Lecture 4: Number Theory

Number theory studies the structure of integers like prime numbers and solutions to Diophantine equations. Gauss called it the "Queen of Mathematics". Here are a few theorems and open problems.

An integer larger than 1 which is divisible by 1 and itself only is called a **prime number**. The number $2^{57885161}-1$ is the largest known prime number. It has 17425170 digits. **Euclid** proved that there are infinitely many primes: [Proof. Assume there are only finitely many primes $p_1 < p_2 < \ldots < p_n$. Then $n = p_1 p_2 \cdots p_n + 1$ is not divisible by any $p_1, \ldots, p_n$. Therefore, it is a prime or divisible by a prime larger than p_n.] Primes become more sparse as larger as they get. An important result is the **prime number theorem** which states that the n'th prime number has approximately the size $n\log(n)$. For example the $n = 10^{12}$'th prime is $p(n) = 29996224275833$ and $n\log(n) = 27631021115928.545...$ and $p(n)/(n\log(n)) = 1.0856...$ Many questions about prime numbers are unsettled: Here are four problems: the third uses the notation $(\Delta a)_n = |a_{n+1} - a_n|$ to get the absolute difference. For example: $\Delta^2(1,4,9,16,25...) = \Delta(3,5,7,9,11,...) = (2,2,2,2,...)$. Progress on prime gaps has been done recently: a paper which just appears showed $p_{n+1} - p_n$ is smaller than 100'000'000 eventually (Yitang Zhang April 2013) $p_{n+1} - p_n$ is smaller than 600 eventually (Maynard). The largest known gap is 1476 which occurs after $p = 1425172824437699411$.

Landau	there are infinitely many primes of the form n^2+1.
Twin prime	there are infinitely many primes p such that $p+2$ is prime.
Goldbach	every even integer $n > 2$ is a sum of two primes.
Gilbreath	If p_n enumerates the primes, then $(\Delta^k p)_1 = 1$ for all $k > 0$.
Andrica	The prime gap estimate $\sqrt{p_{n+1}} - \sqrt{p_n} < 1$ holds for all n.

If the sum of the proper divisors of a n is equal to n, then n is called a **perfect number**. For example, 6 is perfect as its proper divisors $1, 2, 3$ sum up to 6. All currently known perfect numbers are even. The question whether odd perfect numbers exist is probably the oldest open problem in mathematics and not settled. Perfect numbers were familiar to Pythagoras and his followers already. Calendar coincidences like that we have 6 work days and the moon needs "perfect" 28 days to circle the earth could have helped to promote the "mystery" of perfect number. **Euclid of Alexandria** (300-275 BC) was the first to realize that if $2^p - 1$ is prime then $k = 2^{p-1}(2^p - 1)$ is a perfect number: [Proof: let $\sigma(n)$ be the sum of **all** factors of n, including n. Now $\sigma(2^n-1)2^{n-1}) = \sigma(2^n-1)\sigma(2^{n-1}) = 2^n(2^n-1) = 2\cdot 2^n(2^n-1)$ shows $\sigma(k) = 2k$ and verifies that k is perfect.] Around 100 AD, **Nicomachus of Gerasa** (60-120) classified in his work "Introduction to Arithmetic" numbers on the concept of perfect numbers and lists four perfect numbers. Only much later it became clear that Euclid got all the even perfect numbers: Euler showed that all even perfect numbers are of the form $(2^n-1)2^{n-1}$, where $2^n - 1$ is prime. The factor $2^n - 1$ is called a **Mersenne prime**. [Proof: Assume $N = 2^k m$ is perfect where m is odd and $k > 0$. Then $2^{k+1}m = 2N = \sigma(N) = (2^{k+1}-1)\sigma(m)$. This gives $\sigma(m) = 2^{k+1}m/(2^{k+1}-1) = m(1 + 1/(2^{k+1}-1)) = m + m/(2^{k+1}-1)$. Because $\sigma(m)$ and m are integers, also $m/(2^{k+1}-1)$ is an integer. It must also be a factor of m. The only way that $\sigma(m)$ can be the sum of only two of its factors is that m is prime and so $2^{k+1} - 1 = m$.] The first 39 **known Mersenne primes** are of the form $2^n - 1$ with n = 2, 3, 5, 7, 13, 17, 19, 31, 61, 89, 107, 127, 521, 607, 1279, 2203, 2281, 3217, 4253, 4423, 9689, 9941, 11213, 19937, 21701, 23209, 44497, 86243, 110503, 132049, 216091, 756839, 859433, 1257787, 1398269, 2976221, 3021377, 6972593, 13466917. There are 8 more known from which one does not know the rank

of the corresponding Mersenne prime: n = 20996011, 24036583, 25964951, 30402457, 32582657, 37156667, 42643801,43112609,57885161. The last was found in January 2013 only. It is unknown whether there are infinitely many.

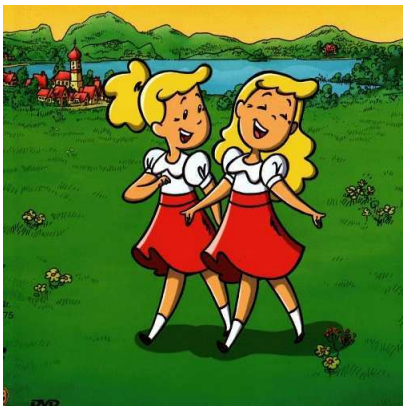
A polynomial equations for which all coefficients and variables are integers is called a **Diophantine equation**. The first Diophantine equation studied already by Babilonians is $x^2 + y^2 = z^2$. A solution (x, y, z) of this equation in positive integers is called a **Pythagorean triple**. For example, $(3, 4, 5)$ is a Pythagorean triple. Since 1600 BC, it is known that all solutions to this equation are of the form $(x, y, z) = (2st, s^2 - t^2, s^2 + t^2)$ or $(x, y, z) = (s^2 - t^2, 2st, s^2 + t^2)$, where s, t are different integers. [Proof. Either x or y has to be even because if both are odd, then the sum $x^2 + y^2$ is even but not divisible by 4 but the right hand side is either odd or divisible by 4. Move the even one, say x^2 to the left and write $x^2 = z^2 - y^2 = (z - y)(z + y)$, then the right hand side contains a factor 4 and is of the form $4s^2t^2$. Therefore $2s^2 = z - y, 2t^2 = z + y$. Solving for z, y gives $z = s^2 + t^2, y = s^2 - t^2$, $x = 2st$.]
Analyzing Diophantine equations can be difficult. Only 10 years ago, one has established that the **Fermat equation** $x^n + y^n = z^n$ has no solutions with $xyz \neq 0$ if $n > 2$. Here are some **open problems** for Diophantine equations. Are there nontrivial solutions to the following Diophantine equations?

$x^6 + y^6 + z^6 + u^6 + v^6 = w^6$	$x, y, z, u, v, w > 0$
$x^5 + y^5 + z^5 = w^5$	$x, y, z, w > 0$
$x^k + y^k = n!z^k$	$k \geq 2, n > 1$
$x^a + y^b = z^c, a, b, c > 2$	$\gcd(a, b, c) = 1$

The last equation is called **Super Fermat**. A Texan banker **Andrew Beals** once sponsored a prize of 100′000 dollars for a proof or counter example to the statement: "If $x^p + y^q = z^r$ with $p, q, r > 2$, then $\gcd(x, y, z) > 1$."
Given a prime like 7 and a number n we can add or subtract multiples of 7 from n to get a number in $\{0, 1, 2, 3, 4, 5, 6\}$. We write for example $19 = 12 \bmod 7$ because 12 and 19 both leave the rest 5 when dividing by 7. Or $5 * 6 = 2 \bmod 7$ because 30 leaves the rest 2 when dividing by 7. The most important theorem in elementary number theory is **Fermat's little theorem** which tells that if a is an integer and p is prime then $a^p - a$ is divisible by p. For example $2^7 - 2 = 126$ is divisible by 7. [Proof: use induction. For $a = 0$ it is clear. The binomial expansion shows that $(a + 1)^p - a^p - 1$ is divisible by p. This means $(a + 1)^p - (a + 1) = (a^p - a) + mp$ for some m. By induction, $a^p - a$ is divisible by p and so $(a + 1)^p - (a + 1)$.] An other beautiful theorem is **Wilson's theorem** which allows to characterize primes: It tells that $(n - 1)! + 1$ is divisible by n if and only if n is a prime number. For example, for $n = 5$, we verify that $4! + 1 = 25$ is divisible by 5. [Proof: assume n is prime. There are then exactly two numbers $1, -1$ for which $x^2 - 1$ is divisible by n. The other numbers in $1, \dots, n - 1$ can be paired as (a, b) with $ab = 1$. Rearranging the product shows $(n - 1)! = -1$ modulo n. Conversely, if n is not prime, then $n = km$ with $k, m < n$ and $(n - 1)! = ...km$ is divisible by $n = km$.]
The solution to systems of linear equations like $x = 3 \pmod 5, x = 2 \pmod 7$ is given by the **Chinese remainder theorem**. To solve it, continue adding 5 to 3 until we reach a number which leaves rest 2 to 7: on the list $3, 8, 13, 18, 23, 28, 33, 38$, the number 23 is the solution. Since 5 and 7 have no common divisor, the system of linear equations has a solution.
For a given n, how do we solve $x^2 - yn = 1$ for the unknowns y, x? A solution produces a square root x of 1 modulo n. For prime n, only $x = 1, x = -1$ are the solutions. For composite $n = pq$, more solutions $x = r \cdot s$ where $r^2 = -1 \bmod p$ and $s^2 = -1 \bmod q$ appear. Finding x is equivalent to factor n, because the greatest common divisor of $x^2 - 1$ and n is a factor of n. **Factoring is difficult** if the numbers are large. It assures that **encryption algorithms** work and that bank accounts and communications stay safe. Number theory, once the least applied discipline of mathematics has become one of the most applied one in mathematics.

Lecture 4: Number Theory

Twin prime conjecture



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

The first twin prime is $(3,5)$. The largest known prime twins $(p, p+2)$ have been found in 2011. It is $3756801695685 \cdot 2^{666669} \pm 1$. There are analogue problems for **cousin primes** $p, p+4$, **sexy primes** $p, p+6$ or **Germaine** primes, where $p, 2p+1$ are prime. Progress: we know that prime gaps of order 600 or smaller appear infinitely often. (Work of Zhang,Maynard,Tao)

Goldbach conjecture

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

The Goldbach conjecture has been verified numerically until $4 \cdot 10^{18}$. 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.

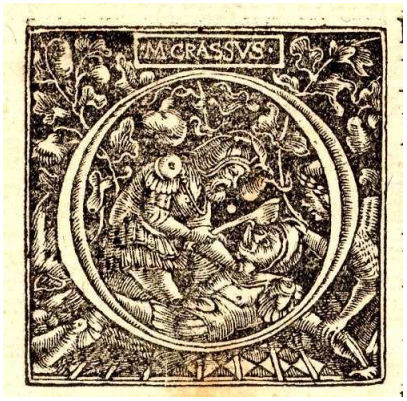
Odd perfect numbers

Probably the oldest open problem 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

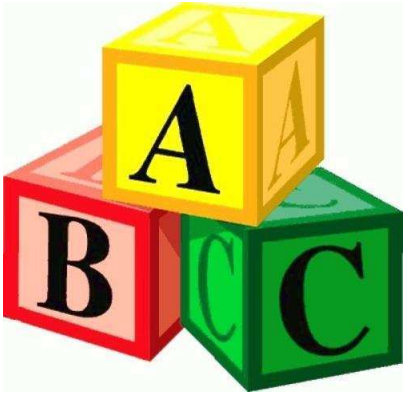


Many problems about Diophantine equations, equations with integer solutions are unsettled. Here is an example:

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 the identity $2682440^4 + 15365639^4 + 18796760^4 = 20615673^4$.

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. In August 2012, there were rumors of an attack by Shinichi Mochizuki. During 2013 various mathematicians have tried to understand and verify the theory.