Western Number Theory Problems, 17 & 19 Dec 2014

for distribution prior to 2016 (Monterey) meeting

Edited by Gerry Myerson based on notes by Kjell Wooding

Draft of 16 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		

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 2014

014:01 (David Bailey) Analytically, evaluate the constant

$$0.618008217158224707417741862455516783449248164143896087979657276528949927817\ldots$$

This is the computed value for the expectation of a Sierpinski gasket triangle — more information at http://www.davidhbailey.com/dhbtalks/dhb-fractal-boxes.pdf.

014:02 (Al Kelley, via Michael Beeson) List by increasing value of $d > 53$ the triples (d, x, y) such that (x, y) is the least solution in positive integers of Pell's equation, $x^2 - dy^2 = 1$. Select the triples in which x is larger than it is in any previous triple, that is, in any triple with a smaller value of d. Is it true that the values of d for the selected triples are all prime?

The sequence of d-values begins

$$53, 61, 109, 181, 277, 397, 409, 421, 661, 1021, 1069, 1381, 1549, \ldots$$

It is closely related to http://oeis.org/A033316. Kelley has found the values to be prime up to the point where x has over three million digits. Kelley's work is available at http://vixra.org/abs/1405.0025.

Remark: Colin Weir notes that the analytic class number formula implies that the residue of the L-function $L_d(s)$ at $s = 1$ is essentially $d^{-1/2}h(d)\log x$, where $h(d)$ is the class number of $\mathbf{Q}(\sqrt{d})$. Also, the residue is bounded above by a constant times $\log d$, so that one expects to find local maxima for x when the class group is smallest. The class group is

$$(\mathbf{Z}/2\mathbf{Z})^{\omega(d)-1} + H$$

where $\omega(d)$ is the number of prime divisors of d, and H is a small group, heuristically the 1-element group 75% of the time. So we'd expect x to be largest when d is prime, in accord with Kelley's observations.

Colin also computed the class number for the first 14 fields that give new maxima, and in all cases the class number was 1.

014:03 (Alex Nichol, http://mathoverflow.net/questions/190738, via Gerry Myerson) Consider the 10-digit number, $n = 3816547290$. Observe that 3 is divisible by 1, 38 by 2, 381 by 3, and, in general, the number formed by the first d digits is divisible by d. This is the only number that uses each digit once, and has this property. Turning to bases other than 10, it is easy to see that there can be such a number only if the base is even. Such numbers are known in bases 2, 4, 6, 10, and 14. Are there any others?

Remarks: 1. I'm sure I've seen the base 10 question in one recreational math book or another, but I'm not sure where. I don't see it in UPINT or any old WCNT problem sets. The earliest reference I have found is David B Gauld, Problem 15 (3816547290 and all that), New Zealand Mathematical Society Newsletter 32 (December 1984) 17. In Newsletter 42 (1988) 19–20, Gauld presents the solution for base 14, and rules out all other bases through 30. The newsletters are available at http://nzmathsoc.org.nz/allnewsletters.php.

2. Relevant entries at the Online Encyclopedia of Integer Sequences are http://oeis.org/A111456 and http://oeis.org/A181736. At the latter, it is stated that there are no more such numbers for any base up to 28. At the former, it is stated that there

are no more such numbers for any base up to 40, and as Russell Hendel notes it also says, "A probabilistic argument says higher bases are increasingly unlikely to produce a value." Elsewhere on the web there are claims that there are no more such numbers up through base 52. The claims are presented without any suppporting documentation.

3. Colin Weir asks what the probabilistic argument referred to above is.

014:04 (Stefan Erickson) How many quadratic discriminants are there, up to x?

Solution: (Claudia Spiro) We want to estimate $\sum 1$, summing over all conductors f of a quadratic field, $f \le x$. This is $\sum_1 + \sum_2 + \sum_3$, where

$$\sum\nolimits_1 = \sum_{n \text{ squarefree}, n \le x, n \equiv 1 \bmod 4} 1, \quad \sum\nolimits_2 = \sum_{n \text{ squarefree}, n \le x/4, n \equiv 2 \bmod 4} 1,$$

$$\sum\nolimits_3 = \sum_{n \text{ squarefree}, n \le x/4, n \equiv 3 \bmod 4} 1$$

We get $\sum_1 \sim (2/\pi^2)x$,

$$\sum\nolimits_2 = \sum_{m \text{ odd, squarefree}, m \le x/8} 1 \sim x/(2\pi^2)$$

and

$$\sum\nolimits_3 = \sum_{n \text{ squarefree}, n \le x/4} (1/2)(\chi_0(n) - \chi_1(n))$$

where χ_0 is the principal, χ_1 the non-principal character mod 4. The term with χ_0 is asymptotically $x/(2\pi^2)$, the other term is $o(x)$. Putting the three sums together gives the asymptotic estimate $(3/\pi^2)x$.

014:05 (Bart Goddard) What's a good way, preferably accessible to undergraduates, to define a sum-of-divisors function on the integers of a number field? It is desired that the function be multiplicative, work even in fields with infinitely many units, and, if possible, not rely too heavily on ideals.

Remark: In response to a question from Colin Weir about using norms, Bart thought he had tried that, but it didn't work.

014:06 (David Thomson) Let V be an n-dimensional vector space over a field, K. Let T be an invertible linear operator on V. Given a basis B of V, define $\overline{B}$ by

$$\overline{B} = B \cup T(B) \cup \cdots \cup T^{n-1}(B)$$

Given V and T, does a basis B exist such that any n elements of $\overline{B}$ form a basis of V?

Remarks: 1. David is particularly interested in the case where K is the field of q elements, and T is multiplication by α, where α has degree n over K.

2. There are trivial examples, where $n = 1$, and trivial counterexamples, where T^k is the identity for some $k \le n-1$. Since $\overline{B}$ has n^2 elements, we also need $n^2 < q^n - 1$.

014:07 (Claudia Spiro) Is it true that there's always a prime between two sufficiently large perfect powers?

Remarks: 1. There are no primes between 8 and 9, between 32 and 36, between 121 and 125, between $2187 = 3^7$ and $2197 = 13^3$, between $32761 = 181^2$ and $32768 = 2^{15}$.

2. Stefan Erickson found 10 such prime-free intervals up to 10^{24}, the largest being between $22434^2 = 503284356$ and $55^5 = 503284375$.

3. Simon Rubinstein-Salzedo gave a heuristic argument that there should only be finitely many n such that there is a cube between n^2 and $n^2 + \log(n^2)$. One expects there to be a prime in such an interval, so only finitely many prime-free intervals between a square and a cube (with similar arguments for squares and fifth powers, and so on).

4. M. Tip Phaovibul referred to work by Reese Scott and Rob Styer on Pillai's conjecture, which involves the number of solutions of $a^x - b^y = c$ for given a, b, and c.

5. Your editor has found that a conjecture that there are only finitely many exceptions to there being a prime between consecutive powers was made by Stephen Redmond and Zhi-Wei Sun in 2006 according to http://en.wikipedia.org/wiki/Redmond-Sun_conjecture, where the ten known exceptions are given. It says the conjecture has been verified for intervals below 10^{12}. At https://oeis.org/A116086 Giovanni Resta is credited with verifying the conjecture up to 4.5×10^{18}.

6. More history. Stephen Redmond posted to the NMBRTHRY list on 23 March 2006, asking whether it was true that between any two powers higher than squares there must be a prime. On 28 March, he acknowledged the counterexample with 3^7 and 13^3, saying there are no other counterexamples up to 100,000,000. Meanwhile, on 25 March, Sun had posted to conjecture there's a prime between powers, squares included, with only four exceptions. On 28 March, Sun reported finding five more prime-free intervals between powers, and mentioned that Kevin Buzzard had found a tenth (the one given in Stefan's remark, above). Sun also wrote that Carl Pomerance had informed him that the conjecture for sufficiently large powers is somewhat reasonable by the famous *abc*-conjecture and the conjecture that for each $c > 0$ and all large x there is a prime between x and $x + x^c$.

014:08 (Kjell Wooding) For x^2+x+A to be prime for many values of x, we want $A \equiv 3 \bmod 8$, and $\left(\frac{A}{p_i}\right) = \left(\frac{-1}{p_i}\right)$ for many primes p_i. Are there other problems where we want n satisfying congruences modulo q not for all primes (or prime powers) q up to some bound x, but just for many?

014:09 (Rob Akscyn) Can an expression of the form $(1 \pm e^{-x})^{-1}$ or e^{-x} be used to resolve the recurrence relation,

$$R(h, q) = R(h, p) - R([h/p], p) - 1$$

where $p < q$ are consecutive primes, and $R(h, 2) = h - 1$?

014:10 (Amy Wooding) Let p be a prime. The elliptic curves, supersingular for p, are all defined over $\mathbf{F}_{p^2}$, and there are only finitely many of them.

Now for each prime $\ell \neq p$, draw an edge joining two of these curves if there is an ℓ-isogeny from the one to the other. This yields a directed, strongly-connected graph. The p-power map is an automorphism of this graph [probabilistically — not formally proved]. Is it true (perhaps for p and/or ℓ sufficiently large) that these graphs have no more non-trivial automorphisms?

014:11 (Claudia Spiro) Are there infinitely many sets $S = \{n, n+2, \ldots, n+14\}$ of eight consecutive odd integers such that $\gcd(m, \phi(m)) = 1$ for all m in S?

Remarks: 1. An example is $n = 695$, as made clear by the factorizations,

$$695 = 5 \times 139; 697 = 17 \times 41; 699 = 3 \times 233; 703 = 19 \times 37; 705 = 3 \times 5 \times 47; 707 = 7 \times 101.$$

(701 and 709 are prime). Further examples are $n = 1685$, $n = 1937$, and $n = 2729$.

2. There are no such sets of nine conecutive odd numbers, as one of any set of nine consecutive odd numbers is a multiple of 9, and 3 divides both $9m$ and $\phi(9m)$.

3. If $n, n+2, n+6, n+8$ are prime, $n+4 = 15p$ where p is prime and $\gcd(15, p-1) = 1$, $n+10 = 3q$ where q is prime and $\gcd(3, q-1) = 1$, $n+12 = 7r$ where r is prime and $\gcd(7, r-1) = 1$, and $n+14 = 5s$ where s is prime and $\gcd(5, s-1) = 1$, then we get an example. On Dickson's Conjecture (which states that $a_i + b_i m$, $m = 1, 2, \ldots, k$, are simultaneously prime for infinitely many m if there is no congruence condition preventing it), there are infinitely many such n.