



MINISTÉRIO DA CIÊNCIA E TECNOLOGIA
INSTITUTO DE PESQUISAS ESPACIAIS

AUTORIZAÇÃO PARA PUBLICAÇÃO
AUTHORIZATION FOR PUBLICATION

AUTORES AUTHORS	PALAVRAS CHAVES/KEY WORDS		AUTORIZADA POR/AUTHORIZED BY
	MIGNOSI'S MATRIX LINEAR DIOPHANTINE EQUATION ENUMERATION SCHEME PSEUDOPOLYNOMIAL		<i>Marco Antonio Raupp</i> Diretor Geral
AUTOR RESPONSÁVEL RESPONSIBLE AUTHOR		DISTRIBUIÇÃO/DISTRIBUTION	REVISADA POR/REVISED BY
<i>Horacio Hideki Yanasse</i>		<input type="checkbox"/> INTERNA / INTERNAL <input checked="" type="checkbox"/> EXTERNA / EXTERNAL <input type="checkbox"/> RESTRITA / RESTRICTED	<i>Luiz A.N. Lorena</i>

CDU/UDC	DATA/DATE
519.852	February, 1987

TÍTULO/TITLE	PUBLICAÇÃO Nº PUBLICATION NO	ORIGEM ORIGIN	
	INPE-4133-PRE/1044	LAC	
AUTORES/AUTHORSHIP	A PSEUDOPOLYNOMIAL TIME ALGORITHM FOR LINEAR DIOPHANTINE EQUATIONS	PROJETO PROJECT	
		POPES	
		Nº DE PAG. NO OF PAGES	ULTIMA PAG. LAST PAGE
		23	A.3
VERSÃO VERSION		Nº DE MAPAS NO OF MAPS	
---		---	

RESUMO - NOTAS / ABSTRACT - NOTES

In this paper we present a pseudopolynomial algorithm for linear diophantine equations based on the calculation of the rank of the Mignosi's matrix. The use of a sufficient test that ensures the existence of a solution which is based on Paoli's theorem is also emphasized.

OBSERVAÇÕES/REMARKS

A versão resumida deste trabalho foi apresentada no 8º Congresso Nacional de Matemática Aplicada e Computacional, 1985, Florianópolis-SC.

RESUMO

Neste trabalho apresenta-se um algoritmo pseudopolinomial para equações diofantinas lineares baseado no cálculo do posto da matriz de Mignosi. Enfatiza-se o uso de um teste suficiente que assegura a existência de uma solução que é baseado no teorema de Paoli.

SUMMARY

	<u>Page</u>
1. <u>INTRODUCTION</u>	1
2. <u>THE ALGORITHM</u>	3
3. <u>FINAL COMMENTS</u>	11
BIBLIOGRAPHY	13
APPENDIX A - POOLI'S THEOREM	

1. INTRODUCTION

The diophantine equations appeared with Diophantus 2000 years ago and deal with the integer solution of the equation

$$\sum_{j=1}^N A(j) X(j)^{C(j)} = B^D,$$

where $A(j)$, $C(j)$, B and D are integers.

Several interesting problems are derived from this general equation:

- a) the famous Fermat's last theorem - "Are there three natural numbers such that the equation $X(1)^N + X(2)^N = B^N$ is satisfied, $N \geq 3$, $N \in \mathbf{N}$?";
- b) the Goodbach's conjecture - "Are there even numbers greater than or equal to 4 that cannot be expressed as the sum of two prime numbers?".

We analyse here the linear diophantine equation (LDE), that is, "Is there a natural N -tuple $(X(1), X(2), \dots, X(N))$ such

$$\text{that } \sum_{j=1}^N A(j)X(j) = B,$$

$$A(j), B \in \mathbf{N}, j=1, 2, \dots, N?" \quad (1)$$

This particular problem appears in a letter by Leibnitz to Bernoulli in 1669 and has been the focus of study of several famous mathematicians like Gauss, Cauchy, Sylvester, Hardy, Ramanujan and others.

In practical settings, LDEs appear in several models in a great number of situations (the interested reader can refer to

Kluyver and Salkin, 1975); therefore, there is a great interest in solving this problem in an efficient manner.

The best method known by these authors to solve this problem was proposed by Gilmore and Gomory (1966) and uses a dynamic programming recursion that requires an $O(B)$ of memory requirements and an $O(NB)$ of computational time.

In a recent article, Yanasse and Soma (1985) presented an algorithm that solves the knapsack problem and has an improved performance as compared with the dynamic programming methods.

The present problem differs from the knapsack problem in the sense that we are only interested whether the linear diophantine equation (1) has or does not have a solution.

A desirable algorithm would have, in the worst case, a polynomial bounded computational time ($O(p(N))$), but since the LDE is NP-complete (see Garey and Johnson, 1979) such an algorithm probably does not exist unless $P=NP$.

In this paper we present a pseudopolynomial algorithm, whose computational time is, in the worst case, limited to

$$O(N(B-A(1)) - \sum_{J=1}^N A(J)) \text{ and the memory requirements is } O(B-A(1)) \text{ and}$$

where, without loss of generality, we assume that

$$A(N) > A(N-1) > A(N-2) > \dots > A(1) > 0 \text{ and } B \geq A(1) + A(N).$$

This algorithm is based on Mignosi's matrix (Mignosi, 1908) and uses also a sufficient test based on Paoli's theorem (Paoli, 1780).

2. THE ALGORITHM

As presented before we assume, without loss of generality, that our data are already sorted, that is

$$0 < A(1) < A(2) < \dots < A(N).$$

We also assume that there is no $A(J)$, $J=1,2,\dots, N$ such that $B/A(J) \in \mathbb{N}$, otherwise the solution to the LDE is trivial. Also, we can assume that $B \geq A(1) + A(N)$ since, otherwise, we can reduce our problem to one with $N-1$ variables since $X(N)=0$.

Before we initialize the algorithm, we perform an $O(N^2)$ sufficient test based on Paoli's theorem to see if the LDE has a solution. We next describe Paoli's theorem.

Paoli's theorem (Paoli, 1780)

Consider the equation

$$AX + BY = C. \tag{2}$$

If the greatest common divisor of A and B , $\text{GCD}(A,B)$, is equal to 1 and $AB \leq C$, then (2) has at least one nonzero natural solution.

Proof: See appendix A.

$$\text{Let } M_{IJ} \triangleq \text{GCD}(A(I), A(J)). \tag{3}$$

Our test then becomes:

If there exists at least one pair of indices I and J , $I, J \in \{1, \dots, N\}$, $I \neq J$ such that

$$M_{IJ} \text{ divides } B \tag{4}$$

and

$$\frac{A(I) \cdot A(J)}{M_{IJ}} \leq B, \quad (5)$$

then

$$A(I)X(I) + A(J)X(J) = B$$

has at least one nonzero natural solution (by Paoli's theorem);

therefore $\sum_{J=1}^N A(J)X(J) = B$ has a solution. We should choose the pairs (I, J) in such a way that $A(I) \cdot A(J)$ is nondecreasing.

It is clear that there are $O(N^2 \log N)$ operations to perform this task.

It is convenient to observe at this point that if M_{IJ} does not divide B , then $A(I)X(I) + A(J)X(J) = B$ has no solution. In the case the sufficient test is not satisfied, we should have either one of the following cases:

- a) for all the pairs (I, J) , $I, J \in \{1, \dots, N\}$, $I \neq J$, M_{IJ} defined as in 3 does not divide B ;
- b) there is a pair (I, J) , $I, J \in \{1, \dots, N\}$, $I \neq J$ where M_{IJ} divides B and $\frac{A(I) \cdot A(J)}{M_{IJ}} > B$.

In case (a), the LDE has no solution with only two variables different from zero. This would suggest aggregating coefficients three by three and solving a new problem with these new additional coefficients. This approach is not explored further in this present work.

In case (b), $\frac{A(I) A(J)}{M_{IJ}} > B$ suggests that a

pseudopolynomial algorithm which is polynomial in B might perform well since B is not relatively large compared with some coefficients of the equation (1).

Both in case (a) and (b), we suggest the use of the algorithm proposed next, which is based on Mignosi's matrix (Mignosi, 1908).

Mignosi (1908) stated that the number of solutions of a LDE is given by

$$n_B = \frac{1}{B!} \left| \det \begin{bmatrix} \sigma(1) & \sigma(2) & \dots & \sigma(B-1) & \sigma(B) \\ -B+1 & \sigma(1) & \dots & \sigma(B-2) & \sigma(B-1) \\ & & \ddots & & \vdots \\ & & & \sigma(1) & \sigma(2) \\ & & & 1 & \sigma(1) \end{bmatrix} \right| \triangleq \frac{1}{B!} \left| \det M \right|,$$

$$\text{where } \sigma(t) = \sum_{j \in J} A(j) \delta(j) \text{ where } \delta(j) = \begin{cases} 1 & \text{if } A(j) \text{ divides } t \text{ and} \\ 0 & \text{otherwise,} \end{cases}$$

$$J = \{1, \dots, N\}.$$

In Soma (1985), it is shown that one can use a $B \times B$ matrix of the form

$$H = \begin{bmatrix} 0 & \dots & 0 & v(A(1)) & \dots & \dots & v(A(N)) & \dots & 0 \\ -1 & & & & & & & & v(A(N)) \\ & & & & & & & & v(A(1)) \\ & & & & & & & & 0 \\ & & & & & & & & -1 \\ & & & & & & & & 0 \end{bmatrix}$$

in place of the matrix M , where $v(A(j))$ can take any positive real value, for $j \in \{1, \dots, N\}$, and study the rank of H . If the rank of H is equal to B then the LDE has at least one solution, otherwise the equation has no solution.

To study the rank of a matrix, one can proceed in several ways. Given the special structure of matrix H , the natural idea is to add to the last column a linear positive combination of some other conveniently chosen column in order to eliminate all possible nonzero elements with the exception of at most one. If the whole column is zero that means that the rank of H is not B , otherwise the rank of the matrix is B , since by an interchange of columns we can get an upper triangular matrix with the whole diagonal different from zero.

Consider a simple example:

$$3x_1 + 4x_2 + 7x_3 = 11.$$

A matrix H associated with this LDE could be

By interchanging columns we can get an upper triangular matrix of the form

$$H^B = \begin{bmatrix} 24 & 0 & 0 & 1 & 2 & 0 & 0 & 3 & 0 & 0 & 0 \\ & -1 & 0 & 0 & 1 & 2 & 0 & 0 & 3 & 0 & 0 \\ & & -1 & 0 & 0 & 1 & 2 & 0 & 0 & 3 & 0 \\ & & & -1 & 0 & 0 & 1 & 2 & 0 & 0 & 3 \\ & & & & -1 & 0 & 0 & 1 & 2 & 0 & 0 \\ & & & & & -1 & 0 & 0 & 1 & 2 & 0 \\ & & & & & & -1 & 0 & 0 & 1 & 2 \\ & & & & & & & -1 & 0 & 0 & 1 \\ & & & & & & & & -1 & 0 & 0 \\ & & & & & & & & & -1 & 0 \\ & & & & & & & & & & -1 \end{bmatrix}$$

which implies that the rank of H is 11 and, therefore, the LDE $3x_1 + 4x_2 + 7x_3 = 11$ has a solution.

It is easily seen (see Soma, 1985) that one need not exactly perform the addition of a multiple of a chosen column with the last column. It is sufficient to keep in mind the position of the nonzero elements of the last column and the new ones that are generated by the additions.

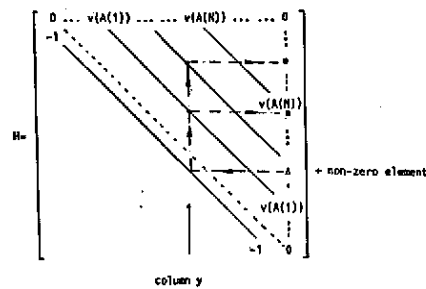
Observe that if at any instant an element k of column B has a value different from zero, this implies that

$$\sum_{j=1}^N A(j)X(j) = B - k + 1$$

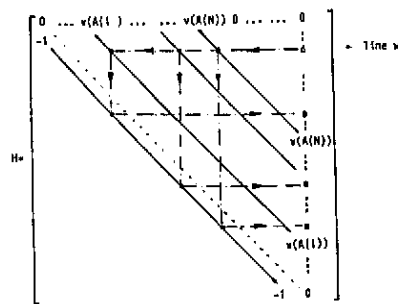
has a solution (see Soma, 1985 for details).

With these observations in mind, one interesting way of determining the rank and consequently obtaining an answer would be the following operations:

- for a column y such that its i^{th} element has value -1 in correspondence with the i^{th} nonzero element of column B in matrix H, we associate all positive values of column y to column B and only these, as shown in the next illustration.



- In a symmetric way we could choose line w and, in correspondence with the positive elements of this line, with the help of the -1 diagonal of the matrix, associate points of column B that would generate the element in the w^{th} line of column B , as shown in the next illustration.



Observe that a combination of the two approaches would result in a interesting procedure. We could start with $y = B - A(1) + 1$ and $w = A(1) + 1$.

There are several criteria to stop the algorithm:

- if after any operation the first element of column B in matrix H becomes nonzero, then the LDE has at least one solution;
- if at any operation we hit a line in column B that is nonzero, either by the first operation or the second one, then the LDE has at least one solution;

c) if $w \geq \lceil B/2 \rceil$ and $y \leq \lceil B/2 \rceil$ with the 1st element of column B zero, then the LDE has no solution. ($\lceil A \rceil$ means ceiling of A).

It is true that if the 1st element of column B is nonzero, then it is always possible to make the matrix H upper triangular through elementary operations of columns, with all the elements of the main diagonal different from zero. Therefore, we can immediately conclude that the rank of H is B. The criterion (a) is based on this observation.

With respect to criterion (b), if we use the second operation, we have that it is possible to find $K(j)$ and J and reach

$$B - \sum_{j \in J} A(j) K(j),$$

where $0 \leq K(j) \leq \lfloor \frac{B}{A(j)} \rfloor$ and J is a subset of $\{1, \dots, N\}$. Also, it is possible to reach $\sum_{i \in I} A(i) K(i)$, where $0 \leq K(i) \leq \lfloor \frac{B}{A(i)} \rfloor$ and I is a subset of $\{1, \dots, N\}$ using the first operation. We have by the criterion that

$$B - \sum_{j \in J} A(j) K(j) = \sum_{i \in I} A(i) K(i) \text{ or } \sum_{j \in J} A(j) K(j) + \sum_{i \in I} A(i) K(i) = B.$$

Therefore the LDE has at least one solution.

Observe that if we go on with the operations and reach a position where $y \leq \lceil B/2 \rceil$ and $w \geq \lceil B/2 \rceil$, then the LDE has no solution since all possible combinations that could give us a solution were considered. This makes criterion (c).

It is possible to run an algorithm with the first operation (or the second operation) alone. In this case, the stopping criteria have to be modified. If only the first operation is used,

criterion (a) can be applied in the same way; criterion (b) and (c) cannot be used. If at some time we have $\left\lfloor \frac{B-A(1)}{2} \right\rfloor + 1$ of the elements in column B different from zero, then we can stop. The LDE has a solution. This is true because of the particular structure of matrix H. Since using the first (second) operation alone we reached half plus one of the relevant positions in column B, then if we use the second (first) operation we would have reached also half plus one of the relevant positions in column B, which implies that the criterion (b) is achieved (implicitly).

The order of convergence can be shown to be $O((B-A(1)) - \sum_{J=1}^N A(J))$ and the memory requirements is $O(B-A(1))$. The interest reader can refer to Yanasse and Soma (1985).

3. FINAL COMMENTS

Although the computational requirements of the algorithm is $O(N(B-A(1)) - \sum_{J=1}^N A(J))$ for any one of the procedures using only the first or only the second or both operations, we think that a better average performance will be attained with the combination of the two operations since the algorithm has an improved chance of stopping due to criterion (b).

It should be pointed out that if the $A(J)$'s are prime two by two, (or if $\text{GCD}(A(1), A(2))=1$), then $B < A(1)A(2)$ and, in this case, this pseudopolynomial algorithm is not as bad as it might appear. We can rewrite the order of convergence of the algorithm in a different form, only in terms of N , $A(1)$ and $A(2)$. We have that

$$O(N(B-A(1)) - \sum_{J=1}^N A(J)) \leq O(NA(1) \cdot (A(2)-2) - \frac{(N-1)}{2}),$$

since $B < A(1)A(2)$, and

$$0 < A(1) < A(2) < \dots < A(N), \text{ where } A(J) \in \mathbf{N}.$$

BIBLIOGRAPHY

- GAREY, M.R.; JOHNSON, D.S. *Computers and intractability - a guide to the theory of NP-completeness*, San Francisco, W.H. Freeman. 1979.
- GILMORE, P.; GOMORY, R. A linear programming approach to the cutting stock problem II. *Operations Research*, 11(6), 863-888, 1963.
- Multistage cutting stock problems of two and more dimensions. *Operations Research*, 13, 94-120, 1965.
- The theory and computation of knapsack functions. *Operations Research*, 14; 1045-1074, 1966.
- GRIFFIN, H. *Elementary theory of numbers*, New York, McGraw-Hill, 1954.
- KLUYVER, C.A.; SALKIN, H.M. The knapsack problem: a survey. *Naval Research Logistics Quarterly*, 2(1), 127-144, 1975.
- MIGNOSI, G. Sulla equazione lineare indeterminata. *Periodico di matematica*, 23, 173-176, 1908.
- YANASSE, H.H.; SOMA, N.Y. A new enumeration scheme for the knapsack problem. INPE-3563-PRE/269. São José dos Campos, SP, June 1985. (presented at the School of Combinatorial Optimization, July 1985, Rio de Janeiro, RJ, Brazil).
- SOMA, N.Y. Um algoritmo exato para o problema da mochila. INPE, São José dos Campos. Master Thesis, 1985.
- PAOLI, P. Number w of positive integral solutions of $ax+by=n$. *Opuscula analytica*, 114, 1780.
- SIDKI, S. *Introdução a teoria dos números*. IMPA, Rio de Janeiro, 1975.

APPENDIX A

PAOLI'S THEOREM

The number w of positive integral solutions of $ax+by=n$, where a and b are positive and relatively prime.

If $ax+by=n$ has integral solutions, any common factor of a and b must divide n and, hence, can be removed from every term. Let henceforth a and b be relatively prime and positive. Let β denote the least positive integer such that $n-a\beta$ is divisible by b . There every solution is given by:

$$x = \beta + bm, \quad y = \frac{n-a\beta}{b} - am.$$

The values of m making x and y positive are $0, 1, \dots, E$, where E is the largest integer less than $(\frac{n-a\beta}{ab})$.

Thus there are $w = E+1$ sets of positive integral solutions x, y .

The previous explanation are not sufficient to understand why the conditions $AB \leq C$ and $\text{GCD}(A, B) = 1$ are sufficient to ensure a nonzero natural solution to the equation $AX+BY=C$. Let's elaborate, therefore, a little further. Consider the following lemma.

Lemma 1: Let A and B be integers. Then $AX \equiv 1 \pmod{B}$ has solution if and only if the $\text{GCD}(A, B) = 1$.

Proof : To check the previous statement let A and X' be integers. Then $AX' \equiv 1 \pmod{B}$ is equivalent to $AX' - BX'' = 1$ for some integer X'' , that is, the $\text{GCD}(A, B) = 1$. On the other hand, if the $\text{GCD}(A, B) = 1$, the existence of X' such that $AX' \equiv 1 \pmod{B}$ is guaranteed by Euclides algorithm (see Sidki, 1975).

Let's consider now the equation $AX+BY=C$. If we plot this equation we have a line that cuts the X-axis in $\frac{C}{A}$ and the Y-axis in $\frac{C}{B}$, as shown in Figure 1.

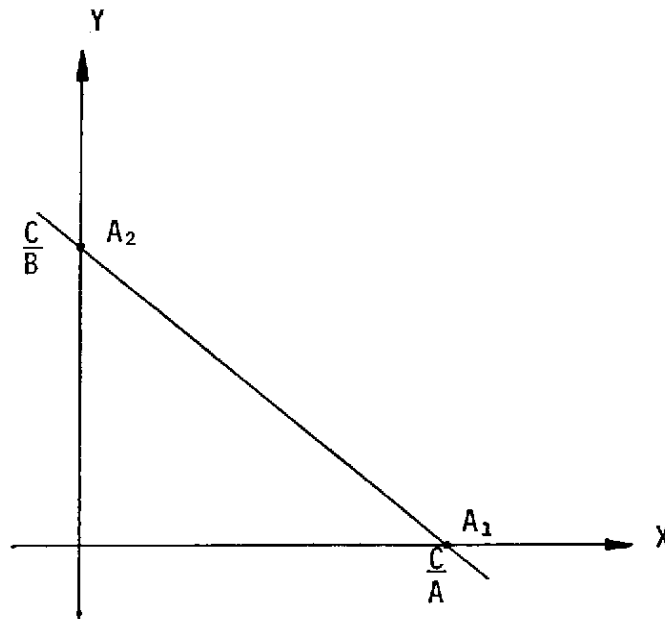


Figure 1 - Line $AX+BY=C$.

Let's call these points A_1 and A_2 , respectively. The distance between A_1 and A_2 is

$$\sqrt{\left(\frac{C}{A}\right)^2 + \left(\frac{C}{B}\right)^2} = \frac{C}{AB} \sqrt{A^2 + B^2}.$$

On the other hand, $AX+BY=C$ has integer solutions if the $\text{GCD}(A,B)$ divides C by Lemma 1.

Observe that if there is one integer solution to $AX+BY=C$, there will be infinitely many integer points in \mathbb{R}^2 that also satisfy this equation since

$$\begin{aligned} AX+BY &= C, \\ n(AB-BA) &= 0, \end{aligned}$$

and, therefore, adding these two equalities we get a third equality

$$A(X+nB) + B(Y-nA) = C,$$

which is satisfied for any $n \in \mathbb{R}$.

From this equality, one can also see that at distances of

$$\sqrt{A^2+B^2}$$

on the line $AX+BY=C$ there is at least one integer solution to this equation. Therefore it is sufficient to have $\frac{C}{AB} > 1$ to ensure an integer solution in the segment $A_1 A_2$.

This completes the explanation.

PROPOSTA PARA PUBLICAÇÃO

DATA
20/2/86

IDENTIFICAÇÃO	TÍTULO <i>A pseudo polynomial time algorithm for linear diophantine equations</i>	
	AUTORIA <i>Nei Yoshitomo Soma</i> <i>Horacio Hideaki Yamaue</i>	PROJETO/PROGRAMA <i>POPE3</i>
		DIVISÃO <i>DEP</i>
		DEPARTAMENTO <i>DIN</i>
DIVULGAÇÃO <input checked="" type="checkbox"/> EXTERNA <input type="checkbox"/> INTERNA MEIO:		

REVISÃO TÉCNICA	REVISOR TÉCNICO <i>Luiz Antonio N. Lorenz</i>	APROVADO: <input type="checkbox"/> SIM <input type="checkbox"/> NÃO <input type="checkbox"/> VER VERSO	APROVAÇÕES
	RECEBI EM: _____ REVISADO EM: _____	DATA _____ CHEFE DIVISÃO _____	
	OBSERVAÇÕES: <input checked="" type="checkbox"/> NÃO HÁ <input type="checkbox"/> VER VERSO	APROVADO: <input checked="" type="checkbox"/> SIM <input type="checkbox"/> NÃO <input type="checkbox"/> VER VERSO	
	DEVOLVI EM: _____ ASSINATURA <i>[Signature]</i>	<i>22/4/86</i> DATA <i>[Signature]</i> CHEFE DEPARTAMENTO	

REVISÃO DE LINGUAGEM	Nº: <i>247</i> PRIORIDADE: <i>2</i>	O(S) AUTOR(ES) DEVE(M) MENCIONAR NO VERSO, OU ANEXAR NORMAS E/OU INSTRUÇÕES ESPECIAIS	DATILOGRAFIA
	DATA: <i>23.05.86</i>		
	REVISADO <input type="checkbox"/> COM <input type="checkbox"/> SEM CORREÇÕES <input type="checkbox"/> VER VERSO	RECEBIDO EM: _____	
	POR: <i>Paula Prado de Carvalho</i> DATA: <i>28.5.86</i> ASSINATURA <i>Paula P. Carvalho</i>	CONCLUÍDO EM: <i>20/2/87</i> DATILOGRAFA: <i>[Signature]</i> ASSINATURA <i>[Signature]</i>	

PARECER	
FAVORÁVEL: <input type="checkbox"/> SIM <input type="checkbox"/> NÃO	VER VERSO <input type="checkbox"/> DATA _____ RESPONSÁVEL/PROGRAMA _____

EM CONDIÇÕES DE PUBLICAÇÃO EM: _____	AUTOR RESPONSÁVEL _____
--------------------------------------	-------------------------

Autorizo a publicação: <input type="checkbox"/> SIM <input type="checkbox"/> NÃO
DIVULGAÇÃO <input type="checkbox"/> INTERNA <input type="checkbox"/> EXTERNA MEIO: _____
OBSERVAÇÕES: _____
DATA _____ DIRETOR _____

SEC	PUBLICAÇÃO: <i>4183-PRE/1044</i> PÁGINAS: _____ ÚLTIMA PÁGINA: _____
	CÓPIAS: _____ TIPO: _____ PREÇO: _____