Lecture 4: Number Theory

Twin prime conjecture

There are infinitely many prime twins $p, p+2$.

The largest known prime twins $(p, p+2)$ are given by $p = 2003663613 \cdot 2^{2195000} - 1$, a number with almost 60'000 digits. It has been found in 2007. There are analogue problems for **cousin primes** $p, p+4$, **sexy primes** $p, p+6$ or **Sophie Germaine** primes, where $p, 2p+1$ are prime.

Goldbach conjecture

Every even integer $n > 2$ is a sum of two primes.

The Goldbach conjecture has been verified numerically until $1.6 \cdot 10^{18}$. It is known that every sufficiently large odd number is the sum of 3 primes. One believes this "weak Goldbach conjecture" for 3 primes is true for every odd integer larger than 7.

Andrica conjecture

The prime gap estimate $\sqrt{p_{n+1}} - \sqrt{p_n} < 1$ holds.

For example $\sqrt{p_{1000}} - \sqrt{p_{999}} = \sqrt{7919} - \sqrt{7907} = 0.067...$. An other prime gap estimate conjectures is **Polignac's conjecture** claiming that there are infinitely many prime gaps for every even number n. It is stronger than the twin prime conjecture. It includes for example the claim that there are infinitely many cousin primes or sexy primes. **Legendre's conjecture** claims that there exists a prime between any two perfect squares. Between $16 = 4^2$ and $25 = 5^2$, there is the prime 23 for example.

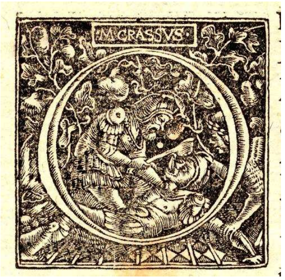
Odd perfect numbers

Probably the oldest problems in mathematics is the question

There is an odd perfect number.

A perfect number is equal to the sum of all its proper positive divisors. Like $6 = 1 + 2 + 3$. The search for perfect numbers is related to the search of large prime numbers. The largest prime number known today is $p = 2^{43112609} - 1$. It is called a Mersenne prime. Every even perfect number is of the form $2^{n-1}(2^n - 1)$ where $2^n - 1$ is prime.

Diophantine equations

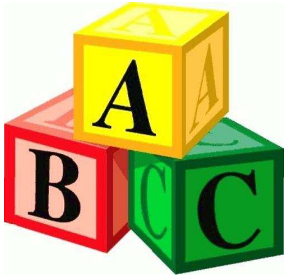


Many problems about Diophantine equations, equations with integer solutions are unsettled. Here is an example:

Solve $x^5 + y^5 + z^5 = w^5$ for $x, y, z, w \in N$.

Also $x^5 + y^5 = u^5 + v^5$ has no nontrivial solutions yet. Probabilistic considerations suggest that there are no solutions. The analogue equation $x^4 + y^4 + z^4 = w^4$ had been settled by Noam Elkies in 1988 who found $2682440^4 + 15365639^4 + 18796760^4 == 20615673^4$.

ABC Conjecture



The abc conjecture is:

If $a + b = c$, then $c \leq (\prod_{p|abc} p)^2$.

For example, for $10 + 22 = 32$, the prime factors of $abc = 7040$ are $2, 5, 11$ and indeed $32 \leq (2 * 5 * 11)^2 = 12100$. The abc-conjecture is open but implies Fermat's theorem for $n \geq 6$: assume $x^n + y^n = z^n$ with coprime x, y, z. Take $a = x^n, b = y^n, c = z^n$. The abc-conjecture gives $z^n \leq (\prod_{p|abc} p) \leq (abc)^2 < z^6$ establishing Fermat for $n \geq 6$. The cases $n = 3, 4, 5$ to Fermat have been known for a long time.