Western Number Theory Problems, 16 & 19 Dec 1995

Edited by Richard K. Guy & Gerry Myerson

for mailing prior to 1996 (Las Vegas) 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 (present set)	95:01–95:19

[With comments on: 90:14, 94:07, 94:12, 94:13, 94:15, 94:26]

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

COMMENTS ON ANY PROBLEM WELCOME AT ANY TIME

Centre for Number Theory Research,
MPCE Building E7A,
Macquarie University,
NSW 2109 Australia.
gerry@mpce.mq.edu.au Australia-2-9850-8952 fax 9850-8114

15 Aug 96

COMMENTS ON EARLIER PROBLEMS

90:14 (D.H. and Emma Lehmer) Let $p = n^2 + 108 = 6f + 1 = 109, 157, 229, 277, 397, \ldots$ be a prime, and

$$\eta_j = \sum_{i=0}^{f-1} \zeta_p^{g^{6i+j}}$$

(ζ_p is a primitive p-th root of unity) be the Gaussian periods of degree 6. Let

$$\delta_j = \eta_j - \eta_{j+k} \qquad\qquad k \perp 6$$

(i.e., k is prime to 6) Then the δ_j satisfy the sextic

$$G(x) = x^6 - p(x-1)^2(x-2)^2 = 0$$

so that

$$G(1) = \prod_{j=0}^{5}(\eta_j - \eta_{j+k} - 1) = 1$$

and hence $\rho_j = \eta_j - \eta_{j+k} - 1$ is a unit. Is ρ_j a fundamental unit? [These primes do not have translation units.]

For $e = 5$ there is only one prime, $p = 211$, known to have this property.

[Editor's note: I think this means that 211 is the only prime of the form $5f + 1$ for which it is known that $\eta_j - \eta_{j+k} - 1$ is a unit, where η_j is a Gaussian period of degree 5.]

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 gives the following solution to (b):

We answer Part (b) by proving that $\lim_{n\to\infty} a_n = 0$. To begin, consider the derivatives of the functions:

$$f_n' = n!x^{n-1} + \cdots + 2x - 1.$$

Each derivative f_n' can be expressed as $g_n(x) - 1$, where $g_n(x)$ is a polynomial with no constant term and only non-negative coefficients. In particular, on $[0, \infty)$, $g_n(x)$ assumes 0 at $x = 0$ and increases.

By elementary calculus, it follows that a_n can be characterized by the properties

1. $g_n(x) < 1$ for $0 \le x < a_n$, and
2. $g_n(x) > 1$ for $a_n < x \le 1$.

Clearly $a_n < 1/2$ for all n. To show that $\lim_{n\to\infty} a_n = 0$, it suffices to prove that, for any $r \in (0,1]$, there is an N such that $g_n(r) > 1$ for every $n > N$. In fact, since $g_n(X)$ is a sum of positive monomials, it suffices to prove the inequality with a single term in place of $g_n(x)$.

Standard theory proves that for any $r > 0$,

$$\lim_{n\to\infty} n! r^{n-1} = \infty$$

In the present context, this remark proves Part (b).

This method will produce estimates for $f_n(a_n)$ as well. (That is Part (a) of the problem.) The derivative of f_n stays between 0 and 1 on $(0, a_n)$. Consequently, $f_n(a_n)$ must lie between $f_n(0) = \frac{n}{n+1}$ and $\frac{n}{n+1} - a_n$. For n large, the latter is a very narrow range.

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. The results will appear in

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

which was presented at CANT'95 at Macquarie University, Sydney, last April. These numbers were mentioned in

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

and Carl Pomerance sends the further references:

G. G. Dandapat, J. L. Hunsucker & C. Pomerance, Some new results on odd perfect numbers, *Pacific J. Math.*, **57**(1975) 359-364.

J. L. Hunsucker & C. Pomerance, There are no odd super perfect numbers less than $7 \cdot 10^{24}$, *Indian J. Math.* **17**(1975) 107-120.

In the first it is shown that if n is odd and super perfect, then neither n nor $\sigma(n)$ is a prime power, and that either n or $\sigma(n)$ has at least 3 distinct prime factors. In the second the title theorem is proved and in an unpublished paper the same authors show that if n is an odd super perfect number, then $n\sigma(n)$ has at least 5 distinct prime factors, and that the number of distinct prime factors in n plus the number of distinct prime factors in $\sigma(n)$ is at least 7.

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: $\sigma^k(n) = \sigma(\sigma^{k-1}(n))$, $\sigma^0(n) = n$. See the Cohen & te Riele paper mentioned above.

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 $d \mid m$,

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

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

Remark: Robert Harley, in email of 8 Feb 96, quotes Bateman to the effect that John Thompson originally asked a more specific question, namely, is it true that $A(d) > 1$ implies $A(m) > 1$ for all m which are multiples of d. If one could find a number m which (a) is a product of four distinct odd primes and (b) has the property that $A(m) = 1$, then there is a good chance that $A(m/p) > 1$ for at least one of the four primes p dividing m.

Harley continues: A few months ago I invented a new algorithm for computing cyclotomic polynomial coefficients quickly and applied it to search for such m. A search up to 1853733 found $S_m = \{ 0, \pm 1 \}$ when m is in

$$\{ 431985, 757335, 865365, 1134915, 1296885, 1297815, 1675365, 1729335 \}.$$

For each $p \mid m$, the coefficients of $\Phi(m/p)$ are again between -1 and 1. I initially expected to find counter examples, but now it looks like the answer is "yes" and I'm looking for a proof! There is a very interesting pattern in the factors of these m:

$431985 = 3 \times 5 \times 31 \times 929$

$757335 = 3 \times 5 \times 29 \times 1741$

$865365 = 3 \times 5 \times 31 \times 1861$

$1134915 = 3 \times 5 \times 29 \times 2609$

$1296885 = 3 \times 5 \times 31 \times 2789$

$1297815 = 3 \times 5 \times 31 \times 2791$

$1675365 = 3 \times 5 \times 61 \times 1831$

$1729335 = 3 \times 5 \times 31 \times 3719$

In each case, a given factor plus 1 (or else minus 1) is divisible by all the smaller factors. This might lead to some insight for a proof.

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

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

be a generic polynomial of degree n. Let $g(x) \in \mathbb{F}_p[b_0, \ldots, b_n][x]$ 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 $c \in \mathbb{F}_p \backslash \{0\}$, and k, α_0, α_1, $\ldots$, $\alpha_n \geq 0$.

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

Remark: In April 1995 the proposer stated that Hendrik Lenstra had proved the conjecture and that the proof would appear in his, Mike Zieve's, thesis.

95:01 (Joel Brenner and Richard Guy) Which primes occur as factors of numbers of the form $6^n + 7^n$ (or, more generally, of numbers satisfying a given second-order constant-coefficient linear recurrence)? Say something about the distribution of the residues of $6^n + 7^n$ (or, more generally, ...) modulo a prime.

Remarks: 1. Concerning the first question, Basil Gordon and Carl Pomerance refer to a paper of Hasse; I think one they have in mind is

Helmut Hasse, Über die Dichte der Primzahlen p, für die eine vorgegebene ganzrationale Zahl $a \neq 0$ von gerader bzw. ungerader Ordnung mod. p ist, Math. Ann. 166 (1966) 19–23, MR 34 #5800, Revnum A16-52.

Carl also writes out the following solution, based on Hasse's argument.

Theorem. The set S of primes p which divides some $7^n + 6^n$ has asymptotic density 2/3 in the set of all primes. Among the density 1/3 of primes which never divide a $7^n + 6^n$ is a subset of density 1/4 (namely 3/4 of the primes which never divide a $7^n + 6^n$) which lie in 1/4 of the residue classes mod 168 coprime to 168.

Proof. Let $\ell(p)$ be the order of 7/6 in the group $(\mathbf{Z}/p\mathbf{Z})^*$ (assume $p \not| 42$). Then $7^n + 6^n \equiv 0 \pmod{p} \iff (7/6)^n \equiv -1 \pmod{p}$. Thus $S = \{\, p : \ell(p) \text{ is even} \,\}$. Let $T = \{\, p : \ell(p) \text{ is odd} \,\}$, so T is the set of primes which can never divide a $7^n + 6^n$. Let $T_k = \{\, p \in T : 2^k \parallel p - 1 \,\}$. Then $T_1 = \{\, p \equiv 3 \pmod{4} : \left(\frac{42}{p}\right) = 1 \,\}$. T_1 is a set of primes of density 1/4 defined via quadratic reciprocity by p lying in residue classes mod 168. By the Chebotarev density theorem, the density of T_k is 4^{-k}. Note that $\sum_{k \geq 1} 4^{-k} = 1/3$. All it remains to note is that for each fixed K, the density of $\cup_{k \geq K} T_k$ is at most 2^{1-K}, since $\cup_{k \geq K} T_k$ is contained in $\{\, p : p \equiv 1 \pmod{2^K} \,\}$. Thus it is correct to add densities, since the density of the "tail," namely $\cup_{k \geq K} T_k$, becomes small as $K \to \infty$.

2. Pieter Moree writes, THE reference for the first part of question 95:01 is:

C. Ballot, Density of prime divisors of linear recurrences, Mem. of the AMS, 551, 1995.

Pieter has two preprints which have a bearing on the question, a discussion of the history, and a good set of references. He continues: As to the second part of the question, here I would phrase the question as: on average how many residue classes (mod p) are covered by $6^n + 7^n \pmod{p}$? So if $6^n + 7^n \pmod{p}$ assumes $r(p)$ values, what is the average value of $r(p)/p$? I expect this to be some positive number. I expect that techniques as first explored by Hooley in his conditional proof (under GRH) of the Artin primitive root conjecture might yield the answer.

95:02 (Peter Montgomery) Find a parametric solution for the diophantine equation $x_1y_1 + x_2y_2 + x_3y_3 = 0$. Are there quadratics $f_1, f_2, f_3, g_1, g_2, g_3$ in indeterminates $z_1, \ldots, z_6$ such that "most" solutions of $x_1y_1 + x_2y_2 + x_3y_3 = 0$ have the form $x_j = f_j(z_1, \ldots, z_6)$, $y_j = g_j(z_1, \ldots, z_6)$, and such that $\sum_1^3 f_j g_j$ is identically zero?

It will not do to let $f_1, f_2, f_3, h_1, h_2, h_3$ be linear in $z_1, \ldots, z_6$ and let $(g_1, g_2, g_3) = (f_1, f_2, f_3) \times (h_1, h_2, h_3)$, because the g_j will typically be much larger than the f_j.

95:03 (J. C. Lagarias) Prove or disprove: every algebraic number field K has a finite extension L whose ring of integers has a power basis.

Remark: This is true for abelian number fields, where we can take L to be a cyclotomic field.

95:04 (Neville Robbins) For $i = 1, 2$ let $F_i(n)$ be the number of partitions of n into parts congruent to $\pm i \pmod 5$. Is it true that $\lim_{n\to\infty} \frac{F_2(n)}{F_1(n)} = 1 - \frac{1}{e}$?

Solution: Basil Gordon answered this in the negative, proving that the limit is in fact $(\sqrt{5} - 1)/2$. See **95:12**.

95:05 (Peter Borwein and David Boyd) Find a polynomial with coefficients in $\{0, \pm 1\}$ and a 5th order zero of modulus strictly less than 1. More generally, show that such a polynomial can have a zero of arbitrarily high multiplicity strictly inside the unit circle.

There is a connection to Lehmer's problem on Mahler's measure.

95:06 (Paul Erdős, via John Selfridge) Let N be relatively prime to 6. Then N can be written as a sum of numbers of the form $2^a 3^b$, no one dividing any other.

1. Is there a function $f(s)$ such that the least summand can be made greater than s for all $N > f(s)$? Thus, $f(1) = 1$, $f(2) = 5$, $f(3) = 11$; is it true that $f(4) = 19$, $f(6) = 31$, $f(8) = 47$, ...?

2. Is it true that for every N the expression with maximum least summand is unique? E.g., for $N = 115$, the least summand must be at least 24, and the only expression with least summand 24 is $115 = 24 + 27 + 64$.

Solution to 1: Claudia Spiro-Silverman solves the first question; at a page and a half, the solution is a bit too long to be included here. It ends as follows:

The function $f(s)$ does, in fact, exist. And, the effectiveness of determining the value of the function $f(s)$ as s increases is as good as the effectiveness of algorithms for determining

$$\max\{K : \text{ there is a power of 2 between } 3^K - d \text{ and } 3^K + d\},$$

as a function of d. Thus, we were able to verify that $f(3) = 11$ by checking that the last solution of $3^K - 2^L = 1$ is $K = 2$, $L = 3$.

[Editor's query: would Ellison's result,

$$|2^x - 3^y| > 2^x e^{-x/10} \text{ for } x > 27$$

(see UPINT F23) be of any use here?]

95:07 (Melvin Knight) Let F_m be the m-th Fibonacci number.

1. If $m = 5^n - 1$, $n = 1, 2, \ldots$, and $m' > m$, then $5^n \mid (F_{m'} - F_m)$, so $\lim_{n\to\infty} F_m$ exists in the 5-adics; what is it?

2. If $m = 5^n$, $n = 1, 2, \ldots$, and $m' > m$, then $5^n \mid \left(\frac{F_{m'}}{m'} - \frac{F_m}{m}\right)$, so $\lim_{n\to\infty} \frac{F_m}{m}$ exists in the 5-adics; what is it?

Solution to 1: Peter Montgomery notes that $F_m^2 - F_mF_{m-1} - F_{m-1}^2 = 1$ if m is odd, and $5^n \mid F_m$ if $m = 5^n$, whence $F_{m-1}^2 \equiv -1 \pmod{5^n}$; it follows that the first limit is $\sqrt{-1}$.

Also with $m = 5^n$, Peter asserts that for every α there is a 5-adic integer K_α such that

$$\frac{1}{m}F_{\alpha m} = K_\alpha - \frac{5}{24}(K_\alpha m)^3 - \frac{5}{384}(K_\alpha m)^5 + O(m^7).$$

He notes that $K_{-1} = K_1$, $K_3 = -3K_1$, $K_5 = 5K_1$, and asks whether $K_\alpha = \alpha(-1)^{(\alpha-1)/2}K_1$ for all α.

95:08 (Gary Walsh) Are there any positive integer solutions to $x^2(x^2+1) + y^2(y^2+1) = z^2(z^2+1)$?

95:09 (Heng Huat Chan) It is well-known that $\sum_{m,n=-\infty}^{\infty} e^{-\pi(m^2+n^2)} = \sqrt{\pi}/\Gamma^2(3/4)$, where $\Gamma(z) = \int_0^\infty e^{-t}t^{z-1}\,dz$. It was recently shown that

$$\sum e^{-2\pi(m^2+mn+n^2)} = \frac{1}{(12)^{1/8}\sqrt{\sqrt{3}-1}}\frac{\pi^{1/2}}{\Gamma^2(3/4)}.$$

For $Q(m,n) = am^2 + bmn + cn^2$, define $V_Q(q) = \sum_{m,n=-\infty}^{\infty} q^{Q(m,n)}$. For which Q and q can we explicitly evaluate $V_Q(q)$? A less ambitious question would be, find an identity analogous to the given ones, involving $\sum q^{m^2+mn+2n^2}$.

95:10 (Graeme Cohen and Herman te Riele) If $1 < a < b$ and $\phi(a) = \phi(b) = \frac{a+b}{k}$, $k \ge 3$, can a be prime?

Remarks: 1. If so, b has at least 12 distinct prime factors.

2. $\phi(a) = \phi(b) = \frac{a+b}{k}$ has infinitely many solutions for $k \ge 3$, none for $k = 1, 2$.

3. a is prime if and only if $(k-1)\phi(b) = b + 1$ — see UPINT B37 for some solutions of this equation.

95:11 (Carl Pomerance) Suppose $d_1 \le d_2 \le \ldots$ and $\sum_{i=1}^k d_i$ is prime for all k. Show that there exists $c > 0$ such that $d_k > ck$ for all k. Must $k^{-1}d_k$ go to infinity?

Remarks: 1. John Selfridge suggests a finite version (presumably, if $d_1 \le d_2 \le \ldots \le d_n$ and $\sum_{i=1}^k d_i$ is prime for $1 \le k \le n$ then bound $n^{-1}d_n$ from below).

2. In email of 15 Feb 96, Carl writes: I was able to solve the first part (that $d_k > ck$) using the sieve. The second part is still open. Here is a related problem. Let $q_1 < q_2 < \ldots$ be any infinite sequence of primes. Is it possible for the second difference sequence for this sequence to have only finitely many values? Can the second difference sequence take values solely in the set 2,4? The second difference sequence is the sequence $q_n - 2q_{n-1} + q_{n-2}$.

95:12 (Bruce Reznick) Suppose $0 \le a_1 < \ldots < a_j < m$ and $0 \le b_1 < \ldots < b_k < n$, and let $p_a(N)$ denote the number of partitions of N into parts congruent to $a_i \pmod m$ and similarly let $p_b(N)$ denote the number of partitions of N into parts congruent to b_i

(mod n). Under what circumstances does $p_a(N)/p_b(N)$ converge to a finite non-zero limit as $N \to \infty$, and how can the limit be expressed in terms of the parameters?

Solution. Basil Gordon writes: It is convenient to replace the inequalities $0 \leq a_1 < \ldots < a_j < m$ and $0 \leq b_1 < \ldots < b_k < n$ by $0 < a_1 < \ldots < a_j \leq m$ and $0 < b_1 < \ldots < b_k \leq n$, respectively. An obvious necessary condition for $p_a(N)/p_b(N)$ to approach a non-zero limit as $N \to \infty$ is that $\gcd(a_1, \ldots, a_j, m) = \gcd(b_1, \ldots, b_k, n) = 1$. Assume henceforth that this holds. Then, as shown by Charles Brenner (J. Comb. Thy. A 43 (1986) 303–319), we have

$$p_a(N) \sim \alpha_0 N^{\alpha_1/2-3/4} e^{\pi\sqrt{2\alpha_2 N/3}}$$

where $\alpha_2 = j/m$, $\alpha_1 = j/2 - \sum_{i=1}^{j} a_i/m$,

$$\alpha_0 = \frac{1}{2\sqrt{\pi}} \left(\frac{\pi^2 \alpha_2}{6}\right)^{1/4-\alpha_1/2} m^{-\alpha_1} \prod_{i=1}^{j} \frac{\Gamma(a_i/m)}{\sqrt{2\pi}},$$

and similarly for $p_b(N)$, with β_j in place of α_j, $j = 0, 1, 2$ (here, $\Gamma(s)$ is the gamma function). It follows that $\lim_{N\to\infty} p_a(N)/p_b(N)$ exists and is non-zero if and only if $\alpha_2 = \beta_2$ and $\alpha_1 = \beta_1$, that is, $j/m = k/n$ and

$$j/2 - \sum_{i=1}^{j} a_i/m = k/2 - \sum_{i=1}^{k} b_i/n = \gamma, \text{ say.}$$

When these two conditions hold, the limit is

$$\frac{\alpha_0}{\beta_0} = (n/m)^{\gamma} (2\pi)^{(k-j)/2} \frac{\prod_{i=1}^{j} \Gamma(a_i/m)}{\prod_{i=1}^{k} \Gamma(b_i/n)}.$$

For example, taking $m = n = 5$, $a_1 = 2$, $a_2 = 3$, $b_1 = 1$, $b_2 = 4$, we have $\alpha_2 = \beta_2 = 2/5$ and $\alpha_1 = \beta_1 = 0$. Hence the limit exists and equals

$$\frac{\alpha_0}{\beta_0} = \frac{\Gamma(2/5)\Gamma(3/5)}{\Gamma(1/5)\Gamma(4/5)}.$$

We now apply the reflection formula $\Gamma(s)\Gamma(1-s) = \pi \csc \pi s$ to get

$$\frac{\alpha_0}{\beta_0} = \frac{\sin \pi/5}{\sin 2\pi/5} = \frac{1}{\cos \pi/5} = \frac{\sqrt{5}-1}{2}.$$

This solves **95:04**.

Gordon notes that simplifications are possible if one only wishes to solve the special case.

95:13 (David Moulton) Find a nice expression for $\sum_{p \text{ prime}} p^{-2}$.

Remarks: 1. John Wolfskill suggests sending it to David Bailey (who has a program for finding linear relations among given constants), and Peter Montgomery suggests checking the Borweins' dictionary of real numbers.

2. In email of 12 Feb 96, Jeff Lagarias notes that

$$\log \zeta(s) = \sum_p (p^{-s} + \frac{1}{2}p^{-2s} + \frac{1}{3}p^{-3s} + \ldots)$$

Now $\log \zeta(2)$ gives the right first-order term, and $\sum p^{-2} = \sum \frac{\mu(n)}{n} \log \zeta(2n)$ comes from inclusion-exclusion.

3. Robert Harley independently gave the same formula for $\sum p^{-2}$. Harley searched briefly for a linear relation with the familiar constants using lattice reduction, without success. He gives the sum to 500 decimals; the first 50 are
0.45224742004106549850654336483224428476745164712962...

95:14 (Richard Schroeppel) Consider a "computer" whose registers can store integers of arbitrary size. The computer can only do addition, subtraction, multiplication, and division with remainder; it can shift the read or write head to a different register, and has a finite state controller.

Adi Shamir, Factoring numbers in O(log n) arithmetic steps, Information Processing Letters 8 (1979) 28–31

showed that one can factor N in polynomial time ($<< (\log N)^c$ operations) on such a computer. Is there an NP-complete problem which can be solved in a polynomial number of operations on such a computer?

Remark: David Moulton suggested the partition problem; given non-negative integers $k_1, \ldots, k_n$, can $\{1, \ldots, n\}$ be partitioned into two sets S, T with $\sum_{i \in S} k_i = \sum_{i \in T} k_i$? This can be done if and only if $\prod(\pm k_1 \pm \ldots \pm k_n) = 0$, taking the product over all choices of signs, and perhaps this product can be reduced by judicious use of identities to one which Schroeppel's computer can handle.

Solutions: 1. Ernest S. Croot III, in email of 3 January 96, writes;

Here is a solution to [Rich Schroeppel's] problem:

The problem of choice to encode is the subset-sum problem. So, suppose that we want to decide whether the number N can be written as a subset sum chosen from the numbers $a_1, a_2, \ldots, a_k$. We consider the polynomial $f(x) = (1 + x^{a_1}) * (1 + x^{a_2}) * \ldots * (1 + x^{a_k})$. $f(x)$ has the following two properties: (1) $f(x)$ can be evaluated at x in polynomial time in the lengths of $a_1, a_2, \ldots, a_k$, and (2) the coefficient of x^m in the expansion of $f(x)$ is the number of ways of representing m as a subset sum chosen from $a_1, a_2, \ldots, a_k$.

Since the total number of subsets is 2^k, the coefficients in the expansion of $f(x)$ sum to 2^k. Clearly then, $f(2^k) \div 2^{Nk} = c_N + c_{N+1}2^k + c_{N+2}2^{2k} + \ldots + c_l 2^{(l-N)k}$, where c_i is the number of ways of representing i as a subset sum chosen from $a_1, a_2, \ldots, a_k$, and $l = a_1 + a_2 + \ldots + a_k$ (recall that $\div$ is integer division). Thus, N can be represented as a subset sum of $a_1, a_2, \ldots, a_k$ if and only if the remainder upon division of $f(2^k) \div 2^{Nk}$

by 2^k is non-zero, and clearly this can be computed in polynomial time on the machine in question.

2. Jeff Lagarias, in email of 18 Jan 96, adds this:

Shamir was not aware that it had already been shown that register machines can solve any problem in PSPACE (which contains all of NP) in a polynomial number of steps, by

J. Simon, On some central problems in computational complexity, Ph.D. thesis, Computer Science, Cornell 1975.

It is also implicit in the paper:

V. R. Pratt and L. J. Stockmeyer, A characterization of the power of vector machines, J. Comput. System Sci. 12 (1976) 198-221.

The vector machine model is slightly different from the register machine model, but they are known to be of computationally equivalent power, according to David S. Johnson.

The Shamir result shows the power of advertising. It was simple and easy to understand, attractively presented, and got a great deal of publicity. The Simon result did not.

95:15 (Doug Bowman) Let $f_0(x) = x$, and, for $x \geq n+1$, define $f_{n+1}(x)$ by $f_{n+1}(x) = \int_{n+1}^{x} \frac{dx}{f_n(x)}$. Is there an efficient way to calculate $f_n(x)$? for example, to find $f_{1000}(1010)$?

95:16 (Basil Gordon, via Gerry Myerson) For fixed $n \geq 3$, are there infinitely many $n \times n$ magic squares whose entries are distinct primes? What is wanted is an unconditional proof using, say, sieves, rather than one depending on unproved hypotheses such as, say, the prime k-tuples conjecture.

95:17 (Gerry Myerson) Let the matrix A be given by

$$A = \begin{pmatrix} 2 & 6 & 14 & 25 & 45 \\ 21 & 9 & 18 & 33 & 11 \\ 24 & 27 & 28 & 5 & 8 \\ 15 & 43 & 19 & 3 & 12 \\ 30 & 7 & 13 & 26 & 16 \end{pmatrix}$$

It is possible to write $A = \sum_1^r c_j P_j$ with $c_1, \ldots, c_r$ positive integers, $P_1, \ldots, P_r$ permutation matrices, and $r = 11$. Is it possible with $r = 10$? The point is that there is such an expression with $r = 10$ for $2A$.

95:18 (Martin LaBar, via Richard Guy) Is there a 3×3 magic square with distinct square entries?

Remarks: This was problem 270, Coll. Math. J. 15 (1984) 69, reprinted as D15 in UPINT2. There is a discussion in the December 1995 Monthly, and John Robertson, 560 Bair Road, Berwyn PA 19312, has a paper in Math. Mag. which may not have appeared yet.

Robertson, in a letter to Richard Guy of 4 December 94, relates the problem to that of finding three Pythagorean triangles with the same area, the squares of whose hypotenuses are in arithmetic progression, and to that of finding three points on an elliptic curve $y^2 = x^3 - n^2x$ which are the doubles of rational points and have their x-coordinates in A.P., where n is a congruent number (see D27 in UPINT).

Andrew Bremner finds six of the required eight magic sums in

$$\begin{pmatrix} 15^2 & 20^2 & 60^2 \\ 36^2 & 48^2 & 25^2 \\ 52^2 & 39^2 & 0^2 \end{pmatrix}$$

Michael Schweitzer (eiffel@swissoft.h.provi.de) shows that any such square must have entries with at least 9 decimal digits. He gives the following specimen in which only one diagonal fails:

$$\begin{pmatrix} 127^2 & 46^2 & 58^2 \\ 2^2 & 113^2 & 94^2 \\ 74^2 & 82^2 & 97^2 \end{pmatrix}$$

Bremner also gives a square of squares over $\mathbf{Q}(t)$, with only the principal diagonal failing. The entries are,

$$\begin{aligned}
&t^2(1249 - 2032t^2 + 2824t^4 - 4576t^6 - 392t^8 + 2624t^{10} - 992t^{12} + 128t^{14} + 16t^{16})^2,\\
&4(-2 + 8t^2 + t^4)^2(-1 - 8t^2 + 2t^4)^2(5 - 2t^2 + 2t^4)^2(-7 + 4t^2 + 2t^4)^2,\\
&4t^2(-1 - 8t^2 + 2t^4)^2(5 - 2t^2 + 2t^4)^4(-7 + 4t^2 + 2t^4)^2;\\
&4t^2(-1 - 8t^2 + 2t^4)^4(5 - 2t^2 + 2t^4)^2(-7 + 4t^2 + 2t^4)^2,\\
&t^2(1201 - 2728t^2 + 1168t^4 + 2384t^6 + 664t^8 - 2272t^{10} + 832t^{12} - 64t^{14} + 16t^{16})^2,\\
&4(-1 - 8t^2 + 2t^4)^2(5 - 2t^2 + 2t^4)^2(-7 + 4t^2 + 2t^4)^2(-2 - 4t^2 + 7t^4)^2;\\
&4(-1 - 8t^2 + 2t^4)^2(5 - 2t^2 + 2t^4)^2(-7 + 4t^2 + 2t^4)^2(2 - 2t^2 + 5t^4)^2,\\
&4t^2(-1 - 8t^2 + 2t^4)^2(5 - 2t^2 + 2t^4)^2(-7 + 4t^2 + 2t^4)^4,\\
&t^2(-1151 + 3488t^2 + 1240t^4 - 5632t^6 + 3448t^8 - 256t^{10} + 352t^{12} - 256t^{14} + 16t^{16})^2.
\end{aligned}$$

It's implicit in the work of Carmichael that there can be no 3 × 3 magic square with entries which are cubes or are fourth powers.

95:19 (Graeme Cohen) Let be P the set of perfect numbers, M the set of multiperfect numbers (excluding 1), and H the set of harmonic numbers (excluding 1);
$P = \{\, n : \frac{\sigma(n)}{n} = 2 \,\}$, $M = \{\, n > 1 : \frac{\sigma(n)}{n} \in \mathbf{Z} \,\}$, $H = \{\, n > 1 : \frac{n\tau(n)}{\sigma(n)} \in \mathbf{Z} \,\}$. Then M and H each strictly contain P, and no odd member of either set is known. Give a "sensible" set which contains M and/or H strictly and for which it appears to be difficult to find an odd member. The set $2\mathbf{Z}$ will be accepted as an answer only if accompanied by a proof that it contains M and/or H.