IMVI
Open Mathematical Education Notes
Vol. 2 (2012), 23–37

ISSN 1840-4383

DIDACTIC NUMBER THEORY AND GROUP THEORY FOR SCHOOL TEACHERS

Jaska Poranen
University of Tampere, Finland
Jaska.Poranen@uta.fi

Pentti Haukkanen*
University of Tampere, Finland
Pentti.Haukkanen@uta.fi

Abstract

The purpose of this article is to present a connection between school and university mathematics. We examine infinite periodic (non-pre-periodic) decimal expansions of rational numbers with mathematical rigor by using the university-level Number Theory and Group Theory. We will find there connections to various concepts and results concerning the multiplicative group modulo m. We illustrate and concretize our considerations, and propose some preliminary task ideas for all school levels. We also describe how the didactic mathematics programs are organized at the University of Tampere, Finland. We present the mathematical background needed in this subject in Appendix section at the end of the paper.

AMS Mathematics Subject Classification (2010): 97D40, 97F40, 97H40

Key words and phrases: long division, decimal expansion, multiplicative group modulo m, didactic mathematics, connection between school and university mathematics

1. Introduction

Transforming a rational number a/b into an integer, decimal fraction or infinite periodic decimal expansion is a very common activity at school. For example

(i) $\dfrac{10}{5} = 2$

(ii) $\dfrac{3}{5} = 0.6, \quad \dfrac{3}{40} = 0.075$

(iii) $\dfrac{4}{9} = 0.444\ldots = 0.\overline{4}, \quad \dfrac{1}{7} = 0.142857142857\ldots = 0.\overline{142857}$

(iv) $\dfrac{1}{6} = 0.1666\ldots = 0.1\overline{6}, \quad \dfrac{7}{30} = 0.2333\ldots = 0.2\overline{3}$
(pre-periodic, i.e., the period does not begin immediately).

Transforming a fraction of type (iii) into an infinite periodic expansion seems to be quite a negligible, mechanical, boring, and insignificant event in school mathematics. However, it includes an almost endless number of quite captivating features. At all school levels teachers would do well to maintain some researcher's mind and inquisitiveness. This, if anything, could have an important transfer effect on the pupils. Our approach is just one of numerous

*Corresponding author.

possibilities where the teacher together with the pupils can take an in-depth look at phenomena. Today the teacher must also have a general view of what is studied and how students carry out studies at the different school levels, no matter what his or her own teaching position in the school system is. With the help of our approach he or she can do at least a little wandering along the timeline of the curricula from the primary school to the upper secondary school—or even further.

We will examine (iii) with mathematical rigor by using the university-level Number Theory and Group Theory. We will find there connections to the Euler totient function, congruence, reduced residue system modulo m, subgroups of groups, cosets, cyclic groups, order of an element in a group, and Lagrange's theorem. First, however, we illustrate and concretize our considerations, and propose some preliminary task ideas for different school levels. But, first of all, we would also like to describe the didactic mathematics programs at the University of Tampere, Finland, which has provided the inspiration for our approach.

Since we completed our research we found that Brenton [4] has also written on decimal expansions and group theory. Our approach is, however, different from that of [4].

2. Didactic mathematics at the University of Tampere

At our University of Tampere some particular student groups are allowed to carry out their 60 credits studies in mathematics as so-called didactic mathematics, i.e.,

- The Master's degree students in the School of Education whose major subject is education and obligatory minor subject mathematics.
- Students in the primary school teacher program.
- Since the autumn of 2010 also the students majoring in mathematics who are going to take the teacher's pedagogical studies. This possibility is restricted to the course of geometry.

Our Secondary Teacher Education Unit in the School of Education has been mainly responsible for the implementation of the basic studies (25 credits) included in the 60 credits. The basic studies have been made up of *Analysis for Teachers* 8 credits, *Geometry* 6 credits, *Number Theory and Algebra for Teachers* 7 credits, and *Learning Mathematics* 4 credits. These courses have been arranged in cycles of two years, one course per each term. Curricula for the courses can be found in [2]; unfortunately only in Finnish. The remaining part (35 credits) of the studies has been arranged in the ordinary teaching program in the subject of mathematics and statistics in the School of Information Sciences which bears the final responsibility for the entirety of didactic mathematics, too.

The Secondary Teacher Education Unit has interpreted the didactical emphasis in the university mathematics course as covering the following three points: accommodating the course contents to school mathematics as well as possible; using such teaching methods and ways of approaching which coach the students to use similar ones in their teaching profession—remembering, of course, the different stages of the pupils' lives; and, thirdly, aiming at a rich and many-sided view of mathematics in school and university mathematics alike (cf. [8]). In this article our focus is mainly on the third point, and our approach comes from the course "Number Theory and Algebra for Teachers".

Through the group concept the school teacher is able to attain a concise picture of many counting structures, take for example the integers or vectors with addition. It has an analogous meaning as a part of the ring and field structures which appear in many places at school

as well. On the other hand, the existence of these "too familiar" models may not motivate the teacher student enough into the studying of even elementary university algebra. However, we have now developed and attached to the group concept a school significance which is not immediately perceptible but which, in fact, is present in the early stages of school mathematics. This is an example of hidden mathematics curriculum, an important notion originally introduced in [1].

3. Concretizing of our approach

In type (iii) the decimal expansion does not terminate, it repeats over and over its period—a string of digits; the period also begins immediately after the decimal point (in Finland, however, we use a comma, not a point, for this purpose; we have also used a bar to indicate the pattern of repeating digits). Generally, we now first make the natural assumptions that $1 \leq a < b$, and that we have a canceled form, i.e., $\gcd(a, b) = 1$, where gcd stands for the greatest common divisor; in addition we assume that $\gcd(b, 10) = 1$. In what follows, these assumptions will always be valid.

Example 1. By the long division we attain $1/7 = 0.142857142\ldots = 0.\overline{142857}$. Behind this method there is the division algorithm, one of the basic tools in number theory. Let us first write $1 = 7 \cdot 0 + 1$; hence we have the first term 0 of the quotient (the whole part of the quotient). The first remainder 1 is equal to 10 tenths; so by writing $10 = 7 \cdot 1 + 3$, we get the next term 1, one tenth, of the quotient. The second remainder 3 (tenths) is 30 hundredths, so we have to write $30 = 7 \cdot 4 + 2$ to get the 4 hundredths in the quotient, etc. The remainders are 1, 3, 2, 6, 4, 5 (in this order)—and then again there is the remainder 1, etc. By the division algorithm, the only possible remainders are 1, 2, 3, 4, 5, or 6 (if 0 were there, the division would terminate). So there must be some recurrence or periodicity. In this example we get the "theoretical maximum length" $7 - 1$, and the period is made up of the digits 1, 4, 2, 8, 5, 7, in this order. The division $1/7$ can be illustrated—at least to some extent—by imagining the apportioning of one-meter-long pizza to seven sisters. Each sister gets one tenth, four hundredths, two thousandths, etc., of the pizza. In fact, the apportioning never ends in the "mathematical world". If the sisters eat their portions as they get them they can eat endlessly, only the portions become smaller and smaller; if they wait for the end of the apportioning they can starve to death.

It follows easily from the division algorithm that generally the length of the (shortest) period of a/b in the long division is at most $b - 1$, because the possible remainders by dividing with b are $1, 2, \ldots, b - 1$. So in the case of $1/7$ we have the maximal length of period, but in the case of $4/9 = 0.444\ldots$ we stay far away from it. Some outer features of the long division have changed many times during the lives of the writers but the division algorithm has not changed and never will.

Studying the lengths of the periods opens up quite interesting views. For example in the case of $a = 1$ and $b = 21$, we have $1/21 = 0.047619047619\ldots = 0.\overline{047619}$, so the "theoretical maximum" $21 - 1$ is not achieved. The length λ of the periodicity is 6. The divisor 21 is not a prime number whereas 7 is. Does this explain the difference? Not exactly, for example, $1/11 = 0.0909\ldots$, so, $\lambda = 2$ (only), despite the fact that 11 is a prime number. We will later demonstrate conclusively that the length λ of the period in the case of (iii) is always a factor of the Euler totient function's value $\phi(b)$ at b.

The Euler totient function $\phi(b)$ counts the number of the integers $1 \leq k \leq b$ for which $\gcd(k, b) = 1$. So, for example, $\phi(7) = 6$, and $\phi(21) = 12$. If b is small enough we just have to write down the integers $1, 2, \ldots, b$, and then delete those integers k for which $\gcd(k, b) > 1$. After that, we simply have to count the number of the integers which are left over. We will later also give a formula by which the value of $\phi(b)$ can be calculated. Most symbolic calculation software have a command for $\phi(b)$. For example, *Wolfram Alpha* is an excellent free on-line tool.

The number $\phi(21) = 12$ gives the order (cardinality) of the multiplicative group modulo 21, too. In fact, the set $\mathbb{Z}_{21}^{\times} = \{1, 2, 4, 5, 8, 10, 11, 13, 16, 17, 19, 20\}$ constitutes the multiplicative group modulo 21. The set $\mathbb{Z}_{21}^{\times}$ is the same as the set of all possible dividends in the case of $a/21$. Similarly, $\phi(7) = 6$ gives the order of the multiplicative group modulo 7.

Let us now again take a look at the long division of $1/21$. The first remainder is the dividend 1, the second remainder is 10, then come the remainders 16, 13, 4, and 19, until the repetition begins. We observe that these remainders also belong to the set $\mathbb{Z}_{21}^{\times}$. Our final decimal expansion is $1/21 = 0.\overline{047619}$, so $\lambda = 6$, and the period is made up of the digits 0, 4, 7, 6, 1, and 9. The set of the remainders $H = \{1, 10, 16, 13, 4, 19\}$ builds up a subgroup for the group $G = (\mathbb{Z}_{21}^{\times}, \odot)$.

We can see this by drawing up a table (Table 1) and using the finite subgroup criteria. For example in the case of $13 \odot 19$ we first have to make the ordinary multiplication $13 \cdot 19 = 247$. Then we have to define the remainder of 247 modulo 21. It is 16, since $247 = 21 \cdot 11 + 16$.

Table 1. $(H, \odot)$ is a subgroup for the group $(\mathbb{Z}_{21}^{\times}, \odot)$, where H is the set of the remainders in the division $1/21$.

$\odot \pmod{21}$	1	4	10	13	16	19
1	1	4	10	13	16	19
4	4	16	19	10	1	13
10	10	19	16	4	13	1
13	13	10	4	1	19	16
16	16	1	13	19	4	10
19	19	13	1	16	10	4

Lagrange's theorem says generally that if H is a subgroup of a finite group G, the order of H is a factor of the order of G—and this is naturally true in our example: $6 \mid 12$.

In the long division the remainder always unambiguously determines (in accordance with the division algorithm) both the digit of the decimal expansion and the next remainder. We could illustrate this process in the following way (see Table 2).

Table 2. Subgroup remainders in the division $1/21$, and the decimals they produce.

Subgroup remainder	1	10	16	13	4	19
The decimal of the period	0	4	7	6	1	9

By looking at Table 2, it is clear that if we, by turns, take as dividends the numbers 4, 10, 13, 16, and 19 other than 1 in our subgroup, the decimal expansion must always repeat cyclically the expansion $1/21 = 0.047619\ldots = 0.\overline{047619}$. Let $a = 13$, for example. Then

$13/21 = 0.619047\ldots$. The period begins thus by 6 which comes from the first remainder 13, and so on. We could glue Table 2 on an adequate cylinder barrel where this phenomenon would be easy to follow and control. This can also be illustrated by a circle, see Figure 1.

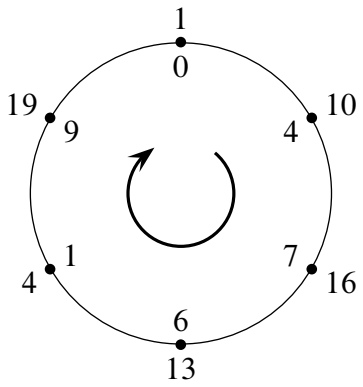

Figure 1. Division $1/21$.

Let us next do the long division $2/21$ where the dividend 2 does not belong to the above defined subgroup H (but is otherwise a possible dividend considering our assumptions). Now the remainders are 2, 20, 11, 5, 8, and 17, and they also belong to the set $\mathbb{Z}_{21}^{\times}$. They also build up a left (or right) coset modulo H. The division $2/21$ gives us the decimal expansion $0.095238\ldots = 0.\overline{095238}$ (cf. Table 3). The length of the period is again 6, and the coset is generated by $2 \in G$, for example. Namely,

$$\begin{aligned} 2 \odot H &= \{\, 2 \odot H \mid h \in H \,\} \\ &= \{2 \odot 1,\ 2 \odot 4,\ 2 \odot 10,\ 2 \odot 13,\ 2 \odot 16,\ 2 \odot 19\} \\ &= \{2, 8, 20, 5, 11, 17\}. \end{aligned}$$

Table 3. Coset remainders in the division $2/21$, and the decimals they produce.

Remainders of the coset $2 \odot H$	2	20	11	5	8	17
The decimal of the period	0	9	5	2	3	8

If we give to the dividend the values 20, 11, 5, 8, and 17 by turns, we always have a cyclic repetition of $0.095238\ldots = 0.\overline{095238}$. The cardinality of the coset $2 \odot H$ is naturally the same as the cardinality of the subgroup (and coset) $H = 1 \odot H$. Together these cosets H $(= 1 \odot H)$, and $2 \odot H$, give a partition of the set $\mathbb{Z}_{21}^{\times}$.

From this, it is clear that the set of all the possible remainders in the division $a/21$ is $(1 \odot H) \cup (2 \odot H) = \mathbb{Z}_{21}^{\times}$, whose number of elements is $\phi(21) = 2 \cdot 6 = 2 \cdot \lambda$, i.e., $\lambda \mid \phi(21)$. By using Tables 2 and 3, we also have a compact representation for all the possible divisions $a/21$. There are certainly many other ways of illustration apart from the tables. In Figure 2 there is a "graph theoretic" picture of the phenomenon.

In Figure 2, if we start from the node 4 (i.e., from the division $4/21$) we come by following the arrows into the period 190476, i.e., $4/21 = 0.190476\ldots = 0.\overline{190476}$.

We can generally know more about the length λ of the period (in the division of a/b) than that $\lambda \mid \phi(b)$; i.e., $\lambda = \mathrm{ord}_b(10)$, the order of 10 modulo b, which will be shown later. Let us come back to the case $b = 21$. We can straightforwardly find the order of 10

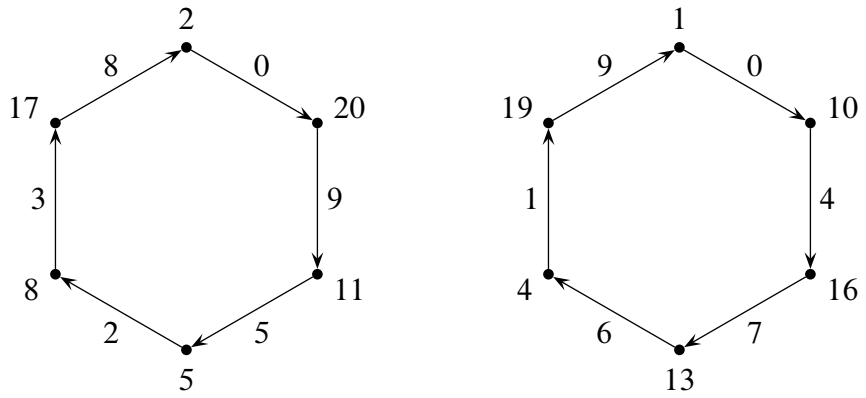

Figure 2. The division $a/21$ represented as directed graphs. The nodes represent all the possible dividends a; by following the arrows we can get the periods of all of the divisions $a/21$.

modulo 21 by studying the remainders of the powers 10^1, 10^2, etc. modulo 21. We have found the order when the remainder $= 1$. So: $10 = 21 \cdot 0 + 10$; $10^2 = 100 = 21 \cdot 4 + 16$; $10^3 = 21 \cdot 47 + 13$; $10^4 = 21 \cdot 476 + 4$; $10^5 = 21 \cdot 4761 + 19$; $10^6 = 21 \cdot 47619 + 1$. Thus the order we search is 6, and it is same as λ. (In fact, it is easier to find the order by means of congruence; however, we have not done so here.)

Obviously, it is generally true that for the maximum length λ of the periodicity (in a/b) the divisor b must be a prime number. This comes from the fact that $\phi(b) = b - 1$ if b is a prime. If b is not a prime, then $\phi(b) < b - 1$; i.e., it is impossible to get the "theoretical maximum" of λ. However, as we have seen, a prime number b as a divisor is not a sufficient condition for getting the maximum length.

4. Some preliminary task ideas for different grades

4.1. Grades 1–5

As stipulated in the Grounds of the National Curriculum in Finland [7], the decimal system and the division are taught as early as in grades 1–2. In grades 3–5, divisibility is dealt with more generally, and connections between common fractions and decimal fractions are taught. The negative integers are also presented, so at least the teacher could recall concepts like a group, subgroup and coset. For instance the integers $5k$ give a subgroup and one coset to the group of integers (equipped with addition and which naturally is not finite). The forms $5k + 1$, $5k + 2$, $5k + 3$, and $5k + 4$ give correspondingly the four other cosets. Together, these cosets divide the integers into five disjoint parts.

Thus there should in principle be no barriers to a presentation of many relevant aspects of our approach in grades 1–5. In connection with divisibility it is not at all strange to speak about the greatest common divisor of two positive integers. Then the basic assumptions concerning our approach could be easily displayed, too. It is one of the learning goals in grades 3–5 that the pupil learns "by examining and observing to construct mathematical concepts and concept systems". For example the idea of the Euler totient function $\phi(b)$ is perfectly near if there is some systematic approaching to the divisions of a/b. We first have to fix b and restrict ourselves to the interval $1 \leq a < b$ (which is not an essential restriction) so that $\gcd(a, b) = 1$. Then we have to ask how many acceptable dividends a there are. It is

good in this kind of material to keep b alternatively as a prime and as a composite number—notwithstanding the fact that these concepts are theoretically unknown to the pupils.

We believe that the long division is mostly seen as an interesting and effective tool in grades 1–5. From the point of view of the subject matter of this article the pupils would do well to process the divisions $1/7$, $2/7$, $3/7$, $4/7$, $5/7$, and $6/7$, for example, and realize the cyclicity of the results. They could also work hard on the divisions $1/13$, $2/13$, $\ldots$, $12/13$, and realize that the situation there is a bit more complicated. They could collect these considerations as tables 2 and 3, or graphs. A suitable use of colors would probably add to the clarity.

The more general idea of periodicity is not difficult either to treat in these grades. The repetition of week days is familiar to all, for example. The teacher could make the pupils also to chart other common repeating phenomena. The character of the (non-terminating) periodic decimal expansion is, no doubt, challenging in many ways, so the teacher has to use the imagination, too. Transforming fractions into the decimal forms is usually credited with easier calculating as calculating with fractions. But this kind of motivation hardly works in the case of a periodic expansion like (iii).

4.2. Grades 6–9

Our curriculum [7] for grades 6–9 includes preparing motivation for proving through the use of grounded conjectures, experiments and counterexamples. In the field of numbers and operations with numbers for instance the following areas are handled: rational and real numbers, opposite and reciprocal numbers, prime factorization, canceling (reducing) fractions, and representing decimals as fractions.

Here are some task ideas for grades 6–9 featuring our approach.

1. Fix b so that $\gcd(b, 10) = 1$, and find $\phi(b)$. (The teacher does not have to tell anything about the Euler totient function; he or she may note, for example, about the number of all possible canceled forms a/b with $1 \leq a < b$.) After finding $\phi(b)$ you have to reflect on the results of the divisions a/b (without calculators, too) by doing first $1/b$. If the length $\lambda = \phi(b)$ in this decimal expansion you have to test that other choices for the dividend a also give a cyclic repetition of the result of $1/b$. Draw up a table or a graph of the results.

   If $\lambda < \phi(b)$ by dividing $\phi(b)$ with the number λ you will find out the number of cosets in the multiplicative group of $\mathbb{Z}_b^\times$. Take one representative a' of each coset, and do the divisions a'/b. Draw up the tables, graphs or other illustrations to get a compact presentation for all divisions a/b.

2. Explain why the length of the period by division a/b does not depend on the dividend a.

3. Demonstrate that b being a prime does not guarantee the maximum length $b - 1$ of the period in the division a/b.

4. Find all primes $p < 100$ which generate the maximal length $p - 1$ of the period by the divisions $1/p$.

5. Is it possible to get the maximal length of the period by the division a/b if b is a composite number? Examine and explain.

4.3. Upper secondary school

Our national curriculum for upper secondary school encourages experimental, invention-oriented, and investigatory action (in the long and short syllabus alike; [6]). In the first courses at upper secondary school a revising and complementing review of the different number domains is conducted. There is also a special optional course on Number Theory and Logic including divisibility, division algorithm, congruence and the fundamental theorem of arithmetic. The Euler totient function could be taught here properly. Small tasks in this context could be, e.g., inventing formulas for cases $\phi(p)$, $\phi(p^k)$, $\phi(p \cdot q)$ where p, q are different primes, $\phi(m \cdot n)$ if $\gcd(m, n) = 1$. That $\phi(b)$ is even for $b > 2$ would be a little bit bigger assignment. Incidentally, the new course on number theory, logic, and *algebra* could be useful, too.

In the studying of congruence it could be possible to examine the sum of the elements of the reduced residue system modulo b, and show that it is a multiple of $\phi(b)$. The reduced residue system modulo b as a multiplicative group (without a word of the group concept) could also be dealt with. An experimental, invention-oriented, and investigatory working model should be applied.

Below you will find a couple of examples of more demanding assignments.

1. Show experimentally that through the forms
$$\frac{1}{99\ldots9} \quad \text{and} \quad \frac{1}{11\ldots1}$$
you can generate as long periods as you want. Why?

2. If you want to get, say, a length 7 of periodicity, you can also look at the number $10^7 - 1 = 9999999$. Let us find its prime factorization (by *Wolfram Alpha*, for example): $9999999 = 3^2 \cdot 239 \cdot 4649$, and, further all its positive factors 1, 3, 9, 239, 717, 2151, 4649, 13947, 41841, 1111111, 3333333, and 9999999. You can use as b all the factors except for the first three ones. How could you produce systematically integers b so that their reciprocals $1/b$ would generate a decimal expansion of type (iii) and the length of periodicity would be the one you want?

3. We saw above that $1/717$ produces an expansion where the length of the periodicity is 7. The expansion itself is $0.0013947\ldots = 0.\overline{0013947}$. Now $\phi(717) = 476$, and $476/7 = 68$, so the group $\mathbb{Z}_{717}^{\times}$ has 68 cosets with 7 elements, concerning the division $a/717$. Hence there are exactly 476 numbers a so that $1 \leq a < 717$ with $\gcd(a, 717) = 1$ and the length of the periodicity is 7. These expansions are distributed into 68 different "cyclic classes".

   By the long division we find out the subgroup $H = \{1, 10, 100, 283, 679, 337, 502\}$ which generates these classes. Now, $\gcd(2, 717) = 1$, and $2 \notin H$, so we get the coset $2 \odot H = \{2, 20, 200, 566, 641, 674, 287\}$ modulo 717 by the methods we have used earlier. Accordingly $674/717 = 0.9400278\ldots = 0.\overline{9400278}$, and $287/717 = 0.4002789\ldots = 0.\overline{4002789}$, i.e., they are cyclic repetitions of each other.

   Make a computer program (in a suitable programming environment) which generates the other 66 cosets.

4. Is it possible to invent a new method by which you can transform a given infinite periodic expansion (without any pre-period) into a fraction? (The "old methods" are based on the convergent geometric series, and multiplying with the number 10^{λ}.)

5. $\phi(21) = 12$, $\phi(21^2) = 252 = 21 \cdot 12$, $\phi(21^3) = 5292 = 21 \cdot 252 = 21^2 \cdot 12$, $\phi(21^4) = 111132 = 21^3 \cdot \phi(21)$, etc. Explain what kind of regularity (in the context of type (iii)) there is in the cases of $b = 21^2, 21^3, 21^4$, etc., (find λ and the number of cosets in each case). An instruction: Examine the cases $1/21^2, 1/21^3, 1/21^4$, etc.

6. Present the themes of periodicity in mathematics curriculum of upper secondary school as extensively as possible.

7. The concept of irrational numbers. How can you construct infinitely many irrational numbers by using just one non-terminating periodic decimal expansion, for example, the expansion $1/21 = 0.047619\ldots$?

8. A wilder idea. What is the basic idea in Hedy Lamarr and George Antheil's "frequency-hopping"? Could the theory of the periodic decimal expansions have some similar applications?

5. Conclusion

We show that decimal expansions of rational numbers have a bearing at all levels of mathematics learning, from primary school to university. Our study is related to the notion of hidden mathematics curriculum introduced by Abramowich and Brouwer in 2003. This important and profound notion should be discussed more extensively and more deeply in mathematics teacher education. The investigation of hidden threads between school mathematics and university mathematics could motivate mathematics teacher students also to train abstract mathematical concepts in their university studies. We encourage the readers to go ahead in this rich field of research and to reveal further examples of mathematical topics implicitly present in school curricula.

Appendix A. Preliminaries on algebra and number theory

We here present only the concepts and results on algebra and number theory needed in this article. More comprehensive treatments can be found, e.g., in [5] and [9]. See also [10].

A.1. Group theory

Let G be a nonempty set equipped with a binary operation $\star$ (i.e., $\star$ is a mapping $G \times G \to G$). Then $(G, \star)$ is said to be a *semigroup* if $(a \star b) \star c = a \star (b \star c)$ for all $a, b, c \in G$ (i.e., the binary operation $\star$ is associative). A semigroup is said to be a *monoid* if there exists an element $e \in G$ (an identity) such that $a \star e = e \star a = a$ for all $a \in G$. A monoid is said to be a *group* if for all $a \in G$ there exists an element $a^{-1} \in G$ (an inverse of a) such that $a \star a^{-1} = a^{-1} \star a = e$. An *Abelian group* is a group in which $a \star b = b \star a$ for all $a, b \in G$ (i.e., the binary operation $\star$ is commutative).

A pair $(H, \star)$ is called a *subgroup* of $(G, \star)$ if H is a nonempty subset of G and $(H, \star)$ is a group. The finite subgroup criterion says that if H is a nonempty finite subset of G, then $(H, \star)$ is a subgroup of $(G, \star)$ if and only if

$$\forall a, b \in H : a \star b \in H,$$

i.e., if and only if H is closed under the binary operation $\star$. Lagrange's theorem says that if $(G, \star)$ is a finite group and $(H, \star)$ is its subgroup, then

$$|H| \,\Big|\, |G|,$$

i.e., the number of elements in H divides the number of elements in G.

Let $(G, \star)$ be a group and let $a \in G$. Denote

$$\langle a \rangle = \{\, a^k \mid k \in \mathbb{Z} \,\}.$$

Then $(\langle a \rangle, \star)$ is the smallest subgroup of $(G, \star)$ containing the element $a \in G$. The number of elements in $\langle a \rangle$ is called the *order* of a in G and is denoted as $\mathrm{ord}(a)$. If there exists an element $a \in G$ such that $G = \langle a \rangle$, then $(G, \star)$ is said to be a *cyclic* group and the element a is referred to as a *generator* of $G = \langle a \rangle$.

Let $(G, \star)$ be a group and let $(H, \star)$ be its subgroup. We say that the *left coset* of $a \in G$ modulo H in G is the set

$$a \star H = \{\, a \star h \mid h \in H \,\}.$$

If e is the identity in G, then $e \star H = H$. More generally, $a \star H = H$ for $a \in H$, and further, $a \in a \star H$ for $a \in G$. The left cosets constitute a partition in the set G, i.e., two left cosets are either equal or disjoint and their union is G. Furthermore, $a \star H = b \star H \Leftrightarrow a \in b \star H \Leftrightarrow b \in a \star H$.

Similarly, the *right coset* of $a \in G$ modulo H in G is the set

$$H \star a = \{\, h \star a \mid h \in H \,\}.$$

If G is an Abelian group, then $a \star H = H \star a$ for all $a \in G$. Each coset (both left and right) modulo H has the same cardinality. In particular, if H is finite, then the number of elements in each coset modulo H is the same. If G is finite, then the number left (and right) cosets modulo H is $|G| \,/\, |H|$.

A.2. Congruences

Let m be a positive integer (≥ 2). Then $a \in \mathbb{Z}$ is said to be *congruent to b modulo m* if $a - b$ is divisible by m, i.e., if $m \mid (a - b)$. This is denoted as $a \equiv b \pmod{m}$. Thus $a \equiv b \pmod{m}$ if and only if $a = b + mk$ for some $k \in \mathbb{Z}$.

The congruence relation $\equiv \pmod{m}$ is an equivalence relation on $\mathbb{Z}$. The equivalence classes are referred to as the *residue classes modulo m*. The residue class determined by a is denoted as $[a]$, and a is termed as a *representative* of $[a]$. The set of all residue classes modulo m is denoted as $\mathbb{Z}_m$. Thus

$$\mathbb{Z}_m = \{[0], [1], [2], \ldots, [m-1]\}.$$

According to the division algorithm, for each $a \in \mathbb{Z}$ there exist unique numbers q and r such that $a = mq + r$ with $0 \leq r < m$. The number q is termed as the *quotient*, and the number r is termed as the *remainder*. It is clear that

$$[a] = [r]$$

and more generally

$$[a] = [b] \Leftrightarrow a \equiv b \pmod{m}.$$

Thus the representative a of the class $[a]$ can be replaced with any number congruent to a modulo m, for instance, with the remainder r of a modulo m.

Addition on $\mathbb{Z}_m$ is defined as

$$[a] \oplus [b] = [a + b],$$

where $[a]$, $[b] \in \mathbb{Z}_m$. This is referred to as the *addition modulo m*. Now, $(\mathbb{Z}_m, \oplus)$ is an Abelian group. In this paper we do not, however, need addition modulo m; we need multiplication modulo m, which we introduce below.

Multiplication on $\mathbb{Z}_m$ is defined as

$$[a] \odot [b] = [ab],$$

where $[a]$, $[b] \in \mathbb{Z}_m$. The multiplication on the right-hand side inside the square brackets is the usual multiplication of integers while the multiplication on the left-hand side is the multiplication on $\mathbb{Z}_m$ or the *multiplication modulo m* defined here. Now, $(\mathbb{Z}_m, \odot)$ is a commutative monoid. An element $[a] \in \mathbb{Z}$ possesses an inverse in $(\mathbb{Z}_m, \odot)$ if and only if $(a, m) = 1$, where $(a, m) = \gcd(a, m)$, the greatest common divisor of a and m. We denote by

$$\mathbb{Z}_m^\times = \{\, [a] \in \mathbb{Z}_m \mid (a, m) = 1 \,\}$$

the set of invertible elements in $\mathbb{Z}$. Now, $(\mathbb{Z}_m^\times, \odot)$ is an Abelian group, the *multiplicative group modulo m*.

The Euler totient function ϕ is defined by

$$\phi(m) = |\{\, a : 1 \le a \le m,\ (a, m) = 1 \,\}|, \quad m \in \mathbb{Z}^+,$$

i.e., $\phi(m)$ is the number of elements in $\mathbb{Z}_m^\times$ or the number invertible integers modulo m. An arithmetical expression for the Euler totient function ϕ is given as

$$\phi(m) = m \prod_{p \mid m} \left(1 - \frac{1}{p}\right),$$

where p goes through all primes dividing m. In particular, $\phi(p^k) = p^k - p^{k-1}$ for prime powers p^k with $k \ge 1$.

Let a and m (> 1) be relatively prime integers, that is, $(a, m) = 1$. Then, according to Euler's theorem, $a^{\phi(m)} \equiv 1 \pmod{m}$. Therefore there exists at least one positive integer x such that $a^x \equiv 1 \pmod{m}$. The *order of a modulo m* is the least positive integer x satisfying this property and and is denoted as $x = \mathrm{ord}_m(a)$. In the language of group theory, $\mathrm{ord}_m(a)$ is the order of a in the multiplicative group $\mathbb{Z}_m^\times$ modulo m. Thus $\mathrm{ord}_m(a)$ divides $\phi(m)$ on the basis of Lagrange's theorem. More generally, for $i, j \ge 0$,

$$a^i \equiv a^j \pmod{m} \iff i \equiv j \pmod{\mathrm{ord}_m(a)}.$$

As an example we find $\mathrm{ord}_7(2)$. It is easy to see that

$$2^1 \equiv 2 \pmod{7}, \quad 2^2 \equiv 4 \pmod{7}, \quad 2^3 \equiv 1 \pmod{7},$$

and thus $\mathrm{ord}_7(2) = 3$. Further, $\phi(m) = \phi(7) = 6$.

A set $\{n_1, n_2, \ldots, n_{\phi(m)}\}$ is a *reduced residue system modulo m* if $(n_i, m) = 1$ for $i = 1, 2, \ldots, \phi(m)$, and $n_i \not\equiv n_j \pmod{m}$ for $i \ne j$. For example, the sets $\{\, n \mid 0 \le$

$n \leq m-1,\ (n,m) = 1\}$ and $\{n \mid 1 \leq n \leq m,\ (n,m) = 1\}$ are reduced residue systems modulo m. The number theoretic concept of a reduced residue system modulo m is an analogue of the group theoretic concept of the multiplicative group modulo m.

It is known [3] that

$$\sum_{i=1}^{\phi(m)} n_i = \sum_{\substack{n=1 \\ (n,m)=1}}^{m} n = m\frac{\phi(m)}{2}.$$

Appendix B. Theory of decimal expansions

Each real number $x \in (0,1)$ can be written uniquely as

$$x = \sum_{n=1}^{\infty} q_n 10^{-n} = 0.q_1q_2\ldots, \tag{1}$$

where q_n's are integers in $[0,9]$ so that for each positive integer N there exists an integer $n > N$ such that $q_n \neq 9$. The last condition assures that, e.g., the expansion of $1/2$ is 0.5, since the expansion $0.4999\ldots$ is not appropriate. The expression (1) is referred to as the *decimal expansion* of x.

A decimal expansion is said to *terminate* if there exists a positive integer n_0 such that $q_n = 0$ for all $n > n_0$. The decimal expansion of $x \in (0,1)$ terminates if and only if $x \in \mathbb{Q}$ and x can be written as

$$x = \frac{a}{b}, \quad 1 \leq a < b,\ (a,b) = 1, \tag{2}$$

where the prime factors of b are 2 or 5. In other words, b belongs to the submonoid of $(\mathbb{Z},\cdot)$ generated by 2 and 5. Then $x = 0.q_1q_2\ldots q_{n_0}$. For example, $7/50 = 0.14$.

A decimal expansion is said to be *periodic* if there exist integers n_0 (≥ 0) and λ (> 0) such that $q_{n+\lambda} = q_n$ for all $n > n_0$. We then write $x = 0.q_1q_2\ldots q_{n_0}\overline{q_{n_0+1}q_{n_0+2}\ldots q_{n_0+\lambda}}$ and say that $q_1q_2\ldots q_{n_0}$ is the *pre-period* and $q_{n_0+1}q_{n_0+2}\ldots q_{n_0+\lambda}$ is the *period* whose *length* is λ. The decimal expansion of a real number $x \in (0,1)$ is periodic if and only if $x \in \mathbb{Q}$ and x is not of the form (2). The length of the pre-period depends on $(b,10)$, and no pre-period occurs (or is of length 0) if $(b,10) = 1$. For example, $1/6 = 0.1\overline{6}$ and $1/7 = 0.\overline{142857}$. The length of the pre-period and the period of $1/6 = 0.1\overline{6}$ are both equal to 1, and the length of the pre-period of $1/7 = 0.\overline{142857}$ is 0 and the length of its period is 6. (Note that if an expansion possesses a period of λ symbols, then it possesses a period of $t\lambda$ symbols for each $t \in \mathbb{Z}^+$. In this article, the period of an expansion always means the shortest period.)

A real number $x \in (0,1)$ is rational if and only if its decimal expansion terminates or is periodic. For example, the number $0.1010010001000010\ldots$ is irrational. The number of 0's between 1's increases throughout the expansion and thus the expansion is not periodic.

In this article we consider rational numbers of the form

$$x = \frac{a}{b}, \quad 1 \leq a < b,\ (a,b) = 1,$$

where $(b,10) = 1$, i.e., $2 \nmid b$ and $5 \nmid b$. Then the decimal expansion of x is periodic with no pre-period. We obtain the decimal expansion $x = 0.q_1q_2\ldots$ of x applying long division.

Consider the long division of $1/b$ with $(b, 10) = 1$. The sequence of quotients is $q_0, q_1, q_2, \ldots$ with $q_0 = 0$. We denote the sequence of remainders as $r_0, r_1, r_2, \ldots$. The remainders r_n possess the recurrence

$$\begin{aligned} 10r_n &= bq_{n+1} + r_{n+1}, \quad n = 0, 1, \ldots, \\ r_0 &= 1. \end{aligned} \tag{3}$$

For example, $1/7$ gives

$$\begin{aligned} 1 &= 7 \cdot 0 + 1 \quad \text{or} \quad 1 = 7 \cdot q_0 + r_0, \\ 10 \cdot 1 &= 7 \cdot 1 + 3 \quad \text{or} \quad 10r_0 = 7 \cdot q_1 + r_1, \\ 10 \cdot 3 &= 7 \cdot 4 + 2 \quad \text{or} \quad 10r_1 = 7 \cdot q_2 + r_2, \\ 10 \cdot 2 &= 7 \cdot 2 + 6 \quad \text{or} \quad 10r_2 = 7 \cdot q_3 + r_3, \\ 10 \cdot 6 &= 7 \cdot 8 + 4 \quad \text{or} \quad 10r_3 = 7 \cdot q_4 + r_4, \end{aligned}$$

etc.

On the basis of (3),

$$\begin{aligned} 10r_n &\equiv r_{n+1} \pmod{b}, \quad n = 0, 1, \ldots, \\ r_0 &= 1, \end{aligned}$$

giving

$$r_n \equiv 10^n \pmod{b}, \quad n = 0, 1, \ldots .$$

Let $\ell = \operatorname{ord}_b(10)$, i.e., ℓ is the least integer $x > 0$ such that

$$10^x \equiv 1 \pmod{b}.$$

Therefore the remainders are congruent to

$$1, 10, 10^2, \ldots, 10^{\ell-1}, 1, 10, \ldots$$

modulo b. Let L stand for the set of appropriate residue classes modulo b, i.e.,

$$L = \{[1], [10], [10^2], \ldots, [10^{\ell-1}]\}.$$

Then L is a nonempty subset of $\mathbb{Z}_b^\times$, since $(b, 10^n) = 1$ for $n = 0, 1, \ldots, \ell - 1$. Further,

$$[10^i] \odot [10^j] = [10^{i+j}] = [10^n] \in L,$$

where n is the remainder of $i + j$ modulo ℓ and thus $n < \ell$. This shows that L is closed under the multiplication $\odot$. Thus, according to the finite subgroup criteria, $(L, \odot)$ is a subgroup of the group $(\mathbb{Z}_b^\times, \odot)$. As a matter of fact, $L = \langle [10] \rangle$, i.e., L is the cyclic subgroup of $(\mathbb{Z}_b^\times, \odot)$ generated by $[10]$. On the basis of the Lagrange theorem $\ell \mid \phi(b)$, where $\ell = |L|$ and $\phi(b) = |\mathbb{Z}_b^\times|$.

The cosets of $(\mathbb{Z}_b^\times, \odot)$ modulo L are given as

$$[a] \odot L = \{[a], [10a], [10^2a], \ldots, [10^{\ell-1}a]\},$$

where $(a, b) = 1$. These are the residue classes modulo b of the remainders in the long division

$$\frac{a}{b}, \quad 1 \le a < b, \ (a, b) = 1,$$

where $(b, 10) = 1$. In other words, the remainders are congruent to

$$a, 10a, 10^2a, \ldots, 10^{\ell-1}a, a, 10a, \ldots$$

modulo b in this order. In fact, the remainders r_n in the long division of a/b possess the recurrence

$$\begin{aligned} 10r_n &= bq_{n+1} + r_{n+1}, \quad n = 0, 1, \ldots, \\ r_0 &= a \end{aligned}$$

giving

$$\begin{aligned} 10r_n &\equiv r_{n+1} \pmod{b}, \quad n = 0, 1, \ldots, \\ r_0 &= a \end{aligned}$$

and further

$$r_n \equiv 10^n a \pmod{b}, \quad n = 0, 1, \ldots .$$

We next show that ℓ is also the length of the period of the decimal expansion of a/b. We know that the length of the period of the sequence of remainders is $\ell = \operatorname{ord}_b(10)$. Therefore the length of the period of the decimal expansion $\lambda \leq \ell$. We prove that $\lambda = \ell$. The idea of the proof is conceived from [9]. Let $a/b = 0.\overline{q_1 q_2 \ldots q_\lambda}$. Thus

$$\begin{aligned} \frac{a}{b} &= \left(\frac{q_1}{10} + \frac{q_2}{10^2} + \cdots + \frac{q_\lambda}{10^\lambda}\right) + \left(\frac{q_1}{10^{\lambda+1}} + \frac{q_2}{10^{\lambda+2}} + \cdots + \frac{q_\lambda}{10^{2\lambda}}\right) + \cdots \\ &= \left(\frac{q_1}{10} + \frac{q_2}{10^2} + \cdots + \frac{q_\lambda}{10^\lambda}\right)\left(1 + \frac{1}{10^\lambda} + \frac{1}{10^{2\lambda}} + \cdots\right) \\ &= \left(\frac{q_1}{10} + \frac{q_2}{10^2} + \cdots + \frac{q_\lambda}{10^\lambda}\right)\left(\frac{10^\lambda}{10^\lambda - 1}\right) \\ &= \frac{q_1 10^{\lambda-1} + q_2 10^{\lambda-2} + \cdots + q_\lambda}{10^\lambda - 1}. \end{aligned}$$

This shows that $b \mid (10^\lambda - 1)$ or $10^\lambda \equiv 1 \pmod{b}$. Therefore, on the basis of the definition of the order of an element modulo b, we obtain $\lambda \geq \operatorname{ord}_b(10) = \ell$. We have now shown that $\lambda \geq \ell$ and $\lambda \leq \ell$, which means that $\lambda = \ell = \operatorname{ord}_b(10)$.

Note that $\operatorname{ord}_b(10) \mid \phi(b)$, that is, the length $\operatorname{ord}_b(10)$ of the period divides the value $\phi(b)$ of the Euler totient function. Furthermore, the length of the period is equal to $\operatorname{ord}_b(10)$ for all rational numbers a/b with $(a, b) = 1$ and $(b, 10) = 1$.

The cosets constitute a partition of $\mathbb{Z}_b^\times$ and the number of cosets equals $\phi(b)/\operatorname{ord}_b(10)$. Consider the decimal expansions of the numbers such residue classes of the numerators belong to the same coset. Assume that $[a]$ and $[a']$ are two distinct members in $[a] \odot L$. Then the remainders in the long division of a/b and a'/b are the same and in the same order but start from a different position. Thus the digits in the decimal expansions are the same and in the same order but start from a different position.

To be more precise, let $a/b = 0.\overline{q_1 q_2 \ldots q_\lambda}$, and suppose that $[a'] \in [a] \odot L$ with $1 \leq a' < b$. Then there exists a unique $i = 0, 1, \ldots, \lambda - 1$ such that $a' \equiv 10^i a \pmod{b}$. Thus the remainders in the long division of a'/b are congruent to $10^i a, 10^{i+1}a, \ldots, 10^{\lambda-1}a$, $a, 10a, \ldots, 10^{i-1}a, \ldots$ modulo b in this order. Therefore the the decimal expansion of a'/b is $a'/b = 0.\overline{q_{i+1} \ldots q_\lambda q_1 q_2 \ldots q_i}$.

For example, let $a = 1$ and $b = 7$. Then $a/b = 1/7 = 0.\overline{142857}$, where $[1] \odot L = L = \{[1], [10], \ldots, [10^5]\} = \mathbb{Z}_7^\times$ and $\lambda = \phi(7) = 6$. Further, let $a' = 3$. Then $[3] \in L$ and $3 \equiv 10^1 \pmod 7$, from which we conclude that $i = 1$ and $a'/b = 3/7 = 0.\overline{q_2 \ldots q_6 q_1} = 0.\overline{428571}$.

Acknowledgments

We would like to thank Professor Abramovich for useful comments on the paper. We would also like to thank Jarmo Niemelä for his expert help in LaTeX-processing.

References

[1] Abramovich, S., and Brouwer, P. (2003). Revealing hidden mathematics curriculum to pre-teachers using technology: the case of partitions. *International Journal of Mathematical Education in Science and Technology*, **34**(1): 81–94.

[2] Anon. (2011). https://www10.uta.fi/opas/opintoKokonaisuus.htm?rid=5028&uiLang=fi&lang=fi&lvv=2011

[3] Apostol, T. M. (1976). *Introduction to Analytic Number Theory*. New York: Springer.

[4] Brenton, L. (2008). Remainder wheels and group theory. *The College Mathematics Journal*, **39**(2): 129–135.

[5] Malik, D. S., Mordeson, J. N., and Sen, M. K. (1997). *Fundamentals of Abstract Algebra*. New York: McGraw-Hill.

[6] The National Board of Education (2003). *The National Core Curriculum for the Upper Secondary School* 2003 (in Finnish). http://www.oph.fi/download/47345_lukion_opetussuunnitelman_perusteet_2003.pdf

[7] The National Board of Education (2004). *The National Core Curriculum for the Primary School* 2004 (in Finnish). http://www02.oph.fi/ops/perusopetus/pops_web.pdf

[8] Poranen, J., and Silfverberg, H. (2011). Didaktinen matematiikka: sanoista tekoihin, teoista sanoihin. In H. Silfverberg and J. Joutsenlahti (Eds.), *Tutkimus suuntaamassa* 2010-*luvun matemaattisten aineiden opetusta, Matematiikan ja luonnontieteiden opetuksen tutkimuksen päivät Tampereella* 14.–15.10.2010. [Integrating Research into Mathematics and Science Education in the 2010s, Annual Symposium of the Finnish Mathematics and Science Education Research Association 14.–15.10.2010 in Tampere. Tampere: School of Education, University of Tampere.]

[9] Rosen, K. H. (2011). *Elementary Number Theory and Its Applications*, 6th ed. Pearson.

[10] Sándor, J., and Crstici, B. (2004). *Handbook of Number Theory II*. Dordrecht: Kluwer Academic Publishers.