Western Number Theory Problems, 17 & 19 Dec 2017

for distribution prior to 2018 (Chico) meeting

Edited by Gerry Myerson based on notes by Kjell Wooding

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 Pacific Grove	014:01–014:11		2015 Pacific Grove	015:01–015:15
2016 Pacific Grove	016:01–016:14		2017 Pacific Grove	017:01–017:21

COMMENTS ON ANY PROBLEM WELCOME AT ANY TIME

48/106 Crimea Road
Marsfield NSW
2109 Australia
Gerry.Myerson@gmail.com
Australia-2-9877-0133

Comments on earlier problems

97:11 (Bob Silverman) Let $N = pq$, p, q odd primes. Then

$$\#\{\, r \text{ in } \mathbf{Z}/N\mathbf{Z} : \text{ order of } r \text{ is } \lambda(N)\,\} > \frac{2e^{-\gamma}}{3}\frac{N}{\log\log N}.$$

1. Can $\frac{2e^{-\gamma}}{3}$ be improved?
2. Suppose $0 < \delta < 1/16$ and $N^{\delta} \geq 2$. Then

$$\#\{\, r \text{ in } \mathbf{Z}/N\mathbf{Z} : (\text{order of } r) \geq N^{-\delta}\lambda(N)\,\} > e^{-\gamma}\frac{N}{\log\log N}.$$

Is this best possible? Note: $\lambda(N) = \operatorname{lcm}\{\, p-1, q-1\,\}$.

Remark: In 2018, Sungjin Kim writes that Theorem 1 of Shuguang Li, On the number of elements with maximal order in the multiplicative group modulo n, Acta Arith. 86.2 (1998) 113–132, improves the constant in the first question to $e^{-\gamma} + \mathrm{o}(1)$ for N sufficiently large. Theorem 1 says,

$$\liminf \frac{\{\, r \text{ in } \mathbf{Z}/N\mathbf{Z} : \text{ order of } r \text{ is } \lambda(N)\,\}}{\phi(N)/\log\log N} = e^{-\gamma}$$

It seems to your editor that this only gives $e^{-\gamma} + \mathrm{o}(1)$ if p and q both go to infinity. If, say, p is held fixed at 3, we just recover Silverman's $\frac{2e^{-\gamma}}{3}$.

Problems proposed 17 and 19 December 2017

017:01 (Bart Goddard) Bart reminds us of Problem 84:05 (Jeff Lagarias and Carl Pomerance): A *humdrum* number is a positive integer n such that e^{e^n} is also an integer; prove or disprove that there are no humdrum numbers.

017:02 (Mike Jacobson) A *noncototient* is a number not of the form $n-\phi(n)$. A noncototient *class* is the noncototients generated by repeatedly multiplying an odd integer by two until the result is no longer a noncototient. A noncototient *chain* is a sequence of consecutive even noncototients.

1. Are there noncototient classes of every integer length $\ell \geq 1$?
2. Are there noncototient chains of every integer length $\ell \geq 1$?
3. Are there infinitely many noncototient pairs (chains of length two)?
4. Is there a positive asymptotic density of noncototient pairs?

Remark: The density of noncototient pairs rises from under 0.019 at $n = 10^4$ to over 0.028 between 10^8 and 10^9 and then falls to below 0.027 at 10^{12}.

017:03 (David Bailey) Let

$$\omega(s) = \sum_{j,k=1}^{\infty} \big(jk(j+k)\big)^{-s}$$

Consider the analytic continuation of this series to the complex plane. It has trivial zeros at the negative integers, and 48 known nontrivial zeros in the upper half-plane. How many nontrivial zeros does it have in the upper half-plane?

Remarks: 1. The known nontrivial zeros all have real part between 0 and 2, and imaginary part at most 64.

2. If z is a zero, so is $\bar{z}$, which is why we only ask about the upper half-plane.

017:04 (Dan Romik) Every Lie group has an associated zeta function, called a Witten zeta function. The zeta function associated with SU(2) is the Riemann zeta function. The zeta function associated with SU(3) is David Bailey's $\omega(s)$. The zeta function associated with SO(5) is

$$f(s) = \sum_{j,k=1}^{\infty} \big(jk(j+k)(j+2k)\big)^{-s}$$

Analyze $f(s)$: show that it has a meromorphic continuation, find its poles and zeros, and so on.

017:05 (Tim Trudgian, via Gerry Myerson) Estermann, Proof that every large integer is the sum of two primes and a square, Proc. London Math. Soc. s2-42 (1937) 501–516 (the same issue also had Turing's famous paper, On computable numbers, with an application to the Entscheidungsproblem), proved (unconditionally) the existence of n_0 such that, if $n > n_0$, then n is the sum of two primes and a square. Prove this for some explicit value of n_0. Very likely, it's already true for $n_0 = 4$.

017:06 (Tim Trudgian, via Gerry Myerson) Linnik, All large numbers are sums of a prime and two squares (A problem of Hardy and Littlewood), I, Mat. Sb. (N.S.) 52 (94) 1960 661–700 and II, 53 (95) 1961 3–38, proved (unconditionally) the existence of n_0 such that, if $n > n_0$, then n is the sum of a prime and two squares. Prove this for some explicit value of n_0. Very likely, it's already true for $n_0 = 3$.

Remarks: 1. Tim suggests this will be harder than **17:05**.

2. Carl Pomerance notes that if the squares are allowed to be zero then $n_0 = 3$ is equivalent to $n_0 = 1$.

3. Enrique Treviño notes that what's needed is to make the error term in Linnik's formula effective.

017:07 (Tim Trudgian, via Gerry Myerson) Conjecture H of Hardy and Littlewood, page 49 of Some problems of ‘partitio numerorum’, III: On the expression of a number as a sum of primes, Acta Math. 44 (1923) 1–70, posits the existence of n_0 such that if $n > n_0$ and n is not a square then n is the sum of a prime and a square. The conclusion is known to be true for almost all n. The known exceptional n are listed at http://oeis.org/A020495; the largest is 21679, and it is reported there that James Van Buskirk has searched out to 3×10^9 without finding any more. Can we push this out to, say, 10^{12}?

Remarks: 1. Carl Pomerance asked whether for sufficiently large n there might be at least two such representations. Conjecture H is that the number of such representations is asymptotic to

$$\frac{\sqrt{n}}{\log n}\prod_{p\geq 3}\left(1-\frac{1}{p-1}\left(\frac{n}{p}\right)\right)$$

2. Sungjin Kim asked for an upper bound on the size of the exceptional set. Hongze Li, The exceptional set for the sum of a prime and a square, Acta Math. Hungarica 99 (2003) 123–142 proved that if $E(x)$ is the number of natural numbers not exceeding x which cannot be written as a sum of a prime and a square then $E(x) \ll x^{0.982}$.

017:08 (Paul Young) Let T_n be given by

$$T_n = T_{n-1} + T_{n-2} + \cdots + T_{n-k}, \quad T_0 = 0, \quad T_i = 1 \text{ for } 1 \leq i \leq k-1$$

For which positive n do we have $T_{-n} = 0$?

Remarks: 1. For $k = 3$ (the Tribonacci numbers), $T_{-1} = T_{-4} = T_{-17} = 0$. These are the only solutions for $k = 3$, and the only known solutions for any k.

2. For k even, there are none (using the 2-adics).

3. For each odd $k \geq 5$, there is at most one such n (but none are known).

4. References were made to work of Shorey and Tijdeman, and of Baker and Wüstholz. Perhaps this work can give an effective bound on n for each k.

5. Russell Hendel has made a conjecture from which it would follow that for $k \geq 4$ and $n \geq 1$ there are no solutions to $T_{-n} = 0$. Namely, Russell conjectures that, letting $n_0 = k^2 - k - 1$, we have

i) $T_{-n} \neq 0$ for $n \leq n_0$,

ii) $T_{-n_0} = (-1)^{k+1}\bigl(k - 2 - (-1)^k\bigr)$, and

iii) $|T_{-n}| \geq |T_{-n_0}|$ for $n \geq n_0$.

Russell writes that he has made some headway toward a proof of iii).

017:09 (Amy Feaver) Can we find a finite group G, together with an ordering of its elements, such that $\{ g_1, g_1g_2, g_1g_2g_3, \dots, g_1g_2g_3 \cdots g_n \}$ forms a proper subgroup H?

Remark: Amy notes that this can’t be done for the cyclic group of order n.

Solution: Certainly not, if n is meant to be the order of the group. For if there were such an ordering, we could let g be an element of G not in H, so $g \neq g_1$, and then we would have hg in H for some h in H, contradiction. If n is allowed to be smaller than the order of G, then for any group containing an element a of order 4, we have $\{ 1, a, aa^2, aa^2a^3 \} = \{ 1, a, a^3, a^2 \}$ as a proper subgroup of G.

017:10 (Clark Lyons) Let x be real such that q^x is rational for all rational q. Show that x must be an integer.

Remarks: 1. Garo Sarajian notes that if n^x is a natural number for all natural numbers n, then x is an integer, and there is a solution online.

2. Your editor first saw the problem Garo mentions when he sat the 1971 Putnam exam—it was Problem A6. He wasted a lot of time trying to prove that if 2^x and 3^x are both natural, then x is natural. Shortly thereafter, he was able to ask Andy Gleason and Serge Lang about the question. It turned out that Gleason was the source of the question. He was surprised it had been used on the exam, as he thought it was too difficult, but he was able to explain the intended solution. Lang said that the $2^x, 3^x$ version was (and still is!) a notorious unsolved problem, a special case of the Four Exponentials Conjecture. Also, it had only recently been proved, as a special case of the Six Exponentials Theorem, that if 2^x, 3^x, and 5^x are all integers then so is x.

Solution: See https://math.stackexchange.com/questions/378130, where the same question was raised. Gerald Edgar noted that -1 is rational, and for $(-1)^x = e^{i\pi x}$ to be rational, x must be an integer. Marc van Leeuwen suggested restricting q to the positive rationals, as I will do in the following.

This, and more, can be proved using the Six Exponentials Theorem. Suppose 2^x, 3^x, and 5^x are all rational. Note that the numbers $\log 2, \log 3, \log 5$ are linearly independent over the rationals. If x is irrational, then the numbers $1, x$ are linearly independent over the rationals, and the Six Exponentials Theorem concludes that at least one of the numbers $e^{\log 2}, e^{\log 3}, e^{\log 5}, e^{x \log 2}, e^{x \log 3}, e^{x \log 5}$ is transcendental. But these are the numbers $2, 3, 5, 2^x, 3^x, 5^x$, which are all rational, by hypothesis. Therefore, x is rational, say, $x = r/s$ in lowest terms. But then $2^x = a/b$ implies $2^r b^s = a^s$, and by unique factorization we must have $s = 1$, so x is an integer.

Whether there is a proof avoiding the deep Six Exponentials Theorem, along the lines of the elementary solutions of the Putnam problem, your editor knoweth not.

017:11 (Kevin McGown) Let M_n be the matrix whose entries are the first n^2 primes, in order, e.g.,

$$M_3 = \begin{pmatrix} 2 & 3 & 5 \\ 7 & 11 & 13 \\ 17 & 19 & 23 \end{pmatrix}$$

In **016:07**, Sungjin Kim asked whether these matrices are all nonsingular, and in a remark Simon Rubinstein-Salzedo asked whether the determinants are always negative. Calculations show the sign is not constant. Let $f(n) = \det M_n$. Can one prove $|f(n)| \geq \exp(n)$ for $n \geq 3$? Does the sign of $f(n)$ exhibit a pattern? Can one show $\#\{\, n \leq x \mid \mathrm{sign} f(n) > 0 \,\} \sim x/2$?

Remark: Carl Pomerance and Simon suggest $\sum^x \mathrm{sign} f(n)$ might be $\mathrm{O}(\sqrt{x})$ Any estimate in $\mathrm{o}(x)$ for the summatory function would settle the last question in the affirmative.

017:12 (Kevin McGown) Let $S_p(n)$ be the sum of the digits in the base-p expansion of n, that is, if $n = \sum a_k p^k$ with $0 \le a_k \le p-1$, then $S_p(n) = \sum a_k$. Fix primes $p_1, p_2, \ldots, p_r$. Estimate

$$\#\{\, n \le x \mid S_{p_i}(n) = p_i - 1 \text{ for all } i \,\}$$

as a function of x and of the p_i.

Remarks: 1. Simon Rubinstein-Salzedo asked whether to expect these sets to be finite.

2. Paul Young referenced work on Bernoulli polynomials by Noriaki Kimura, P. J. McCarthy, Arnie Adelberg and others, in which the condition $S_p(n) = p - 1$ arose.

017:13 (Kjell Wooding) Noting that in **017:02** the density of noncototient pairs is computed up to 10^{12}, and in **017:07** we're asked to push a computation out to 10^{12}, and in Carl Pomerance's talk another computation was carried out to $2^{37} \approx 2 \cdot 10^{12}$, why 10^{12}?

Remark: Clark Lyons posited this was as far as you can compute on a laptop in a day, and there was also a suggestion that RAM issues were involved.

017:14 (Pante Stanica, with Florian Luca) 1. For what values of d are there infinitely many integers a such that the concatenation of a and $a + d$ is a perfect square, with a and $a + d$ having the same number of digits?

2. Are there examples of more than two distinct terms of an arithmetic progression which, concatenated in some order, give a square?

3. Same questions, for bases other than 10.

Remarks: 1. For the first question, Pante and Florian have found that $d = 0, \pm 1$ have the property, while $d = -3$ and $d = 7$ don't.

2. For the second question, Paul Young noted $324 = 18^2$, and your editor proposed $576 = 24^2$. The six-digit examples (three terms of a two-digit AP) are

$$663^2 = 43\,95\,69, \quad 756^2 = 57\,15\,36, \quad 987^2 = 97\,41\,69$$

With a looser definition, we could also include

$$147^2 = 02\,16\,09, \quad 231^2 = 05\,33\,61, \quad 294^2 = 08\,64\,36$$

There are many nine-digit examples with three terms of a three-digit AP, running from $10215^2 = 104\,346\,225$ up to $29202^2 = 852\,756\,804$. Some even have the AP in order, namely,

$$11142^2 = 124\,144\,164, 11553^2 = 133\,471\,809, 14088^2 = 198\,471\,744, 16713^2 = 279\,324\,369,$$
$$18801^2 = 353\,477\,601, 22284^2 = 496\,576\,656$$

or in reverse order,

$$23097^2 = 533\,471\,409, 23718^2 = 562\,543\,524, 26787^2 = 717\,543\,369, 28818^2 = 830\,477\,124$$

With a looser definition, we could include

$$1107^2 = 1\,225\,449, 2466^2 = 6\,081\,156, 2544^2 = 6\,471\,936, 4932^2 = 24\,324\,624, 5571^2 = 31\,036\,041$$

and others. We can also have four or five terms of a one-digit AP:

$$66^2 = 4356 \qquad 74^2 = 5476 \qquad 152^2 = 23104 \qquad 178^2 = 32041$$

There are many eight-digit squares whose digits, suitably reordered, form an eight-term AP, starting with $3678^2 = 13527684$ and going up to $9024^2 = 81432576$. There are 30 nine-digit squares that can be reordered to form the AP $1, 2, \ldots, 9$, from $11826^2 = 139854276$ up to $30384^2 = 923187456$, and 87 ten-digit squares that are reorderings of the AP $0, 1, \ldots, 9$, of which the biggest is $99066^2 = 9814072356$. Details and links can be found at the Online Encyclopedia of Integer Sequences, e.g., at A071519 and A036745.

017:15 (Colin Weir) Fix an odd prime p. What is the asymptotic for the number of n up to x such that the p-Sylow subgroup of the group of units of $\mathbf{Z}/n\mathbf{Z}$ is not cyclic?

Remarks: 1. This was inspired by the Cohen-Lenstra heuristics for class groups.

2. Simon Rubinstein-Salzedo pointed out that if n has two or more prime factors congruent to 1 modulo p, then the p-Sylow subgroup can't be cyclic.

3. Carl Pomerance claimed that for p fixed the subgroup is noncyclic for almost all n. It's better to ask for an asymptotic for subgroups that *are* cyclic. The ones that are cyclic are $Cx/\sqrt{\log x}$.

017:16 (Enrique Treviño) Let $A(x)$ be a polynomial over the field of two elements. We say A is *even* if it is divisible by $x(x+1)$, *odd* otherwise. We say A is perfect if it equals the sum of its divisors. It is known that if A is odd and perfect then it has at least five distinct irreducible factors, and at least 12 irreducible factors, counting with multiplicity. Can we do better?

017:17 (Gary Walsh) Two problems on Diophantine equations.

1. Settle the Jesmanowicz conjecture: if a, b, c are pairwise coprime, and $a^x + b^y = c^z$ has the solution $(x, y, z) = (2, 2, 2)$, then there is no other solution (x, y, z) in positive integers.

2. Find all solutions to $\dfrac{x^2 - 1}{y^2 + 1} = (z^2 \pm 1)^2$.

Remark: Hai and Walsh, On a Diophantine problem of Bennett, Acta Arith. 145 (2010) 129–136, settled all cases of $\dfrac{x^2 \pm 1}{y^2 \pm 1} = (z^2 \pm 1)^2$ except this one. There is an infinite family given by $z = 2r + 1$, $y = (z^2 \pm 1)/2$, $x = 2y^2 + 1$, $r = 1, 2, \ldots$. For $x \leq 20000$, there is one more solution, $(x, y, z) = (2177, 4, 23)$, which comes from $(4 + \sqrt{17})^4 = 2177 + 528\sqrt{17}$.

017:18 (Igor Shparlinski, via Gerry Myerson) A variant of the odd Goldbach conjecture: can we write every odd number $n \geq 7$ as a sum of three primes, with one of the primes being "small", say, $(\log n)^{O(1)}$? Can this be done unconditionally?

Remark: Of course if the even Goldbach conjecture is true then we can take one of the primes in the odd Goldbach conjecture to be 3.

017:19 (Tim Trudgian, via Gerry Myerson) Bambah and Chowla, On numbers which can be expressed as a sum of two squares, Proc. Nat. Inst. Sci. India 13 #2 (1947) 101–103, available at http://www.insa.nic.in/writereaddata/UpLoadedFiles/PINSA/Vol13_1947_2_Art05.pdf proved that if x is sufficiently large then there is a sum of two squares strictly between x and $x + 2\sqrt{2+\epsilon}\,n^{1/4}$. Uchiyama, On the distribution of integers representable as a sum of two h-th powers, J. Fac. Sci. Hokkaido U. Ser. 1, Math. 18(3-4) (1965) 124-127, available at eprints.lib.hokudai.ac.jp/dspace/bitstream/2115/56058/1/JFSHIU_18_N3-4_124-127.pdf proved that for all n there is a sum of two squares strictly between n and $n + 2\sqrt{2}\,\sqrt[4]{n}$. Can we improve on $2\sqrt{2}$ in Uchiyama's result?

Remark: Uchiyama conjectured that we can replace $2\sqrt{2} \approx 2.828$ with $5^{3/4}/\sqrt{2} \approx 2.364$. This was based on the gap between 20 and 25; you can't do better than $5^{3/4}/\sqrt{2}$ because of this gap. Tim found a nastier gap between 1493 and 1508, which shows that you can't do any better than $15/1493^{1/4} \approx 2.41$. Tim has computed up to 10^8 or so without finding any bigger gap (relative to $\sqrt[4]{n}$) — see Uchiyama's conjecture on sums of squares, https://arxiv.org/pdf/1712.07243.pdf.

017:20 (Math Stackexchange User 19405892, via Gerry Myerson) Find a natural number n such that $\gcd(3^{n+1} - 2, 2^n - 3) > 1$, or prove that there are none.

Remarks: 1. This is https://math.stackexchange.com/questions/2121808. The proposer searched up to $n = 7000$ without finding an example. Tim Trudgian has since extended the search into the millions, with no luck.

2. Will Jagy looked at some variants of the question and posted a table of results, but later deleted it. He found, for example, that $\gcd(3^{n+6} - 2, 2^n - 3)$ is 1 for $n \le 1160$, but $\gcd(3^{1167} - 2, 2^{1161} - 3) = 2543$.

3. Carl Pomerance noted that if the gcd isn't 1 then it must be fairly large, as a small gcd would have shown up in the searches already done. He suggested an analogy with Wieferich primes.

017:21 (Ha Tran) Let $\mathbf{b_1}, \mathbf{b_2}$ be linearly independent vectors in $\mathbf{R}^2$. Let $L = \mathbf{b_1}\mathbf{Z} + \mathbf{b_2}\mathbf{Z}$ be the lattice they generate, and assume it contains $(1, 1)$, and assume $(1, 1)$ is not a shortest vector in L. If $\mathbf{x} = (x_1, x_2)$ is in L, and $\mathbf{u} = (u_1, u_2)$ with u_1 and u_2 positive, define $\mathbf{ux}$ to be (u_1x_1, u_2x_2), and define $\mathbf{u}L$ to be $\{\, \mathbf{ux} : \mathbf{x} \in L \,\}$. Given L, determine whether there is a vector $\mathbf{u}$ of the form $\mathbf{u} = (\alpha, \alpha^{-1})$ such that $\mathbf{u}$ is the shortest vector in $\mathbf{u}L$.

Remarks: 1. This is equivalent to saying that the ellipse

$$\frac{x_1^2}{1+\alpha^{-4}} + \frac{x_2^2}{1+\alpha^4} = 1$$

does not contain any nonzero vectors of L.

2. The question has been settled when L is the ideal lattice of a number field of degree 2, but is an open question for all higher degree number fields.

3. The condition $\mathbf{u} = (\alpha, \alpha^{-1})$ is there to ensure the covolume of $\mathbf{u}L$ equals the covolume of L.