PROCEEDINGS

of the Union of Scientists - Ruse

Book 5

Mathematics, Informatics and Physics

Volume 10, 2013

RUSE

The Ruse Branch of the Union of Scientists in Bulgaria was founded in 1956. Its first Chairman was Prof. Stoyan Petrov. He was followed by Prof. Trifon Georgiev, Prof. Kolyo Vasilev, Prof. Georgi Popov, Prof. Mityo Kanev, Assoc. Prof. Boris Borisov, Prof. Emil Marinov, Prof. Hristo Beloev. The individual members number nearly 300 recognized scientists from Ruse, organized in 13 scientific sections. There are several collective members too – organizations and companies from Ruse, known for their success in the field of science and higher education, or their applied research activities. The activities of the Union of Scientists – Ruse are numerous: scientific, educational and other humanitarian events directly related to hot issues in the development of Ruse region, including its infrastructure, environment, history and future development; commitment to the development of the scientific organizations in Ruse, the professional development and growth of the scientists and the protection of their individual rights.

The Union of Scientists – Ruse (US – Ruse) organizes publishing of scientific and popular informative literature, and since 1998 – the "Proceedings of the Union of Scientists- Ruse".

BOOK 5

"MATHEMATICS, INFORMATICS AND PHYSICS"

VOLUME 10

CONTENTS

BOOK 5

"MATHEMATICS, INFORMATICS AND PHYSICS"

VOLUME 10

This is the jubilee 10-th volume of book 5 Mathematics, Informatics and Physics. The beginning was in Spring, 2001, when the colleagues of the former section Mathematics and Physics decided to start publishing our own book of the Proceedings of the Union of Scientists – Ruse. The first volume included 24 papers. Through the years there have been authors not only from the Angel Kanchev University of Ruse but as well as from universities of Gabrovo, Varna, Veliko Tarnovo and abroad – Russia, Greece and USA.

Since the 6-th volume the preparation and publishing of the papers began to be done in English.

The new 10-th volume of book 5 Mathematics, Informatics and Physics includes papers in Mathematics, Informatics and Information Technologies, Physics and materials from the Scientific Conference 'Information Technologies in Education' (ITE), held at the University of Ruse in November 2012 in the frame of Project 2012-FNSE-02.

web: suruse.uni-ruse.bg

USAGE OF THE SYSTEM *MATHEMATICA* IN TEACHING AND LEARNING NUMBER THEORY

Tsetska Rashkova

Angel Kanchev University of Ruse

***Abstract**: The aim of this talk is to present some of the possibilities of the system Mathematica® for using it in the BSc degree course in Number Theory taught for the students in Mathematics and Informatics at the Angel Kanchev University of Ruse. The version used is Mathematica 5.1 and most of the problems discussed follow* [3] *used as a textbook for the course.*

***Keywords:** Division algorithms, Fermat's and Euler's theorems, Congruences, Linear Diophantine equations.*

INTRODUCTION

The system for computer algebra *Mathematica®* gives possibilities for good illustrations of many of the problems included in a BSc degree course in Number Theory. This illustration helps not only the teaching process but the learning process as well. It contradicts at some extent the traditional conception that Mathematics is learned only with a pencil at hand. A good lecturer in Mathematics could prepare good practical lessons on different topics and could reach a better students' understanding of mathematical ideas and motivate many of the students for further work both on mathematical problems and the usage of systems for computer algebra.

The development of modern science and technology depends on the development of adequate methods for representing integers and doing integer arithmetic. Starting as long as 5000 years ago different methods using different integers as bases, have been devised to denote integers. The ancient Babylonians used 60 as the base for their number systems and the ancient Mayans used 20. Our method of expressing integers, the decimal system using 10 as its base, was first developed in India approximately six centuries ago. Today, the binary system, which takes 2 as its base, is used extensively by computing machines.

PROBLEMS CONCERNING THE DIVISION ALGORITHM, THE EXPANSION OF INTEGERS AND APPLICATIONS OF FERMAT'S AND EULER'S THEOREMS

- The division algorithm allows finding the quotient and the remainder when dividing two integers m and n. By *Mathematica* this is done using the functions **Quotient**$[m,n]$ and **Mod**$[m,n]$.

For example

Quotient[67,3]

22

Mod[67,3]

1.

This means that $67 = 3.22 + 1$.

- Finding the base p expansion of a in decimal notation (i.e. using digits to represent multiples of powers of ten) is done in the system by the function **IntegerDigits**$[a, p]$, which gives this p expansion, namely $a = a_n a_{n-1} ... a_{0(p)}$.

For example

IntegerDigits[235,4]

{3,2,2,3}

IntegerDigits[116,7]

{2,2,4}

IntegerDigits[336,5]

{2,3,2,1}.

This means that $235 = 3223_{(4)}$, $116 = 224_{(7)}$ and $336 = 2321_{(5)}$.

- Obtaining the decimal expansion is done directly from the corresponding p expansion, namely

3*8^2+3*8+7

223

1*7^2+5*7+5

89.

This means that $337_{(8)} = 223$ and $155_{(7)} = 89$.

- Transforming p expansion to q expansion for $p,q \neq 10$ needs an intermediate step, namely the decimal expansion of the integer.

For example

IntegerDigits[3*5^2+3*5+3,6]

{2,3,3}

IntegerDigits[7*9+8,8]

{1,0,7}.

This means that $333_{(5)} = 233_{(6)}$ and $78_{(9)} = 107_{(8)}$.

- Finding the greatest common divisor GCD and the least common multiplier LCM of integers by *Mathematica* is done using the functions **GCD[a,b,…]** and **LCM[a,b,…].**

For example the solution of problem 10 on page 2 i.e. Pr.10/2 of [3] is

GCD[126,238]

14

GCD[123456789,987654321]

9

GCD[646,3003]

1.

The last result shows that the integers 646 and 3003 are relatively prime.

For the solution of problem 11 on page 3 of [3] we get

GCD[270,126,342]

18.

The system *Mathematica* has the advantage to find *LCM* only by one function while working by hand we need the formula

$$GCD\{a,b\}.LCM\{a,b\} = ab \qquad (1),$$

i.e. we have to find GCD at first.

For Pr.12/3 we have

LCM[126,238]

2142

LCM[646,3003]

1939938

LCM[270,54,342]

5130.

The system *Mathematica* could illustrate (1) leading to better knowledge of this relation.

For example

GCD[12,33]

3

LCM[12,33]

132

3*132

396

12*33

396.

- The prime-power factorization of an integer n is done by *Mathematica* using the function **FactorInteger[n].** It gives both the prime divisors and its degrees.

For example

FactorInteger[243]

{{3,5}}.

This means that $243 = 3^5$.

- The integer n could be a very big one, its prime divisors and their degrees as well.

For example

FactorInteger[243!]

{{2,237},{3,121},{5,58},{7,38},{11,24},{13,19},{17,14},{19,12},{23,10},
{29,8},{31,7},{37,6},{41,5},{43,5},{47,5},{53,4},{59,4},{61,3},{67,3},
{71,3},{73,3},{79,3},{83,2},{89,2},{97,2},{101,2},{103,2},{107,2},
{109,2},{113,2},{127,1},{131,1},{137,1},{139,1},{149,1},
{151,1},{157,1},{163,1},{167,1},{173,1},{179,1},{181,1},
{191,1},{193,1},{197,1},{199,1},{211,1},{223,1},
{227,1},{229,1},{233,1},{239,1},{241,1}}.

By *Mathematica* we could check if an integer n is prime or not. For this we need the function **PrimeQ[n].**

For example

PrimeQ[13]

True

PrimeQ[3*3+27-4*2]

False.

The last result shows that the integer $3.3 + 27 - 4.2 = 28$ is not prime.

We could define the n-th prime integer p_n by the function **Prime[n].** Thus

Prime[13]

41

Prime[3*3+27-4*2]

107.

This means that $p_{13} = 41$ and $p_{28} = 107$.

- Some applications of Fermat's and Euler's theorems, namely $a^{p-1} \equiv 1(\bmod p)$ for p - prime not dividing a and $a^{\varphi(n)} \equiv 1(\bmod n)$ for a and n relatively prime could be realized by *Mathematica* with the function **PowerMod[m,n,p]** calculating $m^n(\bmod p)$.

Thus the solution of Pr.30/5 is

PowerMod[137,42,100]

69,

meaning that the last two digits in the decimal expansion of 137^{42} are 6 and 9.

If the first digits are 0 they are not given by *Mathematica*. It means that the correct answer needs more digits to be defined. Thus the solution of Pr.28/5 will be

Mod[783^{15},100]

{7}

PowerMod[783,15,1000]

207,

meaning that the last two digits of 783^{15} are 0 and 7.

- By *Mathematica* one could define the Euler's function $\varphi(n)$, which gives the number of integers less or equal to n and relatively prime to n. For this one uses the function **EulerPhi[n].**

Pr. 45/8 has the following solution

EulerPhi[11088]

2880,

meaning that $\varphi(11088) = 2880$.

The function **EulerPhi[n]** for n prime could illustrate as well the formula $\varphi(n) = n - 1$.

For example

EulerPhi[113]

112.

Such a result shows in another way (except by **PrimeQ[n])** that an integer is a prime number.

The better learning of all stated properties of integers could be helped by the students' self work on Pr.13,14,16/3, Pr.32/6, Pr.38/7, Pr.39/7 and Pr.42/8 from [3] for example.

PROBLEMS CONCERNING CONGRUENCES AND LINEAR DIOPHANTINE EQUATIONS

- First degree congruences could be solved by **Solve[eqns && Modulus=p]**. Thus we have

Solve[2x+5==0 && Modulus==15]

{{Modulus->15,x->5}}.

The same function illustrates both the cases when the congruence does not have a solution and when the solutions are more than one. For example

Solve[21x+4==0 && Modulus==9]

{}

Solve[12x+15==0 && Modulus==21]

{{Modulus->21,x->4},{Modulus->21,x->11},{Modulus->21,x->18}}.

- By *Mathematica* we could solve higher degrees' congruences as well. For example

Solve[25x^3-21x^2+33x-13==0 && Modulus==8]

{{Modulus->8,x->1},{Modulus->8,x->5}}

Solve[x^2+4x-1==0 && Modulus==125]

{}.

The last result means that the congruence $x^2+4x-1=0(\mathrm{mod}125)$ does not have a solution.

- If the congruence is a quadratic one and we don't need its solution but only to know if it exists or not, we work with the function **JacobiSymbol[n,m],** calculating $\left(\frac{n}{m}\right)$.

The example

JacobiSymbol[426,491]

-1

shows that the congruence $x^2\equiv 426(\mathrm{mod}\,491)$ does not have a solution, while

JacobiSymbol[-1,17]

1

gives that $x^2\equiv -1(\mathrm{mod}17)$ has a solution. By

Solve[x^2+1==0 && Modulus==17]

{{Modulus->17,x->4},{Modulus->17,x->13}}

we get the two solutions $x\equiv 4(\mathrm{mod}17)$ and $x\equiv 13(\mathrm{mod}17)$ of the congruence $x^2+1\equiv 0(\mathrm{mod}17)$.

We illustrate one more advantage of the system *Mathematica*: Working analytically to find if a congruence has a solution or not and the modulus is not prime we have to make additional transformations in order to use the Gauss' law of reciprocity. In *Mathematica* there are no restrictions for the parameters of the function **JacobiSymbol[n,m]** (the **Jacobi symbol[*n*, *m*]** reduces to the **Legendre symbol** $\left(\frac{n}{m}\right)$ when *m* is an odd prime).

Thus

JacobiSymbol[860,11021]

1.

- For solving systems of first degree congruences *Mathematica* works with the function **ChineseRemainder[list$_1$, list$_2$],** giving the least nonnegative integer r for which **Mod[r, list$_2$] = list$_1$.**

Let list$_1$= $\{5,3\}$ and list$_2$= $\{12,14\}$. Thus $r\equiv 5(\mathrm{mod}12)$ and $r\equiv 3(\mathrm{mod}14)$. It means that r is a solution of the system

$$\left| \begin{array}{l} x\equiv 5(\mathrm{mod}\,12) \\ x\equiv 3(\mathrm{mod}\,14) \end{array} \right. .$$

The function **ChineseRemainder[list$_1$, list$_2$]** is a part of the standard package **NumberTheory`NumberTheoryFunctions`,** which has to be activated before the action of the function.

The solution of the above system by *Mathematica* is

<<NumberTheory`NumberTheoryFunctions`
ChineseRemainder[{5,3},{12,14}]
17
LCM[12,14]
84.

This means that the solution of the system is $x \equiv 17 \pmod{84}$.

We give two examples more: For the system $\left| \begin{array}{l} x \equiv 1 \pmod{3} \\ x \equiv 3 \pmod{7} \end{array} \right.$ by *Mathematica* we get

ChineseRemainder[{1,2},{3,7}]
16
LCM[3,7]
21

and the solution is $x \equiv 16 \pmod{21}$. For the system $\left| \begin{array}{l} x \equiv 6 \pmod{7} \\ x \equiv 1 \pmod{49} \end{array} \right.$ we get

ChineseRemainder[{6,1},{7,49}]
{},

meaning that the last system does not have a solution.

We point that the considered congruences have to be of the form $x \equiv a \pmod{m}$. Thus the system $\left| \begin{array}{l} 19x = 17 \pmod{5} \\ 19x = 17 \pmod{7} \end{array} \right.$ has the following solution by *Mathematica* in activated **NumberTheory`NumberTheoryFunctions`**package):

Solve[19x-17==0 && Modulus==5]
{{Modulus->5,x->3}}
Solve[19x-17==0 && Modulus==7]
{{Modulus->7,x->2}}
ChineseRemainder[{3,2},{5,7}]
23
LCM[5,7]
35.

When the congruences in the system differ only by the modules being relatively prime we could solve the system in another way as well. For example the above system could be solved as

Solve[19x-17==0 && Modulus==35]
{{Modulus->35,x->23}}.

For higher degree congruences *Mathematica* gives all logical possibilities. For example

Solve[7x^{11}-4==0 && Modulus==221]
{{Modulus->221,x->44}}
Solve[x^4-37==0 && Modulus==41]
{{Modulus->41,x->8},{Modulus->41,x->10}
{Modulus->41,x->31},{Modulus->41,x->33}}
Solve[9x^{12}-11==0 && Modulus==29]
{}.

In the last case the congruence $9x^{12}-11\equiv 0(\mathrm{mod}\,29)$ does not have a solution.

- For solving linear Diophantine equations with two unknowns there is no function in *Mathematica*. The equation has to be written as two congruences but the general solution has to fulfill the conditions for its existence, namely: If (x_0, y_0) is a solution of the equation $ax+by=c$, its general solution is given by the formula

$$\left| \begin{array}{l} x = x_0 + \dfrac{b}{(a,b)}t \\ y = y_0 - \dfrac{a}{(a,b)}t \end{array} \right. .$$

Let us consider the equation $4x+19y=5$. As $GCD\{4,19\}=(4,19)=1$, then the general solution is $\left| \begin{array}{l} x = x_0 + \dfrac{19}{(4,19)}t = x_0 + 19t \\ y = y_0 - \dfrac{4}{(4,19)}t = y_0 - 4t \end{array} \right.$ for $4x_0+19y_0=5$.

In *Mathematica* by

ExtendedGCD[4,19]

{1,{5,-1}}

we get $4.5+19.(-1)=1$ being equivalent to $4.25+19(-5)=5$. Then we find x_0 as a solution of $25\equiv x(\mathrm{mod}19)$, namely

Solve[25==x && Modulus==19]

{{Modulus->19,x->6}}.

Now we find y_0 by

Solve[4*6+19y==5]

{{y->-1}}.

Substituting in the above formula we get that the equation $4x+19y=5$ has the solution $\left| \begin{array}{l} x = 6+19t \\ y = -1-4t \end{array} \right.$.

If the equation $ax+by=c$ has no solution (for (a,b) not dividing c) then the congruence $ax\equiv c(\mathrm{mod}\,b)$ has no solution as well.

As an example we use Pr.78(g)/19 i.e. the equation $60x+18y=97$. From

ExtendedGCD[60,18]

{6,{1,-3}}

we get $6=1.60+(-3).18$ but 6 does not divide 97. Solving the congruence $60x\equiv 97(\mathrm{mod}18)$, namely

Solve[60x==97 && Modulus==18]

{}

we get the same answer.

Now we consider the equation $6x+9y=15$. As $(6,9)=3$ and 3 divides 15 the equation has a solution. For it by *Mathematica* we have:

ExtendedGCD[2,3]
{1,{-1,1}}
Solve[-5==x && Modulus==3]
{{Modulus->3,x->1}}
Solve[6*1+9y==15]
{{y->1}}.

Thus the general solution will be

$$\left| \begin{array}{l} x = x_0 + 9t = 1 + 9t \\ y = y_0 - 6t = 1 - 6t \end{array} \right. .$$

The students' self work could include Pr.51-52/10, Pr.56/11, Pr.58/12, Pr.62-63/14, Pr.72/17, Pr.78/19 and Pr.81/20 from [3].

REFERENCES

[1] Rosen K.H. Elementary Number Theory and Its Applications, Third Edition, 1993, Addison-Wesley, 544 p.

[2] Wolfram St. *Mathematica* A System for Doing Mathematics by Computer, Second Edition, 1993, Addison-Wesley, 961 p.

[3] Rashkova Ts. 9+9+9.9 Problems in Number Theory, Second edition, Angel Kanchev University of Ruse, 1999, 26 p. (in Bulgarian).

CONTACT ADDRESS

Assoc. Prof.Tsetska Rashkova, PhD
Department of Mathematics,
Faculty of Natural Sciences and Education
Angel Kanchev University of Ruse
8 Studentska Str., 7017 Ruse, Bulgaria
Phone: (++35982) 888 489
E-mail:tsrashkova@uni-ruse.bg

ИЗПОЛЗВАНЕ НА СИСТЕМАТА *MATHEMATICA* ПРИ ПРЕПОДАВАНЕ И ОБУЧЕНИЕ ПО ТЕОРИЯ НА ЧИСЛАТА

Цецка Рашкова

Русенски университет "Ангел Кънчев"

Резюме: *Докладът представя някои възможности на системата Mathematica при използването ѝ в бакалавърски курс по Теория на числата за студенти от специалност Математика и информатика в Русенския университет. Използваната версия е Mathematica 5.1 и много от разглежданите примери са по [3], използван като учебник за такъв курс.*

Ключови думи*: Алгоритъм за деление, Теореми на Ферма и Ойлер, Сравнения, Линейни Диофантови уравнения.*

ISSN 1314-3077
9 771314 307000