Western Number Theory Problems, 16 & 18 Dec 2015

for distribution prior to 2016 (Monterey) meeting

Edited by Gerry Myerson based on notes by Kjell Wooding

Draft of 17 March 2016

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
2012 Asilomar	012:01–012:17		2013 Asilomar	013.01–013.13
2014 Monterey	014:01–014:11		2015 Monterey	015:01–015:15

[With comments on 013:05]

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

Comments on earlier problems

013:05 (David Thomson). Let p be a prime, let $r = tn + 1$ be a different prime, let $q = p^e$. Let

$$K = \{\, 1, \omega, \ldots, \omega^{t-1} \,\}$$

with ω a primitive t-th root of unity in the field of r elements. Let $K_i = q^i K$. Define the cyclotomic constants t_{ij} by

$$t_{ij} = \#\big(K_i \cap (1 + K_j)\big)$$

Under what conditions does p divide t_{ij}?

Remark: Dave awards bonus points if the K_i are all disjoint; an easy condition for this is if $\mathbf{Z}_r^*$ is generated by q and K.

Remarks: (2015) 1. If the K_i are all disjoint, then the $\alpha_i = \sum_{a \text{ in } K_i} \beta^\alpha$, where β is a primitive rth root of unity in the field of q^r elements, form a normal basis of the finite field. We have $\alpha_i \alpha_j = \sum t_{i,j,k} \alpha_k$ with many of the $t_{i,j,k}$ being zero.

2. Dave Thomson mentioned the book, Berndt, Evans, and Williams, Gauss and Jacobi Sums, and noted the similarity to the sums arising in Colin Weir's question, 015:02.

3. Your editor notes that the t_{ij} are called *cyclotomic constants* and are discussed in the book by Tom Storer, Cyclotomy and Difference Sets, available at better Math libraries everywhere.

Problems proposed 16 and 18 December 2015

015:01 (Bart Goddard) Given a system of congruences $x \equiv a_1 \pmod{m_i}$, $i = 1, 2, \ldots, k$, with no solution, can we find something "close" to a solution? Can we minimize the quantity $\sum_i |x - a_i \bmod m_i|$, where $x - a_i \bmod m_i$ is the absolutely least residue of $x - a_i$ modulo m_i?

Remarks: 1. Dave Thomson asked whether this wasn't "ring learning with errors," see https://en.wikipedia.org/wiki/Ring_Learning_with_Errors.

2. Kjell Wooding asked whether Bart wanted the closest x, or just a sufficiently close x. Kjell also suggested reformulating the question to ask for the shortest vector in a lattice, and then applying the LLL-algorithm.

015:02 (Colin Weir) Let ζ be a primitive complex root of unity of order $2^{2m+1} - 1$. Let I be a subset of $\mathbf{Z}/(2m+1)$ such that we never have $i - j \equiv m \pmod{2m+1}$ for i, j in I. We conjecture that for all $m > 0$,

$$\sum_{\#I \le m} 2^{m+1-\#(I)} \prod_{i \text{ in } I} \left(\zeta^{2^i} + \zeta^{-2^i} + \zeta^{2^i(2^{m+1}+1)} + \zeta^{-2^i(2^{m+1}+1)} \right) = 0$$

Remarks: 1. Dave Thomson suggested looking at Berndt, Evans, and Williams, Gauss and Jacobi Sums. Also, that the terms on the right look like type 2 optimal normal bases, and look a lot like Gaussian periods.

2. Renate Scheidler suggested asking Igor Shparlinski.

3. Your editor notes that

$$\zeta^r + \zeta^{-r} + \zeta^s + \zeta^{-s} = (\zeta^{(r+s)/2} + \zeta^{-(r+s)/2})(\zeta^{(r-s)/2} + \zeta^{-(r-s)/2})$$

At least in the case where $2m+1$ is prime, the factors on the right are both units.

015:03 (Amy Wooding) Let g, m be positive integers with $g/2 \le m \le g-2$. When is there a lattice point strictly inside the triangle formed by $(0,0), (g,m), (g-1,m-1)$? If there are internal lattice points, which one is closest to the top line of the triangle? Note — there are no relative primality or other conditions on g, m.

Remarks: 1. Your editor suggested applying Pick's Theorem.

2. Colin Weir suggested a related problem, what is the set of lattice points (a,b) inside the triangle formed by $(0,0), (g-m,0), (g,m)$ such that there are no lattice points interior to the triangle formed by $(0,0), (a,b), (g,m)$?

Solution: Nitya Mani and Andreas Weingartner, independently, applied Pick's Theorem to find that the number of lattice points inside the triangle is

$$\frac{g-m+1-\gcd(g,m)-\gcd(g-1,m-1)}{2}$$

Amy used this to show that there are no interior lattice points if and only if $g-m$ divides g or $g-1$.

Mark Bauer supplied an algorithm for computing the number of interior lattice points.

015:04 (user210387, via Gerry Myerson) Are there infinitely many n such that n^3 is not a sum of three positive cubes?

Remarks: 1. This is http://math.stackexchange.com/questions/1120136. The person who posted it computed the percentage of n up to x for which there is a solution, for various x:

x	2000	4000	6000	8000	10000
%	85.8	89.8	92.1	93.3	94.2

This person also notes that there is no solution in positive integers to $x^3+y^3+z^3 = 999959^3$. He/she is particularly interested in prime values of n.

2. https://oeis.org/A023042 lists values of n for which there *is* a solution, but it only goes up to 1770 (the number, not the year).

3. David Bailey asked whether there are solutions when we allow negative numbers. I would say, probably, but I haven't tried.

4. Simon Rubinstein-Salzedo thinks there is a parametrization for the surface $x^3+y^3+z^3=n^3$, possibly known as the Ramanujan surface. Perhaps, given a parametrization, one could filter out the positive solutions.

015:05 (Eva Goedhart) Given positive integers a, m, find all positive integer solutions to $(am-1)^x + m^y = (am+1)^z$.

Remark: The problem with a odd was solved in Togbé and Miyazaki, The Diophantine equation $(2am-1)^x+(2m)^y=(2am+1)^z$, Int. J. Number Theory 8 (2012), no. 8, 2035-2044. So, let $a = 2^k a_1$, $a_1 \ge 1$ odd, $k \ge 1$. Then $m = 2^\ell m_1$, m_1 odd, $\ell \ge 1$. The hard case is for x even, z odd. Then $\ell y = \ell + k + 1$. It has been solved for $k \le 4$ using linear forms in logarithms to bound x, and then using continued fractions. So the question really concerns the cases $k \ge 5$.

015:06 (Mike Jacobson and Richard Guy) Let $S(x)$ be the sum of the proper divisors of x. Given a positive integer n, find, efficiently, all x such that $S(x) = n$.

Remarks: 1. The motivation is aliquot sequences, the result of iterating $S(x)$. The Catalan-Dickson conjecture says every aliquot sequence is bounded. Richard Guy and John Selfridge conjecture to the contrary. Bosma and Kane, The aliquot constant, Q. J. Math. 63 (2012), no. 2, 309–323, proved that the geometric mean g of $s(2n)/2n$ over all positive integers n exists and satisfies $g \leq 0.97$. But Guy points out that considering every even integer includes values that are not in the range of $S(x)$ and therefore don't occur in any aliquot sequence. Moreover, values of n for which there are many x with $S(x) = n$ should be factored into the geometric mean with a higher weight. The goal is to redo Bosma-Kane with attention to these observations.

2. Kjell Wooding asked why Guy doesn't believe Catalan-Dickson. There are aliquot sequences that don't seem to be in any hurry to calm down. $n = 276$ is the smallest n for which the aliquot sequence has not been proved bounded. The aliquot sequence for 276 has been calculated out to 1650 terms, with some of the terms having 156 digits. The goto site for the problem is http://www.aliquot.de/aliquote.htm.

3. Simon Rubinstein-Salzedo said Carl Pomerance has some heuristics as to why aliquot sequences shouldn't come down, having to do with the difficulty of changing parity. Simon also asked whether any work has been done on $S(S(x))$.

015:07 (Stan Wagon, via Gerry Myerson) Given jugs of integer capacities $A \geq B \geq C > 0$ and a given integer amount of water in each jug, a classic puzzle asks you to get to some final state by a sequence of steps of pouring water from one jug to another. What bounds are there on the number of steps needed?

Remarks: 1. http://math.stackexchange.com/questions/1178368 is Wagon's post of the question. http://demonstrations.wolfram.com/SolvingDecantingProblemsByGraphTheory/ is his post of a demo.

2. Wagon and Rob Pratt checked the case where the total amount of water in the initial state is at most A. They checked all choices of the capacities under 100, and in all cases the puzzle could be solved in at most $A + 1$ steps. This is best possible in this case, as if the jugs have capacities A, A, and 2, and the initial state is $(A, 0, 0)$, then it takes $A + 1$ steps to reach $(A - 1, 1, 0)$.

3. Every step involves either making one jug empty or making one jug full (or both), so there is no nontrivial path to any configuration that has neither a full jug nor an empty one. Bart Goddard noted that there are some other instances that have no solution at all, e.g., if all capacities and all initial contents have a common divisor $d > 1$, then you can't reach a final state with one or more contents not divisible by d. There are other unreachable final states, e.g., at the Wolfram demo it's noted that with jugs of capacities $(12, 7, 6)$, and initial conditions $(9, 4, 3)$, you can't reach $(12, 3, 1)$, $(12, 2, 2)$, $(8, 7, 1)$, $(7, 7, 2)$, $(7, 3, 6)$, or $(8, 2, 6)$. So for the purposes of the question we restrict to instances that do have a solution.

015:08 (Shiv Gupta, via James McLaughlin) Let α be a real irrational. Must

$$S_\alpha = \{ \pm p \pm q\alpha : p, q \text{ prime} \}$$

be dense in the reals?

Remark: Your editor notes Glyn Harman, Metric diophantine approximation with two restricted variables. III. Two prime numbers, J Number Theory 29 (1988) 364-375, where (a result more general than) the following is proved:

For almost all α, there are infinitely many primes p and q such that $|p\alpha - q| < (\log p)/p$.

Harman's homogeneous result would not seem to apply to the inhomogeneous problem at hand. I also found an inhomogeneous result, Alan Haynes, Inhomogeneous approximation by coprime integers, New York J. Math. 18 (2012) 249–259: for any real irrational α, any real γ, and any $\epsilon > 0$,

$$|n\alpha - m - \gamma| \le |n|^{-(1-\epsilon)}$$

has infinitely many solutions in coprime integers m and n.

Perhaps one should write to Harman.

015:09 (Bart Goddard) Give conditions on $\mathbf{a} = (a_1, \ldots, a_n)$ with $0 < a_1 < \cdots < a_n$ integers such that there exists a real t such that the distance from $t\mathbf{a}$, reduced modulo 1, to $(1/2, 1/2, \ldots, 1/2)$ is less than some given $\epsilon > 0$.

Remarks: 1. Bart notes that in the case $n = 2$ it suffices to choose a_2 sufficiently large compared to a_1.

2. To make it look more like a problem in inhomogeneous Diophantine approximation, we may state it this way: given $\epsilon > 0$, find conditions on integers $0 < a_1 < \cdots < a_n$ such that there exist integers $q_1, \ldots, q_n$ and real t such that $|a_i t - q_i - (1/2)| < \epsilon$ for all i.

015:10 (Xiaolong, via Gerry Myerson) Someone [Rob Akscyn?] quoted Polyà, "For every problem you can't solve, there's an easier problem you can solve: find it." My motto is, for every problem you can't solve, there's a harder problem you can't solve, either.

Let

$$H_n = 1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n} = \frac{p}{q}$$

Say something useful about the values of n such that p is prime.

Remarks: 1. http://math.stackexchange.com/questions/854427/ is the source of this question. Values of n are tabulated at http://oeis.org/A056903.

2. Noam Elkies commented, "Probably the sequence is infinite but there's no known technique that would prove such a thing."

3. Poul Anderson wrote, "I've yet to see any problem, however complicated, which when you looked at it the right way didn't become still more complicated."

015:11 (mathlove, via Gerry Myerson) Let $S(n)$ be the sum of the digits of n (in base 10). Is there a limit to the length of a consecutive run of integers such that $S(n^2)$ is a square?

Remarks: 1. http://math.stackexchange.com/questions/1093266/ is the source of this question. The next two comments come from that page.

2. mathlove found $S(n^2)$ is a square for $9 \le n \le 15$, a run of length 7. Then also $10^{m^2} - 1 \le n \le 10^{m^2} + 5$ is a run of length 7, for all m.

3. peter found $S(n^2)$ is a square for $46045846 \le n \le 46045853$, a run of length 8.

4. There were some suggestions as to other ways to produce a bigger run of length k from a smaller run of length k, but it's not clear that any of them work. In particular, it's not clear whether we can use the length 8 example to produce another length 8 example.

5. I can verify that up to $n = 50,000,000$ there is only the one run of length 8, and the only runs of length 7 are those starting at 9 and at 9,999.

015:12 (Colin Weir) Consider all triples a, b, c of polynomials of degree at most $2k$, with coefficients in the field of q elements. How often does $aX + bY + cZ = 0$ have a solution in

polynomials X, Y, Z of degree at most k? Note that Siegel's Lemma guarantees a solution of degree $k+1$. Equivalently, how often is the following $3k \times 3k$ matrix invertible?

$$\begin{pmatrix} a_0 & \dots & \dots & a_{2k} & 0 & \dots & 0 \\ b_0 & \dots & \dots & b_{2k} & 0 & \dots & 0 \\ c_0 & \dots & \dots & c_{2k} & 0 & \dots & 0 \\ 0 & a_0 & \dots & \dots & \dots & \dots & \dots \\ 0 & b_0 & \dots & \dots & \dots & \dots & \dots \\ 0 & b_0 & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & a_0 & \dots & \dots & \dots & \dots \\ 0 & 0 & b_0 & \dots & \dots & \dots & \dots \\ 0 & 0 & c_0 & \dots & \dots & \dots & \dots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \end{pmatrix}$$

Remarks: 1. The conjectured answer is $Aq^{6(k-1)}$ where $A = (q^3-1)(q^3-q)(q^3-q^2)$ is the number of elements of $\mathrm{GL}(3,q)$, verified for small examples by computer search. The case $k=1$ is easy. The case $k=2$ was done by Colin with Dave Thomson, Siddarth Sankaran, and Simon Rubinstein-Salzedo, last night.

2. Colin sketched the $k=2$ proof, which depended on bringing the 6×6 matrix to reduced row-echelon form. We omit the details. There was some discussion of the possibilities of extending the proof, by induction.

015:13 (Simon Rubinstein-Salzedo) 1. Are there infinitely many n such that each of the numbers $n, n+1, n+2, n+4, n+5$ can be written as the sum of two squares?

2. What about each of the numbers

$$n, n+1, n+2, n+4, n+5, n+8, n+9, n+10, n+13?$$

Remarks: 1. The question for triples $n, n+1, n+2$ was Question A2 on the 2000 Putnam exam. See http://www.cms.zju.edu.cn/UploadFiles/AttachFiles/20108232376816.pdf which is Kedlaya, Poonen, and Vakil, The William Lowell Putnam Mathematical Competition 1985–2000, where several solutions are given.

2. The smallest example for question 1 has $n = 144$.

3. By Dickson's Conjecture, there are infinitely many positive integers u such that

$$20u+1, 576u+29, 1440u+73, 720u+37, \text{ and } 2880u+149$$

are all prime. All are 1 mod 4, so all are sums of two squares. Then if $n = 144(20u+1)$, we find that each of the numbers n, $n+1 = 5(576u+29)$, $n+2 = 2(1440u+73)$, $n+4 = 4(720u+37)$, and $n+5 = 2880u+149$ is a sum of two squares. Presumably, a similar set of linear forms can be found for question 2.

4. All instances of question 1 must have $144 \mid n$. We have $4 \mid n$, else one of the first three numbers is 3 mod 4 and not a sum of two squares. If $n = 8m+4$, then $n+2 = 2(4m+3)$ is not a sum of two squares, so $8 \mid n$. If $n = 16m+8$, then $n+4 = 4(4m+3)$ is not a sum of two squares, so $16 \mid n$. One of the first three numbers is a multiple of 3, hence, of 9; if $(n+1)(n+2)$ is a multiple of 9, then $(n+4)(n+5)$ is a multiple of 3, but not of 9, contradiction, so $9 \mid n$, so $144 \mid n$.

5. The nine numbers in question 2 cover all the residue classes modulo 7, so one of them must be a multiple of 7, hence, of 49. Also, the multiple of 7 can't be any of $n+1$, $n+2$, $n+8$, $n+9$. This condition modulo 49 is a significant restriction, and makes it harder to find values of n for which the nine numbers are sums of two squares than to make just the first eight numbers sums of two squares. Indeed, the first eight numbers are sums of two squares for $n = 2304$ ($n = 201888$ also works), but the smallest n for which each of the nine numbers is a sum of two squares is $n = 409248$ ($n = 705600$ also works). There are 12 such n up to 14,400,000.

015:14 (Alessandro Rezende de Macedo and Riley Zeigler)

Call a Gaussian integer m *norm perfect* if $\sum_{d|m} N(d) = 2N(m)$, where $N(m)$ is the norm of m; more generally, k-perfect if $\sum_{d|m} N(d) = kN(m)$. Are there any norm-perfect Gaussians other than $9+3i$ and its associates and their conjugates? Are there any k-perfect Gaussians for $k \geq 3$? Is there an upper bound on the values of k for which k-perfect Gaussians exist?

Remarks: 1. Just checking: $9 + 3i = 3(1 + i)(2 - i)$ so its divisors (up to associates) and their norms are

divisors	1	3	$1+i$	$3+3i$	$2-i$	$6-3i$	$3+i$	$9+3i$
norms	1	9	2	18	5	45	10	90

and the norms sum to $180 = 2N(9 + 3i)$.

2. Spira, The complex sum of divisors, Amer. Math. Monthly 68 (1961) 120–124, MR0148594 (26 #6101), uses a different definition of perfect Gaussian involving the sum of the complex divisors. With that definition, the smallest is $(1 + i)^{73} - 1 = 2^{36} - 1 + 2^{36}i$.

3. Hausman and Shapiro, Perfect ideals over the Gaussian integers, Comm. Pure Appl. Math. 29 (1976), no. 3, 323–341, MR0424745 (54 #12704), also found $9+3i$, "and show in a lengthy computation that there are no other with fewer than 5 distinct prime factors." There are other results in that paper that are relevant to the question at hand.

015:15 (Bart Goddard)

710

711

712

is a haiku. Are there more?

Remark: Technically, a haiku is supposed to be about nature. Bart's find might better be classed as *senryu*. But Kjell points out that these are *natural* numbers.

Solution: There are more, beginning with each of the following numbers:

$$7010; 14,010; 15,010; \ldots; 7,000,010; 14,000,010; 15,000,010; \ldots; 7,000,000,010;$$
$$14,000,000,010; 15,000,000,010; \ldots; 7,000,000,000,010; \ldots; 1,000,000,000,000,010; \ldots$$

At the risk of veering off-topic, I present

e to the power / π square root one-sixty-three; / Close, but no cigar.