Western Number Theory Problems, 17 to 19 Dec 2021

for distribution prior to 2022 (semi-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
2021 Online	021:01–021:15		

COMMENTS ON ANY PROBLEM WELCOME AT ANY TIME

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

Problems proposed 17 to 19 December 2021

021:01 (Russell Hendel) Extend results on Happy Numbers to the ring of integers of some simple UFD (Unique Factorization Domains) (e.g. quadratic, cubic fields, quartic fields).

021:02 (MathOverflow user Arthut, via Gerry Myerson) MathOverflow 351287 Density of integers related to the size of its order of appearance in the Fibonacci sequence, submitted by Arthut.

The Fibonacci entry point is $z(n) = \min\{\, k > 0 : n \mid F_k \,\}$.

Sallé (https://www.fq.math.ca/Scanned/13-2/salle.pdf) proved $z(n) \leq 2n$, with equality for $n = 6 \times 5^k$. It is known that $\liminf \frac{z(n)}{n} = 0$.

Numerical evidence suggests $A = \{\, n \geq 1 : z(n) > n/4 \,\}$ has positive upper density, that is, $\limsup \#(A \cap [1, x]) \div x > 0$. Can this be established?

Remarks: 1. Posted to https://mathoverflow.net/questions/351287/density-of-integers-related-to-the-size-of-its-order-of-appearance-in-the-fibona

2. The entry points are tabulated at https://oeis.org/A001177.
https://www.fq.math.ca/books.html has "tables of historical interest".

3. Arthut gives no details on what's meant by "numerical evidence".

4. Garry Walsh is willing to bet there are infinitely many primes with maximal entry point (but that's not going to give you positive upper density).

Solution: Sungjin Kim posted the following solution (due to Simon Rubinstein-Salzedo and himself) to MathOverflow:

The answer to this question is "No" as we can prove that the density of A is zero. Simon Rubinstein-Salzedo outlined a solution with one step to be confirmed. Then I filled in the proof of the one step.

Theorem: A has density 0. (Simon Rubinstein-Salzedo)

The argument relies on the following known facts:

Fact: The Fibonacci numbers form a strong divisibility sequence, i.e.

$$\gcd(F_m, F_n) = F_{\gcd(m,n)}$$

It follows that $z(\operatorname{lcm}(m, n)) = \operatorname{lcm}(z(m), z(n))$.

Fact: If p is a prime, then $z(p) \mid p - \left(\frac{p}{5}\right)$.

Thus if $p_1 \ldots, p_k$ are distinct primes different from 2 and 5, then $\frac{z(p_1 \cdots p_k)}{p_1 \cdots p_k} \leq \frac{1}{2^{k-1}} \prod_{i=1}^{k} \left(1 + \frac{1}{p_i}\right)$, and this tends to 0 as $k \to \infty$. Let's write

$$m(k) = \frac{1}{2^{k-1}} \prod_{i=1}^{k} \left(1 + \frac{1}{p_i}\right),$$

where the product is over the first k odd primes other than 5. [continued]

For an integer n, let $r(n) = \prod p$, where the product is taken over all primes p other than 2 and 5 that divide n but whose square doesn't divide n, and let $s(n) = \frac{n}{r(n)}$. I believe (to be confirmed) that for any k,

$$\lim_{x\to\infty} \frac{\#\{n : 1 \le n \le x, \omega(r(n)) \ge k\}}{x} = 1.$$

For any n with $\omega(r(n)) \ge k$, we have

$$\frac{z(n)}{n} \le \frac{z(r(n))}{r(n)} \cdot \frac{z(s(n))}{s(n)} \le m(k) \cdot 2,$$

which tends to 0 as $k \to \infty$. Thus the upper density of A is 0.

Confirming the "density one" result (Sungjin Kim)

The constant $C > 0$ may appear several times, not necessarily the same everytime.

Let P_k be the set of positive integers with fewer than k distinct prime factors. Let $A_k(t) = \sum_{n\le t, n\in P_k} 1$ be the counting function of P_k. By Hardy-Ramanujan, we have an estimate

$$A_k(t) \le C\Psi_k(t) := C\frac{t(\log\log(t+C)+C)^{k-2}}{\log(t+C)}.$$

The numbers satisfying $\omega(r(n)) < k$ can be decomposed as

$$n = my$$

with $m = 2^{\nu_2(n)}5^{\nu_5(n)}r(n)$ so that $\omega(m) < k+2$ and y is powerful, that is, $p|y \Rightarrow p^2|y$.

Let $\mathcal{F}$ be the set of powerful numbers. The estimate of the number of powerful numbers is obtained by Bateman and Grossward in 1958 (as a stronger form than below),

$$\sum_{y\le x, y\in\mathcal{F}} 1 \le C\sqrt{x}.$$

Combining these to estimate the numbers $n \le x$ with $\omega(r(n)) < k$,

$$\le C \sum_{m\le x, m\in P_{k+2}} \sum_{y\le \frac{x}{m}, y\in\mathcal{F}} 1 \le C \sum_{m\le x, m\in P_{k+2}} \sqrt{\frac{x}{m}}.$$

Applying the partial summations to the last sum,

$$\sum_{m\le x, m\in P_{k+2}} \sqrt{\frac{x}{m}} \le C\Psi_{k+2}(x) + C\sqrt{x}\int_1^x \frac{\Psi_{k+2}(t)}{t\sqrt{t}}dt \le C\Psi_{k+2}(x).$$

Hence,

$$\sum_{n\le x, \omega(r(n))<k} 1 \le C\Psi_{k+2}(x).$$

Remark: There remains the question about relative density if we restrict to Fibonacci entry points of primes.

021:03 (David Kogan) Consider numbers k such that $\varphi(x) = k$ has precisely 2 (positive) solutions. This is sequence A007366 on OEIS. Most entries on this list are of the form $p - 1$ with p prime.

Question: Suppose k is composite, and $\varphi(x) = k$ has precisely 2 (positive) solutions. Call these solutions $x_1 < x_2$. Must $x_1 = q^r$ for some odd prime q?

Examples: For $k = 54$ we find $x_1 = 81 = 3^4$. Similarly, $k = 110$ gives $x_1 = 121 = 11^2$.

Solution: (Sungjin Kim) The answer to the question is No.

We apply two results by Kevin Ford to find a lower bound of the number:

$$V_2(x) := |\{n \le x : \varphi(y) = n \text{ has precisely 2 solutions}\}|.$$

Letting $V(x) := |\{n \le x : \phi(y) = n \text{ for some } y\}|$, we have by https://annals.math.princeton.edu/1999/150-1/p08, stated in a stronger form than the following we need,

$$V(x) = \frac{x}{\log x} \exp\{C(\log_3 x)^2 + O(\log_3 x \log_4 x)\}.$$

where $\log_k x$ is the k-times iterated logarithm.

By https://link.springer.com/article/10.1023/A:1009761909132, also stated in a stronger form than what we need, we have

$$\liminf_{x\to\infty} \frac{V_2(x)}{V(x)} > 0.$$

Thus, there is a positive constant c such that for sufficiently large x,

$$V_2(x) \ge cV(x) \qquad (1).$$

Now, we count the number of $n \le x$, $n \in V_2(x)$ that has $\varphi(y) = n$ with $y = p^k$. Such a number is bounded by $cx/\log x$.

By (1), we see that there are many more elements in the set of numbers $n \le x$ with precisely two solutions in $\varphi(y) = n$.

021:04 (Zack Baker) Let $\mathcal{T}_n$ be the set of T_i, the first n triangular numbers taken mod n (including $T_0 = 0$). Is there an (elegant) proof that the elements of $\mathcal{T}_n$ are distinct if and only if $n = 2^k$, $k \in \mathbf{N}$?

Solution: (Evan O'Dorney)

1. If n is odd, then $T_{n-1} \equiv 0 \pmod{n}$, so odd values of n can be discarded.

2. If n has an odd prime divisor p, then by the previous point, not all values mod p occur (since $T_i = i(i+1)/2$ depends only on i mod p if p is odd). Therefore the elements of $\mathcal{T}_n$ are not distinct if n is not a power of 2. [continued]

Now assume that $n = 2^k$. For $0 \le a < b < n$, look at the difference

$$T_b - T_a = \frac{b(b+1)}{2} - \frac{a(a+1)}{2} = \frac{(b-a)(a+b+1)}{2}.$$

The factors in the numerator are of opposite parity and are strictly between 0 and $2n = 2^{k+1}$. So 2^{k+1} does not divide the numerator, and $n \not| T_b - T_a$, as desired.

021:05 (Evan O'Dorney) Let $f(x) = ax^2 + bx + c$ be a quadratic polynomial, where the coefficients a, b, c are integers. The *superdiscriminant* of f is the product

$$I = a \cdot (b^2 - 4ac)$$

of the leading coefficient with the usual discriminant. Call two quadratics f_1, f_2 *equivalent* if they are related by a translation $f_2(x) = f_1(x+t)$. If I is a nonzero integer, let $q(I)$ be the number of quadratics of superdiscriminant I, up to equivalence. Let $q_2(I)$, $q^+(I)$, $q_2^+(I)$ be the number of such quadratics that satisfy certain added conditions:

- For $q_2(I)$, we require that the middle coefficient b be even.
- For $q^+(I)$, we require that the roots be real, that is, that $b^2 - 4ac > 0$.
- For $q_2^+(I)$, we impose both of the last two conditions.

For every nonzero integer n, we have the two identities:

$$q_2^+(4n) = q(n) \quad \text{and} \quad q_2(4n) = 2q^+(n).$$

Find a proof of these using no tools more advanced than quadratic reciprocity. (See my https://arxiv.org/abs/2107.04727, section 2.1.)

021:06 (MathOverflow user 153451, via Gerry Myerson) Conjecture: for every natural m there exists natural r such that $\phi(rm+1) = \phi(rm+r+1)$.

Remarks: 1. Posted to https://mathoverflow.net/questions/356105/how-to-explain-this-property-of-totient

2. Checked for $1 \le m \le 489$. Checking $m = 407$ took a long time; user gave up on $m = 490$.

3. Robert Israel wrote, it might just be a matter of randomness. Seeing no reason for $\varphi(rm+1)$ and $\varphi(r(m+1)+1)$ to be especially related, we might imagine heuristically that $\varphi(rm+1)$ and $\varphi(r(m+1)+1)$ have probability $\sim$ constant$/(rm)$ of being equal. Since $\sum_m 1/m = \infty$, it would then be reasonable to expect there to be infinitely many m for which this is the case. Of course this is not a proof.

This also suggests that if a small m is not found for a particular r, you might need to look very far (something like exp(constant$/r$)) before finding an m that works.

021:07 (Bill Rowan) Define a *supertopological space* as a set S, provided with, for each point $p \in S$, an ideal of filters of subsets of S, called *neighborhood filters* of S, with the ideal being called the *neighborhood ideal* of p. (Note: we order filters by reverse inclusion and ideals by inclusion.) It is required that the neighborhood ideal of p contain the principal filter $Fg(p)$ of all subsets containing p. If $f : S \to T$, then we say f is *supercontinuous* if for every $s \in S$, if F is a neighborhood filter of s, then $f(F)$ is a neighborhood filter of $f(s)$, where $f(F)$ is the filter of subsets of T generated by sets $f(X)$ for $X \in F$. Supertopological spaces and supercontinuous mappings form a category in an obvious manner.

The problem is to find out whether this category is cartesian closed, and then, use this category as a base category, explore abelian groups with a compatible superuniformity, put a closed monadic category structure on it, and do Abstract Harmonic Analysis.

021:08 (MathOverflow user LMZ, via Gerry Myerson) Is this inequality about classical Dedekind sums true? Let

$$s(h,q) = \sum_{a=1}^{q} \left(\left(\frac{a}{q}\right)\right)\left(\left(\frac{ah}{q}\right)\right)$$

where $((x))$ is zero if x is an integer, $x - [x] - (1/2)$ otherwise. Conjecture: If p is prime, then

$$\sum_{h=1}^{p} hs(h,p) \leq 0$$

Remarks: 1. Posted to https://mathoverflow.net/questions/356526/is-this-inequality-about-classical-dedekind-sums-true 4 April 2020, deleted 12 April 2020.

2. Note: $s(h,p) > 0$ for small h (roughly, $h < \sqrt{p}$), $s(h,p) < 0$ for large h (since $s(p-h,p) = -s(h,p)$), so the inequality would not be surprising.

021:09 (MathOverflow user tobias, via Gerry Myerson) How many solutions does the equation

$$\frac{a^2}{a^2-1} \cdot \frac{b^2}{b^2-1} = \frac{c^2}{c^2-1}$$

have in integers a, b, c between 2 and k?

Remarks: 1. Posted to https://mathoverflow.net/questions/359481/natural-number-solutions-for-equations-of-the-form-fraca2a2-1-cdot-fra 5 May 2020.

2. One solution is $(a,b,c) = (9,8,6)$.

3. Dmitry Ezhov contributed several other solutions.

4. $(a,b,c) = (n(n^2-3)/2, n^2-1, n^2-3)$ is a solution for all $n \geq 3$, so there are infinitely many solutions.

5. Some other infinite families of solutions:

$a = 4n(n+1)(n^2+n-1), b = (2n+1)(2n^2+2n-1),\ c = 2(2n+1)(n^2+n-1)$.

$(a,b,c) = (x^2, 2y^2, xy)$ where $x^2 - 2y^2 = \pm 1$.

$(a,b,c) = (3y, x, (3/4)x)$, where $x + y\sqrt{7} = (8+3\sqrt{7})^n$, and n is odd.

021:10 (Zack Baker) Let $c = (0, g_1, g_2, \ldots g_{n-1})$ be an ordering of the elements of $\mathbf{Z}/n\mathbf{Z}$. Call c *constructive* if all partial sums of the elements of c are also distinct modulo n (the values $0, g_1, g_1 + g_2$, etc), and *non-constructive* if this is not the case.

Define a k-left shift on c as the cyclic shift left of the non-zero entries of c by k positions (e.g. a 1-left shift of c produces the ordering $(0, g_2, g_3, \ldots, g_{n-1}, g_1)$). It can be shown that if c is constructive, then 1-left and 2-left shifts produce non-constructive orderings. Is this true for all k-left shifts, for $k \not\equiv 0 \pmod{n-1}$?

021:11 (Vaishavi Sharma) Conjecture: For a fixed prime p, there exists no integer n that satisfies the following: There is a unique prime $q > p$ dividing n such that $\nu_p(\sigma(q^{\nu_q(n)})) = \lceil \log_p(q^{\nu_q(n)}) \rceil$.

021:12 (math.stackexchange user Trevor, via Gerry Myerson) Conjecture: Every prime of the form $x^2 + 1$ for $x > 90$ is a sum of five primes of the form $x^2 + 1$.

Remarks: 1. Posted to https://math.stackexchange.com/questions/3479074/conjecture-all-x21-primes-for-x90-can-be-represented-as-the-sum-of-five 16 December 2019.

2. Confirmed up to 10^6 (although it isn't clear whether this means $x \leq 10^6$ or $x^2 + 1 \leq 10^6$).

3. It is further conjectured that for x sufficiently large one can take one of the five primes to be 5. Also, that for x sufficiently large one can take the five primes to be distinct.

4. Other comments can be found at the stackexchange URL.

021:13 (Gerry Myerson) In this question, "polynomial" means "polynomial with integer coefficients," and "reducible" means "reducible over the integers."

Let $P_n(x) = x(x + 1)(x + 2) \cdots (x + n - 1) + x$. Then for all n, the n "consecutive" polynomials $P_n, P_n + 1, \ldots, P_n + n - 1$ of degree n are all reducible. Given n, can there be more than n consecutive reducible polynomials of degree n?

Yes, for $n = 2$: $6x^2 + 7x$, $6x^2 + 7x + 1 = (6x + 7)(x + 1)$, $6x^2 + 7x + 2 = (3x + 2)(2x + 1)$ are three consecutive reducible quadratics (and there can't be four). Can there be four (or more) consecutive reducible cubics?

Remarks: 1. The question is related to https://mathoverflow.net/questions/149362/large-gaps-between-consecutive-irreducible-polynomials-with-small-heights submitted by Wolfgang, 19 November 2013, where the emphasis was on small coefficients. Gjergji showed there are n consecutive $0, 1$ reducible polynomials, but of very high degree.

2. The question is also related to https://mathoverflow.net/questions/59956/consecutive-irreducible-polynomials submitted by Ewan Delanoy, 29 March 2011, where I mentioned it in a comment.

3. One can attempt to find four consecutive reducible cubics via the Chinese Remainder Theorem. We want a cubic polynomial P, and distinct nonzero rationals r, s, t, such that

$$
\begin{aligned}
P &\equiv 0 \pmod{x} \\
P &\equiv -1 \pmod{x + r} \\
P &\equiv -2 \pmod{x + s} \\
P &\equiv -3 \pmod{x + t}
\end{aligned}
$$

The solution to this system is $P(x) = Ax^3 + Bx^2 + Cx$, with

$$A = \frac{1}{r(s-r)(t-r)} + \frac{2}{s(r-s)t-s)} + \frac{3}{t(r-t)(s-t)}$$
$$B = \frac{s+t}{r(s-r)(t-r)} + \frac{2(r+t)}{s(r-s)t-s)} + \frac{3(r+s)}{t(r-t)(s-t)}$$
$$C = \frac{st}{r(s-r)(t-r)} + \frac{2rt}{s(r-s)t-s)} + \frac{3rs}{t(r-t)(s-t)}$$

The question is whether one can choose rational r, s, t, other than $(r, s, t) = (1, 2, 3)$, such that A, B, C are integers.

021:14 (Gary Walsh) In the question below we will use the following notation. For a non-square positive integer d, let $\epsilon_d = T + U\sqrt{d}$ be the minimal unit of norm 1 in $\mathbf{Z}[\sqrt{d}]$, and for $k \geq 1$, let $\epsilon_d^k = T_k + U_k\sqrt{d}$. In other words, T, U is the smallest solution to the Pell equation $X^2 - dY^2 = 1$, and T_k, U_k is the k-th solution arising from it.

Fix a positive integer m. Computations suggest that there is never more than one positive integer x which is a root of 1 modulo m^2 (i.e. that $T_k = x$, $U_k = m$, $d = (x^2-1)/m^2$) which satisfies the condition $k \geq 3$.

021:15 (Jon Grantham) We call (a, b) a reverse sum-product pair for the base β if the digits of $a + b$ are the reverse of the digits of ab, when written in base β. E.g., in base ten, $(3, 24)$ is such a pair, since the digits of $3 + 24 = 27$ are the reverse of the digits of $3 \times 24 = 72$.

a) What results are there when you allow leading/trailing zeros?

b) We call a rsp "uninteresting" if both a and b have a single digit. There are no interesting rsps for bases $2, 3, 4, 5, 6, 7, 8, 9, 12, 15, 21$; there are interesting rsps for all other bases up to $1,441,440$. We have proved that there interesting rsps for 99.3% of all bases. Are there interesting rsps for all bases 22 and up?

Remark: Claudia Spiro asks, what happens when you allow 3 digits, e.g. $1 + 2 + 3 = 1 \times 2 \times 3$? That is, when is $a + b + c$ the reversal of abc?