Prace Naukowe Wyższej Szkoły Pedagogicznej w Częstochowie
Matematyka VI, Częstochowa 1999

Modular Arithmetic and Examples of Applications

Jan Kopka

In our country there is a tradition to penetrate into mathematical theories to great depth, on the contrary we do not deal with applications so much. I know from my own experience that there are countries where mathematical applications dominate over theories. In my opinion, we should find an approach which would be somewhere between these two extremes.

During educational process of future teachers of mathematics it is essential to introduce mathematical theories to them deeply. But these theories should be appropriately motivated and we should also show to use them inside and outside mathematics.

In my presentation I would like to say something about a basis of modular arithmetic and after it I want to show two different applications of this topic. In addition to this I would like to point at the passages where students can use an investigative approach. It will be the only opportunity to ensure that our students will do the same with their own pupils. The following text is a part of one of my lectures which is included into the course called Basis of Abstract Algebra in the English Language.

Definition 1 *Arithmetic Modulo n*
Let n be a fixed positive integer. For any integers x and y

$$(x+y) \bmod n = \text{the remainder upon dividing } x+y \text{ by } n;$$

$$(x.y) \bmod n = \text{the remainder upon dividing } x.y \text{ by } n$$

Definition 2 *Modular Equations*
If x and y are integers and n is positive integer, we write

$$x = y \text{ if and only if } n \text{ divides } x - y.$$

Consider the **equation**: $x = 3 \bmod 5$
Solution: x is a solution of this equation if and only if $x - 3 = 5k$, for some integer k. Thus is $x - 3 = 0, +5, -5, +10, -10, \ldots$, x is a solution of given

equation if and only if $x \in \{\ldots, -7, -2, 3, 8, 13, \ldots\}$.

Consider the **equation:** $2x = 7 \bmod 8$
Solution: x is a solution of this equation if and only if $2x - 7 = 8k$, for some integer k. But this equation has no solution, because the left side is always odd and the right side is always even.
The solution of these two equations can motivate our students to investigate the conditions under which these equations have a solution. Applying this method we can get the following theorem.

Theorem 1 *When a and n are relatively prime, then equation $ax = b \bmod n$ has a solution.*
The proof will then be the trainer's task.
Proof: If a and n are relatively prime then there are integers r and s such that $ar + ns = 1$. Then $arb + nsb = b$ and $arb - b = -nsb$. Thus $arb - b$ is divisible by n and rb is a solution to our equation.

Modular algebra has very important place in abstract algebra. We shall present here only two basic theorems.

Theorem 2 *The set $Z_n = \{0, 1, 2, \ldots, n-1\}$ for $n \geq 1$ is a group under addition modulo n.* This group is called *the group of integers modulo n.*

Theorem 3 *The set $\{1, 2, \ldots, n-1\}$ is a group under multiplication modulo n if and only if n is a prime.*

Applications of Modular Arithmetic

Modular Arithmetic has a lot of applications inside and also outside of mathematics. Now we shall describe two applications which are interesting particularly for teachers.

A) The generation of „random" numbers

A method for generating such numbers is to use a recursion formula of the form

$$x_{n+1} = (ax_n + c) \bmod m$$

To use such a formula we must choose the modulus m, the coefficients a, c and an initial value for x_0.

Example: $x_{n+1} = (ax_n + c) \bmod m$
If we choose $a = 3$, $c = 7$, $m = 8$, $x_0 = 1$, then

$$x_1 = 3.1 + 7 = 10 = 2 \bmod 8$$
$$x_2 = 3.2 + 7 = 13 = 5 \bmod 8$$

$$x_3 = 3.5 + 7 = 22 \quad = \quad 6 \bmod 8$$
$$x_4 = 3.6 + 7 = 25 \quad = \quad 1 \bmod 8$$

We can see that numbers generated in this way are completely determined by the choice of parameters and the initial value of x_0. So these numbers are not random at all. But they have many properties that we expect of random numbers and so are useful for simulation.

Now the students can start to investigate the relation between the coefficients and modules on the one side (they have to select relatively small numbers) and the generated numbers on the other side. This is, however a considerably complicated problem.

B) The assigning of a check digit to an identification number (used materials are from the USA)

Modular arithmetic is often used in assigning an extra digit to identification numbers. The purpose of this assigning is to detect forgery or errors.

Most products sold in supermarkets have an identification number coded with bars that are read by optical scanners. This code is called the Universal Product Code (UPC). Each coded item is assigned a 12-digit number. The first six digits identify the manufacturer, the next five characterize product and the last is a check.

To calculate the check digit we use the dot product for k-tuples.

Identification number $a_1a_2a_3 \ldots a_{12}$ satisfies the condition (second vector is called weighting vector)

$$(a_1, a_2, a_3, \ldots, a_{12}).(3, 1, 3, \ldots, 1) = 3a_1 + a_2 + 3a_3 + \cdots + a_{12} = 0 \bmod 10.$$

It means that check digits is

$$(a_1, a_2, a_3, \ldots, a_{11}).(3, 1, 3, \ldots, 3) \bmod 10.$$

We can verify that the number 037000707448 satisfies the above condition:

$$(0, 3, 7, 0, 0, 0, 7, 0, 7, 4, 4, 8).(3, 1, 3, 1, 3, 1, 3, 1, 3, 1, 3, 1) = 90 = 0 \bmod 10.$$

Now we shall show two examples of detecting of two types of errors.

Example of a single error *(error in exactly one position):*
Correct number is 037000707448, but into computer the number

037000507448

is entered (the seventh digit is incorrect). Then the computer calculates

$$0.3 + 3.1 + 7.3 + \cdots + 8.1 = 84.$$

Since $84 \neq 0 \bmod 10$, the entered number cannot be correct.

Example of an error involving the transposition of two adjacent digits:

Our identification number is entered as 073000707448 (second and third digits have been transposed). By calculating the dot product, we obtain

$$0.3 + 7.1 + 3.3 + \cdots + 8.1 = 82$$

and $82 \neq 0 \bmod 10$, so the entered number cannot be correct.

The above mentioned examples can motivate the trainees to investigate which single errors and errors involving the transposition of adjacent digits cannot be detected. In the second case they will probably come to the conclusion that the only undetected transposition errors of adjacent digits a, b are those where $|a - b| = 5$.

Let us make a note that at present the products sold in our shops are mostly designated by 13-digit identification numbers.

The next theorems reveal the relationship between the weighting vector and its ability to detect errors.

Theorem 4 *(Error–Detecting Capability 1):*
Suppose an identification number $a_1 a_2 \ldots a_k$ *satisfies*

$$(a_1, a_2, \ldots, a_k).(w_1, w_2, \ldots, w_k) = 0 \bmod n$$

where $0 \leq a_i < n$ *for each* i. *Then all digit errors in th* i*-th position are detected if and only if* w_i *is relatively prime to* n.

Proof: Consider a single error in the i-th position. Let $\acute{a}_i$ be substituted for a_i. Then the dot products differ by $(a_i - \acute{a}_i)w_i$. Thus the error is undetected if and only if $(a_i - \acute{a}_i)w_i = 0 \bmod n$. If w_i is relatively prime to n, then w_i belongs to $U(n)$. (For each integer $n > 1$, we define $U(n)$to be set of all positive integers less then n and relatively prime to n. $U(n)$ is a group under multiplication modulo n.) Therefore, $w_i^{-1} \bmod n$ exists. So $(a_i - \acute{a}_i)w_i w_i^{-1} = 0 \bmod n$ and $\acute{a}_i = a_i$.

If w_i is not relatively prime to n, then an error $\acute{a}_i$ with $|a_i - \acute{a}_i|$ divisible by $\frac{n}{\gcd(w_i, n)}$ will not be detected.

Theorem 5 *(Error–Detecting Capability 2):*
Suppose an identification number $a_1 a_2 \ldots a_k$ *satisfies*

$$(a_1, a_2, \ldots, a_k).(w_1, w_2, \ldots, w_k) = 0 \bmod n$$

where $0 \leq a_i < n$ *for each* i. *Then all errors of the form*

$$\ldots a_i a_{i+1} \ldots a_j a_{j+1} \ldots \rightarrow \ldots a_j a_{i+1} \ldots a_i a_{j+1} \ldots$$

are detected if and only if $w_i - w_j$ *is relatively prime to* n.

Proof: Consider an error of the form

$$\ldots a_i a_{i+1} \ldots a_j a_{j+1} \ldots \rightarrow \ldots a_j a_{i+1} \ldots a_i a_{j+1} \ldots$$

Then the dot products of the correct number and the incorrect number differ by

$$(a_i w_i + a_j w_j) - (a_j w_i - a_i w_j) = (a_i - a_j)(w_i - w_j)$$

Thus, the error is undetected if and only if

$$(a_i - a_j)(w_i - w_j) = 0 \bmod n$$

Let us make a note that after pronouncing Theorem 4 and 5 we should verify them on a concrete examples.

In the end, we can show one method of assigning a check digit which does not use modular arithmetic. This method is very interesting, rather complicated but very efficient.

Check – Digit Scheme Based on D_5

This scheme is based on the dihedral group D_5 of order 10 (D_5 is a group of all symmetries of a regular pentagon).

To describe this method we need the permutation $\alpha = (0)(14)(23)(58697)$ and the table of the dihedral group D_5 of order 10. (Here we use 0 through 4 for the rotations and 5 through 9 for the reflections.)

$\star$	0	1	2	3	4	5	6	7	8	9
0	0	1	2	3	4	5	6	7	8	9
1	1	2	3	4	0	6	7	8	9	5
2	2	3	4	0	1	7	8	9	5	6
3	3	4	0	1	2	8	9	5	6	7
4	4	0	1	2	3	9	5	6	7	8
5	5	9	8	7	6	0	4	3	2	1
6	6	5	9	8	7	1	0	4	3	2
7	7	6	5	9	8	2	1	0	4	3
8	8	7	6	5	9	3	2	1	0	4
9	9	8	7	6	5	4	3	2	1	0

Example of appending a check digit to any n-digit number. Consider the number 853.

$$\begin{aligned} \alpha(3) &= 2 \\ \alpha^2(5) &= 6 \\ \alpha^3(8) &= 7 \end{aligned}$$

Then we compute

$$(7 \star 6 \star 2)^{-1} = (1 \star 2)^{-1} = 3^{-1} = 2$$

This scheme detects all single digit errors, all transposition errors of adjacent digit and approximately 90% of all other types of errors.

The students can verify it with the help of several concrete examples (they have to select numbers with a few digits).

Jan Kopka
Department of Mathematics
J.E.Purkyně University
České mládeže 8
400 96 Ústí nad Labem, Czech Republic