Revista de Matemática: Teoría y Aplicaciones
ISSN: 1409-2433
mta.cimpa@ucr.ac.cr
Universidad de Costa Rica
Costa Rica

Bulat, Mijail; Leon, Dumitru; Bivol, Leon; Ciobanu, Iacob; Zgureanu, Aurel
Generadores de números primos y factorizadores de números compuestos
Revista de Matemática: Teoría y Aplicaciones, vol. 13, núm. 1, enero, 2006, pp. 1-15
Universidad de Costa Rica
San José, Costa Rica

Revista de Matemática: Teoría y Aplicaciones 2006 **13**(1) : 1–15
cimpa – ucr – ccss issn: 1409-2433

GENERADORES DE NÚMEROS PRIMOS Y FACTORIZADORES DE NÚMEROS COMPUESTOS

Mijail Bulat* Dumitru Leon† Leon Bivol‡ Iacob Ciobanu§
Aurel Zgureanu¶

Recibido/Received: 21 Oct 2005 — Aceptado/Accepted: 25 Aug 2006

Resumen

La serie de los números naturales se representa por una matriz multidimensional. En la base de las propiedades de estas matrices se examinan los problemas:

a) la distribución de los números primos en las matrices multidimensionales,

b) la factorización de los números compuestos.

Para resolver el problema de la distribución, se elaboró un generador de números primos en el lenguaje Delphi. Este programa sirve también como generador de números compuestos de Mersenne. Al generar un número compuesto de Mersenne automáticamente se encuentra y uno de sus divisores.

El problema de la factorización en el lenguaje Delphi se resuelve para los números de la forma $2^i - 1$, donde i es un número natural. En particular, para i primo se factorizan los números compuestos de Mersenne.

Palabras clave: matrices multidimensionales, divisores primos, números de Mersenne.

*Departamento de Matemáticas, Academia de Transportes, Informática y Comunicaciones; Chisinau, Moldavia. E-Mail: msbulat@mail.ru

†MOBIASBANC, Chisinau, Moldavia. E-Mail: diLeon@yandex.ru

‡Departamento de Matemáticas e Informática de la Academia de Transportes, Informática y Comunicaciones (ATIC), Chisinau, Moldavia. E-Mail: cirese2006@yahoo.com

§Departamento de Matemáticas e Informática de la Academia de Transportes, Informática y Comunicaciones(ATIC), Chisinau, Moldavia. E-Mail: ciobanu@mail.ru

¶Departamento de Matemáticas e Informática de la Academia de Transportes, Informática y Comunicaciones(ATIC), Chisinau, Moldavia.E-Mail: aurelzgureanu@rambler.ru

Abstract

The sequence of natural numbers presents itself as a multidimensional array. Two problems are solved on the basis of these arrays:

a) distribution of prime numbers in multidimensional array,

b) factoring of composite numbers.

For solving the problems related to the distribution of prime numbers, there was developed a generator of prime numbers in the Delphi programming language. The program serves as well as a generator of Mersenne composite numbers. While generating a Mersenne composite number, one of its divisors is automatically defined.

The problem of factoring in Delphi is solved for numbers of the form $2^i - 1$, where i is a natural number. Mersenne composite numbers are factoring in particular for the prime i.

Keywords: multidimensional array, divisor prime, Mersenne numbers.

Mathematics Subject Classification: 05C60, 68R10.

1 Introducción

Para resolver problemas en sistemas de grandes dimensiones, en [1] y [2] fue introducida la transformación $\Phi(\vec{R})$. Por medio de esta transformación, los sistemas se representan por matrices multidimensionales. En [3] se examinaron unas aplicaciones de tales matrices. Una de estas aplicaciones es la representación de la serie de los números naturales por matrices multidimensionales. Tal representación permite desde otro punto de vista, resolver el problema de la distribución de los números primos en la serie de los números naturales [4]. Actualmente, debido al amplio desarrollo de las tecnologías de información, adquiere cada vez mayor importancia el problema de la protección de la información. Los números primos juegan un papel principal en la resolución de este problema. En sistemas de grandes dimensiones [1], es imposible resolver problemas sin aplicación de la computadora. Las propiedades de las matrices multidimensionales permiten elaborar generadores de números primos y factorizadores para números compuestos. En este trabajo se han examinado unas propiedades adicionales de las matrices multidimensionales. En la base de estas propiedades, junto con otras propiedades, se han elaborado programas en el lenguaje Delphi.

2 Matrices multidimensionales

Sea n conjuntos $X_1 = \{x_{11}, \ldots, x_{1m_1}\}$, $X_2 = \{x_{21}, \ldots, x_{2m_2}\}$,..., $X_n = \{x_{n_1}, \ldots, x_{nm_n}\}$ sobre los cuales, por medio de los elementos del conjunto $\Omega = \{\omega_1, \ldots, \omega_t\}$ están definidas r relaciones $R_{X_{i_1}X_{i_2}\ldots X_{i_d}}$ donde $2 \leq d \leq n$ y $i_j \in \{1, \ldots, n\}$ para cualquier $j \in \{1, \ldots, d\}$. Estas relaciones forman el conjunto R_1. Al ordenar los elementos de este conjunto [1,3] obtendremos el vector $\vec{R}_1$. Según [1,3] por medio de la transformación $\Phi(\vec{R}_1)$ construimos la matriz $n-$dimensional $A = \Phi(\vec{R}_1)$. En [3] se demostró que los elementos de esta matriz

representan números enteros no negativos en la base t. Pasamos a la base 10 y escribimos esta matriz en la forma de una matriz bidimensional

$$A = \begin{bmatrix} a_{11\ldots1} & a_{11\ldots2} & \ldots & a_{1m_2\ldots m_n} \\ a_{21\ldots1} & a_{21\ldots2} & \ldots & a_{2m_2\ldots m_n} \\ \ldots & \ldots & \ldots & \ldots \\ a_{m_1 1\ldots1} & a_{m_1 1\ldots2} & \ldots & a_{m_1 m_2\ldots m_n} \end{bmatrix} \tag{1}$$

Consideremos un caso particular con las condiciones:

$$\Omega = \{0, 1, 2, \ldots, m-1\},\ r = n,\ d = 2 \tag{2}$$

$$m_1 = m_2 = \ldots = m_n = t = m \tag{3}$$

$$\vec{R}_1 = \left(R_{X_1X_2}, R_{X_2X_3}, \ldots, R_{X_{n-1}X_n}, R_{X_nX_1}\right) \tag{4}$$

$$R_{X_1X_2} = R_{X_2X_3} = \ldots = R_{X_{n-1}X_n} = R_{X_nX_1} \tag{5}$$

$$\forall\, i, j \quad R_{X_iX_j} = \begin{bmatrix} 0 & 1 & 2 & \ldots & m-1 \\ 0 & 1 & 2 & \ldots & m-1 \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 1 & 2 & \ldots & m-1 \end{bmatrix} \tag{6}$$

Con estas condiciones la matriz n –dimensional (1) tiene una forma específica

$$A = \begin{array}{c} K_0 \\ K_1 \\ K_2 \\ \vdots \\ K_{m-1} \end{array} \begin{bmatrix} 0 & m+0 & 2m & \ldots & m^n-(m-0) \\ 1 & m+1 & 2m+1 & \ldots & m^n-(m-1) \\ 2 & m+2 & 2m+2 & \ldots & m^n-(m-2) \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ m-1 & m+(m-1) & 2m+(m-1) & \ldots & m^n-1 \end{bmatrix} \tag{7}$$

Denotemos las líneas de esta matriz por $K_0, K_1, \ldots, K_{m-1}$. Para $m = 6$ y $n = 3$ tenemos:

$$A = \begin{array}{c} K_0 \\ K_1 \\ K_2 \\ K_3 \\ K_4 \\ K_5 \end{array} \begin{bmatrix} 0 & 6 & 12 & 18 & 24 & 30 & 36 & 42 & 48 & 54 & 60 & 66 & 72 & 78 & 84 & 90 & 96 & 102 & \ldots & 210 \\ 1 & \mathbf{7} & \mathbf{13} & \mathbf{19} & 25 & \mathbf{31} & \mathbf{37} & \mathbf{43} & 49 & 55 & \mathbf{61} & \mathbf{67} & \mathbf{73} & \mathbf{79} & 85 & 91 & \mathbf{97} & \mathbf{103} & \ldots & \mathbf{211} \\ \mathbf{2} & 8 & 14 & 20 & 26 & 32 & 38 & 44 & 50 & 56 & 62 & 68 & 74 & 80 & 86 & 92 & 98 & 104 & \ldots & 212 \\ \mathbf{3} & 9 & 15 & 21 & 27 & 33 & 39 & 45 & 51 & 57 & 63 & 69 & 75 & 81 & 87 & 93 & 99 & 105 & \ldots & 213 \\ 4 & 10 & 16 & 22 & 28 & 34 & 40 & 46 & 52 & 58 & 64 & 70 & 76 & 82 & 88 & 94 & 100 & 106 & \ldots & 214 \\ \mathbf{5} & \mathbf{11} & \mathbf{17} & \mathbf{23} & \mathbf{29} & 35 & \mathbf{41} & \mathbf{47} & \mathbf{53} & \mathbf{59} & 65 & \mathbf{71} & 77 & \mathbf{83} & \mathbf{89} & 95 & \mathbf{101} & \mathbf{107} & \ldots & 215 \end{bmatrix} \tag{8}$$

Veamos unas propiedades de las matrices (7) [4]:

1. Las líneas K_i representan progresiones aritméticas con la razón m y con el primer término igual a i. Las columnas también representan progresiones aritméticas con la razón igual a 1.

2. Si $x \in K_i$ e $y \in K_j$ entonces $x \cdot y \in K_{(i\cdot j)(\mathrm{mod}\ m)}$ y $x + y \in K_{(i+j)(\mathrm{mod}\ m)}$.

3. Si $(i, m) = 1$ (i y m son recíprocamente primos), entonces la línea K_i contiene un número infinito de números primos (para $n = \infty$).

4. Para $(i, m) \neq 1$ e i compuesto, la línea K_i no contiene números primos; para i primo e $(i, m) \neq 1$ la línea K_i contiene solamente un número primo, esto es el número i.

   Veamos la matriz (8). Ya que $(1, 6) = 1$ y $(5, 6) = 1$ entonces en las líneas K_1 y K_5 la cantidad de los números primos crece infinitamente cuando $n \to \infty$ (el número de líneas se queda constante). Luego, $(2, 6) = 2$, $(3, 6) = 3$. Ya que 2 y 3 son primos, entonces cada una de las líneas K_2 y K_3 contiene solamente un número primo, 2 y 3 respectivamente. En K_0 todos los números son compuestos.

   De las últimas dos propiedades resulta que para m primo, todas las líneas de la matriz contienen números primos. La línea K_0 contiene solamente un número primo (el número m). Las demás líneas contienen un número infinito de números primos.

   En la matriz (8) los números primos están escritos con caracteres gruesos.

5. El número natural N pertenece a la línea K_j si y solo si m es un divisor del número $N - j$, es decir si y solo si se cumple la condición

$$(N - j) \vdots m \tag{9}$$

6. La estructura de la matriz es invariante bajo los parámetros m y n, es decir, al cambiar m y n, la matriz queda compuesta de progresiones aritméticas indicadas en 1).

7. El número de líneas de la matriz (7) que contienen un número infinito de números primos, es igual a la función de Euler $\varphi(m)$ [4,5]. Si $(i, m) = 1$ entonces K_i contiene un número infinito de números primos. Las propiedades de las matrices multidimensionales, nos permiten estimar el porcentaje de los números primos en la serie de los números naturales. En [7] se obtuvo la estimación igual a 26.66% (`http://bajandin.narod.ru`). Consideremos que todos los elementos de la línea K_i son primos. Ya que la matriz tiene m líneas, entonces la cota superior del porcentaje indicado es igual a $\dfrac{\varphi(m)}{m} \cdot 100\% \ \forall\, n$. Calculemos la cota para distintos valores de m. Sea $m = p_1 \cdot p_2 \cdot \ldots \cdot p_k$, donde p_i son números primos. En este caso $\varphi(m) = (p_1 - 1) \cdot (p_2 - 1) \cdot \ldots \cdot (p_k - 1)$ y, por eso $\dfrac{\varphi(m)}{m} = \dfrac{(p_1 - 1) \cdot (p_2 - 1) \cdot \ldots \cdot (p_k - 1)}{p_1 \cdot p_2 \cdot \ldots \cdot p_k}$.

Sea $m = p_1^{\lambda_1} \cdot p_2^{\lambda_2} \cdot \ldots \cdot p_k^{\lambda_k}$. Ya que en este caso $\varphi(m) = p_1^{\lambda_1 - 1} \cdot (p_1 - 1) \cdot p_2^{\lambda_2 - 1} \cdot (p_2 - 1) \cdot \ldots \cdot p_k^{\lambda_k - 1}(p_k - 1)$ entonces

$$\frac{\varphi(m)}{m} = \frac{p_1^{\lambda_1 - 1} \cdot (p_1 - 1) \cdot p_2^{\lambda_2 - 1} \cdot (p_2 - 1) \cdot \ldots \cdot p_k^{\lambda_k - 1}(p_k - 1)}{p_1^{\lambda_1} \cdot p_2^{\lambda_2} \cdot \ldots \cdot p_k^{\lambda_k}}$$

$$= \frac{p_1^{\lambda_1}\left(1-\frac{1}{p_1}\right)\cdot p_2^{\lambda_2}\left(1-\frac{1}{p_2}\right)\cdot\ldots\cdot p_k^{\lambda_k}\left(1-\frac{1}{p_k}\right)}{p_1^{\lambda_1}\cdot p_2^{\lambda_2}\cdot\ldots\cdot p_k^{\lambda_k}}$$
$$= \frac{(p_1-1)\cdot(p_2-1)\cdot\ldots\cdot(p_k-1)}{p_1\cdot p_2\cdot\ldots\cdot p_k}.$$

Así pues, la cota depende solamente de los divisores simples de m. Por eso, es suficiente tomar $m = p_1 \cdot p_2 \cdot \ldots \cdot p_k$. Al tomar, por ejemplo,

$$m = 2\cdot 3\cdot 5\cdot 7\cdot 11\cdot 13\cdot 17\cdot 19\cdot 23\cdot 29\cdot 31\cdot 37\cdot 41\cdot 43\cdot 47\cdot 53\cdot 59\cdot 61\cdot 67\cdot 71\cdot 73\cdot 79\cdot 83\cdot 89$$

obtendremos la cota superior del porcentaje de los números primos en la serie de los números naturales igual a 12,16%.

Veamos otras propiedades de la matriz en dependencia de otros parámetros y de otras condiciones. Supongamos que en (2) tenemos la condición $r > n$ y consideremos el vector $\vec{R}_1^* = \Big(R_{1,2}, R_{2,3}, \ldots, R_{n,1}, R(s_1), \ldots, R(s_k)\Big)$, donde $\forall\, i,j \quad R_{i,j} = R_{x_i,x_j}$ y $R(s_i)$ es la matriz que se obtiene de la matriz (6) por la sustitución de cada uno de sus elementos por el elemento $s_i \in \{0, 1, \ldots, m-1\}$, es decir

$$R(s_i) = \begin{bmatrix} s_i & \ldots & s_i \\ & \ddots & \\ s_i & \ldots & s_i \end{bmatrix} \tag{10}$$

Ya que todos los elementos de esta matriz son iguales entre si, entonces la columna $R(s_i)$ contiene el mismo número s_i en todas las líneas [3].

Sea, $A = \Phi(\vec{R}_1)$, $A^* = \Phi(\vec{R}_1^*)$ y $a_{j_1\ldots j_n}$-un elemento arbitrario de la matriz A. Al aumentar r, según la definición de la transformación $\Phi(\vec{R}_1)$ [1,2], el número de elementos de la matriz no cambia. Pueden cambiar solamente los elementos de la matriz. Por eso podemos designar por $a^*_{j_1\ldots j_n}$ el elemento arbitrario de la matriz A^*.

Teorema 1 *Sea* $\vec{R}_1 = (R_{1,2}, R_{2,3}, \ldots, R_{n,1})$, $\vec{R}_1^* = \Big(R_{1,2},\, R_{2,3}, \ldots, R_{n,1},\, R(s_1)\ldots,\, R(s_k)\Big), A = \Phi(\vec{R}_1)$ *y* $A^* = \Phi(\vec{R}_1^*)$ *entonces*

$$a^*_{j_1\ldots j_n} = a_{j_1\ldots j_n}\cdot m^k + s, \tag{11}$$

donde
$$s = s_1 m^{k-1} + s_2 m^{k-2} + \ldots + s_k. \tag{12}$$

DEMOSTRACIÓN: Los elementos de A y A^* son números enteros no negativos en la base m. Supongamos que $a_{j_1\ldots j_n} = \sigma_1\sigma_2\ldots\sigma_n$, donde $\sigma_i \in \{0, 1, 2, \ldots, m-1\}$. Entonces podemos escribir $a_{j_1\ldots j_n} = \sigma_1 m^{n-1} + \sigma_2 m^{n-2} + \ldots + \sigma_n$ y $a^*_{j_1\ldots j_n} = \sigma_1 m^{n+k-1} + \sigma_2 m^{n+k-2} + \ldots + \sigma_n m^k + s_1 m^{k-1} + s_2 m^{k-2} + \ldots + s_k = m^k(\sigma_1 m^{n-1} + \sigma_2 m^{n-2} + \ldots + \sigma_n) + s_1 m^{k-1} + s_2 m^{k-2} + \ldots + s_k = a_{j_1\ldots j_n}\cdot m^k + s$, donde $s = s_1 m^{k-1} + s_2 m^{k-2} + \ldots + s_k$, lo que se trataba de demostrar. ■

Corolario 1 *Las columnas y las líneas de la matriz A^* son progresiones aritméticas con las razones m^k y m^{k+1} respectivamente.*

En efecto, según la estructura de la matriz (1) para líneas, tenemos: $a^*_{(j_1+1)j_2\dots j_n} - a^*_{j_1j_2\dots j_n} = (a_{(j_1+1)j_2\dots j_n} \cdot m^k + s) - (a_{j_1j_2\dots j_n} \cdot m^k + s) = m^k(a_{(j_1+1)j_2\dots j_n} - a_{j_1j_2\dots j_n}) = m^k$.

Para columnas se obtiene: $a^*_{j_1j_2\dots(j_n+1)} - a^*_{j_1j_2\dots j_n} = (a_{j_1j_2\dots(j_n+1)} \cdot m^k + s) - (a_{j_1j_2\dots j_n} \cdot m^k + s) = m^k(a_{j_1j_2\dots(j_n+1)} - a_{j_1j_2\dots j_n}) = m^k \cdot m = m^{k+1}$.

Corolario 2 *Si $s \in K_i$ de la matriz n-dimensional A con las condiciones (2)-(6) entonces todos los elementos $a^*_{j_1j_2\dots j_n}$ de la matriz A^* pertenecen a K_i de la matriz $(n+k)$–dimensional con las mismas condiciones (2)-(6) en las cuales n está sustituido por $n+k$.*

En efecto. Supongamos que s es un elemento de la matriz A y $s \in K_i$. Ya que $m \in K_0$ entonces, conforme la propiedad (2), para cualquier $a_{j_1\dots j_n}$ se cumple la condición $(a_{j_1\dots j_n} \cdot m^k + s) \in K_i$, es decir $a^*_{j_1\dots j_n} \in K_i$.

De este corolario resulta que si s pertenece a una línea que no contiene números primos, entonces la matriz A^* está conformada solamente por números compuestos. La matriz A^* puede tener números primos solamente en el caso cuando $s \in K_i$ y $(i, m) = 1$.

Hace falta señalar que si $s \in K_i$, entonces $(a_{j_1\dots j_n} \cdot m^k + s) \in K_i$ para cualquier k. Por eso, para obtener intervalos de números con algunas propiedades de la línea K_i, podemos tomar valores arbitrarios de k.

Teorema 2 *Sea* $\vec{R}_1 = (R_{1,2}, R_{2,3}, \dots, R_{n,1})$, $\vec{R}^*_1 = \Big(R(s_1), \dots, R(s_k), R_{1,2}, R_{2,3}, \dots, R_{n,1})$, $A = \Phi(\vec{R}_1)$ *y* $A^* = \Phi(\vec{R}^*_1)$ *entonces*

$$a^*_{j_1\dots j_n} = a_{j_1\dots j_n} + s \cdot m^k, \tag{13}$$

donde $s = s_1m^{k-1} + s_2m^{k-2} + \dots + s_k$.

Demostración: Supongamos que $a_{j_1\dots j_n} = \sigma_1\sigma_2\dots\sigma_n$,donde $\sigma_i \in \{1, 2, \dots, m-1\}$. Entonces, según la transformación Φ tenemos: $a^*_{j_1\dots j_n} = s_1s_2\dots s_k\sigma_1\sigma_2\dots\sigma_n = s_1m^{k+n-1} + \dots + s_km^n + \sigma_1m^{n-1} + \dots + \sigma_n = m^n(s_1m^{k-1} + \dots + s_k) + \sigma_1m^{n-1} + \dots + \sigma_n = a_{j_1\dots j_n} + s \cdot m^n$, donde $s = s_1m^{k-1} + s_2m^{k-2} + \dots + s_k$, lo que se trataba de demostrar. ■

Corolario 3 *Las columnas y las líneas de la matriz A^* son progresiones aritméticas con las razones 1 y m respectivamente.*

Corolario 4 *Si $a_{j_1\dots j_n} \in K_i$ entonces $a^*_{j_1\dots j_n} \in K_i$.*

En efecto, $m \in K_0 \Rightarrow s \cdot m^n \in K_0$. Ya que $a_{j_1\dots j_n} \in K_i$ entonces según la propiedad 2) $a_{j_1\dots j_n} + s \cdot m^n \in K_i$ es decir $a^*_{j_1\dots j_n} \in K_i$.

3 Generadores de números primos

Se sabe [5,6], que si las condiciones

$$a^i \equiv 1(\mathrm{mod}\, N), \quad (a, N) = 1 \tag{14}$$

se cumplen para $i = N - 1$ y no se cumplen $\forall \ \ i < (N - 1)$, entonces N es número primo.

En la base de las propiedades de las matrices multidimensionales y de las condiciones (14), se elaboró un generador de números primos en el lenguaje Delphi (ver la Fig. 1, las inscripciones están hechas en rumano). El generador funciona con las restricciones:

$$7 \leq N \leq 2200000000, \quad a \cdot (N - 1) \leq 2200000000, \quad 2 \leq i \leq N - 1. \tag{15}$$

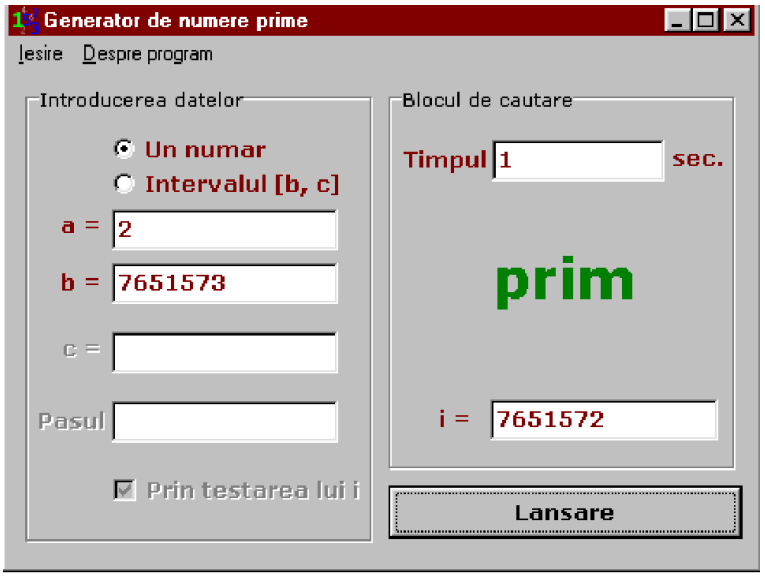

Figura 1: Generador de números primos en lenguaje Delphi, caso $N = 7651573$.

Al círculo "un numar" lo activamos (hacemos click) en el caso cuando investigamos solamente un número. En la celda "a" escribimos el valor de a de las condiciones (14). El número N que se investiga se escribe en la celda "b". Al activar el botón "Lansare", en la pantalla aparece el resultado de la investigación: "Prim"(Primo) o "Compus"(Compuesto). En la celda "i" aparece el valor de i de las condiciones (14). En la Fig.1 se examinó el número 7651573. Ya que $i = N - 1$, entonces el número es primo. En la celda "timpul" aparece la duración de la investigación. En la Fig.2 tenemos el caso cuando el número es compuesto. El resultado "Compus" aparece cuando i no es divisor de $N - 1$ o no existe. Este resultado es definitivo. Si i existe, es menor que $N - 1$ y es divisor de $N - 1$, entonces en la pantalla aparece "Primo". Este resultado no es definitivo. En este caso hay que repetir la investigación con otro valor de a.

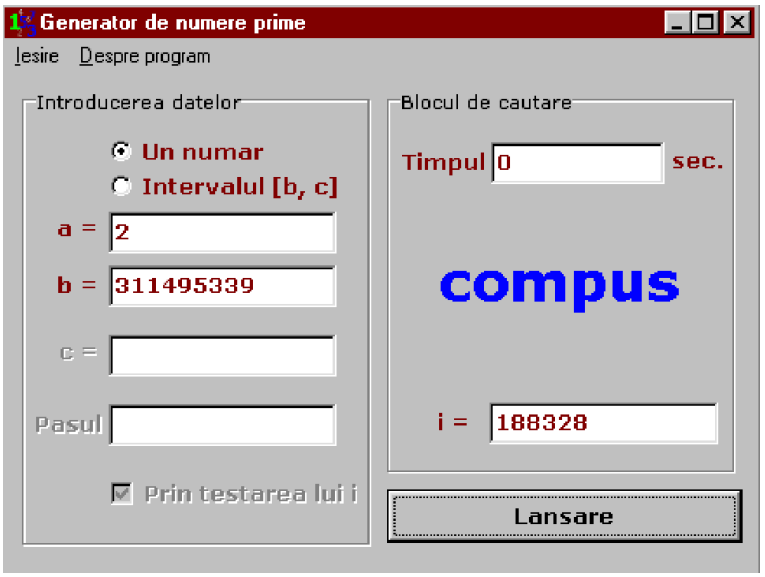

Figura 2: Caso de un número compuesto.

Al activar el círculo *Intervalul [b,c]*, podemos hallar todos los números primos del intervalo [b,c]. Los extremos del intervalo se escriben en las celdas "b" y "c". En la celda "Pasul" escribimos el paso (la diferencia entre dos números vecinos). La celda "Prin testarea lui i " se queda no marcada. Este caso está indicado en la Fig. 3.

La investigación comienza con la presión del botón *Lansare*. El intervalo contiene 10 números primos que están indicados en la lista junto con los valores de i.

Con otros programas [8] en la base de las propiedades de las matrices multidimensionales, se pueden construir números primos mucho más grandes. Al conocer un número primo con k cifras, se construye un número primo con $q > k$ cifras. El mayor número primo que se encontró es el número $n = 15418(2^{86243} - 1) + 1$ que contiene 25966 cifras significativas.

Veamos un caso particular, precisamente se trata de los números de la forma $2^p - 1$, donde p es un número primo. Estos números se llaman **Números de Mersenne** [4,5,6,8]. Para unos valores de p estos números pueden ser primos, para otros son compuestos. Al presente se conocen solamente 43 números primos de Mersenne (`http://www.mersenne.org/works.htm`). El 43–ésimo número fue descubierto en Diciembre del 2005. Este es el número $2^{30402457} - 1$ que contiene 9152052 cifras significativas. Este es el mayor número primo conocido en la ciencia. Todavía no se conoce si el conjunto de los números primos de Mersenne es finito o infinito. Los números compuestos de Mersenne son muchos más. El conjunto de estos números tampoco se conoce si es finito o infinito. El generador de números primos descrito anteriormente, puede servir como generador de números cumpuestos de Mersenne. Para eso activamos el círculo "Intervalul [b,c]" y la celda "Prin testarea lui i", elegimos dos números $b, c \in K_i$ tales que $(i, m) = 1$ y los escribimos en las celdas "b" y "c" respectivamente. En las celdas "a" y "Pasul" es-

Figura 3: Números primos en el intervalo $[b, c]$.

cribimos 2 y el paso respectivamente. La investigación comienza con la presión del botón "Lansare". El resultado de la investigación es la lista de los valores de p ($p = i$) en los números compuestos de Mersenne y de los divisores respectivos de estos números. Veamos un caso concreto. Los números 2002098071 y 2139826583 pertenecen a la línea K_5 de la matriz (8) (se cumple la condición (9)) para $n = 12$. Ya que $(5, 6) = 1$, entonces en la línea K_5 hay números primos. Según el teorema 1 tomamos $s = 2002098071$ y $k = 7$. Con estas condiciones los números indicados son términos de una progresión aritmética con el primer término s y con la razón $6^7 = 279936$. Todos los términos de esta progresión pertenecen a la línea K_5. Marcamos el círculo "Intervalul [b,c]" y la celda "Prin testarea lui i". En las celdas "a", "b" y "c" escribimos respectivamente 2,2002098071 y 2139826583. El resultado de la investigación está indicado en la Fig. 4.

De esta manera, hemos obtenido cuatro números compuestos de Mersenne: $2^{1001468939} - 1$, $2^{2004968719} - 1$, $2^{1053816971} - 1$, y $2^{1061515211} - 1$ con sus divisores respectivos 2002937879, 2049687191, 2107633943 y 2123030423. Tomando otros intervalos se obtuvieron otros números: $2^{5000062311} - 1$, $2^{6124388391} - 1$, $2^{1000000871} - 1$ y $2^{1000001759} - 1$ con sus divisores respectivos 1000012463, 1224877679, 2000001743 y 2000003519.

Con otros programas [8] se encontraron divisores de números Mersenne compuestos mucho más grandes. El mayor de ellos es el número $2^p - 1$ donde

p =375662093344890464881445680922948330514227905416290750436039035193113427960025633179619282272474675142015887211869248932622884793724041584342638184620653370929701895743372528415469209603996473936081119160718148122035890931308451719609498867813426976014647805530184630477159733866963269642334825861866906474984178767224823084747288474488341987274928573507300018140740543953865773319674245947812865963638649205806628195960120072169229969474482528655915375577672286548912154147055591112766026414615089316423169849566512856572461922842660864535300553081271718985426269670643068297483062996595379286420623781195539615471839220

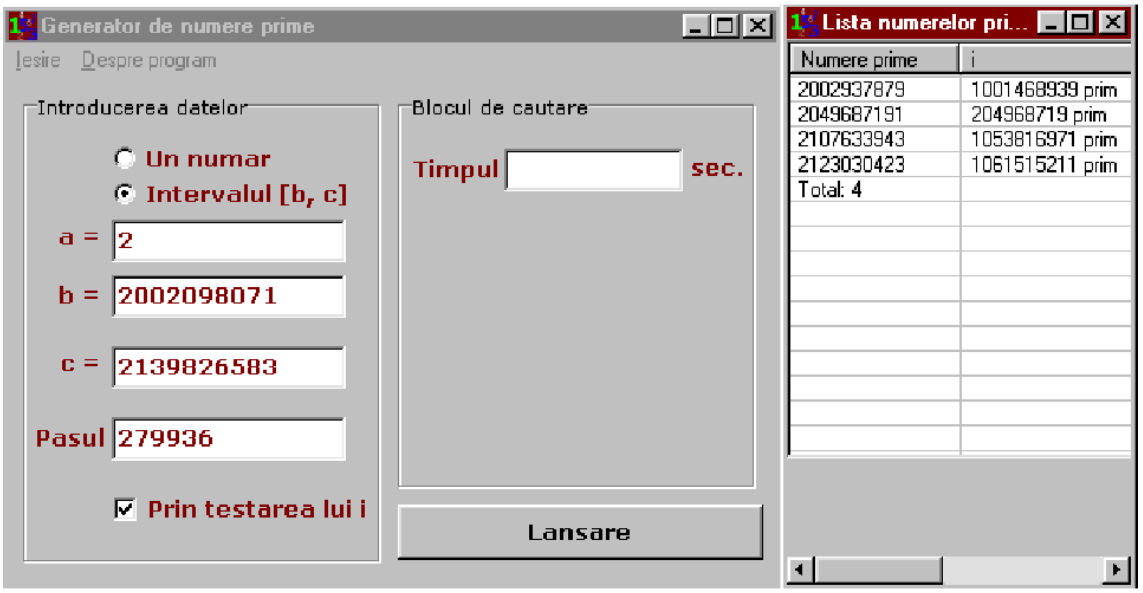

Figura 4: Números compuestos de Mersenne.

$$9171537280400935211029208245727181131159713663333714689676290815318675192145889526838878199852726233520193989760157276653077739577411643650600839089312501281856020871515497651397912384229885119585071218313738407154541689392825043482287254834897950294376362251118133846386216855226115183952870145885280080373253203512894219098076914576581640321158512789744937640515640969096392544785072185373462903826479455376535323939186866406430719366054359206134895082625943166067763036796988950518528130951459622923007.$$

Este número tiene el divisor primo:

$$d = 6010593493518247438103130894767173288227646486660652006976624563089814847360410130873908516359594802272254195389907982921966156699584665349482210953930453934875230331893960454647507353663943582977297906571490369952574254900935227513751981885014831616234364888482954087634555741871412314277357213789870503599746860275597169355956615591813471796398857176116800290251848703261852373114787935165005855418218387292906051135361921154707679511591720458494646009242756584782594466352889457804256422633841429062770717593064205705159390765482573832564808849300347503766820314730289092759729007945526068582729980499128633847549427666744596486414963376467331931634898098555418613339435034820653045098803074334232429422051197643619736323103836162516426449243833238586298409613425429000020509696333944247962422366598147678161913361139493019814514472667030285200695716596077358367204710021796017890141542179469683617842943245922334164481285972051256206307505569230633225306245138536204635919002248250255505542280716561154965975406461223671286024565183026989862502891509856869747298158321322015090657084208588751823208296450095223353966768113, que contiene 1126 cifras significativas.

A propósito, todavía no se conoce ningún divisor de los números compuestos $2^{751} - 1$, $2^{809} - 1$, $2^{997} - 1$, y $2^{1061} - 1$.

4 Factorizadores de números compuestos

Veamos la matriz (7). Sea la función de Euler $\varphi(m) = s$. Componemos el conjunto de números $M = \{m_1, m_2, \ldots, m_s, m_{s+1}\}$, donde $s = \varphi(m)$, $(m_i, m) = 1$ y $m_i < m$ para $i = 1, \ldots, s$; $m_1 = 1, m_s = m - 1$ y $m_{s+1} = m + 1$. Componemos el conjunto $\Delta = \{\Delta_1, \Delta_2, \Delta_3, \ldots, \Delta_s\}$ donde $\Delta_k = m_{k+1} - m_k$ para $k = 1, \ldots, s$. Es fácil ver que para cualquier m se cumple

$$\sum_{k=1}^{s} \Delta_k = m \tag{16}$$

En efecto, $\sum_{k=1}^{s} \Delta_k = \Delta_1 + \Delta_2 + \Delta_3 \ldots + \Delta_s = m_2 - m_1 + m_3 - m_2 + m_4 - m_3 + \cdots + m_{s+1} - m_s = -m_1 + m_{s+1} = -1 + m + 1 = m$.

Ya que $(m_i, m) = 1$, entonces los números primos están en las líneas K_{m_1}, K_{m_2}, $\ldots$, K_{m_i}, $\ldots$, K_{m_s}. Construimos la matriz con estas líneas y designamos las columnas por $0, 1, 2, 3, \ldots, m^{n-1} - 1$.

$$\begin{array}{c} \\ K_{m_1} \\ K_{m_2} \\ \vdots \\ K_{m_i} \\ \vdots \\ K_{m_s} \end{array} \begin{array}{c} \begin{array}{ccccc} 0 & 1 & 2 & \ldots & m^{n-1}-1 \end{array} \\ \left[\begin{array}{ccccc} N_1 & N_{s+1} & N_{2s+1} & \ldots & N_{(m^{n-1}-1)s+1} \\ N_2 & N_{s+2} & N_{2s+2} & \ldots & N_{(m^{n-1}-1)s+2} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ N_i & N_{s+i} & N_{2s+i} & \ldots & N_{(m^{n-1}-1)s+i} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ N_s & N_{2s} & N_{3s} & \ldots & N_{m^{n-1}s} \end{array}\right] \end{array} \tag{17}$$

En esta matriz $N_1 = 1$, $N_2 = N_1 + \Delta_1$, $N_3 = N_2 + \Delta_2$, $\ldots$, $N_s = N_{s-1} + \Delta_{s-1}$, $N_{s+1} = N_s + \Delta_s$. Luego $N_{s+2} = N_{s+1} + \Delta_1$, $N_{s+3} = N_{s+2} + \Delta_2$ y así sucesivamente. Los divisores de cualquier número natural N están sobre estas líneas. En la base de las propiedades de las matrices multidimensiomales se elaboró un factorizador de números de la forma $a^i - 1$ para $a = 2$. El programa verifica para cuáles valores de N_k de la matriz (17) se cumple la condición

$$2^i \equiv 1 (\mathrm{mod}\, N_k). \tag{18}$$

En la Fig. 5 está indicado el factorizador que factorizó el número compuesto de Mersenne $2^{71} - 1$ cuando $m = 2 \cdot 3 \cdot 5 \cdot 7 = 210$. En la celda "i" se escribe el valor de i de la condición (18).

El programa tiene dos formas de funcionamiento:

(*) La búsqueda se efectúa en todas las líneas de la matriz (17) pasando columna tras columna.

(**) La búsqueda se realiza solamente en una línea concreta.

En *Configurare* elegimos la forma de funcionamiento. Al activar *prime* se escoge la forma $(*)$. Otra forma se escoge cuando activamos *Pas*. Primero se escoge la forma de

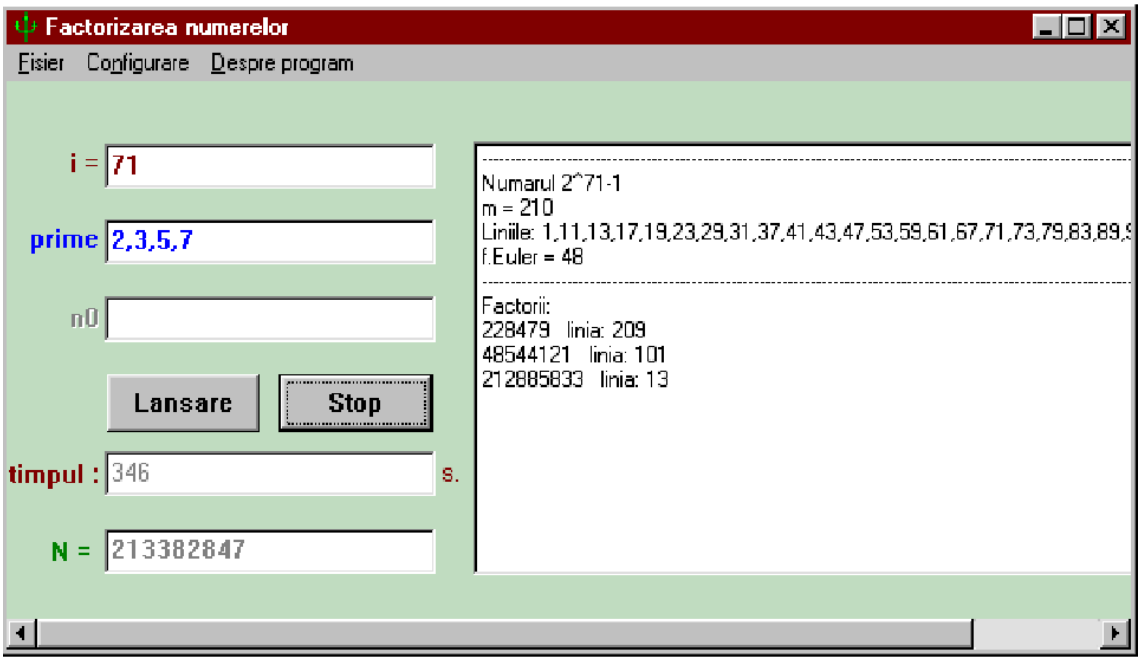

Figura 5: Factorización de $2^{71}-1$ cuando $m = 2 \cdot 3 \cdot 5 \cdot 7 = 210$.

funcionamiento y después se introducen otros datos. En la forma $(*)$ en la celda "Prim", escribimos los factores p_i de $m = p_1 \cdot p_2 \cdot \ldots \cdot p_c$; $c \in \{1,2,3,4\}$ y $p_i \in \{2,3,5,7\}$. Al activar *Lansare* en la pantalla aparece el número que se factoriza, el valor de m, los valores de m_i y la función de Euler $s = \varphi(m)$. Más abajo, después de la investigación, aparecen los factores de N y las líneas de la matriz (17), sobre las cuales se encuentran los factores respectivos. En la celda *timpul* se indica la duración de la investigación. En la celda "N" aparece el último número que se investigó. Si deseamos saber cuál número se está investigando en cualquier momento, activamos *Stop*. El número aparece en la celda *N*. Para continuar activamos *Continuati*. De la Fig. 5 tenemos: $N = 2^{71}-1 = 2361183241434822606847 = 228479 \cdot 48544121 \cdot 212885833$.

Hace falta señalar que en la lista de los factores aparecen tanto los divisores primos, como unos de los divisores compuestos del número N. Si es necesario sacamos de la lista los factores primos.

Si quisiéramos guardar el resultado de la investigación, escogemos *Nou* en *Fisier*. Lo mismo hacemos cuando pasamos a la factorización de otro número. En la Fig. 6 está indicado el resultado guardado de la factorización del número $2^{71}-1$.

Al escoger la forma $(**)$, en la celda *pas* escribimos el valor de m y en la celda n_0 – el número m_i de la línea que se examina en la matriz (17).

Hace falta señalar que los factores p_i del número m, pueden ser divisores del número N que se factoriza. Estos divisores no salen en la lista. La existencia de estos divisores se verifica aparte.

El factorizador funciona con las restricciones:

$$2 \le i \le 2200000000, \quad 2 \le N_k \le 1100000001. \tag{19}$$

La rapidez de la búsqueda de los divisores del número a^i-1 depende considerablemente de la elección de m . Este problema requiere una investigación aparte más profunda. Por

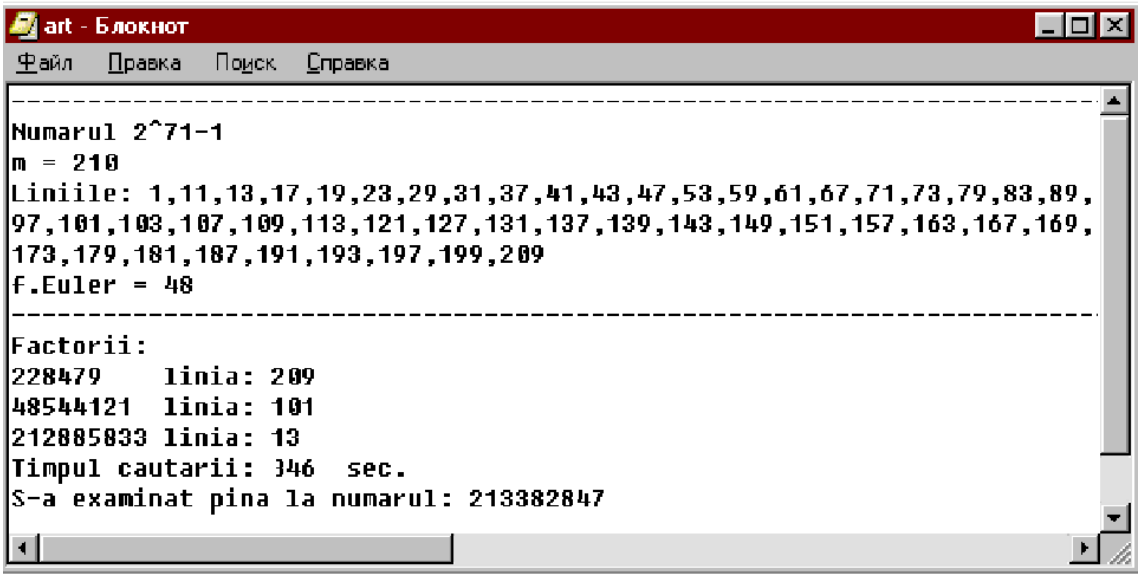

Figura 6: Factorización del número $2^{71} - 1$.

el momento mencionemos que en la forma de funcionamiento $(*)$, m debe tener el mayor valor posible. En el factorizador elaborado este valor es igual a 210. Pero la variante óptima se obtiene en la forma de funcionamieto $(**)$ cuando

$$n_0 = 1 \quad \text{y} \quad m = d \cdot i \tag{20}$$

donde d es el máximo común divisor de los números $\frac{p_1 - 1}{i}, \frac{p_2 - 1}{i}, \ldots, \frac{p_k - 1}{i}$; $p_1, p_2, \ldots, p_k$ son todos los divisores primos del número $a^i - 1$. La factorización del número $2^{71} - 1$ con las condiciones (20) (para $d = 2$, $i = 71$) está indicada en la figura 7. La factorización se realizó mucho más rápidamente que en el caso cuando $m = 210$.

En la forma de funcionamiento $(*)$, no siempre salen los divisores menores que i y a veces tampoco salen unos divisores mayores que i. Estos divisores se buscan adicionalmente.

En todos los ejemplos indicados, las investigaciones se hicieron con una computadora PII-400MHz.

5 Conclusiones

1. Los generadores y factorizadores elaborados son compactos y cómodos para la utilización. Los usuarios no necesitan conocimientos especiales.

2. Los factorizadores son elaborados solamente para números especiales de la forma $a^i - 1$ para $a = 2$. Es fácil transformar los programas para a arbitrario. Para otras formas se necesitan otros programas usando las mismas propiedades de las matrices multidimensionales.

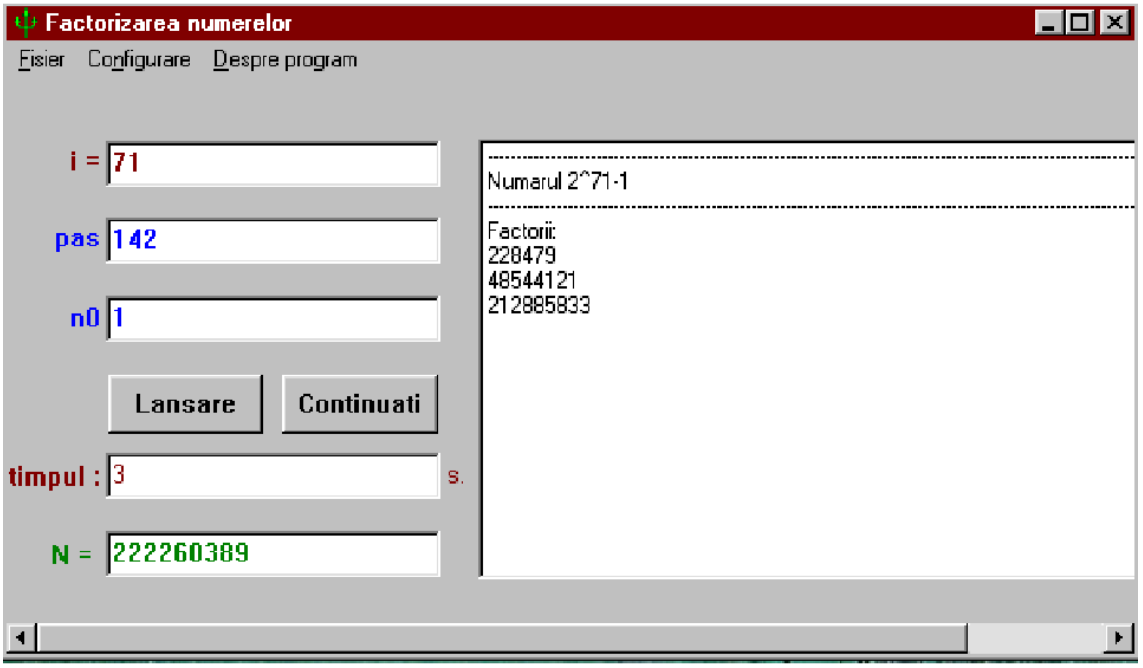

Figura 7: La factorización del número $2^{71} - 1$ con las condiciones (20).

3. Los intervalos de las restricciones (15) y (19) pueden ser ensanchados prácticamente de un modo ilimitado. Para eso se puede, por ejemplo, pasar a la otra forma de representación de los números. Los números pueden representarse como polinomios $P_n(m) = a_0 + a_1 m + a_2 m^2 + \ldots + a_n m^n$ de potencias de m. Teniendo en cuenta la estructura de la matriz (17) y la condición (16), es fácil obtener los elementos de esta matriz en forma de polinomio.

4. El factorizador de números puede servir también como generador de números primos, ya que los factores que se buscan son números primos. Al factorizar los números compuestos de Mersenne, podemos obtener números primos gigantescos en la forma polinomial. Estos números se pueden hallar investigando los elementos de la línea K_1 cuando $m = d \cdot i$.

5. Para buscar los números primos de Mersenne sería bueno elaborar una red de computadores que investiguen (en la forma (∗∗) de funcionamieto) todas las líneas de la matriz (17).

Referencias

[1] Bulat, M. (2001) "Isomorfismo de grandes sistemas", *Acta Academia 2001*, Evrica, Chisinau: 161–170.

[2] Bulat, M. (2000) "Isomorphic sistems of graphs", 3^{rd} *European Congress of Mathematics, Section 06: Discrete Mathematics and Computer Science, Poster number 236*, Barcelona.

[3] Bulat, M. (2002) "Algunas aplicaciones de las matrices multidimensionales", *Anales ATIC-2002, vol.1, Academia de Transportes, Informática y Comunicaciones*, Chisinau, Evrica: 30–38 (en rumano).

[4] Bulat,M. (2003) "La distribución de los números primos en matrices multidimensionales", *Anales ATIC-2003, vol.1, Academia de Transportes, Informática y Comunicaciones*, Chisinau, Evrica: 74–82 (en rumano).

[5] Minuts, P. (1997) *Teoria de los Números*, Vol.1, Editorial Crengutsa Galdau, Iasi (en rumano).

[6] Oleinik, W.(1999) "Métodos de obtención de los números primos. La situación actual y las perspectivas." *Acta Academia 1999*, Evrica, Chisinau: 101–126 (en ruso).

[7] Bajandin, E.(2003) *La distribución de los Números Primos en la Serie de los Números Naturales*. Editorial Nauka, Novosibirsk (en ruso).

[8] Bulat, M.; Zgureanu, A.; Ciobanu, I.; Bivol, L. (2006) "A method for obtaining arbitrary form prime numbers", *Satellite Conference of the ICM 2006. The XIV^{t}h Conference on Applied and Industrial Mathematics*, Chisinau: 70–73.