Western Number Theory Problems, 18 & 20 Dec 2006

Edited by Gerry Myerson

for distribution prior to 2007 (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	96:01–96:18	1997 Asilomar	97:01–97:22
1998 San Francisco	98:01–98:14	1999 Asilomar	99:01–99:12
2000 San Diego	000:01–000:15	2001 Asilomar	001:01–001:23
2002 San Francisco	002:01–002:24	2003 Asilomar	003:01–003:08
2004 Las Vegas	004:01–004:17	2005 Asilomar	005:01–005:12
2006 Ensenada (current set) 006:01–006:15			

[With comments on 005:11]

COMMENTS ON ANY PROBLEM WELCOME AT ANY TIME

Department of Mathematics,
Macquarie University,
NSW 2109 Australia
gerry@math.mq.edu.au
Australia-2-9850-8952 fax 9850-8114

Comment on an earlier problem

005:11 (Lenny Jones) Is it true that if $1 < r < s$ then $\gcd(10^{2^r} + 1, 3^{2^s} + 1) = 1$? It is not true if $r = s$ is allowed, e.g., the gcd is 17 if $r = s = 3$.

Solution: (Mike Filaseta) The answer is, "No." A prime p divides $10^{2^r} + 1$ if and only if $\mathrm{ord}_p(10) = 2^{r+1}$, and similarly an odd prime p divides $3^{2^s} + 1$ if and only if $\mathrm{ord}_p(3) = 2^{s+1}$. One can check that $p = 5 \cdot 2^{127} + 1$ satisfies $\mathrm{ord}_p(10) = 2^{125}$ and $\mathrm{ord}_p(3) = 2^{127}$. Hence,

$$\gcd\left(10^{2^{124}} + 1, 3^{2^{126}} + 1\right) > 1.$$

Mike continues: the following heuristic would suggest that there are many examples like this. The number $p = k \cdot 2^t + 1$ is prime with probability $\gg 1/(t \log 2 + \log k)$ (with implied constants absolute). Given that p is prime, the probability that $\mathrm{ord}_p(10)$ divides 2^t is $\gg 1/k$ and the probability that $\mathrm{ord}_p(3)$ divides 2^t is $\gg 1/k$. Given that these occur, the probability that $\mathrm{ord}_p(10) < \mathrm{ord}_p(3)$ is $\gg 1$. Hence, for fixed positive integers k and t, the probability that the prime p divides $10^{2^r} + 1$ and $3^{2^s} + 1$ for some positive integers $r < s$ is

$$\gg \frac{1}{k^2(t \log 2 + \log k)}.$$

This suggests that if we fix k small and let t vary, we should come up with some examples, which is what I did. Since for fixed k, the sum over t diverges, the heuristic also suggests that there should be infinitely many similar examples.

Problems Proposed 18 & 20 Dec 2006

006:01 (Claude Anderson, via Carl Pomerance) Is it true that if n is even and m is odd then $\sigma(n)/n \neq \sigma(m)/m$?

Remark: If so, then there are no odd perfect numbers.

006:02 (Carl Pomerance) Is it true that if m and n are greater than one and $\gcd(n, m) = 1$ then $\sigma(n)/n \neq \sigma(m)/m$?

Remark: If so, and if there are infinitely many even perfect numbers, then there are no odd perfect numbers.

006:03 (Mel Nathanson, via Carl Pomerance) For p prime, and for $\mathbf{a} = (a_1, \ldots, a_d)$ with non-zero entries modulo p, let

$$h(\mathbf{a}) = \min_{1 \le k \le p-1} \sum_{i=1}^{d} (k a_i \bmod p)$$

where "$u \bmod p$" means the integer in $[0, p-1]$ congruent to u modulo p. Suppose none of the quantities $a_i \pm a_j$, $a_i + a_j + a_k$ vanish modulo p for distinct i, j, and k. Must it be true that $h(\mathbf{a}) \le p(p - 1 - 2d)/4$?

Remark: If so, a conjecture of Chudnovsky, Seymour, and Sullivan in graph theory holds.

006:04 (Bart Goddard) A positive integer n is *abundant* if $\sigma(n) > 2n$, *deficient* if $\sigma(n) < 2n$. It is *abundantly deficient* if

$$\#\{\, 1 \le x \le n : x \text{ is deficient} \,\}$$

is abundant. For example, 14 is a.d. because there are 12 deficient numbers not exceeding 14, and 12 is abundant. For which k are there infinitely many strings of k consecutive a.d. numbers?

With the obvious definition, for which k are there infinitely many strings of k consecutive deficiently abundant numbers?

Solution: Florian Luca calls n a *Goddard number* if it is deficient and abundantly deficient. He proves that there are infinitely many strings of 5 consecutive Goddard numbers, but the proof is too long to include here. He also points out that there cannot be 6 consecutive Goddard numbers, since multiples of 6 cannot be deficient.

006:05 (Andrew Shallue) Given a positive integer m, and integers $a_1, \ldots, a_n$, define X by $X = \sum_{i=1}^{n} a_i x_i$, where x_i are chosen from $\{\, 0, 1 \,\}$ uniformly at random, and let

$$\Delta(X) = \frac{1}{2} \sum_{a=0}^{m-1} \left| \Pr\{\, x \equiv a \pmod{m} \} - \frac{1}{m} \right|$$

(i) Assume a_i are not all in some proper subgroup of $\mathbf{Z}/m\mathbf{Z}$, and assume $m < 2^n$. Find a non-trivial upper bound on $\Delta(X)$.

(ii) Find conditions on a_i, m, and n that make $\Delta(X)$ exponentially small.

006:06 (Florian Luca) Are there infinitely many n such that all the numbers obtained by deleting a single digit of n are prime? An example is $n = 131$.

Remark: Yes, if, as is expected to be the case, there are infinitely many primes of the form $(10^p - 1)/9$. There may be easier ways to prove it.

006:07 (Artūras Dubickas) Is there a nonzero number which is a root of some nonzero polynomial with coefficients 0 and 1 ("Newman polynomial") but is not a root of any polynomial with coefficients -1 and 1 ("Littlewood polynomial")?

006:08 (Florian Luca) A *Niven number* is a number that is divisible by the sum of its digits. Are there infinitely many Fibonacci numbers that are Niven numbers?

Remark: Heuristics, based on the counting function for the Niven numbers being asymptotic to $cx/\log x$, suggest the answer is yes.

006:09 (Roger Oyono) Give a small q_0 such that for every $q > q_0$ and every smooth plane quartic C defined over $\mathbf{F}_q$ there is a line ℓ defined over $\mathbf{F}_q$ such that the intersection points of C and ℓ are all defined over $\mathbf{F}_q$.

Can we also give q_1 (resp., q_2) such that there is a tangent line (resp., tangent line at a flex) such that all the intersection points are defined over $\mathbf{F}_q$?

Remark: It is known that q_0 can be taken to be 10^6; what is wanted is something considerably smaller. Best of all would be the minimal value of q_0.

006:10 (John Brillhart) How can one tell whether a function given by a power series has any multiple roots?

Remark: A polynomial has a multiple root if and only if the resultant of the polynomial and its derivative is zero, and this resultant can be computed as the determinant of a matrix, without knowing (or learning) the roots of the polynomial. The question is whether there is such an algorithm for analytic functions. Since a perturbation in any coefficient of the series could make the difference between existence of multiple roots and nonexistence, it would seem that a finite procedure is impossible.

006:11 (John Brillhart) What is the probability that a polynomial chosen uniformly at random from the polynomials of a given degree n over a given field of p elements has a multiple root in some extension field?

006:12 (Gary Walsh) Find all solutions of $(a^k - 1)(b^k - 1) = y^2$ with $1 < a < b \le 100$, $(a-1)(b-1)$ a square, and $k > 1$.

Remark: Walsh and Luca have found all the solutions in the given range such that $(a-1)(b-1)$ not a square.

006:13 (Gerry Myerson and Jamie Simpson) An incongruent restricted disjoint covering system (IRDCS) for $[1, n]$ is a collection of congruences $x \equiv a_i \pmod{m_i}$, $i = 1, \ldots, t$, with $1 < m_1 < \ldots < m_t$, such that every x in $[1, n]$ satisfies exactly one of the congruences, and every congruence is satisfied by at least two numbers in $[1, n]$. Such things exist; $(a_i, m_i) = (0, 3), (0, 4), (0, 5), (1, 6), (2, 9)$ for $i = 1, \ldots, 5$ is an IRDCS for $[1, 11]$.

If $x \equiv a_i \pmod{m_i}$, $i = 1, \ldots, t$ is an IRDCS for $[1, n]$, then $x \equiv 2a_i \pmod{2m_i}$, $i = 1, \ldots, t$ together with $x \equiv 1 \pmod 2$ is an IRDCS for $[1, 2n + 1]$. We call this *doubling*.

(i) Are there infinitely many IRDCS, not counting those obtained from smaller systems by doubling?

(ii) Is there an IRDCS for $[1, n]$ for all $n \ge 17$?

(iii) Are there IRDCS with arbitrarily large values of m_1?

(iv) Is there an IRDCS with all m_i odd?

(v) Find sharp upper and lower bounds for $h = \sum_{i=1}^{t} (1/m_i)$.

(vi) Given $k > 2$, is there an IRDCS such that every congruence is satisfied by at least k numbers in $[1, n]$?

(vii) Generalize to covering systems for $[1, n_1] \times \ldots \times [1, n_r]$, $r > 1$.

Remarks: Myerson, Jacky Poon, and Simpson have another construction producing infinitely many IRDCS. Given an IRDCS in which n is an odd multiple of 3, the modulus m covering 1 satisfies $m > 2n/3$, $3m - n - 1$ is not a power of 2, and no modulus m_i is a power of 2, we construct an IRDCS for $[1, 3n]$ with the same properties. As we know of an IRDCS for $[1, 27]$ satisfying the properties, the construction yields an affirmative answer to (i).

We have examples of IRDCS for $[1, n]$ for all n with $17 \le n \le 32$, and together with a modification of the doubling procedure this yields an affirmative answer to (ii). There is no IRDCS with $n = 16$, so this is a best possible result.

Concerning (v), we can prove $1/2 \le h \le 3/2$, but in all the examples we have found, $.98834\ldots \le h \le 1.06768\ldots$.

006:14 (Iekata Shiokawa) Let F_n, $n = 1, 2, \ldots$, be the Fibonacci numbers, starting with $F_1 = 2$. Let $\xi_F(s) = \prod_{n=1}^{\infty}(1 - F_n^{-s})^{-1}$. Is $\xi_F(1)$ rational?

006:15 (Florian Luca and Carl Pomerance) Let $U(N) = (\mathbf{Z}/N\mathbf{Z})^*$ be the multiplicative group of units modulo N. Show that the number of solutions A, B, C of $U(A) \oplus U(B) \simeq U(C)$ with $\max(A, B, C) \leq X$ is $X^{2+o(1)}$ (the UABC conjecture).