Western Number Theory Problems, 16 & 19 Dec 1996

Edited by Gerry Myerson

for mailing prior to 1997 (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	89:01–89:32
1990 Asilomar	90:01–90:19	1991 Asilomar	91:01–91:25
1992 Corvallis	92:01–92:19	1993 Asilomar	93:01–93:32
1994 San Diego	94:01–94:27	1995 Asilomar	95:01–95:19
1996 Las Vegas (present set) 96:01–96:18			

[With comment on 95:18]

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

18 July 97

Comment on an Earlier Problem

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

Remark: Martin Gardner (Quantum 6:3, Jan-Feb 1996, 24–26) offers \$100 for the solution of this problem.

Problems Proposed 16 & 19 Dec 96

96:01 (Bob Silverman, via Sam Wagstaff) Let $a_1 < a_2 < \ldots < a_{k-1}$ be positive integers such that congruence considerations do not rule out the existence of infinitely many primes p such that $p+a_j$ is prime for all j, $1 \le j \le k-1$. Then we call $(p, p+a_1, \ldots, p+a_{k-1})$ a k-tuple. E.g., for $k = 2$, we have $(p, p+2)$ but also $(p, p+4)$, $(p, p+6)$, etc.

Given a k-tuple, call it C, and define $R(C)$ by $R(C) = \sum_p (\frac{1}{p} + \frac{1}{p+a_1} + \ldots + \frac{1}{p+a_{k-1}})$, taking the sum over those primes p for which $p+a_1, \ldots, p+a_{k-1}$ are all prime. Let $r(k)$ be the supremum of $R(C)$ as C ranges over all k-tuples.

1. Is it true that $r(2) = R\big((p, p+6)\big)$? It can be shown that $R\big((p, p+6)\big) > R\big((p, p+2)\big)$.

2. Given k, how would one determine the k-tuple C that maximizes $R(C)$? What is the computational complexity of computing $r(k)$ to a given precision?

3. How fast does $r(k)$ go to infinity?

4. Does k exist for which $r(k)$ is rational?

5. Are the numbers $r(2), r(3), \ldots$ algebraically independent? Do there exist distinct k-tuples C, C', possibly corresponding to different values of k, such that $R(C) = R(C')$?

Remarks: 1. There was a suggestion that one might want to expand the notion of k-tuple to include such things as $(p, 2p+1)$.

2. Peter Montgomery asked whether it was easy to see that $r(k)$ is monotone increasing.

3. Carl Pomerance defines $R^*(c) = \sum \frac{1}{p}$, summing over primes p such that $p+c$ is also prime, and $r^*(2) = \sup_{c>0} R^*(c)$. He then proves

Theorem. The prime k-tuples conjecture implies $r^*(2) = \infty$.

Since $R\big((p, p+c)\big) > R^*(c)$, and $r(2) \ge r^*(2)$, this settles Silverman's first question in the negative, conditional on the prime k-tuples conjecture.

Proof. Call a set $B = \{ b_1, \ldots, b_k \}$ of integers *admissible* if for each prime p there is at least one congruence class (mod p) disjoint from B. Let $p_1 < p_2 < \ldots$ be an infinite sequence of primes such that no $p_i - 1$ is divisible by any p_j. Erdős showed that there is such a sequence with $\sum \frac{1}{p_j} = \infty$ (On a problem of G. Golomb, J. Austral. Math. Soc. 2

(1961/62) 1–8.).

Now for any k, $p_1, \dots, p_k$ is admissible. For, if p is not in $\{p_1, \dots, p_k\}$, then no p_i satisfies $p_i \equiv 0 \pmod p$. And if p is in $\{p_1, \dots, p_k\}$, then no p_i satisfies $p_i \equiv 1 \pmod p$.

Assuming the prime k-tuples conjecture, there is a number C_k such that $p_1 + C_k, \dots,$ $p_k + C_k$ are all prime. Then $R^*(C_k) \ge \sum_{i \le k} \frac{1}{p_i}$. But $\sum \frac{1}{p_i} = \infty$, so $r^*(2) = \infty$.

[In fact, the prime k-tuples conjecture implies $r(m) = \infty$ for all m. For there are numbers $C_{k1}, \dots, C_{k,m-1}$ such that $p_i + C_{kj}$ are all prime, $1 \le i \le k$, $1 \le j \le m-1$, whence $R\big((p, p + C_{k1}, \dots, p + C_{k,m-1})\big) > \sum_{i \le k} \frac{1}{p_i}$, etc. This settles all of Silverman's questions, conditional on the prime k-tuples conjecture, except for the last part of question 5.]

4. Pomerance goes on to consider, on a suggestion of Vsevolod Lev, $R'(c) = \sum \frac{1}{p+c}$, summing over p such that p and $p + c$ are both prime. He proves that $\sup_c R'(c)$ is finite. By Brun's sieve,

$$\sum_{\substack{p,\, p+c \text{ prime} \\ 2^j < p+c < 2^{j+1}}} \frac{1}{p+c} \ll \frac{c}{\phi(c)} \frac{1}{j^2}$$

uniformly for all $c > 0$ and all j with $2^j > c$. If $2^j \le c < 2^{j+1}$, the sum is at most the sum of the reciprocals of all the primes in $(2^j, 2^{j+1})$, which is $\ll 1/\log c$. If $2^{j+1} \le c$ then there are no primes p with $p + c < 2^{j+1}$. Thus,

$$R'(c) \ll \frac{1}{\log c} + \sum_{2^j > c} \frac{c}{\phi(c)} \frac{1}{j^2} \ll \frac{c}{\phi(c) \log c}.$$

But $\frac{c}{\phi(c)\log c} \to 0$ as $c \to \infty$ (this can be deduced from Theorem 328 of Hardy and Wright, 4th ed., which states that $\liminf \frac{\phi(n) \log\log n}{n} = e^{-\gamma}$, a theorem of Landau). Thus $R'(c)$ is bounded, and the supremum is attained at some c_0.

Pomerance guesses that $c_0 = 6$ and that in any event the argument above can be made more explicit and c_0 may be found.

5. If it is desired to compute an explicit C such that $R\big((p, p+C)\big) > R\big((p, p+6)\big)$, then instead of using the Erdős sequence above it may be better to use the greedy admissible sequence 3,5,11,17,23,41,47,53,71,....

96:02 (Neville Robbins) Let $H(z) = \sum_{n=0}^{\infty} z^{2^n}$. Can $H(z)$ be expressed in terms of well-known functions?

Remark: Pat Morton points out that this function has been studied, e.g., by Mahler in his work on transcendence. A reference is J. H. Loxton and A. J. van der Poorten, Transcendence and algebraic independence by a method of Mahler, in Transcendence Theory—Advances and Applications, A. Baker and D. W. Masser, eds., 211–226.

Remark: Dick Katz writes, "$H(z)$ has the unit circle as a natural boundary so that if "well known" only allows functions with isolated singularities, then certainly no rational function of such functions will work. Indeed, I think it is unlikely that any algebraic function of such functions could have a dense set of singularities on the unit circle. I don't have a proof of this however."

96:03 (Jon Grantham) Given $r \geq 1$ and x, how many squarefree, composite n are there up to x such that if p is prime and $p \mid n$ then $p^r - 1 \mid n - p$? Call the answer $f_r(x)$. The work of Alford, Granville, and Pomerance shows that $f_1(x) >> x^{2/7}$, while a heuristic argument of Erdős suggests $f_1(x) >> x^{1-\epsilon}$.

A heuristic argument of Pomerance would give $f_2(x) >> x^{1-\epsilon}$, but no such n is known. How can we find one? many?

For $r \geq 3$, what are good heuristics?

The case $r = 3$ relates to Perrin pseudoprimes of type I (no reference supplied).

Remark: Without the condition that n be squarefree, there are trivial examples where n is a prime power. There are also non-trivial examples found by Zachary Franco and Peter Montgomery. Noting that $3^5 \equiv -1 \pmod{5^3 - 1}$ and $5^2 \equiv -1 \pmod{3^3 - 1}$ they find $n = 3^{10}5^8 \equiv p \pmod{p^3 - 1}$ for all $p \mid n$. Also, $n = 53 \cdot 5^{36m} \equiv p \pmod{p^2 - 1}$ for all $p \mid n$, and, if m is chosen so that $\phi(691^3 - 1) \mid 3m$, then $n = 691 \times 7^{3m} \equiv p \pmod{p^3 - 1}$ for all $p \mid n$.

96:04 (Pal Erdős† and Carl Pomerance) Let $S(n) = \sum_{p^a \| n} ap$. Show $\sum_{S(n)=S(n+1)} \frac{1}{n}$ converges.

96:05 (Tom Dence & Carl Pomerance) Suppose a, k are integers with $k > 0$ such that there exist even numbers m with $m \equiv a \pmod{k}$. Are there infinitely many n such that $\phi(n) \equiv a \pmod{k}$?

Dence and Pomerance can show this if there exists an m, $4 \mid m$, with $m \equiv a \pmod{k}$.

96:06 (Paul Feit) Let $\mathbf{F} = \mathbf{Z}/2\mathbf{Z}$, let n be in $\mathbf{N}$, let $g : \mathbf{F}^n \to \mathbf{F}$ be any function. For $i = 0, 1$ define permutations α_i on $\mathbf{F}^{n+1}$ by $\alpha_i(x_0, \ldots, x_n) = \big(x_1, \ldots, x_n, x_0 + i + g(x_1, \ldots, x_n)\big)$. What is the group generated by $\{\alpha_0, \alpha_1\}$? What groups can appear this way?

If g is linear, the group is a semi-direct product of $\mathbf{F}^{n+1}$ with a cyclic group.

96:07 (Vsevolod Lev) Let A be a set of n distinct residues modulo a prime p, with $n < p$. For z in $\mathbf{F}_p$, write $S_A(z) = \sum_{a \in A} e^{2\pi i a z/p}$. Let Z be a set of residues (mod p) with $\#(Z) = m > (1 - \epsilon)p$ for some $\epsilon > 0$. Find a lower bound for $G_Z = \frac{1}{m} \sum_{z \in Z} |S_A(z)|^2$. Is it true that $G_Z \geq 1$?

Using $\prod_{z \neq 0} |S_A(z)|^2 \geq 1$ and the inequality between arithmetic and geometric means, it is easy to prove $G_Z > n^{-2(p-m)/m}$; hence, $G_Z > n^{-2\epsilon/(1-\epsilon)}$ if $m > (1 - \epsilon)p$.

Remark: If $n = 1$ then $G_Z = 1$, so presumably we should exclude this case.

If $n = 2$ and $A = \{\, a, b \,\}$ then $G_Z = 2 + \frac{2}{m} \sum_{z \in Z} \cos 2\pi(a - b)z/p$, and the assertion is easily verified.

Lev reports that S. Konyagin notes that for any $\epsilon > 0$ and any p sufficiently large there exists Z such that $\#(Z) \geq \frac{p}{2}$ and $G < \epsilon$. Thus, the problem should be posed with a restriction like $\#(Z) > (.9)p$.

The same question can be asked more generally in $\mathbf{F}_q$, the field of $q = p^r$ elements. For $A \subset \mathbf{F}_q$ and z in $\mathbf{F}_q$ write $S_A(z) = \sum_{a\in A} e^{2\pi i(\mathrm{Tr}\, az)/p}$, where Tr is the trace from $\mathbf{F}_q$ to $\mathbf{F}_p$. Given $Z \subset \mathbf{F}_q$ with $\#(Z) = m > (.9)q$, find a lower bound for $G_Z = \frac{1}{m}\sum_{z\in Z} |S_A(z)|^2$.

96:08 (Bjorn Poonen, via Ed Schaefer) Given $\epsilon > 0$, does there exist a bound B depending only on ϵ such that the following is true?

Let $m_1, m_2, \ldots, m_r$ be relatively prime positive integers, let $N = m_1 m_2 \ldots m_r$. For $i = 1, 2, \ldots, r$ let S_i be a two-element subset of $\mathbf{Z}/m_i\mathbf{Z}$. Then

$$\#\{\, x \text{ in } \mathbf{Z} : 0 \le x \le N^{1-\epsilon} \text{ and } (x \bmod m_i) \in S_i \text{ for all } i \,\} \le B.$$

Poonen adds the following remarks.

1. The same question can be asked for $\#(S_j) = d$ for any fixed $d \ge 2$, with B allowed to depend on d as well as on ϵ.

2. A positive answer to this question with $d = 4$ would imply the truth of the conjecture that the number of rational preperiodic points of a quadratic polynomial over $\mathbf{Q}$ is uniformly bounded. Moreover, an explicit bound for the latter could be given, if we had an explicit B above. See P. Morton and J. Silverman, Rational periodic points of rational functions, Internat. Math. Res. Notices (1994) 97–110.

3. Andrew Granville has shown that the answer to the question for $\#(S_j) = d$ is yes if one replaces the exponent $1 - \epsilon$ by $\frac{1}{d} - \epsilon$.

96:09 (John Brillhart) Is it true that a base 2 pseudoprime never divides the primitive part of $3^n - 1$? If so, then if $2^{N-1} \equiv 1 \pmod{N}$, and N is a factor of the primitive part of $3^n - 1$, then N is prime.

Solution by Jon Grantham:

Carl Pomerance notes that if $p \equiv 1 \pmod 4$ is prime and $2p-1$ is prime then $p(2p-1)$ is a base 2 pseudoprime. Among the first 20000 such p, 102 have $\mathrm{ord}_p 3 = \mathrm{ord}_{2p-1} 3$, each one answering Brillhart's question in the negative. The smallest of these has $p = 337$ (so $p-1 = 336 = 2^4 \cdot 3 \cdot 7$), $2p-1 = 673$, and $\phi_{168}(3) = 337 \times 673 \times 1009 \times 167329 \times 2108826721$.

Solution by Peter Montgomery:

If $p \equiv 11 \pmod{12}$ is prime and $2p+1$ is prime then $2p+1$ divides both $2^p - 1$ and $3^p - 1$. Also, 50207 divides both $2^{1931} - 1$ and $3^{1931} - 1$. So $n = 3863 \times 50207$ answers Brillhart's question.

John Brillhart remarks that the number of examples found suggests the only problem here is whether the primitive part of $3^n - 1$ itself is ever a base 2 pseudoprime. It might also be interesting if a Carmichael number ever divided (or was equal to) the primitive part of $a^N - 1$ for some $a > 1$.

96:10 (Gerry Myerson) Estimate $\mathrm{LCM}\{\, 2^k - 3 : 1 \le k \le n \,\}$. Note that $\log \prod_{k=1}^{n} (2^k - 3) = \frac{\log 2}{2} n^2 \bigl(1 + o(1)\bigr)$; does the same estimate hold for the logarithm of the LCM?

96:11 (Gerry Myerson) Let $f(m)$ be the smallest odd prime p such that $p \mid m - 2^k$ for some $k = 0, 1, 2, \ldots$. Prove that $f(m) = o(m)$.

Remark: Since $|m - 2^k| \leq \frac{m}{3}$ for some k, we have $f(m) \leq m/3$. We also have $f(m) < x$ unless m is divisible by all the primes $p < x$ for which 2 is a primitive root. Expanding on this we can compute, e.g., $f(m) \leq 23$ for $m < 500000$. Perhaps $f(m)$ is bounded by a fixed power of $\log m$.

96:12 (Gary Walsh) Let $I_S = \{ \prod_{j=1}^{k} p_j^{e_j} : e_j \geq 0 \}$, where $S = \{ p_1, \ldots, p_k \}$ is a finite set of primes. Let $D_S = \{ (p, q) : p, q \text{ prime and } p - q \in I_S \}$. Is D_S infinite? In particular, what if $S = \{ 2 \}$?

96:13 (Jeff Lagarias) These conjectures are made in Frits Beukers, Consequences of Apery's work on $\zeta(3)$, which appeared in $\zeta(3)$ irrationnel: les retombées, an informal proceedings volume of the Rencontres Arithmétiques de Caen 2–3 June 1995, published by the Equipe Algèbre, Algorithmique, Arithmétique at Caen. Let $a_n = \sum_{k=0}^{n} \binom{n+k}{k}^2 \binom{n}{k}^2$. Then $5^p \mid a_n$, where p is the number of 1s and 3s in the base 5 notation for n. (Note: it is not claimed that $5^p \| a_n$). Also, $11^q \mid a_n$, where q is the number of 5s in the base 11 notation for n.

96:14 (Richard McIntosh, via Gerry Myerson) The largest known prime of the type $n = (2^{4p}+1)/17$ has $p = 317$, and n is composite for all primes p such that $317 < p < 10000$. Are there any more primes of this type, or is this a large gap?

96:15 (Bart Goddard, via Gerry Myerson) Given $p(z)$, a polynomial with complex coefficients and degree n, can one find $f(z)$ analytic, or a polynomial of degree at most $n/2$, or of the form $\frac{az+b}{cz+d}$, such that $p\big(f(z)\big)$ is a non-constant polynomial with real coefficients, or with all of its roots on the unit circle?

96:16 (Gerry Myerson) Prove that there is a positive constant c such that

$$\#\{ n \leq x : [(4/3)^n] \text{ is composite} \} > cx.$$

There are heuristic arguments supporting much sharper estimates for the number of primes and composites in an initial segment of the sequence $[(4/3)^n]$, but the statement above would already be far better than any known result.

96:17 (Gerry Myerson) Prove that for every non-zero real α there is a positive integer n (hence, infinitely many n) such that $[10^n \alpha]$ is composite. Equivalently, show that there is no infinite sequence of primes, each obtained from the previous by tacking a single digit on at the end.

The analogous result has been proved for bases 2 through 6.

96:18 (Greg Martin) Let p be a prime, let $N(p)$ be the least quadratic non-residue $(\mathrm{mod}\ p)$, and let $g(p)$ be the least primitive root $(\mathrm{mod}\ p)$. Note that $g(p) \geq N(p)$.

There are Ω-results for $N(p)$(recall that $f(x) = \Omega\big(g(x)\big)$ means $\limsup \frac{f(x)}{g(x)} > 0$).

Unconditionally, $N(p) = \Omega(\log p \log\log\log p)$ (Graham & Ringrose); on the generalized Riemann Hypothesis, $N(p) = \Omega(\log p \log\log p)$ (H. Montgomery).

Can one prove a stronger Ω-theorem for $g(p)$, conditional or otherwise?

Heuristically, one can expect at least $g(p) = \Omega\big(\log p (\log\log p)^2\big)$.