A. Markish
research supervisor: I. A. Sverchevska,
Associate Professor of Algebra and Geometry
Zhytomyr Ivan Franko State University
Language tutor: D.O. Volnytska

FINITE ARITHMETICS

We used to do operations in simple arithmetics, but some tasks are really impossible or very difficult, compared to other arithmetics. Therefore, we should be able to use other arithmetics and do operations.

Finite arithmetics was introduced by using residue classes, which are based on theory of congruences. It was founded by famous German mathematician Carl Friedrich Gauss (1777-1855). He described this theory in his book "*Disquisitiones Arithmeticae*" (1801).

During centuries a lot of mathematicians were involved into studying this problem, but the largest contribution to the theory of numbers and congruences was made by French mathematician Pierre de Fermat (1601-1665), Petersburg academician Leonhard Euler (1707-1783), English mathematician Edward Waring (1736-1798) and French mathematicians Adrien-Marie Legendre (1752-1833) and Joseph-Louis Lagrange (1736-1813). [1, p. 7-8]

We do arithmetic operations automatically, without thinking about how we do them. But these steps require great efforts when we apply them to other arithmetics or number systems.

Modular arithmetic (finite arithmetics) is a system of arithmetic for integers (whole numbers), where numbers "wrap around" upon reaching a certain value – the modulus.

The simplest example of modular arithmetic is in the 12-hour clock, in which the day is divided into two 12-hour periods. If the time is 11:00 now, then 3 hours later it will be 2:00. Usual addition would suggest that the later time should be 11 + 3 = 14, but this is not the right answer because clock time "wraps around" every 12 hours; in 12-hour time, there is no "14 o'clock". Likewise, if the clock starts at 12:00 (noon) and 20 hours elapse, then the time will be 8:00 the next day, rather than 32:00. Because the hour number starts over after it reaches 12, this is an arithmetic *modulo* 12.

The properties of finite arithmetics match the properties of residue classes. All the formulas with multiplication, addition and any number of brackets are performed for finite arithmetics that greatly simplifies calculations. To add or multiply two numbers in modular arithmetic, we should add or multiply them in the usual sense of arithmetic and take the remainder of the module division.

Finite arithmetics has several advantages, for example, it doesn’t have fractions and negative numbers [2, p. 29].

Depending on the module we distinguish arithmetics with simple module, which has properties different from the properties of other arithmetics. For example, in arithmetics with simple module we may enter the imaginary unit.

Finite arithmetics can be applied to:

- the theorem proving;
- the definition of the division remainder;
- the proof of the multiplicity;
- the definition of the last digit number;
- the verification of actions that were made in simple arithmetics;
- solving quadratic equations;
- solving Diophantine equations;
- solving other problems that are unsolved in simple arithmetics.

In conclusion modular arithmetic is a very important chapter of algebra that can help solve a lot of mathematical problems.

LITERATURE

1. Бородін О. І. Теорія чисел / О. І. Бородін. – К. : «Радянська школа», 1960. – 246 с.
2. Лукашова Т. Д. Скінченні арифметики / Т. Д. Лукашова, К. В. Пискун // У світі математики – 2015. – № 1. – С. 26-34.
3. Хмара Т. М. Незвичайні арифметики / Т. М. Хмара // У світі математики. – 1974. – № 5. – С. 7-14.