

Math 4513
Some unsolved problems in number theory

Here are more problems from *Old and New Unsolved Problems in Plane Geometry and Number Theory* by Victor Klee and Stan Wagon (on reserve in the mathematics library). I list the problems with the same numbers they are given in Klee and Wagon's book, so you can look them up there easily if you want to read more about them.

- 13.1** Euler proved in 1753 that it is impossible for the sum of two cubes to equal another cube; that is, there are no natural numbers x , y , and z such that $x^3 + y^3 = z^3$. He also conjectured that it is impossible for the sum of three fourth powers to equal another fourth power, for the sum of four fifth powers to equal another fifth power, and so on. However in recent years, with the aid of computers, this conjecture has been proved wrong for fourth powers and fifth powers: it has been found that

$$95800^4 + 217519^4 + 414560^4 = 422481^4$$

and

$$27^5 + 84^5 + 110^5 + 133^5 = 144^5.$$

What about sixth powers? Is it possible for the sum of five sixth powers to equal another sixth power?

- 14.** If a box has dimensions of x inches by y inches by z inches, then the length of the main diagonal will be $\sqrt{x^2 + y^2 + z^2}$. The faces of the box will also have diagonals of lengths $\sqrt{x^2 + y^2}$, $\sqrt{x^2 + z^2}$, and $\sqrt{y^2 + z^2}$. Is it possible for all of the numbers x , y , z , $\sqrt{x^2 + y^2 + z^2}$, $\sqrt{x^2 + y^2}$, $\sqrt{x^2 + z^2}$, and $\sqrt{y^2 + z^2}$ to be integers? In other words, does there exist a box with sides of integer length whose three face diagonals and main diagonal all have integer length as well?
- 15.** Suppose you are given a fraction $\frac{p}{q}$, and want to express it as a sum of fractions with numerator equal to 1 (called *unit fractions*). You can start by first finding the smallest number n_1 such that $\frac{1}{n_1} < \frac{p}{q}$, and then finding the smallest number n_2 such that $\frac{1}{n_1} + \frac{1}{n_2} < \frac{p}{q}$, and then finding the smallest number n_3 such that $\frac{1}{n_1} + \frac{1}{n_2} + \frac{1}{n_3} < \frac{p}{q}$, and so on. Fibonacci proved in the 1200's that no matter what fraction $\frac{p}{q}$ you start with, this process will always stop after a finite number of steps, at which point you will have

$$\frac{1}{n_1} + \frac{1}{n_2} + \frac{1}{n_3} + \cdots + \frac{1}{n_k} = \frac{p}{q}$$

for some numbers n_1, n_2, \dots, n_k .

What if you restrict all the denominators in the procedure to be odd? In other words, you start with a fraction $\frac{p}{q}$ where q is odd, and then find the smallest odd number n_1 such that $\frac{1}{n_1} < \frac{p}{q}$, and then the smallest odd number n_2 such that $\frac{1}{n_1} + \frac{1}{n_2} < \frac{p}{q}$, and so on. Will this procedure always stop after a finite number of steps? (Notice that this is not the same as asking whether it is possible to express $\frac{p}{q}$ as the sum of unit fractions with odd denominator. Instead, the question is whether *this particular method* for finding such a sum will always work.)

- 16.** Two unsolved problems about perfect numbers, which we mentioned in class: 1. Does there exist an odd perfect number? 2. Do there exist infinitely many even perfect numbers?
- 17.** Let $\pi(x)$ denote the number of primes less than or equal to x . It has been proved that $\pi(x)$ is well approximated by the value of the integral $\int_0^x \frac{1}{\log t} dt$, with the approximation getting better and better as x goes to infinity. The famous Riemann hypothesis asks a seemingly quite technical question about how good this approximation is. Namely, can one find a constant C such that for every real number x , the difference between $\pi(x)$ and $\int_0^x \frac{1}{\log t} dt$ is less than $C\sqrt{x} \log x$? Despite this question seeming to be rather arbitrary and unmotivated, it turns out that this it has deep ramifications in analysis and number theory. The Riemann hypothesis is probably the most famous unsolved problem in mathematics.

A nice book about the Riemann hypothesis, written at an accessible level, is *Prime Obsession* by John Derbyshire. (It's available to read online for free at <http://www.nap.edu/catalog/10532.html>.)

18. An algorithm for determining the prime factorization of a number N is said to be a *polynomial-time* algorithm if for every number N , the algorithm accomplishes its task without having to do more than Cd^k additions and multiplications, where d is the number of digits in the number N , and C and k are fixed constants (independent of N). Does such an algorithm exist? (If such an algorithm were to be found, it would defeat the encryption methods currently used to guarantee secure internet communication.)
19. Starting with any given number n , do the following: if n is even, divide it by 2; but if n is odd, multiply it by 3 and add 1. Now take the result and repeat the procedure. So far, every time people have tried this, they have always found that eventually they reach the number 1. (And people have tried it on trillions of numbers so far.) For example, if we start with 52, the procedure gives the following sequence: 52, 26, 13, 40, 20, 10, 5, 16, 8, 4, 2, 1.

Does there exist any number for which the procedure does not eventually lead to 1?

20. Suppose you are given a polynomial equation, with integer coefficients, in n unknown variables $x_1, x_2, x_3, \dots, x_n$. (For example, the equation $(x_1)^2 - 7x_2(x_3)^4 + 5 = 0$.) Is there an algorithm for deciding whether there exist rational numbers x_1, x_2, \dots, x_n which satisfy the equation? The desired algorithm must work for every possible polynomial in the sense that it will settle the question in a finite number of steps (the number of steps it takes is allowed to be arbitrarily large, though, depending on the polynomial.)

This problem encompasses problems 13.1 and 14 as special cases. It also includes as a special case the famous Fermat conjecture, recently solved by Andrew Wiles (with help from Richard Taylor).

21. No one has yet been able to determine any pattern in the digits of the decimal expansion of π , or to prove that there is no pattern. The question of what constitutes a pattern is open to interpretation, but one way to interpret the absence of a pattern in the digits would be to say that any combination of digits (such as 6574) occurs no more or less frequently in the decimal expansion of π than any other combination. No result along these lines is currently known. For example, it is not known whether 10% of the digits in the decimal expansion of π are sevens.
22. Is π/e a rational number? It is known that both π and e are irrational, but it is not known whether π is a rational multiple of e . Nor is it known whether $\pi + e$ or $\pi \cdot e$ are rational numbers.
23. Can one find an algorithm which computes the first n digits in the decimal expansion of $\sqrt{2}$ by doing an amount of work which is proportional to n ? Thus the amount of work such an algorithm would require to find, say, a million digits would be only ten times the amount of work required to find one hundred thousand digits. You can interpret "amount of work" to mean the total number of additions and multiplications required to find the digits.
24. Euler proved in the 1700's that the infinite series $1 + \frac{1}{2^2} + \frac{1}{3^2} + \dots$ adds up to $\frac{\pi^2}{6}$, and the infinite series $1 + \frac{1}{2^4} + \frac{1}{3^4} + \dots$ adds up to $\frac{\pi^4}{90}$. In fact, he found a method for finding similar formulas for any sum of the form $1 + \frac{1}{2^k} + \frac{1}{3^k} + \dots$, provided that k is an even number. No such simple formula has yet been found for the sum of the series $1 + \frac{1}{2^3} + \frac{1}{3^3} + \dots$; however it was proved not too long ago that the sum of this series is an irrational number. That raises the question: is the sum of the series $1 + \frac{1}{2^5} + \frac{1}{3^5} + \dots$ an irrational number?