Western Number Theory Problems, 17 & 19 Dec 2011

Edited by Gerry Myerson

for distribution prior to 2012 (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	006:01–006:15		2007 Asilomar	007:01–007:15
2008 Fort Collins	008:01–008:15		2009 Asilomar	009:01–009:20
2010 Orem	010:01–010:12		2011 Asilomar	011.01–011.16

COMMENTS ON ANY PROBLEM WELCOME AT ANY TIME

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

Problems proposed 17 and 19 December 2011

011.01 (quasi of the Usenet newsgroup sci.math, via Bart Goddard). Is it true that for every prime $q > 2$ there is a prime $p < q$ such that p is a primitive root modulo q and q is a primitive root modulo p?

Remarks: Carl Pomerance says,

1. It is widely believed that every prime $q > 2$ has a prime primitive root $p < q$, but no such result has been proved.

2. There are infinitely many primes q for which there is a prime $p < q$ such that p is a primitive root modulo q and q is a primitive root modulo p. By a result of Heath-Brown, at least one of the three numbers in $S = \{ 5, 17, 257 \}$ is a primitive root for infinitely many primes q. If p in S is a primitive root modulo q, then it is a quadratic nonresidue modulo q. By quadratic reciprocity, q is a quadratic nonresidue modulo p (since $p \equiv 1 \pmod 4$), hence, a primitive root modulo p (since p is a Fermat prime).

3. (who?) Computations show that for every odd prime $2 < q < 300,000$ there is a prime $p < q$ such that p is a primitive root modulo q and q is a primitive root modulo p. For no q in this range does one need $p > 300$.

011.02 (quasi of the Usenet newsgroup sci.math, via Bart Goddard). Suppose there is a nonconstant polynomial $f(x)$ with integer coefficients, a prime p, and a number a such that for all n every prime q dividing $f(n)$ satisfies $q \equiv a \pmod p$. Is it true that $a \equiv 1 \pmod p$?

Remark: The best-known example takes $f(x)$ to be the mth cyclotomic polynomial $\phi_n(x)$; then it is known that if q is prime and $q \mid f(n)$ for some n then $q \equiv 1 \pmod m$.

Solution: Florian Luca writes, suppose we have such $f(x)$, p, and a. Consider the polynomial $g(x) = f(x)\phi_p(x)$. By the Cebotarev density theorem, there is a prime q such that g splits completely modulo q. Since f has a zero modulo q, we know that $q \equiv a \pmod p$; since ϕ_p has a zero modulo q, we know $q \equiv 1 \pmod p$. Thus, $a \equiv 1 \pmod p$.

011.03 (quasi of the Usenet newsgroup sci.math, via Bart Goddard). Given a positive integer n, we can write $n = 2^{k_1} + 2^{k_2} + \ldots$ with integers $k_1 < k_2 < \ldots$; of course, this is a finite sum. We define $a = a(n) = 2^{k_1} + 2^{-k_2} + 2^{k_3} + \ldots$ and $b = b(n) = 2^{-k_1} + 2^{k_2} + 2^{-k_3} + \ldots$. Is it true that if n is an odd prime and $\max(a/b, b/a)$ is an integer then n is a Fermat prime?

Solution: We find it convenient to change the notation so $k_1 > k_2 > \cdots > k_r = 0$, where r is the number of ones in the binary notation for n, and n is odd. We take

$$a = 2^{k_1} + 2^{-k_2} + 2^{k_3} + \ldots \quad \text{and} \quad b = 2^{-k_1} + 2^{k_2} + 2^{-k_3} + \ldots$$

We note that $a \geq 2^{k_1}$, and it is easy to show that $b < 2^{k_1}$, so

$$\max(a/b, b/a) = a/b = \frac{2^{k_1} + 2^{-k_2} + 2^{k_3} + \ldots}{2^{-k_1} + 2^{k_2} + 2^{-k_3} + \ldots}$$

Note that if $r = 2$ then $a/b = (2^{k_1} + 1)/(2^{-k_1} + 1) = 2^{k_1}$ is an integer, and if $n = 2^{k_1} + 1$ is a prime then it is necessarily a Fermat prime.

Now assume $r > 2$. We'll prove that if n is odd and a/b is an integer then n is composite. We have $a/b = 2^m(u/v)$ where $m = k_1 - k_2$, and $u = 2^{k_1+k_2} + 2^{k_2+k_3} + \ldots + 2^{k_2-k_4} + 1$ and $v = 2^{k_1+k_2} + 2^{k_1+k_4} + \ldots + 2^{k_1-k_3} + 1$ are both odd. Now r and s are both between $2^{k_1+k_2}$ and $2^{k_1+k_2+1}$, so if a/b is an integer then it is 2^m, and $u = v$. The last equation implies

the equations $k_1 + k_{2j} = k_2 + k_{2j-1}$ for $2 \le j \le (r-2)/2$, and also $k_1 = k_2 + k_{r-1}$. This yields the equations $k_{2j-1} = k_{2j} + k_{r-1}$, $1 \le j \le (r-2)/2$. Now it follows that n factors as $n = (2^{k_{r-1}} + 1)(2^{k_2} + 2^{k_4} + \cdots + 2^{k_{r-2}} + 1)$, and we're done.

011.04 (David Terr) A primitive Pythagorean triple (PPT) is a triple (a, b, c) of coprime positive integers such that a is odd, b is even, and $a^2 + b^2 = c^2$.

A type-1a nearly Pythagorean pair (NPP) is a pair of positive coprime integers (m, n) such that there is a PPT (a, b, c) with $mc - nb = \pm 1$.

A type-1b NPP is a pair of positive coprime integers (m, n) such that there is a PPT with $mc - na = \pm 1$.

A type-2 NPP is a pair of positive coprime integers (m, n) such that there is a PPT with $mb - na = \pm 1$.

For example, $(3, 4)$ is a type-1b NPP since $(55, 48, 73)$ is a PPT and $(3)(73) - (4)(55) = -1$.

Let $\pi^{(1a)}(X)$ (respectively, $\pi^{(1b)}(X)$) be the number of type-1a (respectively, type-1b) NPPs (m, n) with $m < n \le X$.

Let $\pi^{(2)}(X)$ be the number of type-2 NPPs (m, n) with $m \le X$ and $n \le X$.

Find asymptotic formulas for $\pi^{(1a)}(X)$, $\pi^{(1b)}(X)$, and $\pi^{(2)}(X)$ as $X \to \infty$.

011.05 (David Bailey) Given coprime integers $b \ge 2$ and $c \ge 2$, the constant

$$\alpha_{b,c} = \sum_{k=0}^{\infty} \frac{1}{c^k b^{c^k}}$$

is known to be normal to base b. In particular, $\alpha_{2,3}$ and $\alpha_{2,5}$ are normal to base 2. Is $\alpha_{2,3} + \alpha_{2,5}$ normal to base 2?

More generally, if $\alpha_{b,c}$ and $\alpha_{b,d}$ satisfy the conditions given here for normality to base b, is $\alpha_{b,c} + \alpha_{b,d}$ normal to base b?

References: 1. David H. Bailey, Michal Misiurewicz, A strong hot spot theorem, Proc. Amer. Math. Soc. 134 (2006) 2495-2501, MR 2007b:11108.

2. David H. Bailey, Jonathan M. Borwein, Cristian S. Claude, Michael J. Dineen, Monica Dumitrescu, Alex Yee, An empirical approach to the normality of pi, manuscript of 27 Nov 2011, http://crd.lbl.gov/∼dhbailey/dhbpapers/normality.pdf

011.06 (Carl Pomerance) Is there a constant C such that if $S \subset \{ 1, 2, \ldots, n \}$ and the Euler ϕ-function is monotone on S then

$$\sum_{n \text{ in } S} \frac{1}{n} \le \log\log n + C$$

Remarks: 1. Of course ϕ is monotone (increasing) on the primes, and there is a constant b such that

$$\sum_{p \le n} \frac{1}{p} \le \log\log n + b$$

2. The problem is related to work with Paul Pollack and Enrique Trevino available in preprint form on www.dartmouth.edu/∼carlp.

011.07 (Carl Pomerance) Is there a number n with fewer than 100 million digits such that for some $S \subset \mathbf{Z}/n\mathbf{Z}$ with $\#(S) > n/2$ we have all the pairwise products of members of S lying outside S?

Remark: By work with Pär Kurlberg and Jeffrey Lagarias, available in preprint form at the site mentioned above, there is such an n with about 160 million digits.

011.08 (Carl Pomerance) Is there a number n with fewer than one billion digits such that for some $S \subset \mathbf{Z}/n\mathbf{Z}$ with $\#(S) > 2n/5$ we have all the pairwise products and all the pairwise sums of members of S lying outside S?

Remarks: 1. By work with Kurlberg and Lagarias, soon to be available at the website above, it is known that such n exist, but not necessarily with fewer than one billion digits. Also, n must be even, and S must be a subset of the odd residues.

2. Note that for $n = 5$, $S = \{2, 3\}$ satisfies the product and sum conditions, and $\#(S) = 2n/5$.

011:09 (Victor Miller; additional information courtesy Joe Buhler) Let n be a positive integer, written in base 3. "Compress" the number by inserting plus signs wherever you wish between pairs of ternary digits of n, and computing the resulting sum. It is known that no matter what n is it takes at most three compressions to reduce the number to a single digit. Is it true that, for all sufficiently large n, two compressions suffice?

Example. Let $n = 121221211222$. Then

$$1 + 2 + 1 + 22 + 1 + 2 + 1 + 1 + 2 + 22 = 1000$$

and $1 + 000 = 1$.

Remark: This problem, for arbitrary bases, is due to Gregory Galperin. The base 2 version (where two compressions always suffice) is given in the Fall 2011 issue of The Emissary, the newsletter of the Mathematical Sciences Research Institute, online at

http://www.msri.org/attachments/media/news/emissary/EmissaryFall2011.pdf

It is known that 3 compressions suffice in any sufficiently large base (likely this just means 3 or larger), and it is possible that 2 compressions suffice in any base when the starting integer has sufficiently large digit sum.

011.10 (Andrew Shallue) Suppose $n = \prod_1^r p_i$ is a product of distinct primes. Is there an algorithm that computes the first m digits of n using $O(m)$ space?

Solution: David Bailey writes, compute $\sum \log p_i$, keeping track of the errors. Kjell Wooding writes, "There are many papers on the subject. The search term to use is 'online arithmetic,' E.g. http://people.ee.duke.edu/~kst/capapers/alg.pdf, though there are many more recent than that. Usually, the approach involves using a redundant representation so you don't have to worry about the carry propagation."

011.11 (David Moulton) Is there an algorithm for computing $2^{2^d} \pmod m$ in time polynomial in $\log d$ and $\log m$?

011.12 (David Moulton) Is there an algorithm to compute $2^{2^{2^d}} \pmod p$ for p prime in polynomial-time?

Remark: This reduces to computing $2^{2^d} \pmod{p-1}$, a case of the previous problem.

011.13 (Nikhil Bellarykar via Gerry Myerson) Let $f(x,y)$ in $\mathbf{Z}[x,y]$ be irreducible such that $f(n,\phi(n))=0$ for infinitely many n (ϕ is Euler's phi-function). Is it possible that f is "not identically zero"?

Remarks: 1. Some examples may clarify the meaning of "not identically zero." If $f(x,y)=x-y-1$, then $f(p,\phi(p))=0$ for all primes p. If $f(x,y)=(x-y)^2-x$ then $f(p^2,\phi(p^2))=0$ for all primes p. These polynomials are identically zero for n having a particular factorization pattern; are there any examples that are "accidentally" zero infinitely often?

2. Florian Luca notes that for an irreducible polynomial $f(x,y)$ to have infinitely many integer zeros, it must be of genus zero. Of course, even if $f(x,y)=0$ has infinitely many integer solutions, it need not have solutions with $y=\phi(x)$. Florian notes two relevant publications:

Yuri F. Bilu, Robert F. Tichy, The diophantine equation $f(x)=g(y)$, Acta Arith. 95 (2000) 261–288, MR 2001i:11031.

Florian Luca, Michal Křížek, On the solutions of the congruence $n^2\equiv 1 \pmod{\phi^2(n)}$, Proc. Amer. Math. Soc. 129 (2001) 21912196, MR 2002b:11006.

011.14 (Syrous Marivani)

Let

$$(a;q)_\infty=\prod_{k=0}^{\infty}(1-aq^k)$$

One can show that

$$\frac{(q;q)_\infty}{(q^{121};q^{121})_\infty}=a+bq+cq^2+eq^4+q^5+fq^7$$

where a,b,c,e,f are power series in q^{11} with integer coefficients. One can also show that

$$\begin{aligned}\sum_{n=0}^{\infty}p(n)q^n&=\frac{1}{(q;q)_\infty}=\frac{(q^{121};q^{121})_\infty^{11}(q^{11};q^{11})_\infty^{12}(q^{121};q^{121})_\infty}{(q^{11};q^{11})_\infty^{12}(q^{121};q^{121})_\infty^{12}(q;q)_\infty}\\&=\frac{(q^{121};q^{121})_\infty^{11}}{(q^{11};q^{11})_\infty^{12}}\frac{\prod_\omega(a+\omega bq+\omega^2cq^2+\omega^4eq^4+\omega^5q^5+\omega^7fq^7)}{a+bq+cq^2+eq^4+q^5+fq^7}\end{aligned}$$

where ω runs through the 11th roots of unity, and $p(n)$ is the partition function.

Can we simplify the right side of this identity when n runs through all the positive integers of the form $11m+6$, and obtain an identity for $\sum_{m=0}^{\infty}p(11m+6)q^{11m+6}$ of the type seen in the proof of Ramanujan's congruence identities modulo 5 and modulo 7, as given in Bruce Berndt's book, Number Theory in the Spirit of Ramanujan?

011.15 (Glenn Henshaw) Find a quadratic form Q in $\mathbf{Z}[x_1,\dots,x_N]$ and a polynomial P in $\mathbf{Z}[x_1,\dots,x_N]$ such that there is a nonzero x in $\mathbf{Z}^n$ such that $Q(x)=0$ and $P(x)\neq 0$, and any such x satisfies

$$\max_i|x_i|\geq|Q|^{(N+r)/2}$$

for some real $r>1$, where $|Q|$ is the sum of the absolute values of the coefficients of Q.

Remarks: 1. R. Dietmann, Small zeros of quadratic forms avoiding a finite set of prescribed hyperplanes, Canad. Math. Bull. 52 (2009) 63–65, MR 2009k:11063, shows that this is not possible if P is a product of linear polynomials.

2. D W Masser, How to solve a quadratic equation in rationals, Bull. London Math. Soc. 30 (1998) 24–28, MR 98m:11017, gives a construction of a quadratic form and a linear form such that every zero of the quadratic form that is not a zero of the linear form is bounded as above, but with $r = 1$.

011.16 (Robert Akscyn) We note that

$$\pi(n) = n - 1 - \sum_{2 \le p \ e\sqrt{n}} R\left(\frac{n}{p}, p\right)$$

where

$$R(h,p) = \#\{\, n \le h : \text{if } q \mid n \text{ and } q > 1 \text{ then } q \ge p \,\}$$

We have the recurrence relation

$$R(h, p_i) = R(h, p_{i-1}) - R\left(\frac{h}{p_{i-1}}, p_{i-1}\right) - 1$$

and we can compute $R(h,p)$ recursively from $R(h,p) = 0$ if $h < p$, $h - 1 - \sum_{2 \le q < p}(R(\frac{h}{q}, q) + 1)$ otherwise. Can this formulation for $\pi(x)$ be trnsformed to a series or closed form which can be readily compared with $\mathrm{Li}(x)$? What's hoped for is something like

$$|\pi(x) - \mathrm{Li}(x)| = O(\sqrt{x} \log x)$$

(which von Koch proved equivalent to the Riemann Hypothesis).