Western Number Theory Problems, 17 to 19 Dec 2019

for distribution prior to 2021 (virtual) 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
2018 Chico	018:01–018:19	2019 Asilomar	019:01–019:18

COMMENTS ON ANY PROBLEM WELCOME AT ANY TIME

48/106 Crimea Road
Marsfield NSW
2122 Australia
gerrymyerson@gmail.com
Australia-2-9877-0133

Comments on earlier problems

96:12 (Gary Walsh) Let $I_S = \{ \prod_{j=1}^{k} p_j^{e_j} : e_j \geq 0 \}$, where $S = \{ p_1, \ldots, p_k \}$ is a finite set of primes. Let $D_S = \{ (p, q) : p, q \text{ prime and } p - q \in I_S \}$. Is D_S infinite? In particular, what if $S = \{ 2 \}$?

Partial solution by Sungjin Kim. We note that by the work of Zhang, Maynard, and Polymath 8b, the answer is yes if S consists of all the primes not exceeding 246.

Carl Pomerance notes that we can replace 246 with 113, since all prime differences (other than those involving $q = 2$) are even.

018:11 (Sungjin Kim) Let $G = \mathrm{SL}_2(\mathbf{Z})$. G acts on the upper halfplane $\mathbf{H}$. Given a real number a, and a positive number d, $0 < d < 1$, the lines through a with slopes d and $-d$ enclose a wedge W in $\mathbf{H}$. Given a point $P = (a_0, b_0)$ in $\mathbf{H}$, we want to estimate the number N of points in the orbit of P under G that lie in the wedge W. When a is rational, we can prove $N \ll_a (1/d) \log(1/d)$. What can be said for irrational a?

Sungjin Kim has sent me a solution to this problem. It is too long to include here, and too difficult for me to summarize. My apologies.

Problems proposed 17 to 19 December 2019

019:01 (Jeff Lagarias) A problem of Turing from 1936: show that Euler's constant γ can't be a dyadic rational, that is, we can't have $\gamma = a/b$ with a an integer and $b = 2^j$ for some integer j.

Remark: Of course, the question of whether γ is irrational is a notorious open question. Much computational effort has gone into ruling out small denominators (thank you, David Bailey). Maybe proving it's not a dyadic rational will prove more accessible than proving it's not rational at all.

019:02 (Renate Scheidler) Given coprime integers $a < b$ and a positive integer $n \geq a + b$, with n even if a and b are both odd, we define an (a, b)-difference necklace to be a circular arrangement of the numbers $0, 1, \ldots, n - 1$ such that any two adjacent terms differ by $\pm a$ or $\pm b$. It is known that if $2a \leq b$ then such exist for n sufficiently large. The problem is to determine existence for $2a > b$.

019:03 (Gary Walsh) In regard to a cubic version of the Ankeny-Artin-Chowla conjecture, find examples of positive cubefree d for which the fundamental unit

$$\epsilon_d = (1/3)(x + y\sqrt[3]{d} + z\sqrt[3]{d^2})$$

of $\mathbf{Q}(\sqrt[3]{d})$ has d dividing y.

Remarks: 1. Simon Rubinstein-Salzedo asks whether, in the quadratic case, it seems that d divides the imaginary part of the fundamental unit with probability $1/d$. Stephens and Williams, Some computational results on a problem concerning powerful numbers, Math. Comp. 50 (1988) 619–632 found only eight values of d with d dividing the imaginary part of the fundamental unit, namely, $d = 46, 430, 1817, 58254, 209991, 1752299, 3124318$ and 4099215. These values of d are all composite, in line with the AAC conjecture.

2. John Friedlander asks whether it can be proved that there are only finitely many examples with d dividing both y and z. What if we further restrict to the case where d is prime?

3. Kevin McGown computes that for squarefree d, $0 < d < 10,000$, the fundamental unit $\epsilon_d = a + b\sqrt[3]{d} + c\sqrt[3]{d^2}$ has d dividing b for exactly the values $d = 3, 6, 15, 39, 42, 57, 330, 1185$. Is there a reason why these are all multiples of three?

4. Hideo Wada, A table of fundamental units of purely cubic fields, Proc. Japan Acad. 46 (1970) 1135–1140, gave the fundamental unit for $2 \le d \le 250$. They get big fast. For $d = 239$, x, y, z have over 180 digits each.

5. I skimmed Hiroshi Ito, Congruence relations of Ankeny-Artin-Chowla type for pure cubic fields, Nagoya Math. J. 96 (1984) 95–112 and didn't see anything directly relevant to the question at hand (but maybe it deserves a closer look).

6. Yoshinosuke Hirakawa and Yosuke Shimizu, Counterexamples to the local-global principle for non-singular plane curves and a cubic analogue of Ankeny-Artin-Chowla-Mordell conjecture, https://arxiv.org/abs/1912.04600 seems more likely to be relevant. They give "a natural cubic analogue of the classical Ankeny-Artin-Chowla-Mordell conjecture... easily verified numerically."

019:04 (Carl Pomerance) Are there infinitely many triples of primes p, q, r with

$$pq = p + q + r$$

Fixing p (or q) reduces the problem to a case of the prime k-tuples conjecture, but perhaps the flexibility of choosing p will make the question tractable.

019:05 (Nilotpal Kanti Sinha, via Gerry Myerson) Look at all the composites between two consecutive primes (e.g., $24, 25, 26, 27, 28$ between the primes 23 and 29). Consider the largest prime divisor of those composites (in our case, 13, a divisor of 26). Does every prime arise that way? Does every prime (other than 2) arise infinitely often? Does any prime arise infinitely often?

Remarks: 1. Posted at https://mathoverflow.net/questions/347801/is-every-prime-the-largest-prime-factor-in-some-prime-gap, also at
https://math.stackexchange.com/questions/3456944/largest-prime-factor-of-the-numbers-between-two-consecutive-primes

2. Verified for all primes $p < 10^{10}$.

3. Tabulated at http://oeis.org/A052248

4. If $p < p'$ are consecutive primes, and if there is a prime q between $2p$ and $2p'$, then p is the largest prime dividing a composite between q and the prime preceding q. Many primes appear this way (about 70%, experimentally). 59 is the first prime for which we must go beyond $2p$, since $2 \times 61 = 122$ is also in the gap between consecutive primes 113 and 127. We must go to $18 \times 59 = 1062$, which lies between the primes 1061 and 1063. John Friedlander asked whether we must go to arbitrarily large multiples of p. Some computational results: we need to go to $550p$ for $p = 1778321$; $783p$ for $p = 725175083$; and $819p$ for $p = 2739366569$.

5. Carl Pomerance suggests it might be easier to show that almost all primes arise in this way.

019:06 (Sungjin Kim) [See the discussion of 96:12, supra] Are there infinitely many pairs of primes differing by a power of two?

019:07 (Mathoverflow user WhatsUp, via Gerry Myerson) Let $n > 1$ be an integer. We call an n-vector of complex numbers $v = (v_1, \ldots, v_n)$ *periodic* if there is a proper divisor d of n such that $v_i = v_{i+d}$ for all i; we call it integral if every v_i is an integer. If an integral vector is a finite sum of periodic vectors, must there also be a way to write it as a finite sum of integral periodic vectors?

Remarks: 1. This was posted as https://mathoverflow.net/questions/342061/is-an-integral-sum-of-periodic-vectors-always-a-sum-of-integral-periodic-vectors

2. It is true when n has no more than two distinct prime divisors.

Solutions: 1. Evan O'Dorney gave a solution.

2. An update to the mathoverflow post notes that the result is already in the literature, where it is known as the Rédei-de Bruijn-Schönberg Theorem. References are,

N. G. de Bruijn, On the factorization of cyclic groups, Indag. Math. 15 (1953) 370-377,

L. Rédei, Ein Beitrag zum Problem der Faktorisation von Abelschen Gruppen, Acta Math. Acad. Sci. Hungar. 1 (1950) 197-207,

I. J. Schoenberg, A note on the cyclotomic polynomial, Mathematika 11 (1964) 131-136.

The de Bruijn paper is online at http://repmus.ircam.fr/_media/mamux/papers/1953-brujin-onfactorisationcyclicgroups.pdf

The Schoenberg paper is behind a paywall at

https://www.cambridge.org/core/journals/mathematika/article/abs/

note-on-the-cyclotomic-polynomial/30AB5C650C8F84B00C37E40F05D17A18

The Rédei paper is behind a paywall at

https://link.springer.com/article/10.1007/BF02021312

019:08 (Simon Rubinstein-Salzedo) Call D a *class number maximum* number (CNM, for short) if $-D$ is a fundamental discriminant, and for all fundamental discriminants $D' < D$ we have $h(-D') < h(-D)$. Let p be prime. Is it true that for all but finitely many CNM D, $-D$ is a quadratic residue modulo p?

Remark: Note that from the formula

$$L(1, \chi) = \frac{h(-D)}{\omega\sqrt{D}} = \prod_p \left(1 - \frac{\chi(p)}{p}\right)^{-1}$$

it is plausible that $h(-D)$ being large goes together with $-D$ being a quadratic residue modulo lots of small primes. The sequence of CNM numbers does not seem to be in the OEIS.

019:09 (Bernardo Recamán Santos, via Gerry Myerson) Let $s(n) = \sigma(n) - n$ be the sum of the proper divisors of n. Note that

$$s(672) + s(673) = 1344 + 1 = 1345 = 672 + 673.$$

Are there other n such that $s(n) + s(n+1) = n + (n+1)$? Are there triples, or longer runs, of consecutive integers with

$$s(n) + s(n+1) + \cdots + s(n+k) = n + (n+1) + \cdots + (n+k)$$

Are there infinitely many runs (of length at least two)?

Remarks: 1. Posted to https://mathoverflow.net/questions/329861/perfect-runs-of-consecutive-integers

2. Freddy Barrera found a length two example with $n = 523776$, and three length three examples, beginning with $n = 5829840$, $n = 3414097920$, and $n = 39339578248$. There are no more of any length for $n \leq 1.8 \times 10^{10}$.

019:10 (Simon Rubinstein-Salzedo) Consider the ordering on the positive integers given by $m <' n$ if $\phi_m(x) < \phi_n(x)$ for $0 < x \leq 1/2$, where $\phi_n(x)$ is the nth cyclotomic polynomial. What can we say about the order type of this ordering?

Remarks: The ordering is well-defined, since $\phi_n(x) - \phi_m(x)$ has no zeros in $(0, 1/2]$. The ordering is not a well-ordering, since $p >' p^2 >' p^3 \cdots$ for each prime p. It is not a reverse well-ordering, since $2 <' 3 <' 5 <' 7 \cdots$ where these are the primes.

019:11 (Dana Mackenzie) Michael Bennett has a list of eight solutions of $x^a - x = y^b - y$, $a > b > 1$, $x > 1$, $y > 1$ (see http://oeis.org/A057896). Show that there are no solutions (other than those on Bennett's list) to these equations, listed in order of increasing generality:

1. $x^{10} - x = y^3 - y$ with y prime. .
2. $x^{2n} - x = y^3 - y$.
3. $x^a - x = y^b - y$, all b, with whatever other conditions you may impose.
4. $x^a - x = y^b - y$, with no conditions (other than those applying to Bennett's list).

Are there any solutions to $x^a + x = y^b + y$, $a > b > 1$, $x > 1$, $y > 1$, other than $30 = 3^3 + 3 = 5^2 + 5$, $130 = 2^7 + 2 = 5^3 + 5$?

019:12 (Kevin McGown) Only two primes p are known for which the least primitive root modulo p is not also the least primitive root modulo p^2, namely, $p = 40487$ and $p = 6692367337$ (see http://oeis.org/A055578). Are there any more counterexamples? A heuristic suggests there may be one near 10^{27}. Also, it's known that the least primitive root modulo p^2 is always less than $p^{0.99}$. Can the exponent be improved?

019:13 (Richard Guy, via Mike Jacobson, Jr.) Let $s(m) = \sigma(m) - m$ be the sum of the proper divisors of m. Given a positive integer p, for what proportion of positive even integers n do there exist precisely p solutions to $s(m) = n$? Is the answer $(p!e)^{-1}$?

Remarks: 1. This would be consistent with experimental findings that 36% of positive even integers are "aliquot orphans", that is, are values of n such that there is no m with $s(m) = n$ (also called "untouchable numbers", also called "nonaliquot numbers", tabulated at http://oeis.org/A005114) and 36% have exactly one parent, 18% have exactly two parents, 6% have exactly three parents, while 1.5% have exactly four parents.

2. Simon Rubinstein-Salzedo notes the conjecture is inconsistent with the theorem stating that 17% of all integers (including odd integers) are aliquot orphans. [citation needed]

3. Evan O'Dorney asks, what happens for odd integers?

019:14 (Emmanuel Amiot, via Gerry Myerson) Let P, Q be monic polynomials with real, nonnegative coefficients. If $R = PQ$ has all coefficients from $\{ 0, 1 \}$, must P and Q also have coefficients from $\{ 0, 1 \}$?

Remarks: 1. Posted to https://math.stackexchange.com/questions/3325163/the-coefficients-of-a-product-of-monic-polynomials-are-0-and-1-if-the-polyn
and later (by User Sil) to https://mathoverflow.net/questions/339137/why-polynomials-with-coefficients-0-1-like-to-have-only-factors-with-0-1-coe

2. Verified by Peter Mueller for degree of R up to 32.

019:15 (Jeremy Booher) Let q be an odd prime or prime power, let a and b be relatively prime to $q-1$, and write $a \bmod m$ for the least nonnegative residue of a modulo m. Suppose $((an-1) \bmod (q-1)) + ((bn-1) \bmod (q-1)) \le q-4$ for all n with $1 \le n \le (q-3)/2$. Does this imply $a \equiv b \equiv 1 \bmod (q-1)$?

Remark: This has been verified for $q \le 1000$.

019:16 (Eva Goedhart) For integer $e \ge 1$, let $j = j_e$ be the smallest integer such that $j! > j^{e-1}$. Prove that for all $k > j_e$, $k! > k^{e-1}$.

Solution: Gary Walsh writes, Problem. Fix a positive integer $e > 1$, and let j_e denote the smallest positive integer with the property that $j_e! > j^e$. Then for any integer $k > j_e$, the same inequality $k! > k^e$ holds.

Solution. We first show that if j is any integer satisfying $j! > j^e$, then $e < j$. Since $j! > j^e$, taking log of both sides shows that $\log 2 + \cdots + \log j > e \log j$, and so by simply dividing both sides by $\log j$ and noticing that each of the $j-1$ summands is at most 1, it follows that $e < j$. (well yes, actually it follows that $e < j-1$, but we don't need this).

To solve the problem, it really just suffices to show that if $j! > j^e$, then $(j+1)! > (j+1)^e$, which is equivalent to showing that $j! > (j+1)^{e-1}$. Furthermore, by our assumption $j! > j^e$, if it can be shown that $j^e > (j+1)^{e-1}$, then we reach our desired conclusion. Let us examine this last inequality, as proving it is evidently equivalent to proving that

$$\begin{aligned} j > ((j+1)/j)^{e-1} &= (1+(1/j))^{e-1} \\ &= 1 + \binom{e-1}{1}(1/j) + \cdots + \binom{e-1}{t}(1/j)^t + \cdots + \binom{e-1}{e-1}(1/j)^{e-1}. \end{aligned}$$

By the fact proved above that $e < j$, the result is proved if it can be shown that each summand is at most 1, i.e. for each $1 \le t \le e-1$, $\binom{e-1}{t} < j^t$. But this follows from the fact that $e < j$, because $\binom{e-1}{t} \le \frac{(e-1)!}{(e-1-t)!} = (e-1)(e-2)\cdots(e-t) < j^t$.

Jeff Lagarias takes care of the cases $e = 1$ and $e = 2$ directly. Now suppose $e \ge 3$. We show that if $j \ge 2$ then $j! \ge j^{e-1}$ implies $(j+1)! \ge (j+1)^{e-1}$.

First we note that $j! \ge j^{e-1}$ implies $j \ge e$.

We have $(j+1)! = (j+1)j! \ge (j+1)j^{e-1}$. Keeping in mind

$$\left(1+\frac{1}{x}\right)^{x-1} \le \left(1+\frac{1}{x}\right)^{x} \le 2.718 < 3\ldots$$

for $x \ge 1$, we get

$$(j+1)^{e-1} \le j^{e-1}\left(1+\frac{1}{j}\right)^{e-1} \le j^{e-1}\left(1+\frac{1}{e}\right)^{e-1} \le 3j^{e-1} \le ej^{e-1} \le (j+1)j^{e-1}$$

and we're done. Jeff suggests that perhaps $\Gamma(j+1) \ge j^{e-1}$ for $j \ge j_e \ge 2$.

019:17 (Jan Vonk, via Evan O'Dorney) Let $\phi = (1+\sqrt{5})/2$. The field $L = \mathbf{Q}(\sqrt{\phi})$ has real embeddings σ_1, σ_2, and complex embeddings σ_3 and $\overline{\sigma}_3$.

$\Gamma = \mathrm{SL}_2(\mathbf{Z}[\phi])$ acts on $L \cup \{\infty\}$ by linear fractional transformations. Fix α in L with $\mathrm{Im}(\sigma_3(\alpha)) > 0$.

$$S = \{\, \beta \text{ in } \Gamma-\text{orbit of } \alpha : \sigma_1(\beta)\sigma_2(\beta) < 0, \mathrm{Im}(\sigma_3(\beta)) \geq \epsilon > 0, |\sigma_3(\beta)| \leq R \,\}$$

is finite. Find an effective and efficient algorithm to compute S.

019:18 (Anton Klyachko, via Gerry Myerson) Suppose S is a finite set of nonzero complex numbers such that $\sum_{z \text{ in } S} z^n = 0$ for infinitely many integers n, but such that S has no proper, nonempty subset T such that $\sum_{z \text{ in } T} z^n = 0$ for infinitely many integers n. Must the number of elements of S be prime?

Remark: Posted to https://mathoverflow.net/questions/322378/perfectly-balanced-sets-of-complex-numbers

Solution: Sungjin Kim has posted an affirmative answer to MathOverflow. There are three steps. First, apply the Skolem-Mahler-Lech Theorem to show that the values of n at which the sum vanishes include an infinite arithmetic progression. Second, use properties of Vandermonde matrices to deduce that each z can be taken to be a root of unity. Third and longest step is to apply results from Lam and Leung, On the vanishing sums of roots of unity, Journal of Algebra Volume 224, Issue 1, 1 February 2000, Pages 91–109 (in particular, Corollary 3.2).