_n$), see P. Erdős and R. L. Graham, *Old and New Problems in Combinatorial Number Theory*, pp. 85–86, and `mathworld.wolfram.com/CoinProblem.html`. A interesting recent paper is A. Barvinok and K. Woods, Short rational generating functions for lattice point problems, `www.math.lsa.umich.edu/~barvinok/sem.ps`.

112. $x = 3 - 2\sqrt{2} = 0.17157287\cdots$

113. The best way to understand this problem is *via* the theory of ordinal numbers (which is taught in beginning courses in logic or set theory). Let ω denote the first infinite ordinal (the ordinal number of the sequence $1, 2, 3, \ldots$). In the total b_n-ary expansion of a_n, replace each b_n with ω. This defines a certain ordinal number α_n. From the definition of a_i it follows immediately that α_{n+1} is a *smaller* ordinal number than α_n unless no b_n's appear in the total b_n-ary expansion of a_n. But a strictly decreasing sequence of ordinal numbers must be finite, so some a_n must have only 1's in its complete b_n-ary expansion (equivalently, $a_n < b_n$), and the proof follows. For some further examples of procedures that unexpectedly terminate, see Chapter 2 of M. Gardner, *The Last Recreations*. For further information see

`http://en2.wikipedia.org/wiki/Goodstein's_theorem`

114. An arbitarily large overhang can be achieved. The first appearance of this result seems to be Problem 3009, *American Math. Monthly* **30** (1923), 76. For further information and references see

`http://mathworld.wolfram.com/BookStackingProblem.html`.

115. (knowledge of linear algebra assumed) Let $n = \#V(G)$. Let A be the adjacency matrix of G mod 2, i.e., with entries in the finite field $\mathbb{F}_2$. Let I denote the $n \times n$ identity matrix, and y the $n \times 1$ row vector of all 1's. We need to show that y is in the row space of $A + I$ [why?]. Now in general we know from linear algebra that if M is any $m \times n$ matrix and z is any $n \times 1$ row vector, then z is in the row space of M if and only if $zv = 0$ whenever $Mv = 0$ (where v is an $n \times 1$ column vector). For the special case that $z = y$, we obtain the following: y is in the row space of M if and only if there do not exist an odd number of rows of M whose sum is the 0 vector. Assume then that there are an odd number of rows of $A + I$ whose sum is 0, say the rows indexed by vertices $v_1, \ldots, v_k$. Let H be the subgraph of G induced by the vertices $v_1, \ldots, v_k$. Let $A + I = (b_{ij})$. Since $\sum_{i=1}^{k} b_{ij} = 0$ for $1 \leq j \leq n$ and $b_{ii} = 1$, it follows that every vertex of H has odd degree. This is impossible since H has an odd number of vertices, a contradiction that completes the proof.

    A special case of this problem was open for several years until K. Sutner, a graduate student at the time, found a proof by linear algebra more complicated than the above prood. The above proof is due to Yair Caro, *Ars Combinatoria* **42** (1996), 175–180.

    NOTE. This problem is equivalent to Problem 10 from the Linear Algebra and Determinants problem set.

116. The farthest distance is $\sqrt{130}/4 \approx 2.8504\cdots$. This problem is due to Yoshiyuki Kotani. It belongs to the genre known as "Spider and Fly problems," as does Problem 91 from Supplementary Problem Set #8. See Dick Hess, Kotani's ant problem, in *Puzzlers' Tribute* (D. Wolfe and T. Rogers, eds.), A K Peters, Natick, MA, 2002, pp. 407–411.

118. (e) Suppose to the contrary that every integer can be uniquely written in exactly one of the forms $m_i x + a_i$. By adjusting the value of a_i

modulo m_i we can assume that $0 \le a_i < m_i$. This implies [why?] the generating function identity

$$\frac{1}{1-z} = \frac{z^{a_1}}{1-z^{m_1}} + \frac{z^{a_2}}{1-z^{m_2}} + \cdots + \frac{z^{a_k}}{1-z^{m_k}}.$$

Multiply both sides by $(1-z^{m_1})\cdots(1-z^{m_k})$, and let $\zeta = e^{2\pi i/m_k}$, a primitive m_kth root of unity. The left-hand side then vanishes at $z = \zeta$; but since m_k is larger than all the other m_i's the right-hand side doesn't vanish at $z = \zeta$, a contradiction.

119. (a) ANSWER: $1/(1-x)$. One can view this result as the "analytic form" of the uniqueness of the binary expansion of a nonnegative integer.

(b) This remarkable result goes back to M. A. Stern in 1858. For further information and references, see `www.math.uiuc.edu/~reznick/stern.pdf`. A forthcoming paper by Bruce Reznick entitled "A Stern introduction to combinatorial number theory" should be the definitive reference.

(c) This astonishing result was proved by David Newman in 2002.

121. If m and n are integers and f is a polynomial with integer coefficients, then it follows from elementary properties of congruences that $f(\ m\ +\ t\ ) \equiv f(m) \pmod{t}$, where m and t are integers. Let $t = f(m)$ to get

$$f(m + f(m)) \equiv f(m) \pmod{f(m)},$$

so

$$f(m + f(m)) \equiv 0 \pmod{f(m)}.$$

Since f is nonconstant we can find infinitely many values of m for which $|f(m)| > 1$ and the numbers $m + f(m)$ are all distinct. Thus $f(n)$ is composite for the infinitely many distinct values $n = m + f(m)$ for which $|f(m)| > 1$.

123. Person A must have a "rule" for deciding what numbers y and $y/2$ to write down. Such a rule is essentially a probability distribution f on the positive real numbers. Thus the probability $P(a,b)$ that the two numbers y and $y/2$ satisfy $a \le y \le b$ is $P(a,b) = \int_a^b f(y)dy$. (If some of the probability distribution is discrete, so that the probability

$P(y)$ of writing down y and $y/2$ is positive, then the integral must be interpreted as a sum over the discrete part and an integral over the continuous part.) From the statement of the problem it follows that $f(x) = f(2x)$ for all x, i.e., it is assumed that it is equally likely that x and $x/2$ are written down as x and $2x$. However, it is not hard to show that there does not exist a probability distribution f with this property.

124. See C. Freiling and D. Rinne, Tiling a square with similar rectangles, *Math. Res. Lett.* **1** (1994), 547–558, and M. Laczkovich and G. Szekeres, Tilings of the square with similar rectangles, *Discrete Comput. Geom.* **13** (1995), 569–572.

125. See F. Ardila, *Fibonacci Quart.* **42** (2004), 202–204; `math.CO/0409418`.

126. Yes. More generally, if m and n are relatively prime positive integers such that f^m and f^n are infinitely differentiable, then so is f. This is a result of Henri Joris in 1982. For a simple proof, see R. Myer, *Amer. Math. Monthly* **112** (2005), 829–831.

129. Note that $\frac{1}{2}(p+q)$ is not prime.

130. Answer:

$$\frac{1}{6}\log\Big(x^6+12x^5+45x^4+44x^3-33x^2+43 \\ +(x^4+10x^3+30x^2+22x-11)\sqrt{x^4+4x^3-6x^2+4x+1}\Big).$$

See solution to Advanced Problem 5812, *American Math. Monthly* **79** (1972), 1144–1146.

132. See P. Erdős and R. L. Graham, On packing squares with equal squares, *J. Combinatorial Theory (A)* **19** (1975), 119–123. A more recent reference is E. Friedman, Packing unit squares in squares: a survey and new results, *Elec. J. Combinatorics* DS7; available at

`http://www.combinatorics.org/Surveys`.

133. Hint. Consider the triangle of least altitude formed by any three of the points that don't lie on a line.

134. This result is due to David Gale and Richard Karp, as a special case of a more general result appearing in *J. Comput. System Sci.* **6** (1972), 103–115. One way to prove it is as follows. It suffices to show that if N is a matrix whose rows are in increasing order, then sorting the columns into increasing order keeps the rows increasing. Clearly [why?] we can assume that N has only two columns c_1 and c_2. If the entries of c_2, written in increasing order, are $y_1 \leq y_2 \leq \cdots \leq y_m$, then y_i is at least as large as the i elements in c_1 in the same rows as $y_1, y_2, \ldots, y_i$. Hence y_i is at least as large as the ith smallest element x_i of c_1. But after we sort the two columns of N the ith row is $[x_i, y_i]$, so this row is increasing. Another reference is pages 184–185 of M. Gardner, *The Last Recreations*. For a generalization see B. Tenner, A Non-messing-up phenomenon for posets, `math.CO/0404396`.

139. Surprisingly, the proof of this result requires the classification of finite simple groups! See W. Feit, Some consequences of the classification of finite simple groups, in *The Santa Cruz Conference on Finite Groups*, Proc. Sympos. Pure Math. **37**, American Mathematical Society, Providence, RI, 1980, pp. 175–181.

Solution to #22 of "Problems on Congruence and Divisibility"

19. No. Note that [why?]

$$a_n = \frac{1}{n-1}(a_{n-1}^2 + (n-2)a_{n-1}),\ n \geq 3.$$

Working modulo 43, it is easy to compute $a_0, a_1, \ldots, a_{43}$, all mod 43. (Note that we never have to divide by 43 in the process of computing these numbers.) We can then check that $a_{43}^2 + 42 \cdot a_{43} \equiv 24 \pmod{43}$. Hence a_{44} is not an integer (its denominator is divisible by 43). An interesting point about this problem is that it's computationally infeasible to compute a_{44} exactly. There's also the interesting question of why $p = 43$ is the smallest prime for which the above argument works. For further discussion, see

www-groups.dcs.st-and.ac.uk/∼john/Zagier/Solution5.3.html.

Comments on #18 of "Problems on Linear Algebra and Determinants"

Let us call an integer n satisfying the conditions of the problem *permissible*. Then the permissible integers are precisely 1,2,4, or 8. Suppose that A is an n-dimensional division algebra over $\mathbb{R}$, not necessarily associative or commutative. Thus A is an n-dimensional vector space over $\mathbb{R}$ with a binary multiplication compatible with the vector space structure (i.e., $\alpha(xy) = (\alpha x)y = x(\alpha y)$ for $\alpha \in \mathbb{R}$, $x, y \in A$) satisfying (1) A has a multiplicative identity 1, and (2) every $0 \neq x \in A$ has a multiplicative inverse y, i.e., $xy = yx = 1$. We can regard any element $x \in A$ as defining a linear transformation $T_x : A \to A$ via $T_x(y) = xy$. The set $\{T_x : x \in A\}$ is then an n-dimensional space of linear transformations on A for which every nonzero element is invertible. Regarding these linear transformations as matrices shows that n is permissible.

It is well-known that the above division algebras A exist for $n = 1, 2, 4, 8$, namely, $\mathbb{R}$ ($n = 1$), $\mathbb{C}$ ($n = 2$), the quaternions ($n = 4$), and the octonions or Cayley numbers ($n = 8$). Hence these values of n are permissible.

It is a very deep result that there do not exist division algebras A (over $\mathbb{R}$) of dimensions other than $1, 2, 4, 8$. Moreover, it can be shown that if n is permissible, then there exists an n-dimensional real divison algebra. Hence $1, 2, 4, 8$ are the only permissible values of n. See e.g. mathworld.wolfram.com/DivisionAlgebra.html for some references. These results are proved by connecting them with a third problem, namely, for which n do there exist $n-1$ linear independent nonvanishing vector fields on an $(n-1)$-sphere? (Such spheres are called *parallelizable*.)

Given any n, let $f(n)$ denote the maximum dimension of a space V of $n \times n$ real matrices such that all nonzero elements of V are invertible. (Thus $f(n) = n$ if and only if $n = 1, 2, 4, 8$.) Write $n = (2a + 1)2^{c+4d}$, where $0 \leq c \leq 3$. Then Adams proved in *Ann. Math. (2)* **75** (1962), 603–632 (in the context of vector fields), that $f(n) = 2^c + 8d$. In particular, $f(n) = 1$ if n is odd. A simple proof follows from the fact that if A, B are two nonzero square matrices of the same odd order, then $\det(A + xB)$ is a polynomial in x of odd degree and therefore has a real zero.