Primes in the Classroom and Beyond:
A First Look at Prime Numbers

Markus Brodmann
Institute of Mathematics
University of Zürich
Switzerland
brodmann@math.uzh.ch

THE SIGNIFICANCE OF NUMBERS

By „Number“ we always mean a non-negative integer, say n = 0,1,2,3,... .

The whole Building of Mathematics is footed on numbers, or – equivalently – on the notion of „Counting.“

„God created the integers, all the rest is human work“. (Leopold Kronecker, 1823 – 1891, German Mathematician).

„Who did say, that 3 and 3 makes 6?“ (Grand-Son Alec, 2015 -).

INTRODUCTORY EPISODE

Recently, when I brought back home Grand-Son Loris (2013 -) by tram after an excursion, he did ask me, whether I could speak with him about Mathematics. I suggested to speak about prime numbers and did ask him, whether he knew what these numbers are. With some help, he got it right: *„These are numbers greater than one, which can only be divided by 1 and themselves.“* We spelled out a few first examples: 2,3,5,7,11,13,... . I did ask him, whether he knew what an even number is. Surely, he said: *„It is the twofold of another number, like 2,4,6,8,10,12,..“.* Next I suggested to take any even number greater than 2 and to write as the sum of two prime numbers (which may be equal). So, we got 4=2+2, 6=3+3, 8=3+5,10=3+7=5+5, 12=5+7, ... I did ask: *„Do you think it works always?“* and Loris answered: *„I do not know.“* I replied: *„No-one knows indeed up today, whether it always works. People have tried by help of computers very, very large even numbers, and it did work for those. But no-one yet knows whether it works always.“* Suddenly, the young Lady sitting in front of us turned around and said:

„Thank you very much! This was a very interesting conversation you had, and I learned a lot from it!“

PRIMES: THE ATOMS OF MATHS

A *Prime (Number)* is a number greater 1 divisible only by 1 and by itself. First examples: 2,3,5,7,11,13,17,19 ...

THE FUNDAMENTAL THEOREM OF ARITHMETICS (EUCLID, ~ 350-300 B.C.): *Each number greater 1 is either a prime or a product of primes – uniquely determined up to order.*

Examples: 12=2x2x3, 98=2x7x7, 159=3x53, 1'024= 2x2x2x2x2x2x2x2x2x2, 75'900=2x2x3x5x5x11x23.

FACIT: *Each number greater 1 is uniquiely composed by primes. So, the primes play the role of atoms for the positive numbers. As the whole building of Mathematics is footed on numbers, we can say:* ***„The Primes are the atoms, Mathematics is built of.“***

THE SET OF PRIMES IS INFINITE

INFINETENESS THEOREM (EUCLID): *There are infinitely many prime numbers.*

Proof: Assume that there are only finitely many primes, say k of them. As 2 and 3 are primes, we must have k > 1. We now may enumerate all primes and write them down as p_1, p_2,..., p_k. Next, we form the number n = p_1 x p_2 x ... x p_k + 1.
Assume first, that n is a prime. Observe that n is greater than all the prime numbers p_1, p_2,..., p_k. This is a contradiction! So, n cannot be a prime, and hence must be a product of some of the the prime numbers p_1, p_2,..., p_k. So, one of the numbers p_1, p_2,..., p_k must divide n = p_1 x p_2 x ... x p_k + 1. So it divides 1. As all p_1, p_2,..., p_k are > 1, this is impossible.

qed.

IN SEARCH OF PRIMES

Let n be a number > 1. *Testing Primality* of n means to decide, whether n is a prime or not. Genuinely, this means, one has to test, whether or not n is divisible by a number q different from 1 and n. In view of the Fundamental Theorem of Arithmetics the choice of numbers q one has to try is fairly restricted, namely:

PROPOSITION: *If n is not a prime, it is divisible by a prime p whose square is at most n.*

A prime p, whose square is at most n, is called a *Test Prime* for n. Hence: *n is prime if and only if it is not divisible by one of its test primes.* Here comes a list of some test primes:

$8<n<25$ => test primes: 2,3.
$24<n<49$ => test primes: 2,3,5.
$48<n<121$ => test primes: 2,3,5,7.

Consequently one often looks for efficient methods that allow to find „at once“ all primes which are less or equal to some given n.

THE SIEVE OF ERATOSTHENES

The Greek Mathematician Eratosthenes of Cyrene (3rd Century B.C.) suggested the following algorithm to determine all primes less or equal to a given number n – called the *Sieve Method:*

1) Write down the complete list 2,3,4,...,,n of all consecutive numbers between 2 and n.
2) First, choose p=2 and mark in your list all proper multiples of p – hence the numbers 2p,3p,4p,... .
3)Then, look at the smallest unmarked number in the list, say q.
4) If q exists, proceed with q as you previously did with p.
5) If q does not exist, you stop. Then the unmarked numbers in your list are precisely the prime numbers less or equal to n.

COMMENT: (A) The multiples 2p,3p,4p,... can be found without multiplying, just by counting. So, unlike to the genuine „primality testing by division“, no calculations are needed.
(B) Today, many variants of Sieve Methods are in use, not only for the search of prime numbers.

AN EXAMPLE FOR THE SIEVE METHOD

	2	3	*4	5	*6	7	*8	*9	*10
11	*12	13	*14	*15	*16	17	*18	19	*20
*21	*22	23	*24	*25	*26	*27	*28	29	*30
31	*32	*33	*34	*35	*36	37	*38	*39	*40
41	*42	43	*44	*45	*46	47	*48	*49	*50
*51	*52	53	*54	*55	*56	*57	*58	59	*60
61	*62	*63	*64	*65	*66	67	*68	*69	*70
71	*72	73	*74	*75	*76	*77	*78	79	*80
*81	*82	83	*84	*85	*86	*87	*88	89	*90
*91	*92	*93	*94	*95	*96	97	*98	*99	*100

OBSERVATIONS: (A) The non-marked numbers are the primes beween 2 and 100: 2,3,5,7,11,13,17,19,23,29,31,37, 41,43,47,53,59,61,67,71,73,79,83,89,97.

(B) In our range, we have the following *Pairs of Twin Primes:* (3,5),(5,7),(11,13),(17,19),(29,31),(41,43),(59,61),(71,73).

FERMAT'S THEOREM

The French Mathematician Pierre de Fermat (1601-1665) proved the following result:

PRIME NUMBER THEOREM OF FERMAT: *Let p be a prime and let q be a number with q < p. Then, p divides q^(p-1) - 1.*

EXAMPLE: Let p=7 and q=2. Then q^(p-1) - 1 = 2^6 – 1 = 64 -1 = 63 = 7x9. So, p=7 indeed divides 63 = q^(p-1) – 1.

REMARK AND EXAMPLE: (A) We choose n > 2 and call n a *Pseudo-Prime* if it divides 2^(n-1) – 1. We know by the previous theorem, that primes are pseudo-primes. An example of a pseudo-prime which is not a prime is n = 341 = 11 x 31. But indeed: ***Most pseudo-primes are primes.*** For example, among the 170 pseudo-primes < 1000 only 2 are not primes, and among the 78'743 pseudo-primes < 1'000'000 only 245 are not primes. (B) So, testing, whether n divides 2^(n-1)-1 is a primality test, failing only with small probability. We call it *Fermat Primality Test.*

LARGE PRIMES

We know, that there are infinitely many primes. This means that there are arbitrarily large primes. In search of those, one is confronted with the problem of primality testing for large numbers n. Just dividing by test primes „soon“ comes to an end if n gets larger and larger. So, a high speed computer able to perform 200'000'000'000 = 2x(10^11) arithmetic operations per second, needs less than one second to test by mere division, whether a number of 10 decimal digits is prime. If n has 20 digits, testing by mere division may need already as much as 2 hours. This hints, that other test methods must be used for large n.

Indeed: ***There are very powerful primality testing algorithms based on advanced mathematical methods other than mere division.*** The fastest of them are of „probabilisic nature“, this means, they leave a small probability of failure. Fermat Prime Testing is a simple example. Probabilistic tests are often combined with non-probabilistic ones.

AN EXAMPLE OF LARGE PRIME

In December 2018, in the framework of th *„Great Internet Mersenne Prime Search“* project (GIMPS) the American Patrick Laroche found the following prime:

2^(82'589'933) – 1, a number with 24'862'048 decimal digits.

This number is of the form 2^n -1 and hence a *Mersenne Prime*, named after the French Priest and Mathematician Marin Mersenne (1588-1648), who first studied such primes. Laroches Number is the 51-th known Mersenne Prime.

For numbers of the form 2^n -1 there is a particularly efficient primality test, the so called *Lucas-Lehmer Test*. It relies on ideas of the French Mathematician Francois Edourd Anatole Lucas (1842 – 1891) and the American Mathematician Derrick Lehmer (1905 – 1991). Moreover it uses the fact, that numbers of the form 2^n – 1 are written as 1111....1 in the dual number system.

Highly doted awards are set out for those, who find large primes. For the first prime with at least 100'000'000 decimal digits a price of USD 150'000 is offered.

WHY LARGE PRIMES?

We just did hear, that substantial sums are paid to those, who find large primes. So, there must be an interest in lage primes, or even in primes at all, which goes beyond pure intellectual curiosity. Primes are indeed one of the „basic raw materials“ used in Coding, Cryptography and Digital Communication. Primes, together with advanced methods of Higher Number Theory are invisibly omnipresent wherever digital data exchange takes place. For example, large primes are of basic importance for the so called *Public Key Codes,* used in civic and military information networks worldwide.

Leopold Kronecker once said: ***„I am happy, that Number Theory finds no application. So, it cannot be misused for warfare.“***

Today we must say: ***„Number Theory shows best, that the gap between Fundamental Science and its Applications is constantly thrinking.“***

ASYMPTOTIC DISTRIBUTION OF PRIMES

To understand the *distribution of primes* among all integers is likewise the most challenging question of Mathematics at all. *„Asymptotically“* this distribution can be described. But, what does this mean?

Let pi(n) denote the number of primes which are less or equal to n. Then, the *Mean Prime Density* in the range 1,2,3,...,n is given by the fraction rho(n)=pi(n)/n. Some values are

pi(1'000)=168	rho(1'000)=0.168
pi(10'000)=1'229	rho(10'000)=0.123
pi(100'000)=9'592	rho(100'000)=0.096
pi(1'000'000)=78'498	rho(1'000'000)=0.078

QUESTION: *How does* rho(n) *behave, if n becomes larger and larger – hence tends to infinity?*

THE PRIME NUMBER THEOREM

ANSWER: The following Theorem answers our question:

PRIME NUMBER THEOREM: *If* n *tends to infinity, then* rho(n)ln(n) *tends to* 1. *(* ln(n) *denotes the natural logarithm of* n.*)*

COROLLARY: *If n becomes larger and larger, rho(n) is better and better approximated by 1/ln(n). Consequently, the number of primes less or equal to n is better and better approximated by the fraction n/ln(n).*

REMARK: The Prime Number Theorem was conjectured to hold by the German Mathematician Carl Friedrich Gauss (1777-1855) in 1793 (!) and – independently – by the French Mathematician Adrien-Marie Legendre (1752-1833) in 1798.
The first proofs were given independently in 1896 by the French Mathematician Jasques Hadamard (1865-1963) and the Belgian Mathematician Charles-Jean Gustave Nicolas Baron de la Vallée Poussin (1860-1962) (which latter even improved on it later).

PRIMES IN THE CLASSROOM: TESTING,

DIVISION BY TEST PRIMES: After the notions of *Prime Number* and *Decomposition in Primes* according to the *Fundamental Theorem* have been introduced and sporadic examples were computed, the notion of *Test Prime* – and *Primality Testing* (by means of division by such) could be explained. It could be a nice group work, to produce a table, showing all primes between 2 and 200.

THE SIEVE OF ERATOSTHENES: An equally nice group work would be to use the *Sieve Method of Eratosthenes* to produce a table as mentioned above.

THE FERMAT PRIMALITY TEST AND QUASI-PRIMES: For a higher class, these notions could be introduced. All n < 12 could be treated. With students familiar with modular arithmetic, testing, whether n divides 2^(n-1) -1 can be replaced by checking whether 2^(n-1) = 1 mod(n). This is a gain of effectivity.

... EUCLID'S INFINITENESS THEOREM,

DISCUSSION OF THE INFINITENESS QUESTION: Once primes have been introduced, it could be a very inspiring question to ask whether there are finitely many primes or not, and make pupils discuss on it. Hint: ***Never miss an opportunity to discuss about infinity in your Maths Lessons***.

EUCLID'S INFINITENESS THEOREM: Resuming the previous discussion, formulate this theorem and add a few words on Euclid himself. This gives you a chance, to speak about his book *„Elements“*: the first Work which proclaimed the *„Axiomatic Approach“* to Mathematics. Hint: ***Never miss to speak about the historic back-ground in your Maths Lessons.***

PROOF OF EUCLID'S THEOREM: In a higher class, give a proof ot this theorem. Explain why a proof is needed. Hint: ***Never miss to speak about proofs in your Maths Lessons and to perform them, if possible.***

... OPEN QUESTIONS, ...

GOLDBACH'S CONJECTURE: This conjecture is due to the German Mathematician Christian Goldbach (1690-1764). We met it already in the Introductory Episode. It says: *Each even number > 3 can be written as a sum of two primes.* Make pupils have their tries with it. Explain to them, what a conjecture is. Tell them, that by computer it has been shown that all even numbers between 4 and 1'000'000'000 are a sum of two primes. But, indeed, it is not known, whether this always holds. Hint: ***Never miss to speak about conjectures in your Maths Lections and to try on them by a few examples, if possible.***

LEGENDRE'S CONJECTURE: This conjecture says: *If* n *is an integer* > 0, *then, there is a prime number* p *in between* n^2 *and* (n+1)^2. We already mentioned Legendre in our remark on the Prime Number Theorem. You may proceed similarly as in the case of Goldbach's Conjecture. By computer calculations it has been shown, that for all positive n < 2'000'000'000 there is prime in between n^2 and (n+1)^2.

... EVEN MORE OF THEM, AND ...

PRIME TWINS: A *Pair of Twin Primes* is a pair (p,q) consisting of two primes p and q, such that q-p = 2. We met such pairs already in our example to the Sieve of Eratosthenes. Many pairs of twin primes have been found, also by means of computers. The „largest pair of twin primes“ actually known, consists of the two primes [2'996'863'034'895 x 2^(2'290'000)] +/-1, which both have 388'342 decimals. Again, let pupils look for some pairs of twin primes beyond the range 2,3,...,100, and keep in mind what was said in relation with Goldbach's Conjecture.

AN EXERCISE IN PROVING (For those familiar with modular Arithmetics): Let p be a prime > 2. Use 1+1=2 to show that 2^(p-1) = 1 mod(p). Use this to prove the Prime Number Theorem of Fermat in the case q = 2. Keep in mind that „Fermat Primality Testing“ relies on this theorem. This shows: Modular Arithmetic is of great practical impact. Hint: ***Never miss to point out in your Maths Lessons by concrete examples the practical impact of mathematical Methods.***

... AND PRIME STORIES

FACTS, EPISODES AND STORIES ON PRIME NUMBERS:
Indeed, in most internet sources, it is easy to find a lot of things about prime numbers, for example in „Wikipedia“. Obviously, the mathematical level of these contributions varies a lot. But quite a number of them can be understood only on the base of Precalculus Mathematics and without methods from Abstract Algebra.
To do the corresponding research of adequate results and to comopse them to „*Prime Stories*“ (hence: „Science Stories on Prime Numbers“) could be a very inspiring and motivating task for a group of Secondary School students. It would help them to learn a lot of things, which go far beyond Mathematics: *Cooperation*, *Sharing Interest and Knowledge*, *Formulate and Present Ideas* in an adequate and coherent way, and last, not least: *Enthusiasm*. Hint: ***Never forget that Intellectual Curiosity and Enthusiasm are driving forces of any Scientific Activity.***

TURNING OUR EYES UPWARDS

We started our *„Excursion to Prime Numbers“* with thoughts of the German Mathematician Leopold Kronecker and my Grand-Son Alec – thoughts, which express, that the marvellous and miracolous Realm of Numbers is the Work of an Infinitely Wise Creator. Let us never forget this, when doing Mathematics, on what level it ever may be.

So, let us conclude with the words of two young Mathematicians:
„O God, we thank you for that Marvellous Creature of Mathematics“ (Ines, former PhD Student in Zurich).

„If I do Mathematics, I see how beautiful God is thinking“ (Terai, Japanese Mathematician).