TEACHING MATHEMATICS WITH A HISTORICAL PERSPECTIVE

OLIVER KNILL

E-320: Teaching Math with a Historical Perspective **O. Knill, 2010-2021**

Lecture 4: Number Theory

3.1. Number theory studies the structure of integers, in particular its building blocks, the prime numbers and solutions of equations involving integers. Gauss called it the "Queen of Mathematics". We look here at a few theorems as well as some open problems in this field.

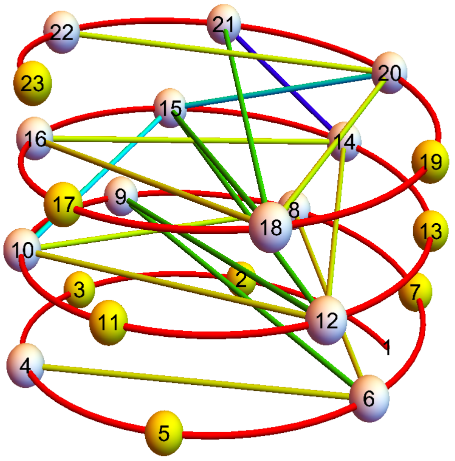


FIGURE 1. The **Eratosthenes sieve** is visualized by aligning the number line on a spiral, then knocking out multiples of 2, then all multiples of 3 etc. What remains after this sieving are the prime numbers.

3.2. An integer larger than 1 which is divisible only by 1 and itself is called a **prime number**. The number $2^{77232917}-1$ is the so far largest known prime number. It has 23249425 digits. **Euclid** proved that there are infinitely many primes: The proof is by contradiction: assume there are only finitely many primes $p_1 < p_2 < \cdots < p_n$. Then $n = p_1 p_2 \cdots p_n + 1$ is not divisible by any $p_1, \dots, p_n$. Therefore, it is a prime or divisible by a prime larger than p_n.

3.3. Primes become less frequent 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 $n = 10^{13}$'th prime is $p(n) = 133472665317708923$ and $p(n)/(n \log(n)) = 1.07323\dots$. Many questions about prime numbers are unsettled. Some of these questions are listed below.

3.4. If the sum of the proper divisors of an integer n is equal to n, then n is called a **perfect number**. The smallest perfect number is 6. Indeed, the proper divisors $1, 2, 3$ of 6 sum up to 6. The next one is $28 = 1+2+4+7+14$. All currently known perfect numbers are even. The question whether **odd perfect numbers** exist is probably the oldest open problem in mathematics and is not settled. Perfect numbers were familiar to Pythagoras and his followers already. Calendar coincidences like that we have 6 work days and that the moon needs "perfect" 28 days to circle the earth might have helped to increase the fascination with perfect number.

3.5. **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. The proof is as follows: let $\sigma(n)$ be the sum of **all** factors of n, including n. It has the general property $\sigma(nm) = \sigma(n)\sigma(m)$. Now $\sigma(2^p - 1)2^{p-1}) = \sigma(2^p - 1)\sigma(2^{p-1}) = 2^p(2^p - 1) = 2 \cdot 2^{p-1}(2^p - 1)$ shows $\sigma(k) = 2k$ and verifies that k is perfect.

3.6. Around 100 AD, **Nicomachus of Gerasa** (60-120) introduced in his work "Introduction to Arithmetic" of perfect numbers and lists four perfect numbers. He also defines **superabundant numbers**, for which the sum of proper factors is larger than n and **deficient numbers** for which it is smaller than n. Also the Greek philosopher **Theon of Smyrna** (70-135) distinguished around 130 AD between **perfect**, **abundant** and **deficient numbers**. Only much later it became clear that Euclid already 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**. The proof is as follows: 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 $2^{k+1} - 1 = m$.

3.7. The first 39 **known Mersenne primes** are of the form $2^n - 1$ $n = 2$, 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 12 more known. But for those, the rank of the corresponding Mersenne prime is not known as there might be some between. The list as of now is n = 20996011, 24036583, 25964951, 30402457, 32582657, 37156667, 42643801,43112609,57885161, 74207281,77232917,82589933. The last was found in January 2018. It is unknown whether there are infinitely many.

3.8. A polynomial equations for which all coefficients and variables are integers is called a **Diophantine equation**. The first Diophantine equation studied already by the Babylonians 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. Here is the 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 $z = s^2 + t^2, y = s^2 - t^2$, $x = 2st$.

3.9. Analyzing Diophantine equations can be difficult. Only 25 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 the **Super Fermat** or **Beals equation**. 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 $\gcd(x, y, z) > 1$."

3.10. 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 $(a+1)^p - (a+1)$.]

3.11. 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 $(n-1)!$ is divisible by $n = km$.]

3.12. 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. or 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.

3.13. **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.

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 on prime gaps has been done recently: $p_{n+1} - p_n$ is smaller than 600 eventually. The largest known gap is $p_{n+1} - p_n = 1550$ appears at $p_n = 18361375334787046697$. Bertrand's postulate assures that $p_{n+1} - p_n < p_n$.

Goldbach

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

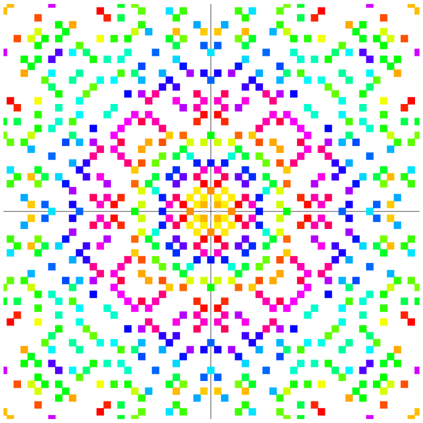
The Goldbach conjecture has been verified numerically until $4 \cdot 10^{18}$. It is known that every odd number larger than 5 is the sum of 3 primes (Helfgott 2013). This was called the "weak Goldbach conjecture".

Andrica

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 gapdf 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.

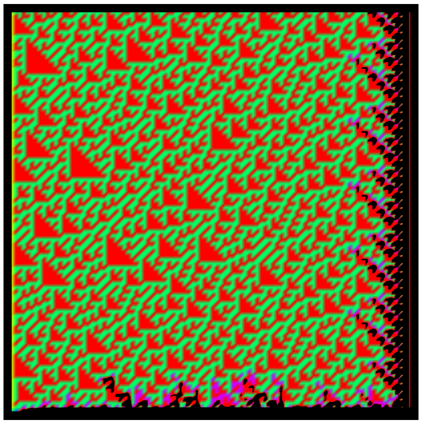
Landau



There are infinitely many primes of the form $p = n^2 + 1$.

This conjecture is one of the most astonishing ones. It restates the question whether there are infinitely many Gaussian primes $a + i$ in the complex plane. A complex integer $p = a + ib$ is prime if and only if $a^2 + b^2$ is prime or $ab = 0$ and $|a|$ is a rational prime of the form $4k+1$. Hardy and Littlewood conjectured that the ratio of primes of the form $p = n^2 + 1$ with $p \leq N$ and primes of the form $p = 4k + 3$ with $p \leq N$ converges to a constant 1.3728.... Hardy and Littlewood statement is much stronger than the Landau problem.

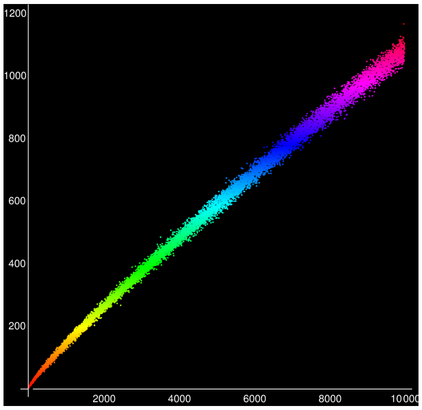
Gilbreath



If p_n is the n'th prime, then $(\Delta^k p)_1 = 1$ for all $k > 0$

This uses the notation $(\Delta a)_n = |a_{n+1} - a_n|$ for the absolute difference. For example: $\Delta^2(1, 4, 9, 16, 25, \dots) = \Delta(3, 5, 7, 9, 11, \dots) = (2, 2, 2, 2, \dots)$.

Legendre



Between successive squares there is always a prime.

In formulas, for every n there exists a prime between n^2 and $(n + 1)^2$. The numerical computation of the number of primes between n^2 and $(n + 1)^2$ shows even an increasing comet.

Odd perfect numbers

Probably the oldest open problem in mathematics is the claim:

There is an odd perfect number.

A **perfect number** has the property that it is equal to the sum of all its proper positive divisors. Like $28 = 1 + 2 + 4 + 7 + 14$. The search for perfect numbers is related to the search of large prime numbers. The largest prime number known today is $p = 2^{77232917} - 1$. It is called a Mersenne prime. Euler proved that 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, meaning equations with integer solutions are unsettled. Here is an example:

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

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 $x^4 + y^4 + z^4 = w^4$ has been settled by Noam Elkies in 1988 who found the identity $2682440^4 + 15365639^4 + 18796760^4 = 20615673^4$.

ABC Conjecture

One special version of the ABC conjecture is

If $a + b = c, \gcd(a, b, c) = 1$, then $c \leq (\prod_{p|abc} p)^2$.

For example, for $10 + 21 = 31$, the prime factors of $abc = 6510$ are $2, 3, 5, 7, 31$ and indeed $31 \leq (2 * 3 * 5 * 7 * 31)^2$. The ABC-conjecture 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 $n = 3, 4, 5$ have been known to Fermat already. A claimed proof of the ABC conjecture by Shinichi Mochizuki is still highly controversial.

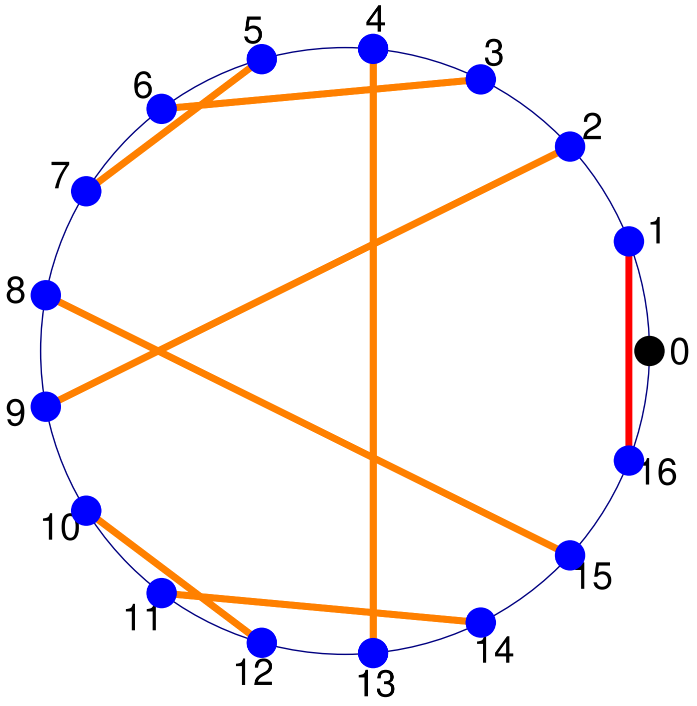
Work problems

3.14. 1) Modify Euclid's proof to show that For every n, there exist consecutive primes which differ by at least n. Do that by verifying that all integers $n! + 2, \dots, n! + n$ are composite.

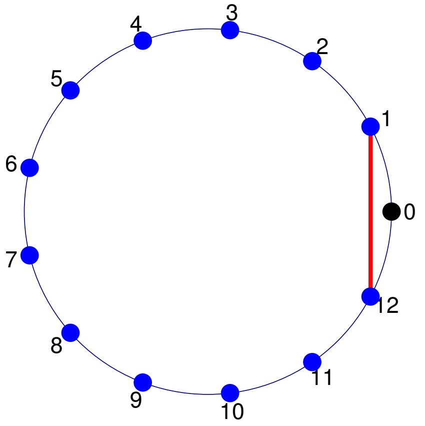
3.15. 2) Wilson's theorem assures:

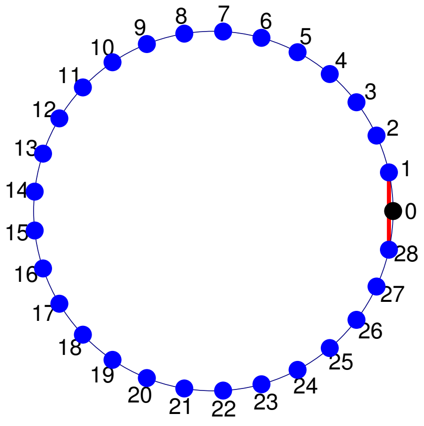
n is a prime if and only if $(n-1)! + 1$ is divisible by n.

3.16. The proof of the theorem has two directions:
If n is a prime, then the equation $xy = 1 \bmod n$ with different x, y has exactly one pair of solution. For $x^2 = 1$, there is only the solution $1, -1$.



Wilson's theorem in the case $p = 17$. We find all pairs which multiply to 1 Like $2*9 = 18, 3*6 = 18, 4*13 = 52, 8*15 = 120$ which all leave rest 1 when dividing by 17. Only the numbers 1 and -1 do not pair. The product $(n-1)!$ multiplies all the numbers together and gives $(-1) \cdot 1(2*9)(3*6)(4*13)(5*7)(8*15)(10*12)(11*14) = -1$.
Verify the proof either in the case $p = 13$ or $p = 29$.





3.17. Lets look at the reverse If $n = pq$ is not a prime and larger than 4, then $(n-1)!$ is divisible by n because it is a multiple of p and q.

Verify this in the concrete case of $n = 15$. Why is

$$15! = 1 * 2 * 3 * 4 * 5 * 6 * 7 * 8 * 9 * 10 * 11 * 12 * 13 * 14$$

a multiple of 15?

Fermat's little theorem

3.18. 3) Fermat's little theorem is:

$a^p - a$ is divisible by p for all prime p.

3.19. The **binomial formula** is

$$(a+b)^n = a^n + \left(\begin{array}{c} n \\ 1 \end{array}\right) a^{n-1}b + \left(\begin{array}{c} n \\ 2 \end{array}\right) a^{n-2}b^2 + ... + \left(\begin{array}{c} n \\ n-1 \end{array}\right) ab^{n-1} + b^n$$

In the case $b = 1$ it means

$$(a+1)^n = a^n + \left(\begin{array}{c} n \\ 1 \end{array}\right) a^{n-1} + \left(\begin{array}{c} n \\ 2 \end{array}\right) a^{n-2} + ... + \left(\begin{array}{c} n \\ n-1 \end{array}\right) a + 1$$

3.20. a) Check that Fermat's theorem is true for $a = 0$ and $a = 1$.

b) Verify that the induction step from a to $a+1$ is equivalent to show that

$$(a+1)^p - a^p - 1$$

is divisible by p if p is a prime.

c) Verify that $(a+1)^p - a^p - 1$ is divisible by p if all all binomial coefficients

$$\left(\begin{array}{c} p \\ m \end{array}\right) = \frac{p!}{m!(p-m)!} = \frac{p \cdot (p-1) ... \cdot (p-m+1)}{m \cdot (m-1) \cdot ... \cdot 1}$$

are divisible by p.

d) Verify that $\frac{p \cdot (p-1) ... \cdot (p-m+1)}{m \cdot (m-1) \cdot ... \cdot 1}$ divisible by p if p is prime.

This is illustrated by the **Pascal triangle**. For rows which are prime, the interior entries are all divisible by the row number. For example, for $p = 5$, the middle entries $5, 10, 10, 5$ are all divisible by 5.

1

1 1

1 2 1

1 3 3 1

1 4 6 4 1

1 5 10 10 5 1

1 6 15 20 15 6 1

1 7 21 35 35 21 7 1

1 8 28 56 70 56 28 8 1

1 9 36 84 126 126 84 36 9 1