DOI: 10.1478/AAPP.921A2

AAPP | Atti della Accademia Peloritana dei Pericolanti
Classe di Scienze Fisiche, Matematiche e Naturali
ISSN 1825-1242

Vol. 92, No. 1, A2 (2014)

FAST RESOLUTION OF INTEGER VANDERMONDE SYSTEMS

ROSA DI SALVO [a] AND LUIGIA PUCCIO [a*]

ABSTRACT. The resolution of polynomial interpolation problems with integer coefficients directly involves the open issue of the integer inversion of a general Vandermonde matrix defined over the field $\mathbb{Z}/p\mathbb{Z}$, for p prime number. The purpose of this paper is to demonstrate the possibility to invert a Vandermonde matrix with integer *mod p* coefficients and exactly compute the integer inverse matrix in the ring $\mathscr{M}at(\mathbb{Z}/p\mathbb{Z})$ of square matrices over $\mathbb{Z}/p\mathbb{Z}$ through the new fast algorithm In$\mathscr{V}$anderMOD. The explicit formula derived for the integer inversion of Vandermonde matrices entirely develops inside the field of the integers *mod p*, with due consideration to the operation of integer division. The inversion procedure In$\mathscr{V}$anderMOD is valid for any prime number p and competitive in terms of computational effort, since its computational cost is less than $O(n^3)$.

1. Introduction

This paper deals with the processing of integers in the field $\mathbb{Z}/p\mathbb{Z}$ with special reference to the problem of the integer inversion of a Vandermonde matrix having integer *mod p* coefficients, issue that has been solved by the construction of a new fast algorithm called In$\mathscr{V}$anderMOD.

Vandermonde matrices play an important role both in mathematics and in applied sciences. The interest in this topic traces back to the sixties of the twentieth century and its relevance in the field of numerical analysis and signal processing is witnessed by many recent contributions (Dejnakarintra and Banjerdpongchai 2000; Eisinberg and Fedele 2006; Wertz 1965).

$$V_n = (x_i^{j-1})_{i,j=1,2,\ldots,n} = \begin{bmatrix} 1 & x_1 & x_1^2 & \ldots & x_1^{n-1} \\ 1 & x_2 & x_2^2 & \ldots & x_2^{n-1} \\ \vdots & \vdots & \vdots & \vdots & \\ 1 & x_n & x_n^2 & \ldots & x_n^{n-1} \end{bmatrix} \tag{1}$$

Eq. 1: *Vandermonde matrix from vector* $\mathbf{x} = [x_1, x_2, \ldots, x_n]$.

An ability to solve Vandermonde systems has been needed in many applications, with particular focus on interpolation, since solving the system of linear equations

$$V_n \mathbf{a} = \mathbf{y} \tag{2}$$

for n-vector $\mathbf{a}$ with V_n a Vandermonde matrix is equivalent to finding the coefficients a_i of the Lagrange interpolating polynomial of degree $\leq n-1$ that passes through the n points $P_i \equiv (x_i, y_i),\ i = 1, 2, \ldots, n$.

In this regard the relevance from the numerical point of view of the search of explicit formulas for the calculation of the analytical inverse of real Vandermonde matrices is due to the fact that Vandermonde problems are usually ill-conditioned and standard numerically stable methods in general fail to accurately compute the entries of the solution vector.
An alternative perspective on the matter is to consider symbolic computations over an algebraic field. It is trivial to observe that the inverse matrix of an integer matrix is not required to be an integer matrix, as the following example shows:

$$V_5 = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & 2 & 4 & 8 & 16 \\ 1 & 3 & 9 & 27 & 81 \\ 1 & 4 & 16 & 64 & 256 \\ 1 & 5 & 25 & 125 & 625 \end{bmatrix} \qquad V_5^{-1} = \begin{bmatrix} 5 & -10 & 10 & -5 & 1 \\ -6.42 & 17.83 & -19.50 & 10.17 & -2.08 \\ 2.96 & -9.83 & 12.25 & -6.83 & 1.46 \\ -0.58 & 2.17 & -3 & 1.83 & -0.42 \\ 0.04 & -0.17 & 0.25 & -0.17 & 0.04 \end{bmatrix}.$$

Let p be a prime number. Our new fast numerical algorithm (approaching the computational complexity of the "best" algorithm introduced by Wertz (1965)) is designed to work out precisely the special matrix inversion instance regarding the calculation of the integer *mod* p elements of the inverse in $\mathscr{M}at_n(\mathbb{Z}/p\mathbb{Z})$ of a Vandermonde matrix defined from a vector of distinct elements of $\mathbb{Z}/p\mathbb{Z}$.

Particularly, given a Vandermonde matrix $\overline{V_n}$ with entries in $\mathbb{Z}/p\mathbb{Z}$, we call "inverse *mod* p" of $\overline{V_n}$ the integer matrix $\overline{V_n}^{-1}$ in $\mathscr{M}at_n(\mathbb{Z}/p\mathbb{Z})$ such that $mod(\overline{V_n}\,\overline{V_n}^{-1},\ p) = I$.
Although this matter had been settled by Althaus and Leake (2006) just in limited circumstances, a resolution of the problem with general validity, as the one here proposed, is still interesting and innovative.

Such a kind of theory has non-trivial applications in the cryptographic context, being particularly linked to the problem of data privacy on Online Social Networks (OSNs), whose security issues have been addressed through the proposal of several key management techniques. An example of such privacy management approaches is given by the "group-oriented convergence cryptosystem" presented by Zhu *et al.* (2010), a scheme whose construction exactly requires the explicit calculation of the integer inverse of a Vandermonde matrix in the ring $\mathscr{M}at_n(\mathbb{Z}/p\mathbb{Z})$ of square matrices of order n over $\mathbb{Z}/p\mathbb{Z}$.

Moreover, it seems important to recall how a quite relevant application of Vandermonde matrices in the case of integer values is related to the computation of discrete Fourier transforms over finite fields, also known as number–theoretic transforms (NTT's), devised to efficiently perform fast cyclic convolutions without round–off errors. In this particular context, however, a fast inverse transformation can be obtained for free merely by replacing all root of unity references with their complex conjugate and scaling by the dimension at the end.

2. Description of the inversion formula

The starting point of the new integer inversion procedure consists in examining the best solution for the classical inversion of a Vandermonde matrix proposed by Wertz (1965).

Let's consider a set of distinct data points $P_i \equiv (x_i, y_i = f(x_i)),\ i = 1,2,\ldots,n$. The polynomial of degree $(n-1)$

$$p(x) = \sum_{i=1}^{n} f(x_i) \prod_{\substack{j=1 \\ j\neq i}}^{n} \frac{x - x_j}{x_i - x_j} = \sum_{k=1}^{n} a_k x^{k-1}, \tag{3}$$

is, of course, the Lagrange interpolation polynomial and, obviously, for x corrisponding to x_i it assumes the values $f(x_i)$.

$$p(x_i) = f(x_i) = \sum_{k=1}^{n} a_k x_i^{k-1} \ \Rightarrow\ \begin{bmatrix} 1 & x_1 & x_1^2 & \ldots & x_1^{n-1} \\ 1 & x_2 & x_2^2 & \ldots & x_2^{n-1} \\ \vdots & \vdots & \vdots & \vdots & \\ 1 & x_n & x_n^2 & \ldots & x_n^{n-1} \end{bmatrix} \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix} = \begin{pmatrix} f(x_1) \\ f(x_2) \\ \vdots \\ f(x_n) \end{pmatrix} \tag{4}$$

Looking at the equivalent system in (4) it is seen that the elements in the mth column of the inverse matrix are quite simply the a_k obtained by taking vectors $\mathbf{f}$ which are columns of the identity matrix

$$\sum_{k=1}^{n} a_k x^{k-1} = 1 \cdot \prod_{\substack{j=1 \\ j\neq m}}^{n} \frac{x - x_j}{x_m - x_j}. \tag{5}$$

Applying Horner's rule and Horner's rule "backwards" to compute the numerator of (5), this inversion method requires the least possible number n^2 of floating point operations.

Wertz's idea has been reformulated by Dejnakarintra and Banjerdpongchai (2000) with the definition of a fast algorithm directly based on the root–coefficient relation of a polynomial and the product of the differences of the roots.

That is, considering an n-th degree polynomial $Pn(z)$ having roots $a_1, a_2, \ldots, a_n$,

$$P_n(z) = (z-a_1)(z-a_2)\ldots(z-a_n) = z^n + A_1 z^{n-1} + \cdots + A_{n-1} z + A_n, \tag{6}$$

its coefficients A_i may be expressed in terms of the roots a_i, by the method suggested by Wertz, successively multiplying out the factors $(z-a_1), (z-a_2)$ and so on up to derive the general rule:

$$\begin{aligned} P_1(z) = (z-a_1) \quad &\rightarrow \quad A_1^{(1)} = -a_1 \\ P_2(z) = (z-a_1)(z-a_2) \quad &\rightarrow \quad \begin{cases} A_2^{(2)} = a_1 a_2 = -a_2 A_1^{(1)} \\ A_1^{(2)} = -a_1 - a_2 = A_1^{(1)} - a_2 \end{cases} \\ P_3(z) \quad &\rightarrow \quad \begin{cases} A_3^{(3)} = -a_1 a_2 a_3 = -a_3 A_2^{(2)} \\ A_2^{(3)} = a_1 a_2 - a_3(-a_1 - a_2) = A_2^{(2)} - a_3 A_1^{(2)} \\ A_1^{(3)} = -a_1 - a_2 - a_3 = A_1^{(2)} - a_3 \end{cases} \\ &\vdots \\ P_k(z) \quad &\rightarrow \quad \begin{cases} A_k^{(k)} = -a_k A_{k-1}^{(k-1)} \\ A_m^{(k)} = A_m^{(k-1)} - a_k A_{m-1}^{(k-1)} \quad (m = k-1, k-2, \ldots, 2). \\ A_1^{(k)} = A_1^{(k-1)} - a_k \end{cases} \end{aligned} \tag{7}$$

Removing the factor $(z-a_j)$ from the original $P_n(z)$

$$\begin{aligned} P_{n-1}(z) &= (z-a_1)\dots(z-a_{j-1})(z-a_{j+1})\dots(z-a_n) \\ &= z^{n-1}+A_{j,1}z^{n-2}+A_{j,2}z^{n-3}+\dots+A_{j,n-1}. \end{aligned}$$

and carrying on the derivation of all the $A_{j,k}$ at step $n-1$

$$\begin{cases} A_{j,1}^{(n-1)} = A_1^{(n)} + a_j \\ A_{j,m}^{(n-1)} = A_m^{(n)} + a_j A_{j,m-1}^{(n-1)} \quad (m=2,3,\dots,n-1), \end{cases}$$

the (j,k) element of V_n^{-1} is given, according to (5), as the quotient

$$A_{j,n-k}^{(n-1)}/D_j, \quad D_j = \prod_{\substack{k=1 \\ k\neq j}}^{n}(a_j-a_k), \tag{8}$$

whose denominator can be directly and efficiently calculated, in agreement with the minimal complexity $O(n^2)$.

2.1. In$\mathscr{V}$anderMOD procedure. Let p be a prime number. We developed an algorithm, called In$\mathscr{V}$anderMOD, to compute the inverse matrix internal on the ring $\mathscr{M}at(\mathbb{Z}/p\mathbb{Z})$ of square matrices over $\mathbb{Z}/p\mathbb{Z}$ of a Vandermonde matrix of order n having coefficients in the algebraic field $\mathbb{Z}/p\mathbb{Z}$.

This new inversion procedure has been explicitly derived on the basis of the relations about polynomial roots and coefficients, in the wake of what was done by Dejnakarintra and Banjerdpongchai (2000) and Wertz (1965), with the considerable innovation of working entirely within the field of integers *mod p*. In$\mathscr{V}$anderMOD (Algorithm **2.1**) takes as input the prime number p, which identifies the algebraic field, and the n-vector $\mathbf{x}$ whose equivalence classes are used to build the Vandermonde matrix reduced *mod p*. It calls first a secondary routine for the calculation of the parameters for the root–coefficient relation and then a procedure to derive the denominators and their inverses in in $\mathbb{Z}/p\mathbb{Z}$. Finally, it outputs the integer inverse matrix, denoted with VI.

A trivial consideration about the construction of this new inversion procedure concerns the choice of the prime number p, which must of course be greater than the size n of the vector $\mathbf{x}$ (which can't contain repeated classes) in order to avoid cases in which V_n results a singular matrix because of the validity of Fermat's Little Theorem:

$$n \geq p \Rightarrow \det \begin{bmatrix} 1 & x_1 & \dots & x_1^{p-2} & 1 & \dots & x_1^{n-1} \\ 1 & x_2 & \dots & x_2^{p-2} & 1 & \dots & x_2^{n-1} \\ \vdots & \vdots & & \vdots & \vdots & & \vdots \\ 1 & x_n & \dots & x_n^{p-2} & 1 & \dots & x_n^{n-1} \end{bmatrix} = \prod_{\substack{i,j=1 \\ i>j}}^{n}(x_i-x_j) = 0.$$

To efficiently derive the inverse *mod p* of a class so as to perform the arithmetic operation of division of two integers in $\mathbb{Z}/p\mathbb{Z}$ we resorted to the extended Euclidean algorithm based on Bezout's identity, stating that if y and p are positive integers, than there are always integers a and b so that the greatest common divisor $gcd(y,p)$ of y and p equals $ya+pb$. The algebraic formulation of this useful procedure calls the division algorithm successively until $gcd(y,p)$ pops out. Precisely, the extended Euclidean algorithm not only computes $gcd(y,p)$, but also returns the numbers a and b such that $gcd(y,p) = ya+pb$ and this property may be

exploited to compute the multiplicative inverse of a number. If $gcd(y,p) = 1$ this solves the problem of computing modular inverses, since a is the inverse of $y \ mod \ p$ and b is the inverse of $p \ mod \ y$.

The application of basic properties of congruences such as

$$\overline{x+y} = \overline{\overline{x}+\overline{y}}, \ \ \overline{x \cdot y} = \overline{\overline{x} \cdot \overline{y}} \ \ \forall \ \ x,y \in \mathbb{Z}$$

allow us to simplify further the procedure by operating the reduction mod p directly on the final result of each calculation. Furthermore, In$\mathscr{V}$anderMOD procedure is suitable to be implemented using appropriate libraries for the development and management of arithmetic on arbitrary-precision integers.

Algorithm 2.1: IN$\mathscr{V}$ANDERMOD(X,p)

comment: All the calculations are intended to be executed mod p.

$n \leftarrow$ LENGTH(X)

comment: External square brackets represent equivalence classes mod p.
The operation $*$ represents the matrix multiplication.

procedure PARAMETERS(X)
 $A[1] \leftarrow [-X[1] - X[2]]$
 $A[2] \leftarrow [X[1] * X[2]]$
 for $i \leftarrow 3$ **to** n
 do $\begin{cases} A[i] = [-X[i] * A[i-1]] \\ \textbf{for } j \leftarrow i-1 \textbf{ to } 2 \\ \quad \textbf{do } A[j] = [A[j] - X[i] * A[j-1]] \\ A[1] = [A[1] - X[i]] \end{cases}$
 return (A)

procedure DENOMINATORS(X)
 $D \leftarrow$ PRODUCTORY$([X[j] - X[k]])$
 $DI \leftarrow$ EXTENDEDEUCLIDEANALGORITHM(D)
 return (DI)

main
 for $i \leftarrow 1$ **to** n
 do $\begin{cases} N[1] = 1 \\ \textbf{for } j \leftarrow 1 \textbf{ to } n-1 \\ \quad \textbf{do } N[j+1] = A[j] + X[i] * N[j] \\ \textbf{for } k \leftarrow 1 \textbf{ to } n \\ \quad \textbf{do } VI[i,k] = N[n-k+1] * DI[i] \end{cases}$
 output (VI)

3. Computational effort

Concerning In$\mathscr{V}$anderMOD computational cost in terms of time complexity, the extended Euclidean algorithm provides a worthwhile solution to improve the efficiency of

the procedure by implementing the calculation of the inverse classes through a recursive function whose complexity, for $p = n+k, k \in \mathbb{N}$, is $O([\log(n+k)]^3) \subset O(n)$ finally.

In addition, the estimate of the costs in the worst case points out $(n-2)(n-1)/2 + 2n(n-1)$ multiplications/additions/reductions *mod* p to compute the intermediate values, to which must be added $n^2 \cdot \xi$ multiplications and as many reductions to complete the derivation of the integer inverse matrix, where ξ is the cost of the inversion *mod* p.

Therefore, our proposed algorithm has on the whole a complexity of $O([\log(p)]^3 n^2)$.

4. Numerical example

In $\mathscr{V}$anderMOD algorithm has been numerically tested for correctness for several values of the prime number p and many input n-vectors $\mathbf{x}$.

Examining the structure of the matrices in different image objects corresponding to various Vandermonde matrices, we observed a sort of peculiar graphical relationship arising from a Vandermonde matrix and its standard inverse. In fact, in general, the image associated with the inverse over $\mathbb{R}$ of a Vandermonde matrix, regardless of the nodal distribution, may be seen as the negative of the one associated with its transposed matrix.

The example reported in Figs. 1-3, which is referred to the case $p = 89$, is instead an evident proof of how the relationship between the graphical structure of a Vandermonde matrix and the one of its classical inverse does no longer continue in the case of the new integer inversion.

$$V_5 = \begin{bmatrix} 1 & 10 & 11 & 21 & 32 \\ 1 & 23 & 84 & 63 & 25 \\ 1 & 45 & 67 & 78 & 39 \\ 1 & 67 & 39 & 32 & 8 \\ 1 & 8 & 64 & 67 & 2 \end{bmatrix}$$

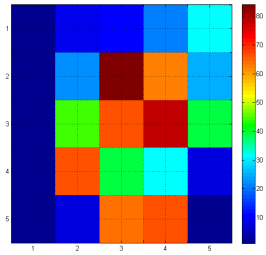

FIGURE 1. *Vandermonde matrix* $V_5 \in \mathscr{M}at(\mathbb{Z}/89\mathbb{Z})$.

$$V_5^{-1} = \begin{bmatrix} 0.9591 & -0.0452 & -0.8663 & 0.3867 & 0.5657 \\ -0.0081 & -0.0055 & 0.0078 & 0.0137 & -0.0079 \\ -0.0075 & 0.0339 & -0.0152 & 0.0012 & -0.0124 \\ -0.0065 & -0.0314 & 0.0262 & -0.0082 & 0.0200 \\ 0.0107 & 0.0121 & 0.0127 & -0.0114 & -0.0241 \end{bmatrix}$$

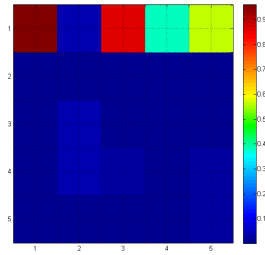

FIGURE 2. *Classical inverse matrix* $V_5^{-1} \in \mathscr{M}at(\mathbb{R})$.

$$\overline{V_5}^{-1} = \begin{bmatrix} 38 & 78 & 6 & 67 & 79 \\ 80 & 44 & 69 & 59 & 15 \\ 5 & 65 & 86 & 41 & 70 \\ 23 & 54 & 28 & 69 & 4 \\ 21 & 79 & 36 & 23 & 19 \end{bmatrix}$$

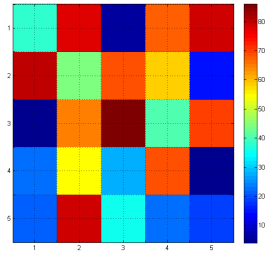

FIGURE 3. *Integer inverse matrix* $\overline{V_5}^{-1} \in \mathscr{M}at(\mathbb{Z}/89\mathbb{Z})$.

Of course,

$$V_5\,\overline{V_5}^{-1} = \begin{bmatrix} 2048 & 4895 & 3382 & 3293 & 1691 \\ 4272 & 11927 & 11481 & 9790 & 7031 \\ 6586 & 13706 & 12461 & 11748 & 6497 \\ 6497 & 7921 & 9167 & 8011 & 4094 \\ 2581 & 8366 & 8010 & 7832 & 4985 \end{bmatrix} = \overline{I_5},$$

where $\overline{I_5}$ is the identity matrix of the ring $\mathscr{M}at(\mathbb{Z}/89\mathbb{Z})$.

5. Conclusion

Taking a cue from a particular cryptographic issue related to privacy protection on online social networks, we explicitly derived the new fast algorithm In$\mathscr{V}$anderMOD for the computation of the inverse over $\mathbb{Z}/p\mathbb{Z}$ of an integer Vandermonde matrix with computational complexity $O([\log(n+k)]^3 n^2)$. Strong points corroborating the use of this procedure are clearly related to the finite representability of integer values in any base, taking into account the fact that the form adopted to represent the numbers on an electronic data processor is a crucial element for the modalities of execution of arithmetic operations.

Closely connected to this fact is the evaluation of the accuracy of descriptions with integer values and the appreciation of the stability of an algorithm exclusively operating on integers with total lack of approximation. Secondarily, it makes sense to reflect on the improvement of the execution time of operations (adding and multiply classes directly), on the speed of a computer unit working with numbers consisting of a few bits (with possible applications in image processing and signals) and, lastly, on the portability of this procedure to specific environments for large integers.

Acknowledgements

This research has been performed within the activities of GNCS of INdAM.

References

Althaus, H. and Leake, R. (2006). "Inverse of a finite-field Vandermonde matrix (Corresp.)" *IEEE Trans. Inf. Theor.* **15**(1), 173–173. DOI: 10.1109/TIT.1969.1054253.

Dejnakarintra, M. and Banjerdpongchai, D. (2000). "An algorithm for computing the analytical inverse of the Vandermonde matrix". *3rd Asian Control Conference (ASCC)*.

Eisinberg, A. and Fedele, G. (2006). "On the inversion of the Vandermonde matrix". *Applied Mathematics and Computation* **174**(2), 1384–1397. DOI: 10.1016/j.amc.2005.06.014.

Golub, G. H. and Van Loan, C. F. (1996). *Matrix Computations*. Johns Hopkins Studies in the Mathematical Sciences. Johns Hopkins University Press.

Wertz, H. (1965). "On the numerical inversion of a recurrent problem: The Vandermonde matrix". *Automatic Control, IEEE Transactions on* **10**(4), 492–492. DOI: 10.1109/TAC.1965.1098206.

Zhu, Y., Hu, Z., Wang, H., Hu, H., and Ahn, G.-J. (2010). "A collaborative framework for privacy protection in online social networks". In: *Collaborative Computing: Networking, Applications and Worksharing (CollaborateCom), 2010 6th International Conference on*, pp. 1–10.

---

[a] Dipartimento di Matematica e Informatica
Università degli Studi di Messina
Messina, Italy

[*] To whom correspondence should be addressed | Email: gina@unime.it

Communicated 5 June 2014; published online 22 October 2014