About Different Kinds of Proofs Encountered Specifically in Arithmetic

Fermat's Little Theorem

Martine BÜHLER, Anne MICHEL-PAJUS

Université Paris VII, Case 7018, 2 place Jussieu, 75 251 Paris Cedex 05, France

Annie.pajus@club-internet.fr, iremmath@yahoo.fr

Abstract

One of the interesting aspects of arithmetic is that mathematical proofs can be constructed without needing a large theoretical arsenal. These proofs are supported by reasoning of a certain subtlety, playing with the notions of infinity and the absurd, and hence non-trivial results can be obtained. This reasoning is easily accessible intuitively because it relates to the integers, giving arithmetic a specific formative character to students undergoing their apprenticeship in proof.

The history of mathematics offers us a large choice of proofs, some more formal, some less, some further from intuition, some closer. We have, moreover, commentaries by mathematicians regarding the elegance or the rigour of certain of these proofs, to which we can refer.

The corpus of texts we have chosen for reading revolves around "Fermat's Little Theorem" which is part of the final programme in secondary school. The basic theoretical baggage is then limited to a single property which appears in different forms — Euclid's Lemma, Gauss' Theorem, The Fundamental Theorem of Arithmetic — according to one's point of view and to the context. The essential core of these methods of proof also manifests itself in different forms (infinite descent, the principle of recursion, the use of the smallest integer in a set of integers).

We shall set out the principal points of our analysis, supported by the reading of original excerpts. A detailed article [7], including all the source texts, is available on the IREM site
http://iremp7.math.jussieu.fr/

1 Introduction

1.1 Our working group

It is called **M.:A.T.H.**, which stands for **M**athematics**:** An **A**pproach through **Texts** from **H**istory. It is composed by Alain Bernard, Martine Bühler, Philippe Brin, Renaud Chorlay, Odile Kouteynikoff, and Anne Michel-Pajus, and works within **IREM** (Institute for the Research in Mathematics Education) in the University of PARIS7 Denis Diderot.

We are engaged in In-Service training for teachers of mathematics in secondary school, through organizing:

- short training sessions (2 or 3 days)
- an open group for collective reading of historical sources, presentations, discussions.

and publishing:

- The **Brochures M.:A.T.H:** collections of tested activities for students at secondary schools, using historical sources. One example will be given at the end of this workshop.
- **Re-editions of old texts**, some of which can be difficult to find.
- **Mnémosyne**, a journal whose objective is to give an opportunity for teachers to share their experiences and to provide food for thought across all areas concerning the history of mathematics.

The No 19 is dedicated to Arithmetic. Many related articles may be found in it.

1.2 The subject: arithmetic. Why did we choose it?

Arithmetic, which was present in the curriculum set out in 1971 and disappeared for twenty years at the start of the eighties, has returned, as much in the college curriculum (Euclid's algorithm) as in the last year of secondary school, for students majoring in mathematics.

More precisely:

- In the 3rd grade (students 15 years old) :Euclid's algorithm and GCD (on given numbers).
- In the 2nd grade (16 years): decomposition in prime numbers and GCD (on given numbers).
- In the 1st grade nothing!
- In Terminale (age 18 years, only for students majoring in mathematics).

Congruence (modular arithmetic); GCD; Gauss and Bézout's Theorems.

Applications to Diophantine equations, cryptography, and Fermat's "Little"Theorem.

Note that this curriculum is intended only for those students more interested in mathematics.[1]

Arithmetic has interesting pedagogical characteristics. We work with those familiar objects, the integers, obtaining non trivial but readily comprehensible results, which can be tested or discovered by experiment, but we deal with multiple, unusual, complex arguments.

Some teachers were never taught arithmetic at Secondary School, and studied only "the theory of numbers" at University. None of the attendees at this workshop, coming from Belgium, China (Hong-Kong), Israel, Italy, France, Portugal, United States, had ever been taught arithmetic in secondary school. It seems it is no longer taught in secondary School, except in France.

So we use mathematical sources, and to be more precise, use the comparison between three different proofs or of Fermat's Little Theorem, in order to give the teachers an opportunity to recall some past learning, to think more deeply about the issues involved, to better structure their knowledge, and to acquire a metaknowledge[2]

This theorem is encountered in two equivalent forms.

- If p is a prime and a an integer which is not divisible by p, then p divides $a^{p-1} - 1$.
- If p is a prime and a any integer, then p divides $a^p - a$.

It is stated without proof by Fermat in his correspondence (in particular, in a letter to Frénicle of 16 October 1640).[3]

[1] All secondary school French programs, with commentaries, are found online at http://www.eduscol.education.fr.

[2] About metaknowledge, see, for instance: Groupe de travail "Math & Méta" 1990–1992. M. Baron, A. Robert (ed.) Cahier DIDIREM, numéro spécial mai 1993, IREM Paris 7.

[3] An early proof is found in Leibniz's manuscripts, but it was published only in 1863. You can find it in Mnémosyne 19.

2 A classification of the tools used in the proofs

As a basis for discussion, we establish a classification of the tools used in the proofs[4]. These items will be better understood after reading the historical sources.

Beyond the simple properties of divisibility (e.g. if an integer a divides both b and c, then a divides the sum $b + c$) and the Euclidean Algorithm, the theoretical arsenal reduces to a single fundamental result, found in diverse equivalent forms throughout history.

- Euclid's Proposition 32 called "Euclid's Lemma": if a prime number divides a product, then it divides one of the factors of the product [2]. This is also encountered in the contrapositive form — if a prime number p divides neither a nor b, then it does not divide the product ab.
- Euclid's Proposition 26: If two numbers a and b are relatively prime to c, the product ab is also relatively prime to c.
- Gauss's Theorem: If a number divides a product and is relatively prime to one of the factors of the product, then it divides the other.

The following is not found in the proofs studied here:

- The Fundamental Theorem of Arithmetic: the decomposition of an integer into a product of prime factors is unique. (Note that the fundamental theorem often refers to the existence of the decomposition as well. This does not concern us here.)

These four theorems are logically equivalent[5].

We have also attempted to classify the methods we have met in the mathematical proofs studied. They are of two types:

Pigeonhole methods

- The pigeonhole principle: The use of a finite number of pigeonholes to hold a strictly larger number of objects. Thus at least one pigeonhole must contain at least two objects. This result is called the "pigeonhole principle" or the "Dirichlet principle".
- Disjunction of cases: The situations studied are partitioned into a number of cases which are then examined exhaustively. This is the method of "disjunction of cases".
- The bijection method: Set up a bijection between two finite sets of the same cardinality.

Staircase methods

- Finite descent: a finite descent arriving at a suitable integer which provides the conclusion either directly or by recourse to absurdity.
- Fermat's method of infinite descent: a descent which carries its own contradiction in itself as it represents a set of strictly decreasing positive integers.
- Argument by recurrence (complete induction)
- The least integer method: this reasoning uses the least element of a non empty subset of A.

The last three methods are logically equivalent.

[4] We have actually analysed a larger corpus of proofs than the ones shown in this paper. For more examples, see Mnémosyne 19 or [7]

[5] For a proof, see Mnémosyne 19 or [7].

3 Reading some proofs

3.1 Euler (First proof) and Legendre

The first published proof, in 1736, is due to Euler. He takes up the same idea in 1747, an idea taken again in Legendre in his "Théorie des Nombres" (Number Theory) of 1798 [5].

Let's begin by reading the proof by Legendre[6]:

Theorem. "If c is a prime number, and N any number not divisible by c, I state that the quantity $N^{c-1}-1$ will be divisible by c, so that we will have $\frac{N^{c-1}-1}{c}$ = an integer$^{(1)}$."

Let x be any integer. If we consider the known formula $(1+x)^c = 1 + cx + \frac{c(c-1)}{1\cdot 2}x^2 + \frac{c(c-1)(c-2)}{1\cdot 2\cdot 3}x^3 + \ldots + cx^{c-1} + x^c$, it is easy to see that all the terms of this series, with the exception of the first and the last, are divisible by c.

Indeed, letting M be the coefficient of x^m, we will have

$$M = \frac{c(c-1)(c-2)(c-3)\ldots(c-m+1)}{1\cdot 2\cdot 3\ldots m},$$

or

$$M\cdot 1\cdot 2\cdot 3\cdot \ldots \cdot m = c(c-1)(c-2)(c-3)\ldots(c-m+1);$$

and since the second part is divisible by c, the first part must also be. But the exponent m, in the terms in question, does not exceed $c-1$. So c, which is supposed prime, cannot divide the product $1\cdot 2\cdot 3\ldots m$; thus it must divide M for every value of m from 1 to $c-1$. Thus the quantity $(1+x)^c - 1 - x^c$ is divisible by c, for any integer x at all.

Now let $(1+x) = N$; the preceding quantity will become $N^c - (N-1)^c - 1$, and, since it is divisible by c, if we omit the multiples of c, we will have $N^c - 1 = (N-1)^c$, or $N^c - N = (N-1)^c - (N-1)$. But, on substituting $(N-1)$for N, and always neglecting the multiples of c, we will similarly have $(N-1)^c - (N-1) = (N-2)^c - (N-2)$. Continuing thus from equal remainders to equal remainders, we will necessarily arrive at the remainder$(N-N)^c - (N-N)$, which is obviously zero. Hence all the preceding remainders are zero; so $N^c - N$is divisible by c.

But $N^c - N$ is the product of N with $N^{c-1} - 1$; thus since N is supposed to be not divisible by c, $N^{c-1} - 1$ must be divisible by c; which is what was to be proven.

*****

$^{(1)}$ This theorem, one of the principal ones of number theory, is due to Fermat; it has been proved by Euler in various places in the *Petersbourg Memoirs*.

The main tool is the binomial expansion. Euclid's Lemma is used in the 2nd paragraph. It comes into the result via the divisibility of the binomial coefficients by a prime p.

The method used for the conclusion is a finite descent of equalities arriving at the suitable integer 0. Note the words " by omitting the multiples by c", a pre-notion of congruence.

In the original proof, Euler too uses the binomial expansion, and Euclid's Lemma. As he doesn't use "omitting the multiples of c", the proof is much longer. The conclusive method is somewhat different:

[6] Working translation from the original French edition, by Stuart Laird.

Corollary 2. [...] if we suppose that the form $a^p - a$is divisible by p, the form $(a+1)^p - a - 1$ is also divisible by p; in the same way, under the same hypothesis, this form $(a+2)^p - a - 2$ and so on $(a+3)^p - a - 3$ etc., and generally $c^p - c$, will be divisible by p.

Théorème 3. If p is a prime, every number like $c^p - c$ will be divisible by p.
If we take $a = 1$, as $a^p - a = 0$ is divisible by p, it follows that the forms $2^p - 2$, $3^p - 3$, $4^p - 4$ etc. and generally this one $c^p - c$ will be divisible by the prime p. Q.O.D.[7]

Here we find a complete induction although we would make it shorter today. As if this method was not well accepted, Euler gives more numbers than are necessary, as we sometimes do with our students.

We have a third formulation of this proof, concisely explained by Gauss in his "Arithmetical Researches" in 1801 [4]. It is very close to Euler's one. Note that he doesn't explain the first part of the proof, but details the induction.

This theorem, remarkable as much for its elegance as for its great utility, is usually called Fermat's Theorem after the name of its discoverer. [...] Fermat did not give a proof of it, although he was definite that he had found one. Euler gave the first in a dissertation entitled "Proofs of some theorems relating to prime numbers". [...] It rests on the expansion of $(a+1)^p$. From the form of the coefficients it can be seen that $(a+1)^p - a^p - 1$ is always divisible by p; so, as a consequence, $(a+1)^p - (a^+1)$ will be also divisible by p if $a^p - a$ is. Now as $1^p - 1$ is divisible by p, $2^p - 2$ will be, consequently $3^p - 3$, and generally $a^p - a$. Thus, if p does not divide a, we will have $a^p - a$ is divisible by p also. What is just given suffices to make the spirit of the proof known.[8]

3.2 TANNERY

A new, very concise proof is found in the lectures given by Jules Tannery at the Ecole Normale Supérieure. His students Emile BOREL and Jules DRACH gave it in [1] in 1894.

In the case where m is a prime number p, each number not divisible by p is prime to this number: so, if in the expression ax, where a is not divisible by p, one substitutes $p-1$ numbers x which are mutually not congruent to each other and to $0 \pmod p$, one will obtain $p-1$ numbers congruent to these same numbers $x_1, x_2, \ldots, x_{p-1}$ set out in another order. The product of the numbers $ax_1, ax_2, \ldots, ax_{p-1}$ is thus congruent $(\mathrm{mod}\, p)$ to the product $x_1 x_2 \ldots x_{p-1}$, and as the last product is prime to p, one concludes $a^{p-1} - 1 \equiv 0 \pmod p$.

This is the celebrated *theorem of Fermat*, which plays an essential role, in number theory, and we will incidentally meet other proofs of. Observe that it can be immediately deduced from the following proposition: *For any integer a and prime number p whatever, we have* $a^p - a \equiv 0 \pmod p$.

This proof rests on the bijection method. It reveals the power of the pigeonhole principle, a principle which appears so self evident, and which is here utilized by its avatar, the bijection principle, in setting up a bijection between two sets of the same cardinality. This method avoids recourse to infinity and to recurrence.

The Fundamental Theorem of divisibility is necessary in order to show that the ax_1, ax_2, ..., ax_{p-1} are all different and different from $0 \pmod p$. But the rules of modular arithmetic avoid its explicitation. Tannery's proof is seductive and elegant by means of its brevity and the magisterial way it uses congruence.

[7] Working translation from the original latin edition, by A. Michel-Pajus.
[8] Working translation, from the french edition, by Stuart Laird.

This proof is found in the document accompanying the Terminal S syllabus. The advantage of using this proof in class is that, even if more than six lines of Tannery are necessary for our Terminal students' understanding, by the end of our efforts the proof can be understood in its totality without forgetting the premises or losing the logical flow.

3.3 Euler (Second proof) and Gauss

In 1758 [2], Euler published an entirely different proof of Fermat's Theorem that appeared, a priori, more complex than the first, and into which we shall go later on. Euler utilized a classification of integer powers according to their remainder on division by the prime p. The method consists of partitioning the set under consideration into a finite number of pigeonholes until it is exhausted, coupled with the use of the least element of a non empty set. At base the theorem rests on Euclid's Lemma. It is this proof that Gauss takes up in his "Arithmetical Researches" of 1801, but in a simpler form due to the language of congruence, and the use of Gauss's Theorem that he proves in the same book.

Why did Euler and Gauss choose a proof that is a priori much more complicated?

Gauss takes up the explanation given by Euler himself: "the binomial expansion seems to be a stranger in number theory". The new proof respects the "purity of arithmetic".

We give here a summary on the proof[9].

Before entering on the proof of the theorem itself, Euler explored the remainders of the powers of 7 modulo 641.

After experimenting with particular powers, Euler took up his exploration of the general case. Recall that, given a prime p and a number a not divisible by p, it is a question of showing that the remainder of the division of a^{p-1} by p is 1. The idea developed by Euler is to "classify" the powers of a according to the $(p-1)$ non null possible remainders modulo p. We summarize the steps of the proof below.

Euler begins by showing that there exist powers of a with remainder 1: indeed, the series $a, a^2, a^3, \ldots, a^\lambda, \ldots$ being infinite, and the number of possible non null remainders of the divisions modulo p being finite and equal to $(p-1)$, there exist powers a^λ and a^μ with $\lambda < \mu$, having the same remainder on division by p. Thus the prime p divides $a^m - a^\lambda = a^{\mu-\lambda}(a^\lambda - 1)$. As the prime p does not divide $a^{\mu-\lambda}$, p divides $a^\lambda - 1$, and the remainder of the division of a^λ by p is certainly 1.

Now consider the smallest, strictly positive integer λ, having this property (the remainder of the division of a^λ by p is 1). Then the λ powers $1, a, a^2, a^3, \ldots, a^{\lambda-1}$ are all different, non null remainders in the division by p. If not, the preceding argument gives an integer λ' such that p divides $a^{\lambda'} - 1$, which has been excluded. If all the $(p-1)$ possible remainders modulo p are obtained, then $\lambda = p - 1$ and the theorem is proved.

If not, let r be one of the non null remainders which has not been obtained. Note that r is prime to p. Consider the λ numbers $r, ra, ra^2, ra^3, \ldots, ra^{\lambda-1}$; these numbers are all the different remainders obtained in the p (if not p would divide $ra^\nu - ra^\mu = ra^{\nu-\mu}(a^\mu - 1)$ and thus $a^\mu - 1$ with $\mu < \lambda$). In the same way, ra^μ et a^ν cannot have the same remainder; if so, p divides $r - a^{\nu-\mu}$ which contradicts the fact that r has not been obtained as a remainder in the division of a power of a by p. If we add these remainders to the preceding, we thus obtain 2λ different, non null remainders modulo p. If we have all of them $(p-1) = 2\lambda$.

If not, consider a remainder s which has not been obtained yet and the numbers s, sa, sa^2, sa^3, $\ldots$, $sa^{\lambda-1}$. In the same way we can show that all of these numbers have different remainders from those obtained before. If all the possible non null remainders have been obtained, $p - 1 = 3\lambda$.

[9] The proof by Euler can be found in English on the web.

If not, we continue... As the number of remainders is finite, the procedure must terminate. When all the possible remainders have been obtained, the same argument proves that there exists an integer t such that: $p-1=t\lambda$.

Then $a^{p-1}-1=a^{t\lambda}-1=(a^{\lambda})^{t}-1$. Now $x^{t}-1$ is divisible by $x-1$ for every integer x, as $x^{t}-1=(x-1)(x^{t-1}+x^{t-2}+\ldots+x+1$. Thus $a^{p-1}-1$ is divisible by $a^{\lambda}-1$. As p divides $a^{\lambda}-1$, p divides $a^{p-1}-1$ also and the theorem is proved.

In modern terms, this argument comes back again by making a partition of the multiplicative group $(Z/pZ)*$ formed from the equivalence classes according to the cyclic subgroups generated by a. This type of idea allows Lagrange's Theorem to be proved: the order of a subgroup of a finite group divides the order of this group. Or inversely, by using the Lagrange's theorem, we find the classical proof of the Fermat's Little Theorem taught at University.

But the interest of this proof not only lies in opening the way for subsequent developments; in spite of its complexity, it also appears relatively natural, resulting from an experimental exploration of the powers of a number.

This point of view returns us to the beginning, for it was in terms of powers that Fermat had stated his theorem in his letter to Frénicle of 18 October 1640.

3.4 Fermat's Letter

It seems to me, after that, it is necessary to talk to you of the foundation upon which I base the proofs of everything concerning geometric progressions.

Every prime number infallibly measures [divides] one of the powers minus 1 of some progression or other, and the exponent of the said power is a factor of the prime number –1. After the first power that satisfies the question has been found, all those whose powers are multiples of the exponent of the first will satisfy the question in the same way.

Example: let the given progression be

1	2	3	4	5	6
3	9	27	81	243	729

etc. with its exponents below.

For example, take the prime number 13. It measures the third power minus 1, of which the exponent, 3, is a factor of 12, which is one less than the number 13, and because the exponent of 729, which is 6, is a multiple of the first exponent, which is 3, it follows that 13 also measures the said power $729-1$.

And this proposition is generally true for all progressions and all prime numbers. I will send you the proof of this, unless I fear it to be too long.

The point at issue here seems to be working with the powers of an integer. And the result is more precise than that generally called "Fermat's Theorem", since it is concerned with the smallest integer n such that the prime p divides $a^{n}-1$. One would love to know the path Fermat's thought took in order to arrive at what he called "The foundation on which I support the proofs of everything concerning geometric progressions."

4 Commentaries and complements[10]

4.1 About Gauss's Theorem and modular arithmetic

It is well known that the book by Gauss: *Disquisitiones arithmeticae* (1801) played a central role in the development of arithmetic. Euler and Legendre follow the euclidean tradition, even if Legendre gives a new proof of Euclid's Lemma in his *Theorie des Nombres* (1798).

[10] for any detail and reference, see [7]

Actually, Gauss was not the first in publishing the Gauss's Theorem. We find it in *Les Nouveaux elements de Mathematiques* by Jean Prestet, 2nd edition, 1689. This book caused little stir because mathematicians at this time were more interested in "Infinitesimal Analysis" than in "Finite Analysis".

Anyway, Gauss began to work on the subject in 1795 "with no idea about what have had done on the subject", as he explains in his preface. He begins (Section I) by establishing the theory of congruence, then (Section II) Gauss's theorem, proved with the method of the least element and an argument by absurdity. He explains why he proves this theorem: " The proof of this theorem was given by Euclide, El.VII,32. But we didn't want to omit it, inasmuch as many modern authors have presented vague reasoning instead of a proof, or have neglected this theorem; in order to give a better understanding, in this very simple case, of the spirit of the method we will use later for very difficult points." Then, Gauss proves the uniqueness of the decomposition into prime numbers. He studies the remainders of the powers in Section III (here we find the proof of Little Fermat's Theorem).

He set up all the tools. However, it is doubtless not by chance that a century was needed after the publication of Gauss's book in order for the Tannery's proof to appear, as brief as it is striking. All this time was necessary for the theory of congruence, used implicitly by Legendre in 1798, then formalized by Gauss in 1801, to dominate completely arithmetic.

For teachers (and maybe for students) it is useful to prove the logical equivalence of the different forms of the Theorem of divisibility.

The syllabus of Terminale S includes Bézout's Theorem. This theorem is stronger than our fundamental theorem of divisibility. Its principle is given by Bachet in *"Problèmes plaisants et délectables"* (1624), et taken again by Bézout in his *"Cours d'Algèbre"* (1766). However, we didn't encounter it in our authors.[11]

4.2 About the methods

The pigeonhole method is an elementary principle which students understand immediately, but would never think of using themselves. We can show them that this principle allows prooving of non-trivial results.

Disjunction of cases is very useful when working modulo an integer. When students have well understood its validity, it is greatly appreciated by certain students who use it spontaneously to solve certain exercises.

The diversity of staircase methods is worth examining more deeply. From an historical and epistemological point of view, we can question the fact that the mathematicians use one or the other.

The method of complete induction is generally attributed to Pascal, even if we could find it earlier (in Maurolycus, for instance)[12]. However, its use is not yet that natural and usual in Euler' and even in Gauss's time.

The complete induction is part of the curriculum, not that easy to appropriate for students.

Fermat prefers its method of infinite descent, but it is strongly criticized by Wallis and others. Later on, Euler and Gauss avoid it , though they read very Fermat carefully. Finite descent avoids recourse to the infinite, often at the cost of an argument by absurdity. (This is not the case with Legendre). Moreover, the method of finite descent translates directly into useful algorithms .

The least integer method too, avoids infinity, often with recourse to absurdity. It has a concise and smart appearance. At the tertiary level, students really like it.

[11] See [9].
[12] See [13].

In line with the objective of training in logic, it is interesting to prove the equivalence of the three staircase methods[13].

4.3 A HOMEWORK ASSIGNMENT

This study of the history of mathematics shows us, for instance, the interest in exploring the powers of a given integer before going on to further developments in Analysis. For our students, it is also interesting to see that even great mathematicians experiment

As an example, we give a homework assignment here, which uses the beginning of the second proof by Euler. It allows us to check students' understanding of congruence. Question I.5 is a very classical question.

"In an article published in 1758, Euler was interested in the remainders of powers of 7 modulo 641."

Preamble: Read the text below and check all of Euler's calculations. Write down all the necessary calculations on your paper. Are all of Euler's calculations necessary to obtain the remainder of 7^{160}? Justify your answer.

"So here is a very rapid method of finding the remainders arising from the division of any power of any number. For example, if we want to find the remainder arising from dividing 7^{160} by the number 641

Powers	Remainders
7^1	7
7^2	49
7^3	343
7^4	478
7^8	288
7^{16}	255
7^{32}	284
7^{64}	-110
7^{128}	-79
7^{160}	-1

Indeed, since the first power 7 gives the remainder 7 the powers $7^2, 7^3, 7^4$ give 49,343, and 478, i.e. -163, whose square 7^8 gives the remainder 163^2 i.e. 288, and the square of which 7^{16} gives the remainder 288^2, i.e. 255. Similarly, the power 7^{32} gives the remainder 255^2 i.e. 284 and the remainder of the power 7^{64} will be -110 and from 7^{128} comes 110^2 i.e. -79, a remainder which multiplied by 284 will give the remainder of $7^{128+32} = 7^{160}$ which will be 640 i.e. -1.

Thus we know that, if the power 7^{160} was 641, the remainder would be 640 i.e. -1, from which we conclude that the remainder of the power 7^{320} is $+1$. Thus, in general, the remainder of the power 7^{160n} divided by 641 will be either $+1$ if n is an even number, or -1, if n is an odd number."

PART 1: A STUDY OF EULER'S TEXT

1. Justify the replacement of 478 by -163 and explain the practical interest of this step.
2. Quote the course result used to calculate the remainder of 7^8.
3. Justify the result given for the remainder of the division 7^{320} by 641 as well as that of the division of 7^{160n} by 641?
4. What is the remainder of the division of 7^{320n} by 641? By using Euler's results without any additional calculations, determine the remainder of the division of 7^{648} by 641.
5. Call r_N the remainder of the division of 7^N by 641. Show this sequence is periodic. From this deduce a method to simplify the calculation of the remainders of the division 7^N by 641.

[13] See [7].

Part II: And for cases other than 641?

1. Calculate the remainders of $7, 7^2, 7^3, 7^4, 7^5, 7^6, 7^7$ under division by 63.
2. Show that the sequence (r_N) of remainders of division by 7^N (for N a strictly positive integer) by 63 is periodic. What is the remainder of the division of 7^9 by 63?
3. Consider a strictly positive integer m. Is the sequence of remainders of the division of 7^N by m always periodic?
4. Euler stated that the remainder of the division of 7^{320} by 641 is equal to 1. Does there exist a strictly positive integer h such that the remainder of the division of 7^h by m is equal to 1 for all strictly positive integers m?

Justify your answers to questions 3 and 4 carefully.

References

Primary Sources

[1] BOREL Emile et DRACH Jules, 1894, *Introduction à l'étude de la Théorie des Nombres et de l'Algèbre*, d'après les conférences de Jules Tannery à l'Ecole Normale Supérieure. Paris : Librairie Nony et Cie.

[2] EULER Leonhard, 1761, "Theorems on residues obtained by the divisions of powers" online at http://front.math.ucdavis.edu (arXiv). Latin ed. in *Nouveaux mémoires de l'Académie de Saint Petersbourg*, T. 7 (1758/9, p. 49–82).

[3] FERMAT Pierre de, 1896, *Œuvres*, T. II et III, Tannery et Henry (ed.). Paris.

[4] GAUSS Friedrich, 1979, *Recherches Arithmétiques*, Traduction Poullet-Delisle. Paris : Courcier 1807. Réédition Paris : Blanchard, (latin edition: *Disquisitiones Arithmeticae*, 1801, available at http://gallica.bnf.fr).

[5] LEGENDRE André-Marie, 1955, *Théorie des Nombres*. Paris : Firmin-Didot, 1830. Réédition Paris : Blanchard.

[6] PRESTET Jean, 1675, *Eléments des Mathématiques*. Paris : André Pralard, (Second ed. 1689).

Secondary Sources

[7] BÜHLER Martine et MICHEL-PAJUS Annie, 2007, "Sur différents types de preuves rencontrées spécifiquement en Arithmétique", in *Mnemosyne* 19, Paris : IREM Paris 7. On line http://iremp7.math.jussieu.fr/

[8] BATTIE Véronique, 2004, *Spécificités et potentialités de l'Arithmétique élémentaire pour l'apprentissage du raisonnement mathématique* (Thèse). Paris : IREM Paris 7.

[9] CHABERT Jean-Luc, et al, 1999, *Histoire d'algorithmes*. Paris : Belin, 1994. Trad. *A History of Algorithms*, Berlin : Springer.

[10] Commission inter I.R.E.M. Histoire et Epistémologie des Mathématiques 1993, *Histoires de problèmes Histoire des Mathématiques*. Paris : Ellipses. Trad. *History of Mathematics, Histories of problems*, Paris : Ellipses, 1997.

[11] GOLDSTEIN Catherine, 1995, *Un théorème de Fermat et ses lecteurs*, Presses Universitaires de Vincennes.

[12] GOLDSTEIN Catherine, 1992, "On a Seventeeth Century Version of the "Fundamental Theorem of Arithmetic" ", *Historia Mathematica*, p. 177–187.

[13] M. GUILLEMOT, 1993, "En route vers l'infini". In *Histoires de problèmes, histoire des mathématiques*. Paris : Ellipses, p. 7–32. *History of Mathematics, Histories of problems*, Ellipses, Paris, 1997.

[14] I.R.E.M. Groupe Epistémologie et Histoire, 1987, *Mathématiques au fil des âges*. Paris : Gauthier-Villars.

[15] PERRIN Daniel, 1981, *Cours d'Algèbre pour l'Agrégation*. Paris : Editions ENSJF.

Many thanks to Pam and Stuart LAIRD for their help in translating.