Western Number Theory Problems, 16 to 18 Dec 2023

for distribution prior to 2024 Asilomar 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	2022 Asilomar	022:01–022:21
2023 Henderson	023.01-023.24		

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

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.

Remark: 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?

Update 2024: Andreas Reinhart, A counterexample to the conjecture of Ankeny, Artin and Chowla, https://arxiv.org/abs/2410.21864, carries the computation further in Remark 3.1:

Let $d \in \mathbf{N}_{\geq 2}$ be squarefree, let $L = \mathbf{Q}(\sqrt[3]{d})$, let $\mathcal{O}_L$ be the ring of algebraic integers of L, let $\eta > 1$ be the fundamental unit of $\mathcal{O}_L$ and let $a, b, c \in \mathbf{N}$ be the unique positive integers with $\eta = (1/3)(a + b\sqrt[3]{d} + c\sqrt[3]{d^2})$. The following are equal:
$\{d \in [2, 10^7] : d \text{ is squarefree and } d \mid b\}$,
$\{d \in [2, 10^7] : d \text{ is squarefree and } 3d \mid b\}$, and
$\{3, \ldots, 1185, 28131, 47019, 89411, 125265, 144147, 435498, 1688610, 4580214, 5123415\}$.
The ellipsis indicates values already computed by Kevin. Note that 89411 is the only number in the set that is not divisible by 3.

Problems proposed 16 to 18 December 2023

023:01 (Alexey Ustinov via Gerry Myerson) Is there a regular pentagon with a rational point on each edge?

Remarks: 1. (Peter Mueller): If so, each slope m is in $\mathbf{Q}(s)$ with $s = \sin(2\pi/5)$. A cubic relation holds for the slope. If $m = m_0 + m_1 s + m_2 s^2 + m_3 s^3$, $m_j \in \mathbf{Q}$, then

$$\begin{aligned} 64m_0m_1^2 - 64m_0^2m_2 - 80m_0m_2^2 - 20m_2^3 + 160m_0m_1m_3 \\ + 40m_1m_2m_3 + 80m_0m_3^2 + 25m_2m_3^2 - 64m_2 = 0. \end{aligned}$$

Solutions of this equation may be points on the extensions of the edges, rather than on the edges.

2. The problem is found at mathoverflow.net/questions/459110.

3. User uranix posted to mathoverflow on 12 January 2024 to prove that a rational point on each edge is impossible. The post contains an example of five rational points, two on the edges of a regular pentagon, the other three on extensions of the other three edges. User Matthew Bolan posted on 18 January 2024 to make progress on the general question, for which values of n can there be a rational point on each edge of a regular n-gon, or on an extension of each edge.

023:02 (Eva Goedhart) Background: teaching 6th graders about percent. One way to solve "what percent of 80 is 12?" is by using other percents, e.g., 50% of 80 is 40, so 5% of 80 is 4, so 15% of 80 is 12.

Similarly, "17% of 80 is what?" can be solved by 10% of 80 is 8, 5% of 80 is 4, 2% of 80 is 1.6, so 17% of 80 is 13.6.

Can we solve "18% of what is 25?" by the same method?

Note: we know there are other ways to solve these questions, but we want to know whether this last sort of question can be solved by the method of combining other "percents".

Solution: (Anay Aggarwal) $x\%$ of y is z can be rephrased as $y\%$ of x is z, reducing it to a problem-type already solved.

023:03 (Gary Walsh) Recall that a *powerful* number is a number n such that if p is a prime dividing n, then p^2 divides n. Equivalently, it is a number that can be written as a^2b^3 for some integers a, b. Is there a quadruple of coprime powerful numbers in arithmetic progression having fewer than 110 digits?

Remark: Prajeet Bajpai, Michael A. Bennett, Tsz Ho Chan, Arithmetic progressions in squarefull numbers, https://arxiv.org/abs/2302.03113, give a quadruple of coprime powerful numbers in arithmetic progression having several hundred digits.

Mention may also be made here of P. G. Walsh, A question of Erdös on 3-powerful numbers and an elliptic curve analogue of the Ankeny-Artin-Chowla conjecture, https://arxiv.org/abs/2404.03970

023:04 (Simon Rubinstein-Salzedo) Let K be a number field and $\mathfrak{o}_K$ its ring of integers. Which elements of $\mathfrak{o}_K$ are sums of two squares?

Remarks: 1. Jiwu Jang asks, is the density of such elements (always) positive? Sungjin Kim answers, no, for $\mathbf{Q}$, $\sum_{n\le x, n \text{ is sum of two squares}} 1 \sim cx/\sqrt{\log x}$.

2. Is there a number field K which has a positive density of elements that are sums of two squares? Sungjin Kim replies, "I do not know the answer. The result for $\mathbf{Q}$ is based on the characterization of the sum of two squares. So, we need an answer to Simon's question about the structure of the sum of two squares in $\mathfrak{o}_K$."

3. Jordan Hardy notes, "this problem seems very difficult in general, but becomes easier if you impose some (major) restrictions. I think that if you restrict to the case where K is totally real and both K and $K(i)$ have class number 1 you can probably figure it out in a way similar to one proof of the characterization for $K = \mathbf{Q}$. Unfortunately such cases might not be very common."

4. Your editor points to

https://math.stackexchange.com/questions/4403865/ is-there-any-variation-known-to-the-sum-of-two-squares-theorem

and also

Niven, Integers of quadratic fields as sums of squares, Trans. Amer. Math. Soc. 48, (1940). 405–417
https://www.ams.org/journals/tran/1940-048-03/
S0002-9947-1940-0003000-5/S0002-9947-1940-0003000-5.pdfx

5. Wenhuan Huang, Sum of two squares in biquadratic fields, "gives an algorithm to determine whether a number in a biquadratic field is a sum of two squares, based on local-global principle of isotropy of quadratic forms." https://arxiv.org/abs/2401.12619

023:05 (Simon Rubinstein-Salzedo) Don Zagier gave a famous proof that every prime $p \equiv 1 \pmod 4$ is a sum of two squares, using involutions. Elsholtz followed up with similar arguments for primes represented by $x^2 + 2y^2$ and $x^2 + 3y^2$. Can we find similar arguments for other quadratic forms, especially those of type $x^2 + Ny^2$? In particular, $x^2 + 14y^2$?

Remarks: 1. The Zagier proof is based on observing that a certain involution on $S = \{(x, y, z) \in \mathbf{N}^3 : x^2 + 4yz = p\}$ has an odd number of fixed points. The Zagier reference is

D. Zagier, A one-sentence proof that every prime $p \equiv 1 \pmod 4$ is a sum of two squares, Amer. Math. Monthly 97 (1990) 144.

The Elsholtz reference may be

Elsholtz, C. (2010). A combinatorial approach to sums of two squares and related problems. In: Chudnovsky, D., Chudnovsky, G. (eds) Additive Number Theory. Springer, New York, NY. https://doi.org/10.1007/978-0-387-68361-4-8,

available at

https://www.math.tugraz.at/∼elsholtz/WWW/papers/papers30nathanson-new-address3.pdf

See also

https://mathoverflow.net/questions/31113/zagiers-one-sentence-proof-of-a-theorem-of-fermat

2. Your editor suggested the article, Roland Bacher (2023) A quixotic proof of Fermat's two squares theorem for prime numbers, The American Mathematical Monthly, 130:9, 824-836, but on closer inspection it doesn't appear to deal with this question.

023:06 (Christian Zhou-Zheng) This can probably be solved on the spot. (x_1, x_2, x_3) is called a *Diophantine triple* if $x_i x_j + 1$ is a square for $1 \le i < j \le 3$. T_a denotes the *triangular number* $a(a + 1)/2$. An example of a Diophantine triple of triangular numbers (T_a, T_b, T_c) is $(1, 3, 120) = (T_1, T_2, T_{15})$. A more general form is $(a, b, c) = (n, n + 4, 4n^2 + 20n + 8)$. Now, take an ordered Diophantine triple of triangular numbers (T_a, T_b, T_c) with $a < b < c$ and let $d = 4ac + 2a + 2c - b$ and $e = 4bc + 2b + 2c - a$. Then it appears (a, c, d) and (b, c, e) also correspond to the indices of another triangular Diophantine triple. Is this always true?

Let's write it all out. Writing T_n for $n(n + 1)/2$, letting a, b, c be such that $T_aT_b + 1$, T_aT_c+1, and T_bT_c+1 are all squares, and letting $d = 4ac+2a+2c−b$ and $e = 4bc+2b+2c−a$, is it necessarily the case that $T_aT_d + 1$, $T_cT_d + 1$, $T_bT_e + 1$ and $T_cT_e + 1$ are also all squares? Surely a good computer algebra system can tell us?

023:07 (Christian Zhou-Zheng) Is it true that, in the notation used above, the only d such that $a < c < d$ yields a Diophantine triple of triangular numbers, and the only e such that $b < c < e$ yields a Diophantine triple of triangular numbers, are those given by the preceding formulas? Furthermore, is *every* triangular Diophantine triple generated by applying the transformation(s) given above to a triple indexed by $(1, 2, 15)$ or $(n, n + 4, 4n^2 + 20n + 8)$, then applying the transformation repeatedly to the newly generated triple?

023:08 (Richard Guy via Renate Scheidler)

Math problem for people who don't know how to add fractions: Find all integers a, b, c, d such that $\frac{a}{b} + \frac{c}{d} = \frac{a+c}{b+d}$, $bd \neq 0$, $b \neq -d$.

Solution: The question is solved at

https://math.stackexchange.com/questions/1861846/for-which-integers-a-b-c-d-does-fracab-fraccd-fracacbd

(continued)

Remarks: 1. (Andrew Lavengood-Ryan) This type of "fraction addition" comes up in hyperbolic geometry.

2. Your editor recalls that many years ago (before his time), it was a thing for math faculty at SUNY Buffalo to go out to local schools to help. On one such visit, Al Fadell found a teacher telling the class to add fractions by adding the numerators and adding the denominators, that is, by $\frac{a}{b} + \frac{c}{d} = \frac{a+c}{b+d}$. He was horrified, and took the teacher aside after the class was let out, to show the teacher the right way to add fractions.

Al came back to that class some weeks later, and was astonished to see the teacher still using $\frac{a}{b} + \frac{c}{d} = \frac{a+c}{b+d}$. Again, he took the teacher aside after class, and asked, didn't I show you the right way to add fractions? The teacher replied, yes, and I tried to teach that, but the students found it too difficult.

3. Aaron Wong suggested the related problem of reducing fractions $\dfrac{16}{64} = \dfrac{1\not{6}}{\not{6}4} = \dfrac{1}{4}$ by cancelling the sixes.

4. Christian noted that the cancellation problem appeared on this year's SuMaC entrance exam as the first question.

023:09 (MathOverflow user Jean via Gerry Myerson) Is there is Liouville number ξ such that e^ξ is a Liouville number?

Remark: This problem was posted at mathoverflow.net/questions/459643 on 2 December 2023.

023:10 (M.Tip Phaovibul) Given $k \in \mathbf{N}$, do there exist n such that $\sigma(n+k) = \sigma(n) + k$ where σ is the sum of divisors function. How about for φ?

Remarks: 1. A recent paper by Kevin Ford proves that for a positive proportion of k, $\sigma(n+k) = \sigma(n)$ has infinitely many solutions n. The proof relied on recent progress on the prime k-tuple conjecture. See https://ford126.web.illinois.edu/wwwpapers/phink.pdf published as Solutions of $\phi(n) = \phi(n+k)$ and $\sigma(n) = \sigma(n+k)$, Kevin Ford, IMRN 2022 (2022), Issue 5, Pages 3561-3570, https://academic.oup.com/imrn/article/2022/5/3561/5896974, https://doi.org/10.1093/imrn/rnaa218

2. (Anay Aggarwal) "For $k = 1$, is $n = 2$ the only solution? For this k, n must be of the form $r^2, r^2 - 1, 2(2r-1)^2$, or $2(2r-1)^2 - 1$ (as noted by Sam). I've checked with a program that there are no other solutions for $r \le 3465$ (and therefore $n \le 10^7$). This computation took around half an hour on my computer (C++, non-parallelized, compiled with O3 optimizations)."

3. Your editor notes that if p, q are primes with $q = p + k$ then $\sigma(p+k) = \sigma(p) + k$. So assuming, as everyone believes, that for every even k there are primes differing by k, there are solutions for all even k. Also, for every prime p there is a solution for $k = p - 2$.

4. Let $\sigma'(n) = \sigma(n) - n$ be the aliquot divisor sum of n, the sum of the proper divisors of n. Then we are looking for n, k such that $\sigma'(n+k) = \sigma'(n)$. An unsystematic search turns up the following values of k, not covered by the previous cases:

k	7	13	19	33	37	73	93	113	293	327	573	593	669	677	753	903
n	74	4418	6	18	44	18	32	64	36	34	98	36	98	36	64	58

The smallest value of k for which I have no solution is $k = 23$.

5. Sungjin Kim points out that, using the Maynard-Tao theorem on prime gaps, for some even $k \le 246$, there are infinitely many p such that $q = p+k$ is prime. Then $\sigma(p+k) = \sigma(p)+k$.

023:11 (Jiwu Jang) Fix $P, Q \in \mathbf{Z}(x)$ and let $f \in \mathbf{Z}[x]$. Does the solution set of f for $P(f(x)) = f(Q(x))$ in $\mathbf{Z}[x]$ uniquely extend to $\mathbf{R}[x]$ for all P, Q? Is it possible to characterize all such P, Q? (One example that does work, to my knowledge, is $P(x) = -x/(x+1)$ and $Q(x) = x/(x-1)$, giving the family $f = \pm(x-1)^n - 1$.)

023:12 (Michael Allen) $12 + 1$ and $11 + 2$ are both partitions of 13, and "twelve plus one" and "eleven plus two" are anagrams. Are there any other (fundamentally different) instances of this?

Remarks: 1. (Andrew Lavengood-Ryan) This feels combinatorial, so I wonder if there's a way to build a program that pulls from a dictionary. . ..

2. (Anay Aggarwal) Jean-Charles Meyrignac found the smallest anagram sum in French:

$$345 + 221 + 215 = 592 + 156 + 32 + 1, \text{ and}$$

"trois cent quarante cinq + deux cent vingt et un + deux cent quinze" is an anagram for "cinq cent quatre vingt douze + cent cinquante six + trente deux + un."

3. (Jiwu Jang) Take a torsion-free commutative monoid M, additively written, generated by letters a to z, and a map $f : \mathbf{N} \to M$ that maps each positive integer to a string of its characters, then the question is whether there are a_1, a_2, ..., a_n and b_1, b_2, ..., b_m distinct such that $\sum a_i = \sum b_i$ and $\sum_{i\in[1,n]} f(a_i) = \sum_{i\in[1,m]} f(b_i)$. One direction would be to look at the behavior of f.

4. Your editor says, see

https://erich-friedman.github.io/mathmagic/1008.html

for some math/language/anagram fun. Also, just for French,

http://www.cetteadressecomportecinquantesignes.com/Eleven.htmc

023:13 (William Hu via Gerry Myerson) mathoverflow 457719, 4 Nov 2023.

$$\binom{11}{2} = 55, \quad \binom{11}{3} = 165, \quad \binom{12}{4} = 495, \quad \binom{55}{2} = 1485$$

a geometric progression with common ratio 3, and

$$\binom{13}{3} = 286, \quad \binom{13}{6} = 1716, \quad \binom{144}{2} = 10296, \quad \binom{352}{2} = 61776$$

with common ratio 6 are the only known geometric sequences of length four among non-trivial binomial coefficients (thanks to Renate Scheidler for a correction here) ("non-trivial" means $\binom{n}{k}$ with $2 \le k \le n/2$). Are they the only such sequences?

Remark: Brendan McKay finds no others with integer common ratio and largest term less than 10^{17}; no others with rational common ratio and largest term less than 10^{13}. There are infinitely many such sequences of length three, e.g.,

$$\binom{n^2+n-1}{n-1}, \binom{n^2+n-1}{n}, \binom{n^2+n}{n+1}$$

has ratio n.

023:14 (Bogdan Grechuk via Gerry Myerson) mathoverflow 453864, 2 Sept 2023. What is the "taxicab number" for rational fourth powers?

The smallest positive integer represented in two ways as a sum of
two positive integer squares is $50 = 7^2 + 1^2 = 5^2 + 5^2$;
two positive integer cubes is $1729 = 12^3 + 1^3 = 10^3 + 9^3$;
two positive integer fourth powers is $635318657 = 134^4 + 133^4 = 158^4 + 59^4$.

It is a well-known open question as to whether there is an example for fifth powers.

The smallest positive integer represented in two ways as a sum of
two positive *rational* squares is $1 = (3/5)^2 + (4/5)^2 = (5/13)^2 + (12/13)^2$;
two rational cubes is $6 = (37/21)^3 + (17/21)^3 = (223772/960540)^3 + (-1805723/960540)^3$.

What about two rational fourth powers?

Remarks: 1. 82 is the smallest number not yet ruled out.

2. There are numbers which are a sum of two rational fourth powers but not two integer fourth powers, e.g., $5906 = (149/17)^4 + (25/17)^4$. Bremner, A., Morton, P. A new characterization of the integer 5906. Manuscripta Math 44, 187?229 (1983). https://doi.org/10.1007/BF01166081

023:15 (Rob Akscyn) Life is a series of realizations that didn't occur previously, which is you can use the problem session to save time during your upcoming talk. Topic: INTEREST? Declining interest in mathematics. E.g., growing number of engineering courses with no math requirements.

What led you to be interested in the following?
(1) Math
(2) Number Theory
(3) Problem(s)
(4) WCNT

023:16 (Varun Vejalla via Gerry Myerson), math.stackexchange.com/questions/4737448.

Write $\{x\}$ for the fractional part of x. Let ϕ be the golden ratio. Then

$$\{\phi^{-1}\} = \{\phi\} = \{\phi^2\}.$$

Find other real x such that $\{x^n\}$ has the same non-zero value for 3 (or more) integers n.

Remarks: 1. If $\{x^r\} = \{x^s\} = \{x^t\}$, then we get trivial variations when $y = x^{1/k}$; $\{y^{rk}\} = \{y^{sk}\} = \{y^{tk}\}$.

2. The other known examples:

If x is the real root of $x^3 - x - 1$, then your editor found $\{x^{-4}\} = \{x\} = \{x^3\}$, and Peter Košinár found $\{x^5\} = \{x^4\} = \{x^{-9}\}$.

If x is the real root of $x^3 - x^2 - 1$, then Peter found $\{x^3\} = \{x^2\} = \{x^{-5}\}$.

We tried other polynomials of the form $x^a - x^b - 1$, without success.

3. A related question is https://math.stackexchange.com/questions/382227.

023:17 (Austin Docherty) (Inspired by **023:12**.) Given $n, m \in \mathbf{N}$, what is the partition of n of exactly m summands that maximizes the number of distinct subsums? E.g., 6 and 3: $1+2+3$ gives us all seven possible subsums, whereas $1+1+4$ gives only six: we get 0, 1, 2, 4, 5, 6 but not 3. Is there an algorithmic way to get $P_{n+1,m}$ or $P_{n,m+1}$ given $P_{n,m}$? Here, $P_{n,m}$ is an optimal partition of n into m parts.

Remarks: 1. (Anay Aggarwal) If $m \geq \frac{n}{2}+1$, a construction is $\underbrace{1,1,\ldots,1}_{m-1}, n-m+1$. The subsums must be in the interval $[0,n]$, so their amount is bounded by $n+1$. This clearly achieves all such sums.

2. (Simon Rubinstein-Salzedo, following a car discussion with M.Tip Phaovibul and Sungjin Kim)

Case 1: $m \geq \log_2(n) + \mathrm{o}(1)$

$n = 1+2+4+\cdots+2^k+$ whatever is left.

We get every sum from 0 to n

Case 2: $m < \log_2(n) + \mathrm{o}(1)$ Optimal: 2^m distinct sums. Then make sure that each part is at least 2 times the previous part

$n = 1+2+4+\cdots+2^{m-2}+$ whatever is left.

023:18 (Sungjin Kim from math.stackexchange.com/questions/4796258, posted by Danka Makabre, 29 October 1923.) $\{\sqrt{s} : s \in \mathbf{N},\ \text{square} - \text{free}\}$ is $\mathbf{Q}$-linearly independent.

Let $f \in \mathbf{Z}[z]$ with $\deg f \geq 1$. Does $f^{-1}\mathbf{Z} = \{z \in \mathbf{C} \mid f(z) \in \mathbf{Z}\}$ have infinitely many $\mathbf{Q}$-linearly independent numbers?

Remarks: 1. If $g(z)^2 | f(z)$ for some $g \in \mathbf{Z}[z]$, $\deg g \geq 1$, it is true.

2. (Simon Rubinstein-Salzedo) This should follow from Hilbert irreducibility.

023:19 On a lighter note, a limerick by Renate Scheidler's student: works with any course that ends in "teen" (ideally a 3-digit number; in this specific case the course number was 418):

This term I took four-eighteen

The instructor was really quite mean

Though I gave it my best

I did not pass the test

Now I have to go see the dean

Remarks: 1. Too bad the course number wasn't 429; the student might have written This term I took four twenty-nine/ The instructor was really quite fine ....

2. I think this was meant as a comment on our schedule: "We meet at nine ... okay fine ... afterwards, we will dine ...."

023:20 (Simon Rubinstein-Salzedo and ChatGPT) Do there exist integers a, b for which we can prove that the sequence $\{a^n + b\}$ contains infinitely many primes?

023:21 (Renate Scheidler with Peter Zvengrowski and Julius Korbas)
$\mathcal{P}(K) = \{k = (k_{m-1}, \ldots, k_0) | 2^{m-1} \leq k < 2^m,\ k_i \geq 0,\ K = \sum_{i=0}^{m-1} k_i 2^i\}$, a set of binary partitions of K.

For example, for K=5: $5 = 5 \cdot 1 = 1 \cdot 2 + 3 \cdot 1 = 2 \cdot 2 + 1 \cdot 1 = 1 \cdot 4 + 1 \cdot 1$, so we have 4 binary partitions of 5.

Above is a well known object. Its count is given by entry A018819 in the On-Line Encyclopedia of Integer Sequences. What we are really interested in is the following:

$$C(K, J) = \sum_{k \in \mathcal{P}} \prod_{i=0}^{m-1} \binom{J}{k_i}$$

Again, for K=5, we get $C(5, J) = \binom{J}{5} + \binom{J}{1}\binom{J}{3} + \binom{J}{2}\binom{J}{1} + \binom{J}{1}\binom{J}{1}$.

Claim: Let $m \in \mathbf{N}$ and take $J < 2^m, K < 2^m, J + K > 2^m$. Then $C(K, J)$ is even. The only case left to do is J odd and K even.

Properties of $C(J, K)$:

$$C(2K, J) = \sum_{k=0}^{K} \binom{J}{2k} C(K - k, J),\ C(2K + 1, J) = \sum_{k=0}^{K} \binom{J}{2k + 1} C(K - k, J)$$

One can prove that this implies the following: that if J is even, then $C(2K + 1, J)$ is even, and if J is odd, then $C(2K + 1, J)$ is even if and only if $C(2K, J)$ is even.

023:22 (Daqing Wan) Define for a prime p, and positive integers d, k,

$$G_k(d, p) = \sum_{x \in \mathbf{F}_{p^k}} e^{\frac{2\pi i}{p} \mathrm{Tr}(x^d)} \in \mathbf{Z}[\zeta_p].$$

where the trace is from $\mathbf{F}_{p^k}$ to $\mathbf{F}_p$.

What is the degree of $G_k(d, p)$ for various values of k? Note that we always have $\deg G_k(d, p) | (p - 1)$.

We have from Gauss, if $k = 1$ and $d | (p - 1)$ then $\deg G_k(d, p) = d$. If $d | (p - 1)$ and d, k are relatively prime, $\deg G_k(d, p) = d$. If $d | (p - 1)$ but we don't know $\gcd(d, k)$, we can still conclude $\deg G_k(d, p) = \frac{d}{\gcd(d,k)}$.

A reference is

Daqing Wan, Exponential sums over finite fields, J. Sym. Sci. Complexity 2021.

023:23 (Simon Rubinstein-Salzedo) A historical question. Euler's Pentagonal Number Theorem says,

$$\prod_{n=1}^{\infty} (1 - x^n) = 1 + \sum_{n=1}^{\infty} (-1)^n \left[x^{\frac{3n^2 - n}{2}} + x^{\frac{3n^2 + n}{2}} \right] = 1 - x - x^2 + x^5 + x^7 - x^{12} - x^{!5} + x^{22} + x^{26} - \cdots$$

$\sigma(n) = \sigma(n - 1) + \sigma(n - 2) - \sigma(n - 5) - \sigma(n - 7) + \sigma(n - 12) + \sigma(n - 15) - \cdots$ with two caveats: $\sigma(k) = 0$ if $k < 0$, and if we encounter $\sigma(0)$, we treat it as n.

Euler noted that this implicitly contains a primality test, which was used to show 301 is composite.

What other kinds of interesting primality tests did mathematicians of that age notice?

Wilson's thm?

023:24 (Jordan Hardy et al.) What is the worst possible primality test? Each step along the way must be relevant to the problem of deciding primality. Some candidates:

1. Wilson's Theorem

2. For each x from 2 to $n-1$, for each y from 2 to $n-1$, compute xy and see whether it equals n.

3. Compute $\binom{n}{k}$ for each k from 1 to $n-1$ and see whether they are all divisible by n.