Prime numbers

Frans Oort
Department of Mathematics
University of Utrecht

Talk at
Dept. of Math., National Taiwan University (NTUmath)
Institute of Mathematics, Academia Sinica (IoMAS)
17-XII-2012

$\cdots$ *prime numbers "grow like weeds among the natural numbers, seeming to obey no other law than that of chance, and nobody can predict where the next one will sprout."* Don Zagier

Abstract. In my talk I will pose several questions about prime numbers. We will see that on the one hand some of them allow an answer with a proof of just a few lines, on the other hand, some of them lead to deep questions and conjectures not yet understood. This seems to represent a general pattern in mathematics: your curiosity leads to a study of "easy" questions related with quite deep structures. I will give examples, suggestions and references for further study. This elementary talk was meant for freshman students; it is not an introduction to number theory, but it can be considered as an introduction: "what is mathematics about, and how can you enjoy the fascination of questions and insights?"

Introduction

In this talk we study *prime numbers*. Especially we are interested in the question "how many prime numbers are there, and where are they located"? We will make such questions more precise. For notations and definitions see § 2.

The essential message of this talk on an elementary level: mathematicians are curious; we like to state problems, find structures and enjoy marvelous new insights. Below we ask several questions, and we will see that for some of them there is an easy an obvious answer, but for others, equally innocent looking, we are completely at loss what the answer should be, what kind of methods should be developed in order to understand possible approaches: fascinating open problems.

(0.1) Definition. For every $x \in \mathbb{R}$ we define $\pi(x)$ as the number of prime numbers at most equal to x:

$$\pi(x) = \#\left(\{p \mid p \text{ is a prime number, } p \leq x\}\right), \quad \pi : \mathbb{R} \to \mathbb{Z};$$

here $\#(V)$ denotes the number of elements of the set V.

This is a "step function": for $0 < x < 2$ we have $\pi(x) = 0$; then the function jumps to $\pi(y) = 1$ for $2 \leq y < 3$, and so on; in this way this function climbs this staircase with steps of height one.

Drawing the graph of $\pi(x)$ for $x < 100$ (i.e. on a small scale) we see the steps:
a weird and seemingly irregular shape;

however seeing the graph of $\pi(x)$ for $x < 50,000$
it seems as if this concerns a smooth function
(which we know it isn't).

This gives the suggestion that we should be able to say something about the global behavior of $\pi(x)$ (always follow daring ideas); indeed Gauss had this idea long ago; he made notes (never published) in his table of logarithms:

"Im Jahr 1792 oder 1793 $\cdots$ Primzahlen unter $a(=\infty)\frac{a}{\ln(a)}$",

as he communicated in 1849 to his friend Encke, see [12]. This idea was also conjectured by Legendre (1797/1798), see [27].

This idea/conjecture/result, the *prime number theorem* (abbreviated as PNT) was proved by Chebyshev, Hadamard and De la Vallée-Poussin (results published in the period starting 1848, final complete proof in 1896). This is an astonishing (and also deep) result: *without knowing all prime numbers, without being able to compute them all, still we can say something* whether somewhere (above a given number, or how many approximately on a given interval) they can be found (without explicitly computing any of them);

we see a "regular" behavior of an irregular function.

In § 7 we cite this result (but we are not able to give a proof on an elementary and simple level); however we will also see that some weaker statements are very easy to prove, and these can be used to obtain amazing results (we will see examples).

(0.2) What is the structure underlying a question? Below I start by asking questions. Please try for every question to decide whether you understand the question, and whether an answer would be obvious and easy or difficult. We will see that some of them have a quick and simple answer; however some others are difficult, and hide unsolved problems where some of the great mathematicians in the past in vain tried to reveal secrets hidden in these gems of mathematical exploration. All of a sudden we are confronted with our lack of knowledge (and so often I had and still have that feeling in mathematical research). It makes this field a rich source for inspiration and challenges.

This is characteristic for mathematical research: a question triggers your curiosity. Sometimes you see (or somebody else tells you) that this "of course" is simple. However the next question, equally easy in its formulation, escapes a solution, and the more you contemplate, the more you feel that you basically have no understanding of the true structure involved.

We will see that (sometimes) computing examples gives you insight, but (as we have experienced) it may give completely wrong suggestions and ideas; see § 9. Also we see that abstract methods can give astonishing insight and results.

We should try to find the structure underlying a question. The mathematician Yuri Manin recently said in his interview "Good proofs are proofs that make us wiser":

" *I see the process of mathematical creation as a kind of recognizing a preexisting pattern*";

see [29]. And I agree with this belief: what we are trying to discover exists already, we "just" have to find the right language, the key to the secret.

Therefore, in everything below try to find the underlying pattern, the basic idea of the questions discussed.

Understanding notions and questions in "elementary number theory" may lead to deep theory, may reveal beautiful structures in algebra, geometry and analysis, and usually quite other disciplines in mathematics are necessary to proceed, and to solve "easy" questions.

(0.3) How can you use this paper?

- Start reading questions posed in § 1. Try to understand these, and look for an answer (and for the hidden structures). Which of these have an easy solution? Keep such questions in mind.

- This paper contains only a very small part of this interesting field. If you want to learn more, google any of the following words, and you will find much more information: prime number, prime number theorem, Fermat primes, Mersenne primes, Sophie Germain primes, twin primes, prime number races, Chebotarev density theorem, heuristic argument, Riemann hypothesis, ABC conjecture, 3x+1 problem, odd perfect number, scientific calculator, factoring calculator, prime constellations, ... For example you google <prime number> and you obtain the site

  `http://en.wikipedia.org/wiki/Prime_number` .
  Or <prime number theorem> and the site

  `http://en.wikipedia.org/wiki/Prime-number-theorem`
  surfaces.

- Many problems about prime number were born out of completely different questions in geometry, number theory, or other fields of mathematics; e.g. see §§ 5 - 6. Be alert in doing mathematics for such "cross-fertilizations".

- Section 8 is strange. Some arguments used are definitely wrong (you could try to prove with those "methods" that "there are infinitely many even prime numbers" ..... is that a correct statement?);

  "the *chance* that a given positive integer N is prime is equal to ... "
  is nonsense: a given number is a prime number or it is not.

  However the essence of "heuristics" can give you a feeling, an intuition what kind of answers certain questions should have. After you have understood Section 8 try this method out on problems you want to consider.

- In § 11 you will find four exercises. After you have seen many difficult questions and conjectures you might have fun in solving some easy problems yourself.

- Try to make computations connected with some of the problems posed. You can try to see whether you obtain some insight. Sometimes it will lead you to correct expectations. Sometimes you will get nowhere. In this way you feel how mathematicians are thinking and trying to find new structures and answers. Andrew Wiles in his BBC documentary (1996) said:

Perhaps I could best describe my experience of doing mathematics in terms of entering a dark mansion. One goes into the first room and it's dark, completely dark, one stumbles around bumping into the furniture and then gradually you learn where each piece of furniture is, and finally after six months or so you find the light switch, you turn it on suddenly it's all illuminated, you can see exactly where you were.

`http://www.cs.wichita.edu/~chang/fermat.html`

- In Section 10 we mention some **open problems**, still unsolved, even great mathematicians even have no idea where to start, what is the theory to be developed? which new directions in mathematics do we have to explore? For young mathematicians a nice idea that still so many things are waiting for you.

- **A small warning.** It is nice to make many computations. And indeed, we are in good company (in his younger years Gauss spend free time in computing prime numbers, thus getting a feeling for "how many there are"). However, computations can "go on forever". Know where to proceed making computations, and know where to stop and start thinking. (Example: you can try to write even numbers as sums of primes: $4 = 2+2, 6 = 3+3, 8 = 3+5, 10 = 3+7, \cdots$, and do you want to go on "forever "?)

- For me, here are the big surprises in this field:

  "simple" questions can be very hard; as long as we have no description of underlying theory, most problems are out of reach of exact methods;

  however, we can give exact approximations (e.g. for the number of primes in a given interval), without computing any of the relevant cases, and these methods are usually easy.

What to read. The books [8], [18], [26] are books of fiction, very interesting to read. Also [32] is fiction; this beautiful book tries to describe the (mathematical) childhood of Sophie Germain; very nice to read. See
`http://kasmana.people.cofc.edu/MATHFICT/default.html`
for many more suggestions.

To obtain an idea about elementary number theory see [19] and [4]. For basic knowledge about algebra there are many books; we mention: [25].

(0.4) Some sites you can use for computing,
a scientific calculator, e.g.:
`http://web2.0calc.com/#`
factoring numbers, e.g.:
`http://eng.numberempire.com/factoringcalculator.php`
finding the Nth prime (for $N < 10^{12}$):
`http://primes.utm.edu/nthprime/`
finding Collatz trees:
`http://www.nitrxgen.net/collatz.php`
finding a sequence of integers, once you know how it starts
http://oeis.org/

1 Some questions

(1.1) Question 1. *Is the set of all prime number finite or infinite?*
[Where do you start? Just computing and making a (finite) list of prime numbers, would that help? Or should we rather start thinking?]

For an answer, see § 3.

We study whether consecutive prime numbers are far apart, or close together.

We say N is the length of a *gap in the sequence of prime numbers* if there are two consecutive prime numbers $p < q$ with $N = q - p$.

(1.2) Questions 2. *Is the length of gaps in the sequence of prime numbers bounded or unbounded?*
[What do you try? Think, or make examples?]

See (4.1) and Section 7.

We study whether (many) primes can be as close together as possible

We say we have a pair of *twin primes* if there are prime numbers $p < q$ with $q - p = 2$.

We say we have a 3-sequence of prime numbers (not a standard terminology ...) if we have $p < q < r$ with $q - p = 2$ and $r - q = 2$.

(1.3) Question 3.

(2) *Is the set of twin primes finite or infinite?*

(3) *What is the set of* 3*-sequences of prime numbers?*

[Making (many) examples would that help? How do we obtain any insight?]

See (4.4).

(1.4) Question 4. Consider the set of numbers

$$F_0 = 3, \quad F_1 = 5, \quad F_2 = 17, \quad F_3 = 257, \quad F_4 = 65537, \cdots, \quad F_i = 2^{2^i} + 1.$$

Are all numbers in this sequence prime?
If not, is the number of prime numbers in this sequence finite or infinite?
[Note that even for small i the number F_i is large; how can you make computations? Or do you want to think first? What else are you going to do, in order to understand these numbers?]

See § 5 and (10.6).

(1.5) Question 5. We write

$$p_1 = 2 < p_2 = 3 < \cdots < p_i < p_{i+1} < \cdots$$

for the ascending sequence of all prime numbers.
Is there a formula which for every choice i allows you to compute the i-th prime number p_i?
[Did we formulate the question in the right way? Does this make sense?]

See (4.5); see § 7.

(1.6) Question 6. We see:

$$4 = 2 + 2, \quad 6 = 3 + 3, \quad 8 = 3 + 5, \quad \cdots, \quad 36 = 5 + 31 = 7 + 29, \quad \cdots (?)$$

Can every even number $N = 2n \geq 4$ be written as sum of two prime numbers?
[Where do you start? Just start computing until you find a counter example? Is there another approach possible?]

See: *the Goldbach Conjecture* (10.2). See (10.3).

(1.6)(bis). **Another question.**

$$2 = 5 - 3, \ 4 = 47 - 43, \ 6 = 13 - 7, \quad \cdots, 18 = 47 - 29, \cdots$$

Can every even number as the **difference** *of two prime numbers?*

See (10.5)

(1.7) Question 7. *Does there exist a prime number with* 2013 *decimal digits?*
[How to start? Just write down any number between 10^{2012} and 10^{2013} and try whether that choice gives a prime number? Is the chance big or small by just an "ad random choice" to construct such a prime number? What else could you try?]

See (4.9). See (7.4), (7.8).

(1.8) Question 8. Try to find $A, a, D, d \in \mathbb{Z}_{\geq 2}$ with

$$A^a + 1 = D^d.$$

"I.e. can pure powers differ by one?" We see $2^3 + 1 = 8 + 1 = 9 = 3^2$ is one solution. *Are there any other solutions?*
[Write pure powers $4, 8, 9, 16, 25, 27, 32, 36, \cdots$ and try to see whether anywhere the difference 1 appears. Is this a good method? What else should we try? Does this question have an easy, or a difficult, or no answer? A "pure power" is an integer of the form A^a with $A, a \in \mathbb{Z}_{\geq 2}$.]

See (4.10).

(1.9) Question 9. We say a prime number p is a *Sophie Germain prime number* if also $q := 2p + 1$ is a prime number. *Is the number of Sophie Germain prime numbers finite or infinite?*

See (10.8)

(1.10) Question 10. Define the function

$$C : \mathbb{Z}_{>0} \longrightarrow \mathbb{Z}_{>0}$$

by:

$$C(2m) := m, \qquad C(2m + 1) = 3(2m + 1) + 1$$

(i.e., for *even* n choose $C(n) = n/2$, for *odd* n choose $C(n) = 3n + 1$). Start with an arbitrary $a_1 \in \mathbb{Z}_{>0}$ and produce the sequence $\{a_1, \cdots, a_{i+1} := C(a_i), \ldots\}$. *Does the number* 1 *appear in such a sequence for every choice of* a_1*?*

See (10.9)

We can pose many more of such questions. However these 10 already give enough material to think about, and to develop a feeling for this kind of mathematics. Try to decide which problem has an easy answer, which one follows from general theory, and perhaps you get stuck at some of them (that happens to every mathematician contemplating about nice questions). (In your mathematical life, do not get discouraged by problems you cannot solve: it is part of the beauty of our profession. Once I was working on a hard problem, got stuck for long time, thought I had a solution, found the mistake in my arguments, and was not unhappy with the idea probably I would never see a solution; however, as a bonus after 7 years I solved the problem.)

Below I will discuss answers, and the final outcome (for this moment) is listed in (10.11).

2 Some definitions

(2.1) We write $\mathbb{Z} = \{\cdots, -2, -1, 0, 1, 2, 3, \cdots\}$ for the set of integers.
For $a, b \in \mathbb{Z}$ we say a is a *divisor* of $n = b$ if there exists $d \in \mathbb{Z}$ with $da = b$.
Notation: $a \mid b$.

A number $p \in \mathbb{Z}_{>1}$ is called a *prime number* in case 1 and p are the only positive divisors of p. In other terms: if every i with $1 < i < p$ is not a divisor of p.
Examples: $2, 3, 5, 7, 11, 13, 17, 19, \cdots, 61, 67, 71, \cdots, 613, 617, 619, \cdots$ etc.
Remark. In modern terminology the integer 1 is not a prime number (although Euler called the number 1 also a prime number).

(2.2) The largest common divisor. Suppose given $m, n \in \mathbb{Z}$ with $m \neq 0$. Consider the set of common divisors:

$$\{d \in \mathbb{Z} \mid 1 \leq d,\ d \mid m,\ d \mid n\}.$$

Because $m \neq 0$ this set is finite. As $1 \mid m$ en $1 \mid n$ this set is not empty. The largest number in this set we write as $\gcd(m, n)$, called *the greatest common divisor*.
Remark. We can show: for $\gcd(m, m) = d$ there exist $x, y \in \mathbb{Z}$ with $xm + yn = d$.
Remark. We can show that $\gcd(m, m) = d$ is the smallest non-negative integer in the set $\{xm + yn \mid x, y \in \mathbb{Z}\}$. See Section § 12.

If $\gcd(m, n) = 1$ we say "m and n are relatively prime".

(2.3) The logarithm. Logarithms are defined and computed with a base number. For $a \in \mathbb{R}_{>1}$ we write:

$$^a\log(x) = y \quad \Longleftrightarrow \quad x = a^y.$$

!! We write

$$\boxed{\log(x) :=^e \log(x)}\ ;\ \text{here } e \text{ the Euler constant.}$$

Probably you were/are accustomed to write $\ln(x) =^e \log(x)$ and $\log(x) =^{10} \log(x)$. However mathematicians (and also in this paper) we write $\log(x) =^e \log(x)$.

3 A proof by Euclid

(3.1) Theorem (Euclid). *There are infinitely many prime numbers.*
Proof. We know there exists at least one prime number (e.g. $p = 37$). Suppose given a finite set of prime numbers $\{P_1, \cdots, P_m\}$ with $m > 0$ (i.e. this set is non-empty); using this set we construct a prime number P not appearing in this list. If we can show this it proves that the set of all prime numbers in non-finite.
Construction. Consider

$$M = P_1 \times \cdots \times P_m + 1.$$

Note that $M > 1$. Choose P as the smallest divisor of M with $P > 1$. We show P is a prime number; indeed, any divisor $d \mid P$ with $1 < d \leq P$ is also a divisor of M; hence $d = P$: this shows P is a prime number.
Claim. *The prime number P is not contained in the set $\{P_1, \cdots, P_m\}$.*
Assume the contrary, assume $P = P_i$ for some $1 \leq i \leq m$. Then

$$BP + 1 = BP_i + 1 = M = AP \text{ with } B := P_1 \times \cdots \times P_{i-1} \times P_{i+1} \times \cdots \times P_m;$$

hence

$$(A - B)P = 1.$$

This shows $B - A = \pm 1$, and $P = \pm 1$; this is a contradiction with $P > 1$. This shows P is a prime number with $P \notin \{P_1, \cdots, P_m\}$. QED

Remark / advice. Just remember this proof. Isn't it remarkable that you can say something about an infinite set in a finite set of arguments? That you say there are infinitely many prime numbers without constructing them all. Here lies the strength of mathematical reasoning. If someone is truly interested why we should do mathematics, this is the first example of our beautiful profession you can present.

See (5.1) for another proof there exist infinitely many prime numbers.

(3.2) A variant. For a set of prime numbers $\{P_1, \cdots, P_m\}$ and $M = P_1 \times \cdots \times P_m + 1$ as above we can define $P_{m+1}, \cdots, P_r$, all prime numbers appearing in the factorization of M (use (12.2)), continue inductively with $\{P_1, \cdots, P_m, \cdots, P_r\}$ and finish the proof of (3.1) in this way.

Remark. We did not claim the number M considered in the proof is a prime number. E.g. starting with $p = P_1 = 2$ we construct $P_2 = 3$, and $P_3 = 2 \times 3 + 1 = 7$, and $P_4 = 2 \times 3 \times 7 + 1 = 43$, however $2 \times 3 \times 7 \times 43 + 1 = 1807 = 13 \times 139$. In fact, the number of primes of the form $N! + 1$ (for all N up to a given bound) should be relatively small, see [5], 4.6.

We did not show we can construct all prime numbers this way. Indeed I expect:

starting with any non-empty set of prime numbers and proceeding inductively as in (3.2), *the infinite set of prime number we eventually obtain this way is not equal to the set of all prime numbers*; can we prove this?

4 Some answers

(4.1) Gaps in the sequence of prime numbers. Here is an answer for (1.2).
We show: for every $N \in \mathbb{Z}_{\geq 3}$ there exists a pair of consecutive prime numbers (p_i, p_{i+1}) with

$$p_{i+1} - p_i \geq N$$

(i.e. the length of gaps in the sequence of all prime numbers is unbounded.)
We give a *simple* proof. Consider

$$M := N! = 2 \times \cdots \times (N-1) \times N.$$

Let p_i be the largest prime number with $p_i \leq M + 1$. Note:

$$M+2, \quad M+3, \quad \cdots, \quad M+N-1, \quad M+N \quad \text{are not prime.}$$

Indeed any j with $2 \leq j \leq N$ is a divisor of M. Hence the next prime number p_{i+1} has the property $p_{i+1} \geq M + N + 1$. From

$$p_{i+1} \geq M + N + 1 \text{ and } p_i \leq M + 1 \text{ we deduce } p_{i+1} - p_i \leq M + N + 1 - M - 1 = N.$$

QED

Although the proof is really short, in many cases it does not give the lowest case of constructing large gaps.
Example. For $1 \leq j \leq 33$ the number $1327 + j$ is not a prime number, and we see a gap of (at least) length 34; note that

$$34! \quad \approx \quad 2.95 \times 10^{38}$$

and hence the gap of length 34 starting at 1327 comes much earlier than the one constructed by the proof.

Example. For $p_i = 31397$ we have $p_{i+1} - p_i = 72$, while

$$72! \quad \approx \quad 6.12 \times 10^{103}.$$

See `http://en.wikipedia.org/wiki/Prime-gaps`
Also see [13], page 10. Also see the last page of this paper.

Remark. Here is another proof of the fact that the length of gaps in the sequence of prime numbers is unbounded.

Suppose every gap has length at most N. This would imply that in any interval of length N there is at least one prime number. This would imply $\pi(x) > x/N$ for every $x \in \mathbb{R}$. However we will see in § 7 that $\pi(x) < Bx/(\log(x))$ for some constant B (and a proof, e.g. for the case $B = 3$ is easy). We derive a contradiction for every x with $B/(\log(x)) > N$.

We can wonder which gaps do appear. Does every positive integer appear as the length of a gap? (A simple question, and we will see the answer is partly very easy.)
Remark. *There are no prime numbers p and q with $q - p = 7$.*
Proof. In case p and q are even their difference is even, hence not equal to 7. For $p = 2$ the number $q := 2 + 7 = 9$ is not a prime number. QED

See (11.3) for odd length. See (10.5) for even length.

(4.2) If we wold know enough about the length of gaps, perhaps we could decide upon:

Conjecture (Legendre, 1798). *For every $n \in \mathbb{Z}_{>0}$ there exists a prime number p such that*

$$n^2 < p < (n+1)^2. \qquad (?)$$

See [27]; see `http://arxiv.org/pdf/1201.1787v3.pdf`

(4.3) Twin primes. Do we know an answer to (1.3)(2)? Many pairs of twin primes are known. We *expect* there are infinitely many, see (10.4). Very large pairs are known, e.g. see the first few lines of [5]. Heuristics are very convincing. These give asymptotic estimates that fit with great precision every time we can actually compute the exact number of twin primes up to a certain bound. Hence we strongly believe there are infinitely many. However the question is still unsolved, and I think we basically do not understand which structure lies behind this question.

There are two ways to generalize the concept of twin primes. Either we can study pairs of primes further apart (and this wil be done in two ways: either consecutive primes, or the possible differences between arbitrary primes). Or we can study longer chains of given length between consecutive primes. In all these cases we obtain interesting questions, a lot of partial results, and interesting expectations, none of which have been settled.

(4.4) 3-sequences of prime numbers. An answer to (1.3)(3).
We show: $\{3, 5, 7\}$ is the only 3-sequence of prime numbers.
Proof. Suppose $\{p, p+2, p+4\}$ is a 3-sequence of prime numbers. We can write $p = 3i$, or $p = 3i+1$ or $p = 3i+2$.

In case $p = 3i$ we obtain the sequence $\{3, 5, 7\}$.

In case $p = 3i+1$ we see that $p+2$ is divisible by 3, hence equal to 3, and we would have $p = 1$: however that is not a prime number.

In case $p = 3i+2$ we see that $p+4$ is divisible by 3, hence we would have $p = -1$, also a contradiction. QED
In short: in any sequence of integers $\{n, n+2, n+4\}$ exactly one of these is divisible by 3.

We see the notion of a "3-sequence of prime numbers" is not a very interesting one; we dismiss this. There is a much better notion.
Definition. A set of prime numbers $\{p,\ q,\ r\}$ is called a *prime triplet* if
either $q = p+2$ and $r = q+4$, e.g. $\{5, 7, 11\}, \cdots, \{41, 43, 47\}, \cdots, \{857, 859, 863\}, \cdots$
or $q = p+4$ and $r = q+2$, e.g. $\{7, 11, 13\}, \cdots, \{613, 617, 619\}, \cdots$.
You can easily produce many prime triplets.
See `http://en.wikipedia.org/wiki/Prime-triplet`
Expectation. *The number of prime triplets is infinite.*(?)
This question has not been answered. See
`http://en.wikipedia.org/wiki/Prime_triplet`
`http://primes.utm.edu/glossary/xpage/PrimeTriple.html`

We can go much further: *prime quadruples*: a string of consecutive primes

$$\{p = p_i, p_{i+1}, p_{i+2}, p_{i+3} = p+8\}.$$

We expect there are infinitely many prime quadruples. Prime constellations of length four (prime quadruples) fit the single pattern (p, p+2, p+6, p+8). (Examples: (5,7,11,13), (11,13,17,19).)

If the length is five or six we have the patterns: (p, p+2, p+6, p+8, p+12), (p, p+4, p+6, p+10, p+12), and (p, p+4, p+6, p+10, p+12, p+16). It is expected that there are infinitely many of each admissible prime constellation. None of these questions have been solved.
http://primes.utm.edu/glossary/xpage/Quadruple.html
http://primes.utm.edu/glossary/xpage/PrimeConstellation.html

(4.5) Does there exist a formula which for every i computes the i-th prime number p_i?
Unfortunately the formulation of the question is not precise enough. What do we expect from such a formula? We show such a formula exists in case we already know all prime numbers

(4.6) Example. There exists a number $\alpha \in \mathbb{R}$ with the property:

$$p_n = \lfloor 10^{1+\cdots+n} \cdot \alpha \rfloor - 10^n \cdot \lfloor 10^{1+\cdots+(n-1)} \cdot \alpha \rfloor;$$

notation: for $\beta \in \mathbb{R}$ we write $\lfloor \beta \rfloor$ for the largest integer smaller or equal β:

$$\lfloor \beta \rfloor = m \in \mathbb{Z} \quad \Longleftrightarrow \quad m \leq \beta < m+1.$$

Indeed, such an $\alpha \in \mathbb{R}$ exists. Write

$$\alpha = 0.2030050007000110000 13 \cdots = \sum_{n=1}^{n=\infty} p_n \times 10^{f(n)}$$

where $f(n)$ is equal to $1+2+\cdots+n$-(the number of decimal digits of p_n). We use that $p_n < 10^n$ (which can be easily seen). It is clear that the formula above indeed gives p_i for every i.

Is this useful? In order to know α you need precise information about all prime numbers:

$$\text{knowing } p_1, \cdots, p_n \text{ precisely, you can compute } p_n;$$

not very astonishing: it is easy to find a formula giving all prime number if you know already all prime numbers.....
See `http://primes.utm.edu/glossary/xpage/FormulasForPrimes.html`
In [47] the question is raised: what is the difference between a formula and a good formula? Also see [20].

(4.7) Example. Euler showed that substituting $T = i$ into T^2+T+41 for every $0 \leq i \leq 39$ a prime number appears. Does there exist a polynomial "which gives all prime numbers"?

Matiyasevich showed in 1971 the existence of a polynomial such that every positive value is a prime number. Later an explicit example of a polynomial in 26 variables of degree 25 with such a property was constructed, see [21].

Does this help? Yes, from an abstract point of view. This theorem was of great importance in logic. Can we compute easily prime numbers in this way? It turns out to be difficult to compute a single prime number in this way. And, I do not see how to use this method to decide whether a give number is prime.
See `http://primes.utm.edu/glossary/xpage/MatijasevicPoly.html`

(4.8) Modern technology and the internet allow us to determine every prime number wanted under 10^{12}, see `http://primes.utm.edu/nthprime/`
For example $p_{100} = 541$, $p_{500} = 3,571$, $p_{10,000} = 104,729$, $p_{1,000,000} = 15,485,863$, $p_{100,000,000} = 2,038,074,743$, $p_{100,000,000,000} = 2,760,727,302,517, \cdots$.
Is this interesting? On that site you can also compute $\pi(x)$ for every $x < 3{\cdot}10^{13}$.

On the following site you can check whether a given integer (at most 16 digits) is a prime number
`http://primes.utm.edu/curios/includes/primetest.php`

(4.9) Does there exist a prime number with exactly 2013 digits? Is there a table we can consult to find such a prime number? No, certainly not: the number of prime numbers up to 10^{2012} is about 10^{874}; we think the number of elementary particles in the universe to be around 10^{78}. Hence no such table can be made.

So, how can we answer the question? We have given the function $\pi : \mathbb{Z} \to \mathbb{Z}$ counting the number of primes, see (0.1). In § 7 we show $\pi(10^{2012}) < \pi(10^{2013})$ (simple considerations, no deep theorems used). Conclusion: indeed there exists a prime number with exactly 2013 digits (however we do not give a single precise example, we just show existence). See (7.4), (7.8).

(4.10) The Catalan conjecture,

$$A^a + 1 = D^d, \quad A, D \in \mathbb{Z}_{>1}, \quad a, d \in \mathbb{Z}_{\geq 2}.$$

Eugène Charles Catalan formulated in 1844 the conjecture that $8+1 = 9$ is the only solution to this equation with $A, D \in \mathbb{Z}_{>1}$ and $a, d \in \mathbb{Z}_{\geq 2}$. Indeed, computing through small values of the variables this sounds reasonable. Then may computations were done, but no counterexamples were found. Tijdeman showed in 1976 that there is an upper bound for the solutions. However as the bound is large, something like $\exp(\exp(\exp(\exp(730))))$ (where the notation $\exp(a) := e^a$ is used), a solution using computers was still impossible; this bound was improved upon, but still reality was far out of reach of direct computation.
See http://en.wikipedia.org/wiki/Tijdeman

We thought this was one of those problems too difficult for us. However it became clear that existing algebraic methods were sufficient to solve the problem: indeed $8 + 1 = 9$ is the only solution, and the Catalan conjecture was proved as Preda Mihăilescu showed in 2004; see [31]. No big computers, just pure thought and "easy" theory. To some of us this came as a surprise.
See `http://en.wikipedia.org/wiki/Catalan\%27s-conjecture`.

5 Fermat (prime) numbers

Consider the numbers

$$F_i := 2^{2^i} + 1, \quad i \in \mathbb{Z}_{\geq 0}.$$

These are called *Fermat numbers*. Pierre de Fermat wondered whether all of these numbers are prime. We see that

$$F_0 = 3, \quad F_1 = 5, \quad F_2 = 17, \quad F_3 = 257, \quad F_4 = 65537$$

indeed are prime numbers. However Euler proved in 1732:

$$F_5 = 2^{32} + 1 = 4294967297 = 641 \times 6700417;$$

hence F_5 is not a prime number. Also see (13.7).

A lot of research and a huge amount of computational search has been done to find new Fermat prime numbers
See `http://en.wikipedia.org/wiki/Fermat-number`

At present we do not know a single Fermat prime number with $i > 4$. For many values of i we know F_i is not a prime number; see:
`http://www.prothsearch.net/fermat.html`

(5.1) Exercise. Show: (1) For every $i > 0$ we have $F_i = F_0 \times \cdots \times F_{i-1} + 2$.
(2) For every $0 < i < j$ we have $\gcd(F_i, F_j) = 1$.
(3) Write P_i for the smallest prime divisor of F_i. Show that $\{P_i \mid i \in \mathbb{Z}_{>0}\}$ is an infinite set. Conclude: the set of prime numbers is infinite (and we obtain another proof of (3.1)).

(5.2) Exercise. Assume $2^m + 1$ is a prime number. Then there exists i with $m = 2^i$.
Hint: use the equality $Y^a + 1 = (\sum_{j=0}^{j=a-1} (-1)^j Y^j)(Y + 1)$ for odd $a \geq 3$.
[The question of primality of numbers of the form $2^m = (2^b)^a$ where $m = ba$ has an odd divisor a bigger than one in not very interesting ...]

(5.3) Construction of regular n-gons. Since mathematics in Greek antiquity it was known that a construction with ruler and compass could be carried out for a regular 3-gon (a triangle), and a regular 5-gon; also bisection of angles could be carried out with with ruler and compass. What is the list of all $n \in \mathbb{Z}_{\geq 3}$ such that a regular n-gon can be thus constructed? This question remained unanswered for many centuries. – Before you read on, please contemplate: is this a geometric question, or does it have its natural place in another branch of mathematics?

Gauss proved on 29-March-1796 (in the morning lying in bed, he was 18 years old) that a regular 17-gon could be constructed with ruler and compass. Later he published in [11], Chapter VII the following result:

Theorem (Gauss, 1796). *A regular n-gon can be constructed with ruler and compass if and only if $n \geq 3$ can be written as*

$$n = 2^\alpha \times P_1 \times \cdots \times P_t$$

with $\alpha \in \mathbb{Z}_{\geq 0}$ and $P_1 < \cdots < P_t$ are mutually different Fermat prime numbers.

Discussion. We do not know whether Gauss indeed had an actual proof for this result. He never published a proof. The case $n = 17$ was proved in [11] by a direct computation (giving the length of a side of a regular 17-gon explicitly). A complete proof was published in 1837 by Pierre Wantzel.

A modern proof can be given by using Galois theory, a method not yet known in the time of Gauss. I would like to know what Gauss had in mind. Did he foresee this implication of Galois theory? (Here the Galois group is abelian.) Was he close to that result, e.g. in

the abelian case, but did not further develop his ideas? Perhaps we never can decide this. Interesting historical material and questions.

We see that a problem (which regular n-gons can be constructed with ruler and compass) is a problem in number theory (which Fermat numbers are prime; still unsolved), and not a geometric problem, as we might have thought earlier.

See http://www.prothsearch.net/fermat.html
for the known factoring status of Fermat numbers. You find information such as: no Fermat prime F_i is known for $i > 4$, and 269 Fermat numbers are known to be composite, $F_{2543548}$ is not prime, and much more.

6 Mersenne (prime) numbers

We introduce Mersenne numbers:

$$M_n := 2^n - 1.$$

Which of these numbers are prime?

(6.1) Exercise.

$$M_n \text{ is a prime number } \implies n \text{ is een prime number.}$$

Hint: give a factorization of $Y^{ab} - 1$ with $a, b \in \mathbb{Z}_{>1}$.

(6.2) However the opposite implication is not correct:

$$11 \text{ is a prime number, but } 23 \text{ divides } M_{11}.$$

Indeed: $M_{11} = 2^{11} - 1 = 2047 = 23 \times 89$.

(6.3) For a prime number $q = 2n + 1$ we have

$$2^{q-1} - 1 = (2^n - 1)(2^n + 1);$$

hence q divides either $2^n - 1$ or $2^n + 1$. Here are two examples:

$$11 \quad \text{divides} \quad 2^5 + 1 = 33;$$

$$2^{21} + 1 = 43 \times 48771.$$

Here is a general statement for Sophie Germain prime numbers:

Suppose p is a prime number, with $p \equiv 3 \pmod 4$
and $q := 2p + 1$ is also a prime number; in that case q is a divisor of $2^p - 1$.

(6.4) Exercise. The number $219,975,517$ is a prime number; *is it a Sophie Germain prime number?*.
Hint: what is the remainder after division by 6 of a Sophie Germain prime number?

At present we know 48 Mersenne prime numbers, see
`http://en.wikipedia.org/wiki/Mersenne-prime`
`http://primes.utm.edu/largest.html#largest`

Does this give any evidence whether there are only finite or infinitely many Mersenne prime numbers? Example: there are (only) exactly 20 Mersenne prime numbers $M_i < 10^{2916}$; see `http://primes.utm.edu/mersenne/`

Give an estimate of the density of the density of Mersenne prime numbers on this interval. (Does this convince you there are very few Mersenne prime numbers?)

(6.5) Originally the interest in Mersenne number came from a very classical topic:
Definition (Greek antiquity). A number $N \in \mathbb{Z}_{>0}$ is called a *perfect number* if the sum of the positive divisors of N equals $2N$, or, if the sum of the divisors $1 \leq d < N$ equals N:

$$N \text{ is perfect } \stackrel{\text{def}}{\iff} N = \sum_{1 \leq d < N,\ \ d|N} d.$$

We see:
$6 = 2{\cdot}M_2$ is a perfect number, $28 = 2^2{\cdot}M_3$ is perfect,
$496 = 2^4{\cdot}M_5$ is perfect ; can we continue $\cdots$?
Show $2^{10}{\cdot}M_{11}$ is not perfect.

(6.6) Theorem (Euclid, Book IX, Proposition 36, and Euler). *A number $N = 2m$ is* perfect *if and only is there is a prime number p such that*

$$M_p \textit{ is prime, and } N = 2^{p-1}{\cdot}(2^p - 1) = 2^{p-1}{\cdot}M_p.$$

Examples: $p = 2, 3, 5, 7, 13, 17, \cdots$. Warning: the theorem treats *even* perfect numbers.

We show one implication, already proved by Euclid:

$$M_p \text{ is prime } \implies \quad N := 2^{p-1}{\cdot}M_p \text{ is perfect.}$$

Define $\sigma(N)$ to be the sum of divisors d of N with $1 \leq d \leq N$. Check:

$$\sigma(2^{p-1}{\cdot}M_p) = \sigma(2^{p-1}){\cdot}\sigma(M_p) = (1 + 2 + 4 + \cdots + 2^{p-1}){\cdot}(1 + M_p) = (2^p - 1){\cdot}2^p = 2N.$$

QED$\Rightarrow$

(6.7) Exercise. *Give a proof of the other implication in this theorem.*

(6.8) A new Mersenne prime number was found in 2013:

$$2^{57,885,161} - 1 \text{ is a prime number,}$$

discovered on January 25, 2013 by Curtis Cooper at the University of Central Missouri. This is an amazing result; the organization needed for using many private computers is impressive. However did we get "any wiser"? This number has $17,425,170$ digits. See
`http://www.isthe.com/chongo/tech/math/digit/m57885161/prime-c.html`

(6.9) Exercise. In 1603 Pietro Cataldi claimed (amongst others) that $2^{29}-1$ and $2^{31}-1$ are prime numbers; can you decide how far he was correct?

We see that interest in Mersenne primes originated in the quest to find perfect numbers. However at present the main interest in this topic is to see how efficient factorization programs are. And it would be a great achievement if we can find the underlying structure here.

For the history of Mersenne and his quest for (what we now call) Mersenne prime numbers, see
`http://primes.utm.edu/glossary/page.php?sort=MersennesConjecture`

(6.10) Where are Mersenne primes located? See [5], Figure 1 on page 15: the ratio of $^2\log(^2\log(n\text{-th Mersenne prime number}))$ versus n is very close to linear, as far as we can see for known Mersenne primes. Again an example of "regularity" of the irregular behavior of prime numbers. See
`http://primes.utm.edu/mersenne/heuristic.html`
`http://primes.utm.edu/notes/faq/NextMersenne.html`

(6.11) Exercise. Mersenne thought that M_{67} is a prime numbers. Was he correct?
Hint: use a scientific calculator, e.g.
`http://web2.0calc.com/#` and
`http://eng.numberempire.com/factoringcalculator.php`

(6.12) Exercise. Is the number 25364758967463524364875683 4 a perfect number? (Underlying structure: you might want to decide first what can be the last digit of a perfect number, prove your result by pure thought, and then finish the exercise.) See (13.8).

We have seen that a geometric problem (construction of regular n-gons) gave rise to the further study of Fermat numbers (and the problem remains basically open), while the search for **even** perfect numbers is equivalent to finding Mersenne prime numbers (and also here the final outcome is basically open).

7 The Prime Number Theorem PNT

(Please remember that $\log(x)$ stands for the logarithm with base e, see (2.3).)

As we saw in the introduction we like to have insight in the "function" $\pi(-):\mathbb{R}\to\mathbb{Z}$. After ideas by Gauss and by Legendre mathematicians thought it would be difficult to prove their conjecture, untill Chebyshev in 1852 proved the first result, astonishingly simple and powerful. Then Hadamard and De la De la Vallée-Poussin proved in 1896 this deep theorem.

(7.1) The Prime Number Theorem (Chebyshev, Hadamard en De la Vallée-Poussin).

$$\pi(x) \quad \sim \quad \frac{x}{\log x}.$$

This says:

$$\lim_{x\to\infty}\left(\pi(x)/\frac{x}{\log x}\right)=1.$$

Here is another formulation: $\forall \epsilon \in \mathbb{R}_{>0} \quad \exists N \in \mathbb{Z}$ with:

$$x > N \Longrightarrow (1-\epsilon)\frac{x}{\log x} < \pi(x) < (1+\epsilon)\frac{x}{\log x}.$$

Or: for real numbers A, B with $0 < A < 1 < B$ there exists $N \in \mathbb{Z}$ such that

$$A\frac{x}{\log x} < \pi(x) < B\frac{x}{\log x} \quad \forall x > N.$$

(7.2) A slightly better estimate is

$$\pi(x) \sim \frac{x}{\log(x) - 1};$$

see [37], 2.19.

The history is that Chebyshev proved that for large x we have

$$\frac{92}{100} < \left(\pi(x)/\frac{x}{\log x}\right) < \frac{111}{100},$$

see [6], before PNT was proved to be correct. Clearly this is not enough to show that a limit exists, leave alone that the limit would be equal to 1. However it was a breakthrough. For a description of a simple and elementary proof giving such a result, see [48]. It took another more than 40 years before the beautiful and deep theorem PNT was proved, see [16], [17], [42], [43]. Afterwards many new proofs were given. Some were "elementary" (though not easy nor simple). For this fascinating story and many references (which we have also used), see [7].

Sylvester showed in 1982

$$0.95695 < \left(\pi(x)/\frac{x}{\log x}\right) < 1.04423 \qquad x \gg 0$$

refining the result by Chebyshev, using his methods.

In the literature we find many effective versions (fixing one triple A, B, N), basically weaker than the PNT, but which are very useful. We cite (and will use) the following

(7.3) Theorem (an effective version, weaker than PNT).

$$\frac{x}{\log x} < \pi(x) \qquad x > 17; \quad \pi(x) < \frac{5}{4}\cdot\frac{x}{\log x} \qquad x > 113.6,$$

see [37], Coroll. 1 and Coroll. 2 on page 69.

Also see
`http://en.wikipedia.org/wiki/Prime-number-theorem`
For example:

$$x \geq 55 \quad \Longrightarrow \quad \frac{x}{\log(x)+2} < \pi(x) < \frac{4}{\log(x)-4}.$$

(7.4) An example. Because

$$2013 < 8 \times 2012$$

we conclude:

$$\pi(10^{2012}) \;<\; \frac{5}{4}\cdot\frac{10^{2012}}{2012\cdot\log 10} \;< \frac{10^{2013}}{2013\cdot\log 10} \;<\; \pi(10^{2013}).$$

Hence there exists a prime number with 2013 decimal digits. Note that we showed existence, thus answering (1.7), but we did not give a single example of such a prime number.

Remark. Also the much weaker version $x/(3\log(x)) < \pi(x) < 3x/\log(x)/x$ (easy to prove) gives the result just proved.

(7.5) Corollary of PNT. *The sequence* $\{p_n \mid n \in \mathbb{Z}_{>0}\}$ *of all prime numbers with* $p_i < p_{i+1} \;\; \forall i$ *satisfies*

$$p_n \sim n\log n.$$

In other terms: for real numbers $0 < C < 1 < D$ there exists N such that

$$n \geq N \quad \Longrightarrow \quad C{\cdot}n\log n < p_n < D{\cdot}n\log n.$$

A more refined version:

$$p_n \sim n(\log(n) + \log(\log(n)) - 1),$$

see [37], 2.19.

We can give an effective (weaker) version as follows

(7.6) Effective weak form. *For* $n \geq 6$ *we have:*

$$\log n < \frac{p_n}{n} < \log n + \log(\log n).$$

See `http://en.wikipedia.org/wiki/Prime-number-theorem`;
see [37], Coroll. of Th. 3 on page 69.

(7.7) An example. A calculation shows

$$p_{100,000,000,000} = 2,760,727,302,517;$$

For $n = 100,000,000,000$ we have

$$n\log(n) \approx 2,532,843,602,293 \text{ and } \log(n) + \log(\log(n)) \approx 2,856,036,374,098$$

Indeed

$$2,532,843,602,293 < 2,760,727,302,517 < 2,856,036,374,098,$$

and we see that pure thought plus very little computation gives a lower bound off less than 5% and an upper bound off less than 4%.

(7.8) An application. Choose $n = 22 \times 10^{2007}$. We see

$$\log(10^{2007}) \approx 4621.288281639 \quad \text{and} \quad \log(n) = 22 \cdot \log(10^{2007}) \approx 101668.342196059;$$

hence

$$1.01 \times 10^{2012} < n \log n < p_n.$$

Also we have $\log(\log n) \approx 8.439097441$; hence

$$p_n < n(\log n + \log(\log n)) < 22 \times 10^{2007} \cdot (4621.29 + 8.44) \approx 101854.06 \times 10^{2007} < 1.02 \times 10^{2012}.$$

Conclusion:

$$10^{2012} + 10^{2010} < p_n < 10^{2012} + 2 \cdot 10^{2010}.$$

We see this prime number is situated in the interval given, hence $p_{22\times 10^{2007}}$ has exactly 2013 decimal digits. However we do not the exact value of this prime number. Can you give a reasonable guess? Can you give an exact lower bound?

How many prime numbers are situated on the given interval $(10^{2012} + 10^{2010}, 10^{2012} + 2 \cdot 10^{2010})$? Can you give a reasonable guess, or an estimate? Can you give an exact lower bound? However I think it is difficult (impossible ?) to compute the exact number by abstract methods. As these numbers seem too large to do exact calculations, it seems there is no way to decide upon the exact number of prime numbers in this interval (and, would we really care to know?).

8 Heuristics

"*Clearly, no one can mistake these probabilistic arguments for rigorous mathematics and remain in a state of grace. Nevertheless, they are useful in making educated guesses as to how numbertheoretic functions should 'behave'.* " See [1], page 248.

We will discuss "heuristic arguments", see
http://primes.utm.edu/glossary/xpage/Heuristic.html

Such "educated guesses" usually do not prove anything. However, as we will see our intuition can be guided by it. Moreover we will see that they lead to expected results which many times fit very well with reality as soon as we can do the necessary, cumbersome computations. Hence it gives us the firm belief we are on the right track. Please try to digest these ideas below. However (again), please be aware that you do not prove anything this way. Apply these intuitive methods on whatever problem you feel attracted to (and we will give many examples).

Consider the statement:

"the chance that a given number $n \in \mathbb{Z}_{>0}$ is a prime number equals $\frac{1}{\log n}$."

This is shear nonsense. The "chance that $n = 1000$ is a prime number" is zero, and the "chance that 997 is a prime number" is equal to 1. So what are we talking about? However this approach turns out to be useful.

There are basically two merits. Suppose you consider $n \in \mathbb{Z}_{>0}$ and an interval of positive integers containing n of length Δ. The number of primes in this interval is about $\Delta / \log n$.

We see in § 7 this can be made precise: we can give exact upper and lower bounds for this number (not a guess, no statistics involved, but concrete results which can be proved). In this way we have access to proofs.

We can also use this (dubious) method to obtain a feeling for a possible answer. As long as we realize this is just guessing (and we realize it does not prove anything), there is nothing wrong with it. Here is an example (Fermat numbers):

(8.1) The chance (?) that F_i is a prime number equals $1/\log(2^{2^i}) = (1/2^i)(1/\log 2)$;
let us assume Fermat numbers are "randomly chosen"
(whatever that is; also it is not quite correct; these numbers are all odd, so have a bigger "chance" to be prime, and also two different Fermat numbers are relatively prime, so they are not completely "at random"). However let us not bother about such details and sum these chances:

$$\sum_{0<i<\infty} \frac{1}{\log(2^{2^i})} = \frac{1}{\log 2} \sum_{0<i<\infty} \frac{1}{2^i} < 2 \cdot \frac{1}{\log 2}.$$

Hence there is a reasonable guess that the number of Fermat prime numbers should be *finite*.

(8.2) Here is an example to show we have to be very careful. Let us "prove"
"there are infinitely many even prime numbers" (??)
"Proof." The "chance" that $2n$ is a prime number equals $1/\log(2n)$ (?), and
clearly the sum $\sum 1/\log(2n)$ diverges (the last statement is right as Euler proved long ago).

(8.3) Exercise. Use this heuristic method on *Mersenne numbers*. Although we only know very few Mersenne primes, we have the firm belief that there are infinitely many Mersenne prime numbers. Using the heuristics, we can predict where approximately the next undiscovered Mersenne prime number should be located, and every time such predictions turn out to be rather accurate.

Try to give an estimate where the n-th Mersenne prime number can be found, and confirm (6.10).
See `http://primes.utm.edu/mersenne/heuristic.html`

(8.4) Exercise. Use this heuristic method on the set of *twin primes*; also here this method suggests a final outcome (which we belief to be true).

Such methods have been refined. One can use heuristic methods to predict the number of twin primes below a given bound. Once this process of pure thought has been carried out, an *easy computation* predicts this number. Then one can try to compute the actual number (a hard and long computation to obtain the exact number). We see that, e.g. up to 10^{15}, the expected value is less than $1/10^6$ apart from the exact value, see [5], Table 1. (In actual life, or in court, this would immediately be accepted as "proof").

(8.5) Exercise. Use a heuristic method to convince yourself there should be infinitely many *Sophie Germain prime numbers*; see (10.8)

(8.6) Exercise. Use a heuristic method to convince yourself there should be infinitely many *prime triplets*.

(8.7) Exercise. Use a heuristic method to get a feeling for Polignac's conjecture, see (10.5)(1).

Methods mentioned in this section should be taken with a grain of salt, as long as we insist on true facts, and proved results. However we use these methods for getting a feeling in which direction we should look for resutls.

See [5] for a discussion of heuristic methods, and for many tables which show that such considerations can give predictions with an amazing precision when compared with the actual numbers computed.

(8.8) Exercise. Consider all primes of the form $p = n^2 + 1$ for all $n \in \mathbb{Z} > 0$. Is this number finite or infinite? What do you expect if you apply heuristics? See [5], 3.8.

9 Computations can create wrong expectations.

As a little warning, we mention some cases of (a finite number of) computations that can give a totally wrong impression. Questions can be asked, and we could try to obtain a feeling what might be the general answer by computing special cases. That can be a useful approach. However sometimes we observe that the result suggested could be wrong. Sometimes it even appears that the expected conclusion is false in infinitely many cases. There are examples that an abstract argument shows the expectation is wrong, but that a computation that would show this is out of reach (e.g. cases where numbers should be considered with many more digits than the expected number of elementary particles in our universe).

(9.1) One can ask whether the sum

$$\sum_{p<N} \frac{1}{p},$$

taken over all prime numbers with $p < N$ is bounded or unbounded for $N \to \infty$. Performing computations, even centuries long on a fast computer, could give a wrong impression. It would take longer than the age of the universe to reach a sum above 6. However we know that Euler already long ago showed that

$$\sum_{p} \frac{1}{p} \quad \text{is divergent, i.e. unbounded.}$$

See `http://en.wikipedia.org/wiki/Proof_that_the_sum_of_the_reciprocals_of_the_primes_diverges`
`http://en.wikipedia.org/wiki/Meissel%E2%80%93Mertens_constant`
`http://primes.utm.edu/infinity.shtml`
On can show:

$$\lim_{x\to\infty} \left(\sum_{p \text{ prime } \leq x} p - \log(\log(x)) \right) = B_1,$$

as conjectured by Gauss in 1796 and proved by Mertens in 1874; note that this sum indeed diverges very slowly. The "Mertens constant" is $B_1 \approx 0.261497$. For example, a machine computing 1000 prime numbers every second, and adding $1/p$ to the previous sum needs something like 25×10^{88} years to reach $\sum_{p<x} 1/p > 6$.

(9.2) The Chebyshev's bias. In 1835 Chebyshev performed computation which suggested that (under every upper bound x) the number $\pi_{4,3}(x)$ of prime numbers $p \equiv 3 \pmod 4$ is larger than the number $\pi_{4,1}(x)$ of prime numbers $q \equiv 1 \pmod 4$; also see (13.6). This (finite) number of computations gave a certain suggestion. However Littlewood showed that $\pi_{4,3}(x) - \pi_{4,1}(x)$ changes sign infinitely often for $x \to \infty$. Even in the capable hands of Chebyshev the wrong conclusion was suggested. Also see (13.6).

(9.3) In 1895 Hermite computed:

$$e^{\pi \times \sqrt{163}}.$$

He knew that this is not an integer. An approximation for this number is:

$$e^{\pi \times \sqrt{163}} \approx 262537412640768743.99999999999925007 \cdots.$$

Suppose we should start this computation not knowing theory behind this phenomenon. Seeing so many numbers 9 appearing (twelve in number) we could easily jump to the conclusion this indeed could be an integer. See "The French paper of Hermite (1859) 'Sur la thorie des equations modulaires' freely available at Google books" (google: <hermite 163>). In [39], A4 on page 192 we find an explanation how you could come to the idea just computing this number.

(9.4) Li and pi. In the PNT as discussed in § 7 we see estimates for the function $\pi(x)$ which is counting the number of prime numbers below x. We discussed the approximation $x/\log(x)$. A different one is given by the function $\mathrm{Li}(x)$:

$$\mathrm{Li}(x) := \int_2^x \frac{1}{t} dt;$$

see
`http://en.wikipedia.org/wiki/Prime_number_theorem`
for details. This could be a better approximation for $\pi(x)$. For "small" values of x we have:

$$\mathrm{Li}(x) > \pi(x);$$

Gauss and Riemann expected this inequality to hold for all x. However, Littlewood proved in 1914:

- there do exist x with $\mathrm{Li}(x) < \pi(x)$;
- however the smallest one where this happens could very well somewhere close to 10^{316};
- the sign of $\mathrm{Li}(x) - \pi(x)$ changes infinitely often for $x \to \infty$.

Concrete examples seem out of reach of actual computations. We see again that a finite amount of computations can be misleading.

(9.5) The Mertens conjecture. We say $k \in \mathbb{Z}_{>0}$ is *square-free* if for every $d \in \mathbb{Z}_{>1}$ the number d^2 does not divide k.
We say that $k \in \mathbb{Z}_{>0}$ is *not square-free* in case there is some $d \in \mathbb{Z}_{>1}$ where d^2 divides k.

The Möbius-function. For every $k \in \mathbb{Z}_{>0}$ we define $\mu(k) \in \{-1, 0, +1\}$:

- $\mu(k) = -1$ in case k is square-free and the number of prime factors in the factorization of k is *odd*;
- $\mu(k) = 0$ if k is not square-free;
- $\mu(k) = +1$ in case k is square-free and the number of prime factors in the factorization of k is *even*.

See `http://nl.wikipedia.org/wiki/M%C3%B6biusfunctie`

We write

$$M(n) := \sum_{k=1}^{k=n} \mu(k).$$

Suggestion. Compute $\mu(k)$ for all $1 \leq k \leq 50$, and compute $M(n)$ for all $1 \leq n \leq 50$. What do we see?

The Mertens conjecture, 1897.

$$\mid M(n) \mid < \sqrt{n} \qquad \forall\ n > 1 \quad (??); \quad \text{see [30].}$$

This seems reasonable. Our computation for small n suggests that $\mid M(n) \mid$ does not grow fast. And we can contemplate, and we can "explain" this: the prime numbers 2 and 3 come first, contributing -1, $\mu(4) = 0$, and only for $\mu(6) = +1$ we obtain a positive contribution. Does this vague idea lead anywhere?

For some time this conjecture was unproved (and not refuted). As Mertens did, and later attempts showed, computations seemed to confirm the conjecture (for "small" x).

Moreover it was shown that the Mertens conjecture would imply the Riemann hypothesis (but probably not conversely). We understand the interest in this conjecture.

In 1985 Andrew Odlyzko and Herman te Riele showed the Mertens conjecture to be false, see [33]. An impressive result. The proof uses abstract methods combined with extensive computations. Also we understand why our previous computations did not reveal the truth in this case:

- there is a number $n < e^{1.95 \times 10^{40}}$ such that $\mid M(n) \mid > \sqrt{n}$;
- for $n < 10^{14}$ we have $\mid M(n) \mid < \sqrt{n}$;
- a precise value n for which the Mertens conjecture fails has not been found up to now.

See `http://en.wikipedia.org/wiki/Mertens_conjecture`
I think this is a beautiful example how misleading a finite amount of computations can be.

Postscript. Doing computations in order to obtain a feeling for a mathematical problem can be a valuable approach. However at the same time we should keep in the back of our mind that behavior of a finite number of possibilities need not to give the right suggestion in case an infinite amount of cases is considered. Especially in number theory we see misleading situations.

10 Some open problems

Warning. Below we record some open problems. They seem easy (at least in formulation). However many mathematicians have tried hard to crack these nuts. If you want, do some computations (but please realize that huge computers and intricate algorithms already have been used, and no concluding evidence has been found as yet). It might be wise not spend the rest of your (mathematical) life to solve any of these. (However in case you have a proof or a counter example to any of the problems below you will be front page news.)

It seems mathematicians have not yet found the right angle of view, the decisive technique to tackle these problems. Often a completely new insight is necessary (and that is the merit of beautiful open problems).

Here is an example. Fermat's Last Theorem (formulated around 1637) was an "isolated problem" for a long period of time. In the 19-th century a new approach seemed fruitful (ideal theory); indeed it did solve some cases (and it is wonderful and gave rise to an important new tool; you see how a question can trigger new developments). However FLT in general remained out of reach then.

Here we write FLT for "Fermat's Last Theorem":

$$x, y, z, n \in \mathbb{Z},\ n \geq 3,\quad x^n + y^n = z^n \quad \stackrel{?!}{\Longrightarrow} \quad xyz = 0.$$

(For $n = 1$ and for $n = 2$ this equation has many solutions. Fermat claimed he had proved there are no solutions in positive integers for $n \geq 3$.)

Then large computers were used, no counter examples were found, and a huge (but finite) list of special cases was solved.

In 1985 Gerhard Frey indicated a possible connection with another open problem (elliptic curves and the conjecture of Shimura-Taniyama-Weil) and Ribet showed indeed STW $\Rightarrow$ FLT. All of a sudden FLT was not anymore an isolated problem but a corollary of something we all thought to be true. Andrew Wiles knew the problem FLT from his childhood, and elliptic curves and the STW conjecture were in the heart of his specialty; once this connection was made Wiles started working on this, and the great triumph (for Wiles, but also for pure mathematics) was a solutions for both problems; pure thought was winning the match started 350 years before, and computers were not needed (except for processing and communicating manuscripts).

Conjecture or Expectation? We sometimes use the word "conjecture" for a statement we have the firm idea, but not yet a proof, that it should be true. Personally I use this word in a restrictive sense. If there is no **structural evidence**, or other indications what kind of underlying structure would imply the result, but still we are quite convinced this should be true, I tend to use the word "expectation".

For all questions below "heuristic methods", as in Section 8, hint in the direction of expectations below. Abstract methods, intricate algorithms, extensive computer searches and many other methods have been used.

(10.1) Odd perfect numbers. See (6.5) for the definition of a perfect number. We have reasonable insight (but no definite conclusion) about the problem of all **even** perfect numbers.

Does there exist an **odd** *perfect number?*

There is a huge amount of partial results, and of literature about this problem. No odd perfect number is found as yet, and we know there is no such below a large bound (which is constantly improved upon); e.g. at present we know that an odd perfect number, if it exists, has at least 300 decimal digits and has a prime factor greater that 10^{20}; this might discourage you to find an odd perfect number by hand.
See `http://mathworld.wolfram.com/OddPerfectNumber.html`

Expectation. *There is no odd perfect number.*(?)

Why should this be true? Up to now no examples have been found. However I fail to see any structure or evidence supporting this expectation. For further references see
`http://primes.utm.edu/mersenne/`

Besides "numerical evidence" (they were not found by many computations up to now), I see very little evidence for this; also I do not see any heuristics for this. Numerical evidence is a subjective argument; checking a finite amount of numbers is still 0% of all possible cases.

(10.2) The Goldbach conjecture. In 1762 Christian Goldbach wrote a letter to Euler stating a conjecture. (By the way, this is the first time in history, to my knowledge, that the word conjecture was used with this meaning.)
Expectation. *Every even number $N = 2n \geq 4$ can be written as the sum of two prime numbers.*(?)

See `http://en.wikipedia.org/wiki/Goldbach27s_conjecture`
The conjecture has been shown to hold up through 4×10^{18} and is generally assumed to be true, but remains unproven despite considerable effort.
See `http://en.wikipedia.org/wiki/Prime-number#Open-questions`

Heuristic methods indicate Goldbach's conjecture should hold (but as we have seen and argued before this is not a mathematical proof).

It is interesting to consult papers throughout history, and see that there is a constant shift in terminology, it resembles the tides, between "Goldbach's problem" and "Goldbach's conjecture".

(10.3) A variant. We say a prime p is a t-prime if either $p-2$ or $p+2$ is a prime number (i.e. if p belongs to a twin).
Expectation (Goldbach's conjecture for t-primes). *Every sufficiently large even integer is the sum of two* t*-primes.*(?)

(10.4) Twin primes. A *twin prime* is a pair of prime numbers $\{p, q\}$ with $q = p+2$. There are many examples. Computing twin primes you see that sometimes they are close together (as close as possible), sometimes consecutive pairs are relatively far away from each other. We write

$$\pi_2(x) = \#(\{p \mid p \leq x, \text{ and } p \text{ and } p+2 \text{ are prime}\}).$$

http://en.wikipedia.org/wiki/First-Hardy-Littlewood-conjecture
Expectation. *There are infinitely many twin primes.*(?)

The function $\pi_2(-)$ again seems to be an example of an "irregular function which is very regular when considered on a large scale".

In fact this can made more precise in the form of the following expectation

$$\pi_2(x) \stackrel{?}{\approx} 2 \times 0.66 \times \frac{x}{(\log x)^2}.$$

See http://en.wikipedia.org/wiki/Twin-prime
Numerical results (a huge amount of computing) fit very well with this.

An example:

$$\pi_2(10^{18}) = 808,675,888,577,436,$$

and

$$2 \times 0.66 \times \frac{10^{18}}{(\log 10^{18})^2} \approx 768,418,024,862,131.$$

The predicted number is 95% of the actual number

Computation have produced large twin primes:
"On December 25, 2011 PrimeGrid announced that yet another record twin prime had been found. It is $3756801695685 \times 2^{666669} \pm 1$. The numbers have 200700 decimal digits."

For the history of the twin prime conjecture see
http://arxiv.org/abs/1205.0774

Recently we have seen a spectacular new development. Yitang Zhang showed that the set of gaps between prime numbers has an accumulation point below 7×10^7; see [50]. (The twin-prime-number conjecture states that 2 appears infinitely often, i,e, the smallest accumulation point is expected to be equal to 2.) See the three wonderful papers by Henryk Iwaniec, Lizhen Ji and William Dunham about this new result and about the twin-prime-number conjecture in this journal: ICCM Notices vol. **1** No. 1, July 2013.

The notion of twin primes has been generalized in the following way.

(10.5) Gaps in the sequence of prime numbers.
(10.5)(1) Expectation, Polignac conjecture, 1849; see [34], [35].
For every $m = 2n \in \mathbb{Z}_{>0}$ *there are infinitely many pairs of* consecutive *prime numbers* (p_i, p_{i+1}) *with* $p_{i+1} - p_i = m$.(?)

This has neither been proved nor disproved for any even $m = 2n \geq 2$.
http://en.wikipedia.org/wiki/Twin-prime

In 1849 Alponse de Polignac stated the conjecture (10.5) that every even number does appear infinitely often as a prime gap, see [35]. We have to be cautious for two reasons. One is that Polignac stated his idea as "Théorème"; however from the text we see clearly that he did not

prove anything, but just computed some evidence. (The word "Théorème" clearly stood for "statement" and not for a proved fact.)

The second warning is that Polignac also stated:

Theorem (?!).
Every odd number can be written as the sum of a power of 2 *and a prime number*

with the claim that this was verified up to three milion. However we readily see that (as Euler already noted) that 127 and 959 cannot be written in this way.

(10.5)(2) Expectation *For every positive number* $m = 2n \in \mathbb{Z}_{>0}$ *there are infinitely many pairs of prime numbers* (p, q) *with* $q - p = m$.(?)

Clearly, if (10.5)(1) holds, then (10.5)(2) holds.

For heuristic evidence for the Polignac conjecture see [5]; from that paper, Table 2: for $m = 210$ consider the number of pairs of primes $(p, p+210)$ with $p < 10^9$; heuristics predict this number to be equal to $10,960,950$; exact computation of this number gives $10,958,370$; the prediction is less than 0.03% off. Just one example of the incredible precision of such heuristic predictions (for the cases which can be verified).

Remark. We need to consider gaps of even length; for gaps of odd length, see (11.3).

For tables of record gaps between prime constellations (A. Kourbatov), see:
`http://xxx.lanl.gov/pdf/1309.4053.pdf`

(10.6) Is the number of Fermat prime numbers bounded?
See Section 5. We write $F_i = 2^{2^i}$ for $i \in \mathbb{Z}_{\geq 0}$.

Expectation. *The number of Fermat prime numbers is finite.*(?)
See [23] for more information.

(10.7) Is the number of Mersenne prime numbers unbounded?
See Section 6. We write $M_n = 2^n - 1$ for $n \in \mathbb{Z}_{>0}$. We know that M_n is prime implies n is prime.

Expectation. *There are infinitely many Mersenne prime numbers.*(?)

Our experience and computations suggest: "most of the Mersenne numbers are composite". However we still do not have an answer to:
(10.7)(bis) *Is the number of* composite *Mersenne numbers infinite.*?

(10.8) Is the number of Sophie Germain prime numbers unbounded?
We say a prime number p is a *Sophie Germain prime number* if also $q := 2p + 1$ is a prime number; http://oeis.org/ gives:

$2, 3, 5, 11, 23, 29, 41, 53, 83, 89, 113, 131, 173, 179, 191, 233, 239, 251, 281, 293,$
$359, 419, 431, 443, 491, 509, 593, 641, 653, 659, 683, 719, 743, 761, 809, 911, 953, 1013,$

$1019, 1031, 1049, 1103, 1223, 1229, 1289, 1409, 1439, 1451, 1481, 1499, 1511, 1559, \cdots$
Further examples:

$$\cdots, \quad 137211941292195 \times 2^{171960} - 1, \cdots, \quad 18543637900515 \times 2^{666667} - 1, \ \cdots.$$

Expectation. *There are infinitely many Sophie Germain prime numbers.*(?)
For $p < 10^4$ there are 190 Sophie Germain prime numbers and for $p < 10^7$ there are 56032.
See `http://en.wikipedia.org/wiki/Sophie-Germain-prime`
See Conjecture (3.6) and Table 6 in [5] (a heuristic prediction for the number of Sophie Germain prime numbers below a certain bound, which is incredibly precise as far as we can check up to now).

Sophie Germain had a correspondence (at first under de name Monsieur Le Blanc) with Gauss, and Gauss was very impressed. For the primes mentioned above she showed a proof for a case of FLT for such prime exponents. She did not obtain (as a woman) enough recognition for her mathematical contributions, but Gauss made a Doctor Honoris Causa title for her available in Göttingen; however she died before she knew (and before she could receive that honor).

(10.9) The Collatz problem, or the $3x + 1$ conjecture.
See (1.10). We define a function $C : \mathbb{Z}_{>0} \longrightarrow \mathbb{Z}_{>0}$ by:

$$C(2m) := m, \qquad C(2m + 1) = 3(2m + 1) + 1;$$

(for n *even* we have $C(n) = n/2$ while for n *odd* we have $C(n) = 3n + 1$.

Start with an arbitrary $a_1 \in \mathbb{Z}_{>0}$ and produce the sequence $\{a_1, \cdots, a_{i+1} := C(a_i), \ldots\}$. This is called a *Collatz sequence*. For example, starting with $a_1 = 17$ we obtain

$$17, \quad 52, \quad 26, \quad 13, \quad 40, \quad 20, \quad 10, \quad 5, \quad 16, \quad 8, \quad 4, \quad 2, \quad 1 \cdots$$

Observe that this ends with

$$4 \mapsto 2 \mapsto 1 \mapsto 4 \mapsto 2 \mapsto 1 \mapsto 4 \ \text{ etc. .}$$

Expectation. *Every Collatz sequence sequence ends with* $\{4, 2, 1 \ \text{ etc.}\}$ (?).
This has not been solved. We seem not to understand which mechanism could give access to this problem.

Suggestion. Construct some of these sequences (every time by choosing a_1 to start with), and observe the puzzling experience indeed the sequence ends as expected (or do you try to find a counter example? In that case you better start with a number with more than 500 decimal digits.)

We find a discussion of this problem and many references in
J. C. Lagarias *The ultimate challenge: the* $3x + 1$ *problem.* AMS, 2010.
See `http://www.math.lsa.umich.edu/~lagarias/`
Also see: `http://arxiv.org/pdf/math/0608208v6.pdf`

http://www.math.grin.edu/~chamberl/papers/3x-survey-eng.pdf
http://en.wikipedia.org/wiki/Collatz-conjecture

You can go to http://www.nitrxgen.net/collatz.php,
start with a positive integer (at most 500 decimal digits), and you see the Collatz sequence appear.

Here is an example. Start with 27. After 111 steps we see the end-tail of the Collatz sequence:

$$27, 82, 41, 124, 62, 31, 94, 47, 142, 71, 214, 107, 322, 161, 484, 242, 121, 364,$$

$$182, 91, 274, 137, 412, 206, 103, 310, 155, 466, 233, 700, 350, 175, 526, 263,$$

$$790, 395, 1186, 593, 1780, 890, 445, 1336, 668, 334, 167, 502, 251, 754, 377,$$

$$1132, 566, 283, 850, 425, 1276, 638, 319, 958, 479, 1438, 719, 2158, 1079, 3238,$$

$$1619, 4858, 2429, 7288, 3644, 1822, 911, 2734, 1367, 4102, 2051, 6154,$$

$$3077, 9232, 4616, 2308, 1154, 577, 1732, 866, 433, 1300, 650, 325, 976,$$

$$488, 244, 122, 61, 184, 92, 46, 23, 70, 35, 106, 53, 160, 80, 40, 20, 10, 5, 16, 8, 4, 2, 1$$

Question. *Is there a formula that for every $a_1 \in \mathbb{Z}_{>0}$ computes the number of steps in the Collatz sequence starting with a_1 until the first time* 1 *appears in this sequence?* Experience shows that this length jumps up and down (in a rather unpredictable way ?) for growing a_1.

We have only mentioned a very small part of conjectures about prime numbers. For more see
http://en.wikipedia.org/wiki/Category:Conjectures-about-prime-numbers

We should have discussed the most intriguing one (with many important implications): *the Riemann hypothesis*. Unfortunately that would lead us much too far.

(10.10) In 1912 at the International Congress of Mathematicians Landau listed four problems:

(1) Goldbach (10.2),
(2) $n^2 < p < (n+1)^2$ (4.2),
(3) twin primes (10.4) and
(4) there are infinitely many primes of the form $p = n^2 + 1$ (8.8).

These were open (old) conjectures then, and still we seem far from satisfactory answers or results.
See [9]; see page 2 of http://arxiv.org/pdf/1205.0774v1.pdf

Topics which I should have like to discuss, but which would make this paper much too long:

RSA cryptography, however see [41] and
http://nl.wikipedia.org/wiki/RSA_28cryptografie29

and the ABC conjecture, however see
http://en.wikipedia.org/wiki/Abc-conjecture
http://www.math.leidenuniv.nl/~desmit/abc/index.php?set=1
http://www.kurims.kyoto-u.ac.jp/~motizuki/top-english.html

(10.11) Conclusion. We return to the list of 10 questions in Section 1. I hope that you were surprised by the fact that some are easy, while other problems are difficult and remain unsolved. For some we have a feeling about what the answer should be (but without conclusive proof), and some of the problems can be answered with the help of some deep, well-developed theory.

- Questions 1 and 2 have an answer, and proofs are very easy.
- Questions 3, 4, 5, 6, 9, and 10 lead to difficult open problems, and we still have no idea even where to start. However "heuristics" give us a clear clue, with great precision, what we should expect (I find this amazing the "regularity" in such irregular processes).
- Questions 7 an 8 have an answer which can be given now that we understand the underlying structure.

11 Four easy exercises

After so many easy and difficult questions, here are three exercises: problems which you can solve by just being somewhat clever.

(11.1) Exercise 1. *Show the set of prime numbers with*

$$p \equiv 3 \pmod 4$$

to be infinite.

Remark. It can be shown there are infinitely many prime numbers with $p \equiv 1 \pmod 4$; see (13.4).

(11.2) Exercise 2. *Suppose given $n \in \mathbb{Z}_{>0}$. Show there exists $a \in \mathbb{Z}_{>0}$ such that in the arithmetic progression*

$$\{a, a+n, a+2n, \cdots\} = \{a + in \mid i \in \mathbb{Z}_{>0}\}$$

there are infinitely many prime numbers.

Remark. A (deep) result by Dirichlet says that for any $a, n \in \mathbb{Z}_{>0}$ with $\gcd(a, n) = 1$ in the arithmetic progression

$$\{a, a+n, a+2n, \cdots\} = \{a + in \mid i \in \mathbb{Z}_{>0}\}$$

there are infinitely many prime numbers. In the previous exercise you are supposed to give a(n easy and elementary) proof of the special case as in the exercise, without using Dirichlet's theorem.

(11.3) Exercise 3. *Show there exist infinitely many $N \in \mathbb{Z}_{>0}$ such that N is not the difference between two prime numbers.*

(11.4) Exercise 4. Is it true that $7^{100} + 1 = 19^{66}$?

12 Appendix I: Factorization of integers.

We record a result which can be found in (almost) every textbook on algebra. You can try to give proofs of statement below just by yourself.

(12.1) Remark. Every $a \in \mathbb{Z}_{>1}$ is divisible by a prime number.

(12.2) Theorem. *Every $a \in \mathbb{Z}_{>1}$ can be factored $a = p_1 \times \cdots \times p_t$ as a product of prime numbers.Once a is given, these factors are unique up to ordering.*

(12.3) Warning. We are so accustomed to uniqueness of factorization (of integers) that we might overlook this property does not hold in other number systems. Consider the ring

$$T := \mathbb{Z}[\sqrt{-5}] = \{x + y{\cdot}\alpha \mid x, y \in \mathbb{Z}\},$$

with $\alpha^2 = -5$, e.g. as subset of $\mathbb{C}$. Note that

$$2{\cdot}3 \quad = \quad 6 \quad = \quad (1 + \sqrt{-5}){\cdot}(1 - \sqrt{-5})$$

holds in T. It is easy to see that the factors $2, 3, (1 + \sqrt{-5}), (1 - \sqrt{-5}) \in T$ are irreducible. We see that units in T are $+1, -1 \in T$. We conclude that factorization in T is not unique (not even up to units, not even up to ordering the factors).

It might very well be that Fermat overlooked this fact when stating that his FLT should hold. In any case in the 19-th century a "proof" of FLT was presented based on this false assumption, see
`http://fermatslasttheorem.blogspot.nl/2006/01/lams-proposed-proof.html`
although Kummer already had shown that uniqueness of factorization in the ring of integers in an arbitrary cyclotomic field need not hold.

In case you want to find a proof you might use:

(12.4) Lemma (division with remainder). *Assume given $n, d \in \mathbb{Z}$ with $d > 0$. There exist $q, r \in \mathbb{Z}$ such that*

(12.5) Lemma. *Suppose given $a,\ b \in \mathbb{Z}$. Write $d := \gcd(a, b)$. There exist $x, y \in \mathbb{Z}$ such that*

$$xa + yb = d.$$

Give a proof of (12.4), of (12.5), and use these to prove Theorem (12.2).

13 Appendix II: Integers modulo n

This section contains a description of a well-known elementary method.

(13.1) Computing modulo n. Suppose given $n \in \mathbb{Z}_{>1}$. Consider the set of symbols

$$\mathbb{Z}/n := \{\overline{0}, \overline{1}, \cdots, \overline{n-1}\}.$$

In this set we define addition, subtraction and multiplication. We put $\overline{m} = \overline{m - in}$, and we give the map

$$\mathbb{Z} \longrightarrow \mathbb{Z}/n, \quad m \mapsto \overline{m}.$$

In other words: for $m \in \mathbb{Z}$ we write $m = dn + r$ with $0 \leq r = r(m) < n$ (division with remainder) and we map $m \in \mathbb{Z}$ onto $\overline{r(m)} = \overline{r}$. We write $\overline{a} + \overline{b} = \overline{a+b}$ ("addition mod n), and analogous definitions for $\overline{ab}$ en $\overline{a-b}$.

In technical terms: $\mathbb{Z}/n$ is a ring, and the natural map $\mathbb{Z} \to \mathbb{Z}/n$ is a ring-homomorphism. Taking n into account of the notation, we write $\overline{m} = m \bmod n$.
Please distinguish $(m \bmod n) \in \mathbb{Z}/n$ (the residue class of m mod n) on the one hand and $a \equiv b \pmod{n}$ on the other hand.

An example. Does the equation $T^2 = 47440033367001212$ have a solution in $\mathbb{Z}$? [Compute mod 3.]
Or: which decimals appear at the end of a square in $\mathbb{Z}$? [I.e. compute mod 10.]

Moreover, as we can see: *for every prime number p every $0 \neq \overline{a} \in \mathbb{Z}/p$ has an inverse.*
Can you prove this? In technical terms: $\mathbb{Z}/n$ is a field if and only if n is a prime number.

We will often use the following theorem.

(13.2) Theorem (the Chinese remainder theorem). *For $m, n \in \mathbb{Z}$ with $\gcd(m,n) = 1$ there is a natural map*

$$\mathbb{Z}/(mn) \quad \xrightarrow{\sim} \quad \mathbb{Z}/m \times \mathbb{Z}/n$$

which is an isomorphism (a bijective map respecting $+$ and $\times$ and $-$).

(13.3) Proposition (sums of squares). *Let $A, B \in \mathbb{Z}_{>0}$ and let p be a prime number that divides $A^2 + B^2$ but does not divide A* (and hence p does not divide B). *Then*

$$p \not\equiv 3 \pmod{4}.$$

For a proof you might want to use the group structure of the multiplicative group $(\mathbb{F}_p)^* := \mathbb{F}_p - \{0\}$.
See Th. 5 in `http://www.maa.org/editorial/euler/how%20euler%20did%20it%2041%20factoring%20f5.pdf`

Remark. There are infinitely prime numbers with $p \equiv 3 \pmod{4}$. See (11.1).

(13.4) Corollary. *There are infinitely many prime numbers p with $p \equiv 1 \pmod{4}$.*
Proof. (We present a variant of the proof of Euclid, see (3.1).) Assume $P_1, \cdots, P_t$ are odd prime numbers with $t > 0$. We show there exists a prime number P with

$$P \equiv 1 \pmod{4} \quad \text{en} \quad P \notin \{P_1, \cdots, P_t\}.$$

This claim would prove the proposition.

Take

$$M := (P_1 \times \cdots \times P_t)^2 + 4.$$

Note that M is odd. From (13.3) we conclude that every prime number P dividing M has the property $P \equiv 1 \pmod 4$. If we would have $P \in \{P_1, \cdots, P_t\}$ we would conclude

$$P \text{ divides } M - (P_1 \times \cdots \times P_t)^2 = 4,$$

a contradiction. Hence $P \notin \{P_1, \cdots, P_t\}$. We have constructed a new prime number with $P \equiv 1 \pmod 4$. QED

(13.5) Remark. We proved that any prime of the form $\equiv 3 \pmod 4$ is not a sum of squares in $\mathbb{Z}$. Conversely, 2 and every prime of the form $\equiv 1 \pmod 4$ can be written as a sum of squares.

(13.6) Remark. Write $\pi_{4,1}(x)$ for the number of prime numbers with $p \equiv 1 \pmod 4$ and $p \leq x$; analogously $\pi_{4,3}(x)$ for the number of prime numbers with $p \equiv 3 \pmod 4$ and $p \leq x$. Try to compute these numbers for small x. You will note that these numbers are close. (Which one seems bigger?) Indeed, asymptotically, for $x \to \infty$ they are equal:

$$\lim_{x \to \infty} \frac{\pi_{4,1}(x)}{\pi_{4,3}(x)} = 1,$$

as follows form a much more general theorem, Chebotarev's density theorem; see
`http://en.wikipedia.org/wiki/Chebotarev%27s_density_theorem`

In a letter in 1835 Chebyshev writes to Fuss that it seems that $\pi_{4,3}(x) > \pi_{4,1}(x)$ for every x. This is now called "Chebyshev's bias". This started a fascinating history, with beautiful results; see
`http://arxiv.org/pdf/1210.6946v1.pdf`

In fact, much later Littlewood showed (1914):

$$\pi_{4,3}(x) - \pi_{4,1}(x) \textit{ changes sign infinitely often for } x \to \infty.$$

See [28]. A more precise result is in [38]. See [14], a beautiful paper on a fascinating subject. It was proved that Chebyshev was nearly correct: for "many" values of x we have $\pi_{4,3}(x) > \pi_{4,1}(x)$.

An example that an "easy" question can lead to beautiful research, that a simple-minded problem can lead to deep results (as is the case so often in mathematics). Also we see that a finite amount of computation (even by a great mathematician like Chebyshev) may lead to a wrong impression.

(13.7) An example of computing modulo n. *We show that* 641 *divides* F_5.
We see:

$$641 = 640 + 1 = 5{\cdot}2^7 + 1 = 625 + 16 = 5^4 + 2^4.$$

This implies

$$5{\cdot}2^7 \equiv -1 \pmod{641}, \text{ hence } 5^4{\cdot}2^{4\times 7} \equiv +1 \pmod{641};$$

hence

$$-2^4 \cdot 2^{28} \equiv 5^4 \cdot 2^{28} \equiv +1 \pmod{641}; \text{ hence } F_5 \equiv 0 \pmod{641}.$$

QED

Also see:

`http://www.maa.org/editorial/euler/how%20euler%20did%20it%2041%20factoring%20f5.pdf`

(13.8) Exercise. (1) Show that the last decimal digit of a number of the form 2^n is 2, 4, 6 or 8.
(2) Show that the last decimal digit of a Mersenne prime number is 1, 3 or 7; show all these cases do occur.
(3) Show that the last decimal digit of an even perfect number is either 6 or 8.

14 Some mathematicians

We list some mathematicians mentioned above.

(300 BC) Euclid of Alexandria

(1552 -1626) Pietro Antonio Cataldi

(1588 - 1648) Marin Mersenne

(1601 or 1607/8 - 1665) Pierre de Fermat

(1690 - 1764) Christian Goldbach

(1707 - 1783) Leonhard Euler

(1752 - 1833) Adrien-Marie Legendre

(1776 - 1831) Marie-Sophie (Sophie) Germain

(1777 - 1855) Carl Friedrich Gauss

(1814 -1894) Eugène Charles Catalan

(1817 - 1890) Alphonse de Polignac

(1821 - 1894) Pafnuty Chebyshev

(1865 - 1963) Jacques Solomon Hadamard

(1866 - 1962) Charles Jean de la Vallée-Poussin

(1906 - 1998) André Weil

(1910 - 1990) Lothar Collatz

(1927 - 1958) Yutaka Taniyama

(1943 -) Robert Tijdeman

(1930 -) Goro Shimura

(1937 -) Yuri Ivanovitch Manin

(1944 -) Gerhard Frey

(1947 -) Yuri Matiyasevich

(1948 -) Kenneth Alan Ribet

(1951 -) Don Bernhard Zagier

(1953 -) Andrew Wiles

References

[1] E. Bach & J. Shallit *Algorithmic number theory. Vol. 1. Efficient algorithms. Foundations of Computing Series.* MIT Press, Cambridge, MA, 1996.

[2] A. H. Beiler - *Recreations in the theory of numbers: The queen of mathematics entertains.* Dover Publ., pocket, 1964.

[3] E. T. Bell – *Men of mathematics.* Simon & Schuster. 1937.

[4] D. M. Burton - *Elementary number theory.* Allyn & Bacon, 1980.

[5] C. Caldwell - *An amazing prime heuristic.*
`http://www.utm.edu/staff/caldwell/preprints/Heuristics.pdf`

[6] P. Chebyshev - *Mémoire sur les nombres premiers.* J. de Math. Pures Appl. **17** (1852), 366-390. Also in Mémoires présentés à l'Académie Impériale des sciences de St.-Pétersbourg par divers savants **7** (1854), 15-33. Also in Oeuvres 1 (1899), 49-70.

[7] H. Diamond - *Elementary methods in the study of the distribution of prime numbers.* Bulletin American Mathematical Society **7** (1982), 553–589.

[8] Apostolos Doxiades – *Uncle Petros and Goldbach's conjecture: a novel of mathematical obsession.*
Originally in Greek:
O Theios Petros kai i Eikasia tou Goldbach (1992).
see: `http://en.wikipedia.org/wiki/Apostolos-Doxiadis`
`http://www.ams.org/notices/200010/rev-jackson.pdf`
`http://www.authortrek.com/uncle-petros.html`

[9] P. Erdös & J. Surányi - *Topics in the Theory of Numbers.* Springer, 2003.

[10] A. Fröhlich & M. J. Taylor – *Algebraic number theory.* Cambridge Std. Advanc. Math. 27, Cambridge Univ. Press, 1991.

[11] C. F. Gauss – *Disquisitiones Arithmeticae.* Written in 1798, published in 1801.

[12] C. Gauss, Letter to Encke, 24 Dec. 1849, Werke, vol. 2, Kng. Ges. Wiss., Göttingen, 1863, pp. 444-447.

[13] A. Granville – *Harald Cramér and the distribution of prime numbers.* Scandinavian Actuarial Journal **1** (1995), 12–28.
`http://www.dartmouth.edu/~chance/chance-news/for-chance-news/Riemann/cramer.pdf`

[14] A. Granville & G. Martin – *Prime number races.* American Mathematical Monthly **113** (2006), 1–33.

[15] R. K. Guy – *Unsolved problems in number theory.* Springer, 3rd Edition 2004.

[16] J. Hadamard - *Étude sur les propriétés des fonctions entières et en particulier d'une fonction considérée par Riemann.* J. de Math. Pures Appl. **9** (1893), 171-215; reprinted in Oeuvres de Jacques Hadamard, C.N.R.S., Paris, 1968, vol. 1, pp. 103-147.

[17] J. Hadamard - *Sur la distribution des zéros de la fonction $\zeta(s)$ et ses conséquences arithmétiques.* Bull. Soc. Math. France **24** (1896), 199-220; reprinted in Oeuvres, vol. 1, pp. 189-210.

[18] M. Haddon – *The curious incident of the dog in the night-time.* Jonathan Cape (UK) Doubleday (US), 2003.
`http://en.wikipedia.org/wiki/The-Curious-Incident-of-the-Dog-in-the-Night-Time`

[19] G. H. Hardy & E. M. Wright - *An introduction to the theory of numbers.* Oxford, Clarendon Press, fourth edition, 1975.

[20] J. Jones – *Formula for the Nth prime number.* Canad. Math. Bull. **18** (1975), 433434.

[21] J. Jones, D. Sato, H. Wada & D. Wiens – *Diophantine representation of the set of prime numbers.* Amer. Math. Monthly, **83** (1976), 449–464.

[22] D. Kehlmann – *Die Vermessung der Welt.* Rowohlt 2005.
English translation: *Measuring the world.*
For a review see: `http://www.ams.org/notices/200806/tx080600681p.pdf`

[23] M. Krízek, F. Luca & L. Somer -*17 Lectures on Fermat numbers from number theory to geometry.* CMS Books in Mathematics Springer, New York 2002.

[24] S. Lang – *Algebraic number theory.* Graduate Texts in Mathematics, Vol. 110, Springer, 1986.

[25] S. Lang - *Algebra.* Graduate Texts in Mathematics, Vol. 211. Springer, 2002.

[26] D. Leavitt - *The Indian clerk.* Bloomsbury, 2007.

[27] A.-M. Legendre - *Essai sur la théorie des Nombres.* Duprat, Paris, 1798.

[28] J.Littlewood - *Sur la distribution des nombres premiers.* Comptes Rendus, **158** (1914), pp. 1869–1872.

[29] Yuri I. Manin – *Good proofs are proofs that make us wiser.* Interview by Martin Aigner and Vasco A. Schmidt. The Berlin Intelligencer, 1998, pp. 16–19.

[30] F. Mertens - *Über eine zahlentheoretische Funktion.* Sitzungsberichte der Kaiserlichen Akademie der Wissenschaften, Mathematisch-Naturwissenschaftliche Klasse, Abteilung 2a, **106** (1897), pp. 761–830.

[31] P. Mihăilescu – *Primary cyclotomic units and a proof of Catalan's conjecture.* Journ. Reine angew. Math. 572 (2004), 167–195.

[32] D. Musielak - *Sophie's diary: A historical fiction.* AuthorHouse, 2004.

[33] A. Odlyzko & H. te Riele - *Disproof of the Mertens conjecture*, Journ. reine angew. Mathematik **357** (1985), 138–160.

[34] A. de Polignac - *Six propositions arithmologiques déduites de crible d'Ératosthène.* Nouv. Ann. Math. **8** (1849), 423–429.

[35] A. de Polignac - *Recherches nouvelles sur les nombres premiers.* Comptes Rendus Paris **29** (1849), pp. 397–401 and 738–739.

[36] H. Riesel - *Prime numbers and computer methods for factorization.* Progress Math. 57, Birkhäuser, 1985.

[37] J. Rosser & L. Schoenfeld – *Approximate formulas for some functions of prime numbers,* Illinois J. Math., **6** (1962), 64–94.

[38] M . Rubinstein & P. Sarnak - *Chebyshev's bias.* Experiment. Math. **3** (1994), 173–197.

[39] J-P. Serre - *Lecture on the Mordell-Weil theorem.* Asp. Math. E 15, Vieweg, 1989.

[40] D. Shanks – *Solved and unsolved problems in number theory.* Chelsea Publ. Cy., 1978.

[41] S. Singh – *The code book: the evolution of secrecy from Mary, Queen of Scots to quantum cryptography.* Simon Singh Doubleday Books, 1999.

[42] C. de la Vallée Poussin - *Recherches analytiques sur la théorie des nombres premiers.* Ann. Soc. Sci. Bruxelles **20** (1896), 183-256.

[43] C. de la Vallée Poussin - *Sur la fonction $\zeta(s)$ de Riemann et le nombre des nombres premiers inférieurs à une limite donnée.* Memoires Couronnés de l'Acad. Roy des Sciences, Belgique **59** (1899-1900); reprinted in Colloque sur la Théorie des Nombres (Bruxelles, 1955), Thone, Liège, 1956, pp. 9- 66.

[44] P. Vojta – *Diophantine approximations and value distribution theory.* Lect. Notes Math. 1239, Springer-Verlag, New York, 1987.

[45] A. Weil – *Number theory, an approach through history, from Hammurapi to Legendre.* Birkhäuser 1984.

[46] E. Weiss – *Algebraic number theory.* Mc-Graw-Hill Cy, 1963.

[47] H. Wilf – *What is an answer?* Amer. Math. Monthly, **89** (1982), 289–292.

[48] D. Zagier – *The first 50 milion prime numbers.*
`http://sage.math.washington.edu/edu/2007/simuw07/misc/\\zagier-the-first-50-million-prime-numbers.pdf`
Published in *The Mathematical Intelligencer*, Vol. **0**, August 1977.

[49] D. Zagier – *Newmans short proof of the prime number theorem.* Amer. Math. Monthly **104** (1997), 705–708.

[50] Y. Zhang – *Bounded gaps between primes.* To appear: Ann. Math.
`http://annals.math.princeton.edu/articles/7954`

The text by Don Zagier in [48]:
There are two facts about the distribution of prime numbers of which I hope to convince you so overwhelmingly that they will be permanently engraved in your hearts.

The first is that, despite their simple definition and role as the building blocks of the natural numbers, the prime numbers belong to the most arbitrary and ornery objects studied by mathematicians: they grow like weeds among the natural numbers, seeming to obey no other law than that of chance, and nobody can predict where the next one will sprout.

The second fact is even more astonishing, for it states just the opposite: that the prime numbers exhibit stunning regularity, that there are laws governing their behaviour, and that they obey these laws with the almost military precision.
Don Zagier

This table compare x with $\pi(x)$, gives $\pi(x) - \frac{x}{\log x}$, and $\pi(x)/\frac{x}{\log x}$, and the average length of gaps under the bound given.

Copied from:
`http://en.wikipedia.org/wiki/Prime-number-theorem`

x	$\pi(x)$	$\pi(x) - \frac{x}{\log x}$	$\pi(x)/\frac{x}{\log x}$	$x/\pi(x)$
10	4	-0.3	0.921	2.500
10^2	25	3.3	1.151	4.000
10^3	168	23	1.161	5.952
10^4	1,229	143	1.132	8.137
10^5	9,592	906	1.104	10.425
10^6	78,498	6,116	1.084	12.740
10^7	664,579	44,158	1.071	15.047
10^8	5,761,455	332,774	1.061	17.357
10^9	50,847,534	2,592,592	1.054	19.667
10^{10}	455,052,511	20,758,029	1.048	21.975
10^{11}	4,118,054,813	169,923,159	1.043	24.283
10^{12}	37,607,912,018	1,416,705,193	1.039	26.590
10^{13}	346,065,536,839	11,992,858,452	1.034	28.896
10^{14}	3,204,941,750,802	102,838,308,636	1.033	31.202
10^{15}	29,844,570,422,669	891,604,962,452	1.031	33.507
10^{16}	279,238,341,033,925	7,804,289,844,393	1.029	35.812
10^{17}	2,623,557,157,654,233	68,883,734,693,281	1.027	38.116
10^{18}	24,739,954,287,740,860	612,483,070,893,536	1.025	40.420
10^{19}	234,057,667,276,344,607	5,481,624,169,369,960	1.024	42.725
10^{20}	2,220,819,602,560,918,840	49,347,193,044,659,701	1.023	45.028
10^{21}	21,127,269,486,018,731,928	446,579,871,578,168,707	1.022	47.332
10^{22}	201,467,286,689,315,906,290	4,060,704,006,019,620,994	1.021	49.636
10^{23}	1,925,320,391,606,803,968,923	37,083,513,766,578,631,309	1.020	51.939

Here are the 168 primes under $1,000$:

2 3 5 7 11 13 17 19 23 29 31 37 41 43 47 53 59 61 67 71 73 79 83 89 97 101 103 107 109 113
127 131 137 139 149 151 157 163 167 173 179 181 191 193 197 199 211 223 227 229 233 239
241 251 257 263 269 271 277 281 283 293 307 311 313 317 331 337 347 349 353 359 367 373
379 383 389 397 401 409 419 421 431 433 439 443 449 457 461 463 467 479 487 491 499 503
509 521 523 541 547 557 563 569 571 577 587 593 599 601 607 613 617 619 631 641 643 647
653 659 661 673 677 683 691 701 709 719 727 733 739 743 751 757 761 769 773 787 797 809
811 821 823 827 829 839 853 857 859 863 877 881 883 887 907 911 919 929 937 941 947 953
967 971 977 983 991 997

Some gaps are quite large; copied from:
`http://www.dms.umontreal.ca/~andrew/PDF/cramer.pdf`

p_n	$p_{n+1} - p_n$
31397	72
370261	112
2010733	148
20831323	210
25056082087	456
2614941710599	652
19581334192423	778

Prof. Dr F. Oort
Mathematisch Instituut
Pincetonplein 5
3584 CC Utrecht NL
The Netherlands
email: f.oort@uu.nl