Western Number Theory Problems, 1989–12–18 & 21

Edited by Richard K. Guy

for mailing prior to 1990 Asilomar meeting

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

1967 Berkeley	1968 Berkeley	1969 Asilomar	1970 Tucson
1971 Asilomar	1972 Claremont	72:01–72:05	
1973 Los Angeles	73:01–73:16	1974 Los Angeles	74:01–74:08
1975 Asilomar	75:01–75:23		
1976 San Diego	1–65	i.e., 76:01–76:65	
1977 Los Angeles	101–148	i.e., 77:01–77:48	
1978 Santa Barbara	151–187	i.e., 78:01–78:37	
1979 Asilomar	201–231	i.e., 79:01–79:31	
1980 Tucson	251–268	i.e., 80:01–80:18	
1981 Santa Barbara	301–328	i.e., 81:01–81:28	
1982 San Diego	351–375	i.e., 82:01–82:25	
1983 Asilomar	401–418	i.e., 83:01–83:18	
1984 Asilomar	84:01–84:27	1985 Asilomar	85:01–85:23
1986 Tucson	86:01–86:31	1987 Asilomar	87:01–87:15
1988 Las Vegas	88:01–88:22	1989 Asilomar (present set)	89:01–89:32

[With comments on earlier problems: 70:XY, 76:15, 85:03, 88:09, 88:12, 88:17, 88:21.]

UPINT = Richard K. Guy, Unsolved Problems in Number Theory, Springer, 1981.
[Second edition being prepared: comments especially welcome before 90-09-30.]

COMMENTS ON ANY PROBLEM WELCOME AT ANY TIME

Department of Mathematics and Statistics,
The University of Calgary,
Calgary, Alberta, Canada, T2N 1N4.

90–06–25

COMMENTS ON EARLIER PROBLEMS

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

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

76:15 (Hugh Edgar) For primes p and q, and h an integer, how many solutions (m, n) does $p^m - q^n = 2^h$ have? At most one? Only finitely many? Examples are $3^2 - 2^3 = 2^0$; $5^3 - 11^2 = 2^2$; $5^2 - 3^2 = 2^4$.

This appeared as Advanced Problem 6110* in *Amer. Math. Monthly*, **83**(1976) 661, proposed by David M. Battany, Oceanside, California, with the suggestion "at most one". It is also in section **D9** on page 87 of UPINT.

Reese Scott, in an as-yet-to-be-published paper, "On the equation $|p^n - q^m| = c$", goes a fair way towards settling the question. He observes that the finiteness of the number of solutions for given (p, q, c) follows from a result of Pillai. The reference is

S. Sivasankaranarayana Pillai, On the inequality "$0 < a^x - b^y \leq n$", *J. Indian Math. Soc.*, **19**(1931) 1–11; Zbl. **1** 268b.

There are also:

S.S. Pillai, On $a^x - b^y = c$, *ibid.* (N.S.) **2**(1936) 119–122; Zbl. **14** 392e.

S.S. Pillai, A correction to the paper "On $A^x - B^y = C$", *ibid.* (N.S.) **2**(1937) 215; Zbl. **16** 348b.

The review of the former mentions

Aaron Herschfeld, The equation $2^x - 3^y = d$, *Bull. Amer. Math. Soc.*, **42**(1936) 231–234; Zbl. **14** 8a.

which in turn refers to the earlier Pillai paper and mentions Siegel's theorem.

Reese Scott proves the following theorems:

I: For distinct positive primes p and q, and for positive integer c, the equation $p^n + c = q^m$ has at most one solution n, m where m is a positive integer and n is a positive *odd* integer, except for the five cases $(p, q, c) =$ (2,3,1), (3,2,5), (3,2,13), (5,2,3), (3,13,10) which each have exactly two solutions. When n is a positive *even* integer, $p^n + c = q^m$ has at most one solution.

II: $p^n + c = 2^m$ has at most one solution n, m for fixed prime p and fixed integer $c > 0$, except for the three cases $(p, c) = (3,5), (3,13), (5,3)$ which each have exactly two solutions.

III: The equation $|p^n - q^m| = c$, where p and q are positive primes and c is any positive integer, has at most three solutions n, m, where n and m are positive integers. There are just three choices of (p, q, c) which give three solutions: (2,3,1), (2,5,3), (2,3,5).

IV: If $q > 2$ and $(p|q) = -1$, then $p^n + c = q^m$ has at most one solution, except for $(p, q, c) = (2,3,1)$.

85:03 (D.H. Lehmer) If c_n is the coefficient of x^n in $(1+x+x^2)^n$, show that the determinant of the matrix

$$\begin{bmatrix} c_0 & c_1 & \dots & c_k \\ c_1 & c_2 & \dots & c_{k+1} \\ \vdots & \vdots & \ddots & \vdots \\ c_k & c_{k+1} & \dots & c_{2k} \end{bmatrix}$$

is 2^k.

Remark: A solution by David Cantor was included with the 1988 problems set, where it was mentioned that Andrew Granville had also given a solution. This has appeared:

Andrew Granville, On a class of determinants, *Fibonacci Quart.*, **27**(1989) 253–256.

88:09 (Brian Conrey) Let $P(z)$ be a polynomial with real non-negative coefficients and $P(0) \neq 0$. Then P has no real positive zeros. Let ζ be a complex zero of P such that $|\arg\zeta|$ is minimal, where $-\pi < \arg \leq \pi$. Define

$$P_1(z) = \frac{P(z)}{(z-\zeta)(z-\bar{\zeta})}$$

where $\bar{\zeta}$ is the complex conjugate of ζ. Then $P_1(z)$ has real coefficients: are they all non-negative?

Remarks: Brian Conrey & Kevin McCurley each since reported that a group at Texas Tech. are rumored to have proved that the answer is "yes". Paul Bateman draws our attention to Advanced Problem 6631, Amer. Math. Monthly, **97**(1990) 432, proposed by Ron Evans & Peter Montgomery:

We say that $f(z) = a_0 + a_1 z + \ldots + a_k z^k$ is a unimodal reciprocal polynomial with positive coefficients if

$$0 < a_0 = a_k < a_1 = a_{k-1} < a_2 = a_{k-2} < \ldots < a_{\lfloor k/2 \rfloor} = a_{\lfloor (k+1)/2 \rfloor}.$$

(i) If $z_1, z_2, \ldots, z_n$ are the n-th roots of 1 and if $2\pi/n < t$, prove that

$$\prod_{|\arg z_j| > t} (z - z_j)$$

is a unimodal reciprocal polynomial with positive coefficients. Here $-\pi < \arg z \leq \pi$.

(ii) If $z_1, z_2, \ldots, z_n$ are the n-th roots of -1 and if $\pi/n < t$, prove that

$$\prod_{|\arg z_j|>t} (z - z_j)$$

is a unimodal reciprocal polynomial with positive coefficients.

88:12 (Emma Lehmer: revision of **86:12**) $p = ef + 1$ is prime and

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

are the Gaussian periods of order e.

(1) Find constants c_i, $0 \le i \le e-1$, not all 1 or -1, such that

$$\theta_j = \sum_{i=0}^{e-1} c_i \eta_{i+j}$$

are units.

For $e = 5$, $\quad p = 25n^4 + 25n^3 + 15n^2 + 5n + 1, \quad \prod \eta_i = n^{10}$.

For $e = 6$, $\quad p = 144n^2 + 12n + 1, \quad \prod \eta_i = n^6$.

For $e = 7$, $\quad p = n^6 + 7n^5 + 21n^4 + 49n^3 + 147n^2 + 343n + 343$.

For $e = 8$, $\quad p = 16n^4 + 1$.

Remark. replace the original remark by: Another example for $e = 5$, $p = 25n^4 - 25n^3 + 165n^2 - 95n + 211$ gives $\prod_{i=0}^{4} \theta_i = 1$, for $p = 211$ and $\theta_i = \eta_i - \eta_{i+1} - 1$. In terms of Dickson's form

$$16p = x^2 + 50u^2 + 50v^2 + 125w^2 \quad \text{with} \quad xw = v^2 - u^2 - 4uv$$

we have $u + v = 1$, $w = 5$. We note that for $\theta_i = \eta_i + c$ we have $u + v = 1$, $w = \pm 1$.

n	p	x	u	v	w	q
0	211	1	2	−1	5	31
1	281	11	−3	4	5	37
−1	521	31	7	−6	5	29
2	881	61	−8	9	5	29
5	16361	451	−23	24	5	7
−5	23561	551	−26	27	5	41
8	99611	1201	−38	39	5	7

where q is the least quintic residue.

(2) Are there primes for which $\prod \eta_i = n^e$ for $e = 7$ and $e = 8$?

Emma Lehmer, Connection between Gaussian periods and cyclic units, *Math. Comput.*, **50**(1988) 535–541.

Remarks by Gene Ward Smith (Berkeley) Consider conductors f for quintic cyclic extensions such that

$$f = n^4 + 5n^3 + 15n^2 + 25n + 25.$$

We may factor the above polynomial over $\boldsymbol{Q}(\zeta_5)$ to obtain

$$f = \prod_{\sigma \in \mathrm{Gal}(\boldsymbol{Q}(\zeta_5)/\boldsymbol{Q})} (n + 2 + \zeta_5 + 2\zeta_5^2)^\sigma.$$

If we put these conjugate values in the generic polynomial defined in my thesis "Generic Cyclic Extensions", we obtain

$$\begin{aligned} z^5 - 10fz^3 - 5f(4n^2 + 10n + 5)z^2 &- 5f(3n^4 + 15n^3 + 20n^2 - 50)z \\ &- f(4n^6 + 30n^5 + 65n^4 - 200n^2 - 125n + 125), \end{aligned}$$

where $f = n^4 + 5n^3 + 15n^2 + 25n + 25$.

Modulo 5, this polynomial is $(z + n^2)^5$. This suggests the transformation $z = 5x - n^2$; making this substitution one gets

$$\begin{aligned} x^5 - n^2x^4 &- 2(n^3 + 3n^2 + 5n + 5)x^3 \\ &- (n^4 + 5n^3 + 11n^2 + 15n + 5)x^2 + (n^3 + 4n^2 + 10n + 10)x - 1. \end{aligned}$$

What happens when we try the same technique on the proposed

$$f = n^6 + 7n^5 + 21n^4 + 49n^3 + 147n^2 + 343n + 343$$

of problem **88:12**? We first factor this, and find it is the product of the conjugates of

$$n + 2 + 2\zeta_7^2 + 2\zeta_7^3 + \zeta_7^4.$$

Inserting this into the generic polynomial as before, we obtain a polynomial of degree 7 which mod 7 is congruent to $(z + n^3)^7$. If we then transform by $z = 7x - n^3$, we do *not* obtain a polynomial with norm ± 1. Moreover, it does not seem to be possible to transform the polynomial we do obtain into a polynomial with norm ± 1.

The difficulty is that we must do more than find a polynomial for the conductor which passes through a few primes congruent to 1 mod 7. We must find primes which all have the "Gaussian period integer translation" property, of having units which are translates of Gaussian periods. I don't think

$$n^6 + 7n^5 + 21n^4 + 49n^3 + 147n^2 + 343n + 343$$

has this property! A list of primes congruent to 1 mod 7 with this property would seem to be the place to start attacking this problem.

88:17 (Dick Katz via John Selfridge) Is $\frac{1}{8} + \frac{1}{16} + \frac{1}{64} + \frac{1}{128} + \frac{2}{256} + \frac{1}{512} + \frac{1}{2048} + \ldots$ rational, where the numerators are the numbers of "large" digits, 5, 6, 7, 8 or 9, in the decimal representation of 2^k?

Remark: The problem is to find generalizations, to other sets of digits, since Eugene Levine [Problem 386, *Coll. Math. J.*, **19**(1988) 448; solution, John P. Quinn, *ibid.* **21**(1990) 151–152, with generalizations by Levine and by Dave Ohlsen], asks readers to show that the sum is 2/9, as do Doug Bowman & Tad White in Advanced Problem 6609, *Amer. Math. Monthly*, **96**(1989) 743. In their original submission, Bowman & White also gave the example

$$\sum_{n\geq 0}\frac{f(n)}{2^n}=\frac{20}{89}$$

where, for each n, $f(n)$ is the sum of the Fibonacci numbers F_i over those i for which the i-th digit in the base 10 representation of 2^n is greater than 4. They asked for generalizations to other sets of digits and other bases. Unfortunately their paper, "On a problem of Levine", has run afoul of the large *Monthly* backlog. They prove a theorem which solves these problems as particular cases:

Let $\{r_n\}_{n\geq 0}$ be a sequence of integers with $r_n > 1$, and define a_n inductively by $a_0 = 1$, $a_{n+1} = a_n r_n$. Working in base b, let the b-ary expansion of a_n be $\sum_{i\geq 0} d_{n,i}b^i$. Then the computation of a_{n+1} is a multiplication which is usually laid out as follows:

$$\begin{array}{cccc}
\cdots & c_{n,2} & c_{n,1} & c_{n,0} \\
\cdots & d_{n,2} & d_{n,1} & d_{n,0} \\
\times & & & r_n \\
\hline
\cdots & d_{n+1,2} & d_{n+1,1} & d_{n+1,0}
\end{array}$$

where the $c_{n,i}$ denote carries, $c_{n,0} = 0$ for each n, and $0 \leq d_{n,i} < b$ for all n and i. Note that if $r_n < b$, the base b representation of r_n is a 1-digit number, and our ordinary elementary-school definition of the carry is valid. If $r_n \geq b$, one multiplies as shown in the above diagram; in other words the multiplication is distributed over the b-ary expansion of a_n, but not over the expansion of r_n. The resulting equation is

$$r_n d_{n,i} + c_{n,i} = d_{n+1,i} + bc_{n,i+1}$$

for all $n \geq 0$ and $i \geq 0$. Then the theorem is:

THEOREM. *For any fixed complex number z such that $|z| < b$, define $g_z(n) = \sum_{i\geq 0} c_{n,i}z^i$. Then*

$$\sum_{n\geq 0}\frac{g_z(n)}{a_{n+1}}=\frac{z}{b-z}.$$

88:21 (Peter Montgomery) concerning the product $\prod_{j=1}^{n}(x^2 + 2x\cos(2j-1)\theta + 1)$.

Remark: See problem quoted under **88:09** above.

PROBLEMS PROPOSED 89–12–17 & 20

89:01 (Bruce Reznick via Jim Propp) The function

$$\frac{x}{(1-x)(1+x)^2} = x - x^2 + 2x^3 - 2x^4 + 3x^5 - 3x^6 + \ldots$$

is a rational function whose power-series expansion contains every integer as a coefficient. Is there a rational function whose power-series expansion involves every integer as a coefficient infinitely often?

Remark: Gerry Myerson writes: The answer is "no" ...David Cantor outlined a proof ...minutes after problem was presented. Alf van der Poorten ...much the same proof ...are planning ...exposition ...idea is ...Skolem-Mahler-Lech theorem asserts (in effect) that if $\sum_0^\infty a_n x^n$ is a rational function and c is an integer then the set of all j such that $a_j = c$ is the union of a finite (possibly empty) set and a finite number (possibly zero) of arithmetic progressions. If a_j is constant on an arithmetic progression with common difference d, and α is a zero of the denominator of the rational function, then so is $\alpha\zeta$ for some d-th root of unity ζ. Now the denominator has only finitely many zeros, so there are only finitely many d, so only finitely many arithmetic progressions, so only finitely many integers that occur infinitely often.

89:02 (David Boyd) Are there primes p and q such that $2^p \equiv 3 \bmod q$ and $2^q \equiv 3 \bmod p$?

[The Lehmers found the solution $n = 4700063497 = 19 \times 47 \times 5263229$ of the congruence $2^n \equiv 3 \bmod n$. See UPINT **F10**.]

89:03 (Raphael Robinson) For any positive integers $r_1, r_2, \ldots, r_n$, let $B(r_1, r_2, \ldots, r_n)$ be the largest coefficient of the polynomial $(1+x^{r_1})(1+x^{r_2})\ldots(1+x^{r_n})$. For $d \geq n$, let $A(n,d)$ be the minimum of $B(r_1, r_2, \ldots, r_n)$ over all partitions $d = r_1 + r_2 + \ldots + r_n$ of d into n parts. Show that $A(n,d) \leq A(n,d-1)$ for $d > n$.

89:04 (Erdős Pal) If n is an integer and $1 = a_1 < a_2 < \ldots < a_{\phi(n)}$ be the numbers relatively prime to n, then $J(n) = \max(a_{i+1} - a_i)$ is Jacobsthal's function. I proved 27 years ago (*Math. Scand.* **10**(1962) 163–170; MR **26** #3651) that for almost all n,

$$J(n) = (1 + o(1))\frac{n}{\phi(n)}\omega(n)$$

where $\omega(n)$ is the number of distinct prime factors of n. Is it true that $J(n)/\omega(n)$ is bounded if $n/\phi(n)$ is bounded, or

$$J(n) < f\left(\frac{n}{\phi(n)}\right)\omega(n) \qquad (1)$$

If true, give an explicit function $f(x)$ which satisfies (1).

Put $n_k = 2 \cdot 3 \cdot \ldots \cdot p_k$. I thought that every even $2t < J(n_k)$ can be written in the form $a_{i+1} - a_i$, but Lacampagne & Selfridge found a counterexample for $k = 6$. Estimate the smallest $2t_k < J(n_k)$ not of the form $a_{i+1} - a_i$. Is it true that the number of distinct $2t$ of the form $a_{i+1} - a_i$ is greater than $cJ(n_k)$ where c is an absolute constant?

89:05 (Erdős Pal) Is it true that every interval $(a, a+k)$, $a < k^2$ contains ck integers all of whose prime factors are less than k? Presumably this holds for every k^α with c depending on α, but in our work with Lacampagne & Selfridge we only needed it for $a + k \leq k^2$. Is it clear that in this case the number of integers in $(a, a+k)$ all of whose prime factors are $\leq k$ tends to infinity with k?

Solved! Erdős, in an 89-12-29 letter, writes that this is in:

John B. Friedlander & Jeffery C. Lagarias, On the distribution in short intervals of integers having no large prime factor, *J. Number Theory* **25**(1987) 249–273; MR **88d**:11084.

89:06 (L. Babai via Andy Odlyzko). Let $p = ef + 1$ be a prime, $\zeta = e^{2\pi i/p}$, and

$$\eta = \sum_{k \in S} \zeta^k,$$

where $S = \{g^{ej+a} : 0 \leq j \leq f - 1\}$, $a \in \mathbb{Z}$, and g a primitive root of p. [Then η is a classic cyclotomic period.] How large can $|\eta|$ be? [η is not *necessarily* real.]

(1) Can $f - |\eta|$ be very small? (2) If $e \approx f \approx \sqrt{p}$, are there lower bounds on $|\eta|$?

89:07 (Joel L. Brenner) Many classes C in the symmetric group S_n are proved to have the **covering property**, i.e., $CC = A_n$, the alternating group, where the **product** CD of two sets is the collection of products xy as x runs through C and y runs through D. For each $r \geq 1$, take $1 \leq k_1, \ldots, k_r$ and define $k = \sum_1^r k_i$. If $\lfloor 3n/4 \rfloor + r - 1 \leq k \leq n$, $n \geq 4r - 1$, then the class $C \sim 1^{n-k} k_1^1 \ldots k_r^1$ with $n - k$ (or more) fixed points in S_n is **conjectured** to have the covering property. A proof is given for $r = 1, 2, 3$; the methods are new, as are the results when $r = 2, 3$. Note that "$4r - 1$" cannot be replaced by a smaller number. If the conjecture is true, then (asymptotically) almost all classes in A_n have the covering property. A further conjecture is that the last assertion holds for any **infinite ascending** series of **finasigs** (= finite nonabelian simple groups).

89:08 (Peter J. Cameron, from 12th Brit. Combin. Conf.) Let q, n, k be positive integers with $q > 1$, $n > 3$.

(1) Show that $\displaystyle\binom{k}{2} - 1 = \frac{q^n - 1}{q - 1}$ has no solutions.

(2) Show that $\displaystyle\binom{k}{2} - 1 = q^n + 1$ has only the solution $q^n = 64$, $k = 12$.

89:09 (Richard McIntosh) Prove that for primes $p \geq 5$ we have

$$3\sum_{k=1}^{p-1} k^{p-3} \equiv 2\sum_{k=1}^{p-1} k^{-2} \bmod p^2$$

[This was claimed to be the corrected form of the congruence on the last page of the article: A. Gardiner, Four problems on prime power divisibility, *Amer. Math. Monthly*, **95**(1988) 926–931.]

If n is not prime, prove or disprove

$$3 \sum_{(k,n)=1} k^{\phi(n)-2} \equiv 2 \sum_{(k,n)=1} k^{-2} \bmod n^2.$$

For what n is $\sum_{(k,n)=1} k^{-2} \equiv 0 \bmod n^2$? E.g., $n = 39$ and lots more, but only one *prime* is known, namely 16843.

[Brinkmann showed that

$$\binom{2p-1}{p-1} \equiv 1 - \frac{2}{3}B_{p-3}p^3 \bmod p^4$$

for primes $p \geq 5$. See Emma Lehmer, On congruences involving Bernoulli numbers and the quotients of Fermat and Wilson, *Ann. of Math.*(2) **39**(1938) 350–360; *Zbl.* **19**.005.]

Remarks: (Andrew Granville) The "2" and "3" in the first equation should be interchanged. The second equation is not the correct generalization. Here is somewhat more than the correct generalization.

Let r be a fixed, even positive integer. If n is a positive integer such that $p-1 \nmid r$ for all primes $p|n$, and $\phi(n) > r$, then

$$r \sum_{\substack{1\leq k\leq n \\ (k,n)=1}} k^{\phi(n)-r} \equiv (r-\phi(n)) \sum_{\substack{1\leq k\leq n \\ (k,n)=1}} k^{-r} \bmod n^2$$

Granville gives a proof, from which it also follows that

$$\sum_{\substack{1\leq k\leq n \\ (k,n)=1}} k^{-2} \equiv nB_{\phi(n^2)-2}\prod_{p|n}(1-p^{\phi(n^2)-3}) \bmod n^2$$

so that McIntosh's last question is equivalent to: when does n divide

$$B_{\phi(n^2)-2}\prod_{p|n}(1-p^{\phi(n^2)-3})?$$

If $n = p$ is prime this is equivalent to $p|B_{p-3}$. In general if n is squarefree then this is equivalent to $p|B_{p-3}$ or $p|q^3-1$ for some $q|n$, for each $p|n$. To construct such n Peter Montgomery takes $n = pq$ where p, $q = p^2+p+1$ are primes.

89:10 (Andrew Granville & Ladislav Skula) Define q_p to be the least positive integer q such that there is an a with $1 \leq a \leq q$ and

$$B_{p-1}\left(\frac{a}{q}\right) - B_{p-1} \not\equiv 0 \bmod p$$

where $B_n(x)$ is the n-th Bernoulli polynomial and $B_n = B_n(0)$.

Find a good upper bound on q_p.

[I have $q_p < (\ln p)^2$ for all $p \geq 5$: improve this! Conjecture that $\forall p$, $q_p = 2$ or 3.]

89:11 (Andrew Granville) Suppose that we are given an $m \times n$ $(m \geq n)$ matrix $M(X)$ with (i, j)-th entry $X^{a_{ij}}$ for some non-negative integers a_{ij} such that *every* $n \times n$ submatrix of $M(X)$ has a non-zero determinant. Suppose that $M(t)$, where t is a complex number (but not 0 or a root of 1), has less than full rank (i.e., rank $\leq n-1$). Prove that $m \leq 2n$.

[Note: this upper bound is independent of the a_{ij}.]

Results: (1) (Bombieri–Granville) $m \leq e^{e^{e^{\cdot^{\cdot^{\cdot^{e^n}}}}}}$ $(n! + 2$ times).

(2) (Granville–van der Poorten) If t is not a unit (first and last coefficients of minimum polynomial ± 1), then $m \leq n^3/2$.

89:12 (Sun Qi) Ko Chao, *J. Chinese Math. Soc.*, **2**(1940) 205–207, found infinitely many integer solutions of $x^x y^y = z^z$. Are there solutions with $2 \nmid xy$?

89:13 (Sun Qi) Are there integer solutions of $w^w x^x y^y = z^z$ with $1 < w < x < y$? [See UPINT **D13**.]

89:14 (Sun Qi) Has the equation $3^m - 2q^n = 1$ any integer solutions with $m > 1$, $n > 1$, $2 \nmid m$, q an odd prime, other than $q = 11$, $m = 5$, $n = 2$?

89:15 (Sun Qi) Ko Chao, *J. London Math. Soc.*, **11**(1936) 218–219, gave integer solutions of $x^3 + y^3 + 2z^3 = n$ for all $n \leq 100$, except $n = 76$ and $n = 99$. Are there solutions in these cases?

[See UPINT **D5** where it's implied that 99 is settled. Are each of $n = 148$, 183, 230, 253, 356, 418, 428, 445, 482, 491, 519, 580, 671, 734, 788, 923, 931 and 967 still in doubt?]

89:16 (Sun Qi) Let $A(s)$ be the number of positive integer solutions of

$$\sum_{i=1}^{s} \frac{1}{x_i} - \frac{1}{x_1 \ldots x_s} = 1, \quad 0 < x_1 < \ldots < x_s \tag{2}$$

e.g., $A(6) = 17$ (Sun Qi & Cao Zhenfu, *Acta Sci. Sichuan Univ.*, **5**(1985) 700). For $n \geq 3$ is $A(n+1) > A(n)$?

89:17 (Sun Qi) For each $n > 1$, let $X(n)$ denote the number of solutions of the following problem. Each of n integers $x_i > 1$ is a proper divisor of $x_1 \ldots x_{i-1}x_{i+1} \ldots x_n - 1$. Li-Shuguang has shown that $X(2) = X(3) = 0$ and that $X(n) > 0$ for $n \geq 4$. Is it true that $X(n+1) > X(n)$ for $n \geq 4$?

89:18 (Sun Qi) If

$$f(x_1, \ldots, x_m) \in \mathrm{GF}(p)[x_1, \ldots, x_m]$$

and there are primitive roots $\alpha_1, \ldots, \alpha_m$ mod p such that $f(\alpha_1, \ldots, \alpha_m) \equiv 0$ mod p, then are there always primitive roots $\beta_1, \ldots, \beta_m$ mod p^l such that $f(\beta_1, \ldots, \beta_m) \equiv 0$ mod p^l? [Neither Andrew Granville nor Gerry Myerson can understand this, so it's evidently not properly posed.]

89:19 (Bart Goddard) Let $0 = x_1 < x_2 < \ldots < x_n$ be integers with $\gcd(x_2, \ldots, x_n) = 1$ and let $d_1 \leq d_2 \leq \ldots \leq d_{\binom{n}{2}}$ be the positive differences of the x_j, with multiplicities included. How do we choose the x_i so that the d_j are "evenly spread"? I.e., let $e_j = d_{j+1} - d_j$ for $j = 1, 2, \ldots, \binom{n}{2} - 1$, and s and t be the average values of the d_j and the e_j. Then minimize $a + b + c$, where a is the number of pairs (i, j) with $i < j$ and $d_i = d_j$, b is the average value of $|s - d_j|$, and c is the average value of $|t - e_j|$.

For example, if $n = 5$, then $(0, 1, 2, 6, 9)$ gives $s = 4.6$, $t = 8/9$, $a = 1$, $b = 2.4$, $c = 16/81$ and $a + b + c = 1457/405$ and, for $n = 6$, $(0, 6, 9, 10, 17, 24)$ gives $s = 154/15$, $t = 23/14$, $a = 1$, $b = 374/75$, $c = 95/98$ and $a + b + c = 51127/7350$.

89:20 (Hugh Edgar) Characterize those positive integers n for which

$$\alpha + \beta + \gamma = \alpha\beta\gamma = 1 \tag{*}$$

is solvable in $\mathbb{Z}[\zeta_n]$.

Remarks. Since $1 + i + (-i) = 1 \cdot i \cdot (-i) = 1$, all positive integer multiples of 4 qualify. The equations (*) are solvable in the ring of integers of $\mathbb{Q}(\theta)$, where $\mathrm{Irr}(\theta, X, \mathbb{Q}) = X^3 - X^2 - 4X - 1$. $\mathbb{Q}(\theta)$ is a cyclic cubic extension of $\mathbb{Q}$, and $\mathbb{Q}(\theta)$ is a subfield of $\mathbb{Q}(\zeta_{13})$ so all positive integer multiples of 13 qualify. Edgar notes that Andrew Bremner, *Manuscripta Math.*, **65**(1989) 479–487, shows that the field arising from $X^3 - X^2 - 4X - 1$ is the one and only cyclic cubic extension of $\mathbb{Q}$ on which (*) have solutions.

89:21 (Doug Bowman) Find an asymptotic upper bound for $f(n)$, the number of partitions of n into parts which divide n.

[This will appear as Advanced Problem 6640 in the Nov. 1990 *Monthly.*]

Solution: Bateman gave proofs that

$$\{1+o(1)\}\left\{\frac{\tau(n)}{2}-1\right\}\ln n \le \ln f(n) \le \{1+o(1)\}\frac{\tau(n)}{2}\ln n$$

where $\tau(n)$ is the number of divisors of n. The lower bound is due to Odlyzko & Erdős, and is obtained by considering the number of partitions of n in which you take the divisor d, $1 < d < n$, either $0, 1, 2, \ldots$, or $\lfloor n/d\tau(n)\rfloor$ times and fill out with parts 1. The upper bound is by Bateman himself who notes that $f(n)$ is the coefficient of x^n in

$$\prod_{d|n}\frac{1}{1-x^d} = \prod_{d|n}(1+x^d+x^{2d}+\ldots+x^n+\ldots)$$

which is at most the sum of the coefficients, $\prod_{d|n}(\frac{n}{d}+1)$.

89:22 (Morris Newman) Let H_q be the Hecke group generated by the matrices

$$T=\begin{pmatrix}0 & 1\\ -1 & 0\end{pmatrix} \qquad S=\begin{pmatrix}1 & 2\cos\frac{\pi}{q}\\ 0 & 1\end{pmatrix}$$

where q is an odd prime. Then H_q is the free product of the cyclic group $\{T\}$ of order 2 and the cyclic group $\{ST\}$ of order q. Prove that the number of subgroups of H_q of index $2q-1$ is in fact just $2q-1$. [True for all primes $q \le 41$ by direct calculation.]

Solution by R.B. Howlett, Univ. of Sydney, via Gerry Myerson and John Mack.

Let $G = \langle x, y \,|\, x^2 = y^q = 1\rangle$ where q is an odd prime. Suppose that $H \le G$ and $|G : H| = 2q-1$. Observe that G acts transitively by left multiplication on the set $\mathcal{C} = \{gH \mid g \in G\}$, which has $2q-1$ elements. The orbits of $\langle x\rangle$ on $\mathcal{C}$ all have length either 1 or 2, and since $|\mathcal{C}|$ is odd, at least one of these orbits has length 1. So we may choose $C_1 \in \mathcal{C}$ such that $xC_1 = C_1$.

If $yC_1 = C_1$ then $gC_1 = C_1$ for all $g \in G$, since x & y together generate G. This contradicts transitivity of G on $\mathcal{C}$. So C_1 lies in an orbit of $\langle y\rangle$ which has length greater than 1. Since $\langle y\rangle$ has prime order q, any non-trivial orbit of $\langle y\rangle$ must have exactly q elements. Hence C_1, $C_2 = yC_1$, $C_3 = y^2C_1$, $\ldots$, $C_q = y^{q-1}C_1$ are distinct elements of $\mathcal{C}$.

Let $\mathcal{C}_0 = \{C_i \mid i = 1, 2, \ldots, q\}$ and $\mathcal{C}_0' = \{C \in \mathcal{C} \mid C \notin \mathcal{C}_0\}$. Since $\mathcal{C}_0$ is a $\langle y\rangle$-orbit, its complement $\mathcal{C}_0'$ is a union of $\langle y\rangle$-orbits, all of which must have length 1, since any non-trivial $\langle y\rangle$-orbit has q elements and $\mathcal{C}_0'$ has only $q-1$ elements. So $yC = C$ for all $C \in \mathcal{C}_0'$.

Let $C \in \mathcal{C}_0'$. If $xC \in \mathcal{C}_0'$, then $x(C \cup xC) = C \cup xC$ and $y(C \cup xC) = C \cup xC$, giving $g(C \cup xC) = C \cup xC$ for all $g \in G$ and contradicting transitivity of G on $\mathcal{C}$. So $xC \in \mathcal{C}_0$. If $xC = C_1$ then $C = x^2C = xC_1 = C_1$ contradicting $C \notin \mathcal{C}_0$; so $xC \in \{C_2, C_3, \ldots, C_q\}$. Thus $C \mapsto xC$ gives a bijective correspondence between $\mathcal{C}_0'$ and $\{C_2, C_3, \ldots, C_q\}$. Let $C_{q+1} = xC_2$, $C_{q+2} = xC_3$, $\ldots$, $C_{2q-1} = xC_q$. Note that $H = C_i$ for some i.

For each $g \in G$ define $\phi(g) \in S_{2q-1}$ (the symmetric group) by

$$gC_i = C_{\phi(g)(i)} \quad \text{for all} \quad i \in \{1, 2, \ldots, 2q-1\}$$

Then $\phi : g \mapsto \phi(g)$ is a homomorphism $G \to S_{2q-1}$. Furthermore,

$$\left\{ \begin{array}{lcl} \phi(y) & = & (1, 2, \ldots, q) \qquad \text{and} \\ \phi(x) & = & (2, q+1)(3, q+2) \ldots (q, 2q-1) \end{array} \right\} (*)$$

It is easily proved that $\phi(x)$ and $\phi(y)$ generate the alternating group A_{2q-1}. Observe that

$$H = \{g \in G \mid gC_i = C_i\} = \{g \in G \mid \phi(g)(i) = i\}.$$

Without assuming that G has a subgroup of index $2q-1$, it is trivial that $(*)$ defines a surjective homomorphism $\phi : G \to A_{2q-1}$. For each i the group $S_i = \{\pi \in A_{2q-1} \mid \pi(i) = i\}$ is a subgroup of index $2q-1$ in A_{2q-1}, and the preimages $H_i = \phi^{-1}(S_i)$ are $2q-1$ distinct subgroups of G of index $2q-1$. Our argument above showed that an arbitrary subgroup of G of index $2q-1$ must equal one of these.

89:23 (James P. Jones) Show that

$$\binom{2n}{n} \equiv 2 \bmod n^3 \quad \text{implies that} \quad \binom{2n}{n} \equiv 2 \bmod 2n^3.$$

Solution: Richard McIntosh uses Kummer's theorem and proves the following two theorems.

Theorem 1

$$\binom{2n-1}{n-1} = \prod_{d|n} \binom{2d-1}{d-1}',$$

where

$$\binom{2d-1}{d-1}' = \prod_{(k,d)=1}^{d} \frac{2d-k}{k}.$$

Theorem 2

For $n \geq 3$ *we have* $\binom{2n-1}{n-1}' \equiv 1 \bmod n^2.$

[Also solved by Andrew Granville.]

89:24 (Landon Curt Noll) Given the sequence product:

$$S^l_{n,k} = \prod_{i=0}^{i<n} (k + li) = p_1^{x1} p_2^{x2} \dots p_c^{x_c}$$

what is the relationship of c, the number of distinct prime factors, to S?

E.g. If $S^1_{3,k}$ contains a twin prime, how rare is $c = 4$?

89:25 (Erdős, Lacampagne & Selfridge) For each k are there infinitely many sets of k consecutive numbers $n + i = ip_i$, $1 \le i \le k$ with each p_i prime? E.g., $k = 5$, $19441 = 1 \times 19441$, $19442 = 2 \times 9721$, $19443 = 3 \times 6481$, $19444 = 4 \times 4861$, $19445 = 5 \times 3889$. In such cases, if $p(m)$ denotes the least prime divisor of m, then

$$p\left(\binom{n+k}{k}\right) = \frac{n+k}{k}.$$

We call a binomial coefficient $\binom{N}{k}$ **exceptional** if $p(\binom{N}{k}) > \frac{N}{k}$.

Conjecture 0. $\binom{62}{6}$ is the only exceptional binomial coefficient with $N \ge k^2 - 1$.

Conjecture 1. There are no exceptional binomial coefficients with $N > 17.125k$.

Conjecture 2. If $\binom{N}{k}$ is exceptional, then $p(\binom{N}{k}) \le 17$ except for $p(\binom{62}{6}) = 19$, $p(\binom{959}{56}) = 19$, $p(\binom{474}{66}) = 23$ and $p(\binom{284}{28}) = 29$.

[We have so far found eight exceptional binomial coefficients with $p(\binom{N}{k}) = 17$. Conjecture 2 implies Conjecture 1.]

89:26 (Erdős Pal) Let $g(k)$ be the smallest n such that $\binom{n}{k}$ has $p(\binom{n}{k}) > k$. For large n it seems obvious that $g(k) > k^2$ — in fact $>$ any power of k, but we have only *proved* $g(k) > k^{1+\epsilon}$.

89:27 (Erdős Pal) Given n integers $a_1 < \ldots < a_n$, how many A.P.s, $a_i, a_i + d, a_i + 2d$ with distinct differences d can they contain? Erdős & Rusza gave $n^{1+\epsilon}$ explicitly, and Erdős & Spencer proved probabilistically that you can get $n^{3/2}$, and this may be best possible.

89:28 (Andrew Granville) Define

$$((x)) = \begin{cases} x - \lfloor x \rfloor - \frac{1}{2} & x \notin \mathbb{Z} \\ 0 & x \in \mathbb{Z} \end{cases}$$

A theorem of Franel states that for any positive integers a and b

$$\textstyle\int_0^1 ((ax))((bx))\,dx = \frac{(a,b)^2}{12ab}. \qquad (*)$$

(An elegant proof appears in Hans Rademacher & Emil Grosswald, Dedekind Sums, Carus Math. Monograph **16**, Math. Assoc. Amer., 1972, pp.24–25 [copied, with acknowledgement, from Edmund Landau, Vorlesungen über Zahlentheorie, Chelsea, zweiter Band, Satz 484, pp. 170–171 – RKG].)

Find a similar "simple" formula for

$$\int_0^1 ((ax))((bx))((cx))((ex))\,dx$$

Remark: Bruce Berndt writes that while this generalization is *not* in his paper, two generalizations of (*) are Lemmas 4.2 and 7.1 in

B.C. Berndt, Reciprocity theorems for Dedekind sums and generalizations, *Adv. Math.*, **23**(1977) 285–316.

89:29 (Mike Filaseta — from Emil Grosswald, Mar. '88, but not originating with him) For odd n the Legendre polynomials are divisible by x, but otherwise they are irreducible. Can two Legendre polynomials share the same non-trivial factor? Similar question for Hermite polynomials.

89:30 (Gene Smith) Let

$$R = \prod_{p_i^{e_i} < n,\, e_i \geq 1} p_i^{\pm e_i}$$

be a product of all primes less than a bound n, each raised to an exponent k such that $p^{|k|} < n$, so that R is the *least* such product with $R > 1$. Write $R = P/Q$ in reduced form, and $f(n) = P - Q$.

(1) Are there infinitely many n such that $f(n) < n$, i.e., such that $f(n) = 1$?

(2) Are there infinitely many n such that $n < f(n) < n^2$, i.e., such that $f(n)$ must be prime?

The same questions with $|k| = 1$, so that $e_i = \pm 1$.

89:31 (Gerry Myerson) A **covering set** is a set of $m \times m$ integer matrices such that $\bigcup_{A \in S} \mathbb{Z}^m A = \mathbb{Z}^m$, that is, for every integer row m-vector $\mathbf{h}$ there exists an integer row m-vector $\mathbf{k}$ and an element $A \in S$ such that $\mathbf{k}A = \mathbf{h}$.

(1) Find conditions on $\Delta_1, \Delta_2, \ldots$ such that there exists a covering set $S = [A_1, A_2, \ldots]$ with $\det A_j = \Delta_j$ for all j. (E.g., for every prime p there is a covering set of $p + 1$ matrices of determinant p)

(2) Is every left-covering a right-covering? I.e., does

$$\bigcup_{A \in S} \mathbb{Z}^m A = \mathbb{Z}^m \quad \text{imply} \quad \bigcup_{A \in S} A\mathbb{Z}^m = \mathbb{Z}^m?$$

Solution: (of (2); (1) is still open) On an 89-12-28 postcard Gerry Myerson notes that if

$$S = \left\{ \begin{pmatrix} 0 & -1 \\ 2 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix} \right\},$$

then it's easy to verify that $\forall a, b \in \mathbb{Z}$, $\exists A \in S$ and $x, y \in \mathbb{Z}$ such that $(x, y)A = (a, b)$, but $A \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 2 \\ 1 \end{pmatrix}$ has no solution $A \in S$ and $x, y \in \mathbb{Z}$ — that is, S is a left-covering but not a right-covering.

A particular case of (1) is: is there a finite covering (say in the case $m = 2$) with no two determinants equal in absolute value? Equivalently, can $\mathbb{Z} \oplus \mathbb{Z}$ be expressed as a finite union of proper subgroups, no two of the same index?

89:32 (Leo Chouinard via Bart Goddard) Let $0 < a_1 < a_2 < \ldots < a_n$ be integers. Consider inequalities of the forms $a_i + a_j < a_k$ or $a_i + a_j > a_k$. Note that the systems

$$\left\{ \begin{array}{rcl} a_i + a_j & < & a_k \\ a_i + a_j & > & a_{k+m} \end{array} \right. \quad \text{and} \quad \left\{ \begin{array}{rcl} a_i + a_j & > & a_k \\ a_{i+m} + a_j & < & a_k \end{array} \right.$$

are "obviously unsolvable".

(1) Are there any systems of inequalities of these forms which are unsolvable, but contain no obviously unsolvable subsystems?

(2) How about if $0 \le a_1 \le a_2 \le \ldots \le a_n$?