ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 4, Issue 6, December 2014

Solving Simultaneous Linear Equations using Finite Fields On Hybrid GPU-Accelerated Multi-core Systems

González, H.E.[1], and Carmona, L., J.J.[2]
[1] Information Technology Department, ININ,
[2] Information Technology Department, ININ

Abstract*— In this paper a parallel code for solving simultaneous linear equations with integral coefficients are presented. The solution is obtained by applying the "Chinese Remainder Theorem" avoiding floating point operations. Modular arithmetic is the best for solving ill conditioned matrices. The algorithm used can be extended to sets of equations with the same algebraic structure with real coefficients. These algorithms present an $O(n^3)$ computational complexity when $(\mathbf{A}, \mathbf{b}) \subset \mathbf{R}^n$ on hybrid gpu-accelerated multi-core systems.

***Index Terms*— Chinese Remainder Theorem, equations over finite fields, GPU Multi-core Systems, , ill conditioned matrices, modular arithmetic, simultaneous linear equations.**

I. INTRODUCTION

A Linear System of Equations (LSE) can be defined as a set of *m* equations with *n* unknowns represented by a matrix **A**, a vector **b** and an unknown vector **x**, namely, $\mathbf{Ax} = \mathbf{b}$. Many methods have been proposed to solve such linear equations. Recently the authors proposed a new **LU** decomposition which solves the system of linear equations like Cramer's rule but efficiently [1-2], this can cause a buffer overflow when the word length of the computer is exceeded, so to avoid this, Modular Arithmetic is proposed.

II. ALGEBRAIC STRUCTURE

Modular Arithmetic is a very versatile tool discovered by K.F.Gauss (1777-1855) in 1801 [3-9]. Two numbers **a** and **b** are said to be equal or congruent modulo **N** written **N**|(**a-b**), if their difference is exactly divisible by **N**. Usually (and in this paper) **a**,**b**, are nonnegative integers and **N** is a positive integer. We write **a** ≡ **b** (**mod N**).

The set of numbers congruent modulo **N** is denoted $[\mathbf{a}]_N$. If $\mathbf{b} \in [\mathbf{a}]_N$ then, by definition, **N**|**(a-b)** or, in other words, **a** and **b** have the same remainder on division by **N**. Since there are exactly **N** possible remainders upon division by **N**, there are exactly **N** different sets $[\mathbf{a}]_N$.

Quite often these **N** sets are simply identified with the corresponding remainders**:** $[\mathbf{0}]_N = \mathbf{0}$, $[\mathbf{1}]_N = \mathbf{1}$,..., $[\mathbf{N-1}]_N = \mathbf{N-1}$. Remainders are often called *residues*; accordingly, the **[a]'s** are also known as the *residue classes*.

It is easy to see that if **a** ≡ **b (mod N**) and **c** ≡ **d (mod N)** then **(a+c)** ≡ **(b+d) (mod N).** The same is true for multiplication. This allows us to introduce an **algebraic structure** into the set $\{[\mathbf{a}]_N: \mathbf{a=0,1,...,N-1}\}$.

By definition:

1. $[\mathbf{a}]_N + [\mathbf{b}]_N = [\mathbf{a} + \mathbf{b}]_N$
2. $[\mathbf{a}]_N \times [\mathbf{b}]_N = [\mathbf{a} \times \mathbf{b}]_N$

Subtraction is defined similarily:

$$[\mathbf{a}]_N - [\mathbf{b}]_N = [\mathbf{a} - \mathbf{b}]_N$$

and it can be verified that the set $\{[\mathbf{a}]_N: \mathbf{a=0,1,...,N-1}\}$ becomes a **ring** with **commutative** addition and multiplication.
Division cannot be always defined. To give an obvious example:

$[\mathbf{5}]_{10} * [\mathbf{1}]_{10} = [\mathbf{5}]_{10} * [\mathbf{3}]_{10} = [\mathbf{5}]_{10} * [\mathbf{5}]_{10} = [\mathbf{5}]_{10} * [\mathbf{7}]_{10} = [\mathbf{5}]_{10} * [\mathbf{9}]_{10} = [\mathbf{5}]_{10}$.

So $[\mathbf{5}]_{10}/[\mathbf{5}]_{10}$ cannot be defined uniquely.

We also see that:

$[\mathbf{5}]_{10} * [\mathbf{2}]_{10} = [\mathbf{5}]_{10} * [\mathbf{4}]_{10} = [\mathbf{5}]_{10} * [\mathbf{6}]_{10} = [\mathbf{5}]_{10} * [\mathbf{8}]_{10} = [\mathbf{5}]_{10} * [\mathbf{0}]_{10} = [\mathbf{0}]_{10}$.

Something we never had either for integer or real numbers. The situation improves for prime **N's** in which case division can be defined uniquely. Observe the multiplication tables below for prime **N**. For the multiplication and division table we have removed the **0** column and row. Every row (and column) contains all non-zero remainders mostly messed up. So every row is a permutation of the first row in the table. This provides an easy way to construct division tables too. For prime **N**, the set $\{[\mathbf{a}]_N: \mathbf{a=0,1,...,N-1}\}$ can be upgraded to a **field.**

Table N=5

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 4, Issue 6, December 2014

Addition

	0	1	2	3	4
0	**0**	**1**	**2**	**3**	**4**
1	**1**	**2**	**3**	**4**	**0**
2	**2**	**3**	**4**	**0**	**1**
3	**3**	**4**	**0**	**1**	**2**
4	**4**	**0**	**1**	**2**	**3**

Subtraction

	0	1	2	3	4
0	**0**	**1**	**2**	**3**	**4**
1	**4**	**0**	**1**	**2**	**3**
2	**3**	**4**	**0**	**1**	**2**
3	**2**	**3**	**4**	**0**	**1**
4	**1**	**2**	**3**	**4**	**0**

Multiplication

	1	2	3	4
1	**1**	**2**	**3**	**4**
2	**2**	**4**	**1**	**3**
3	**3**	**1**	**4**	**2**
4	**4**	**3**	**2**	**1**

Division

	1	2	3	4
1	**1**	**2**	**3**	**4**
2	**3**	**1**	**4**	**2**
3	**2**	**4**	**1**	**3**
4	**4**	**3**	**2**	**1**

For **non prime N**, most **rows contain zeros** and **repeated entries**.
The tables exhibit a variety of patterns. To mention a few
a) For addition, consecutive rows result from the first one by circular rotation of entries.

b) Addition and multiplication tables are symmetric with respect to the main diagonal (the line that goes from the top left to the bottom right corner.)

c) Subtraction tables are not symmetric but the rows are still obtained from the first one by rotation of entries. (We subtract numbers in the leftmost column from the numbers in the topmost row.)

d) In multiplication tables, the last row is always a reverse of the first row.

e) In multiplication tables modulo **N**, rows corresponding to numbers *coprime* with **N** contain permutations of the first row.

f) For prime **(N+1)**, multiplication tables offer multiple and simultaneous solutions to the rook problem: On an **NxN** board position **N** rooks so that they command the whole board and none may capture another. To solve, select a digit, replace all its occurrences with a rook, remove all other digits.

g) Under the same conditions, *1* always appears in the upper left and lower right corners and nowhere else on the main diagonal.

h) 6/5 = 4 (mod 7) or, which is the same, $\mathbf{[6]_7/[5]_7 = [4]_7}$

i) One can use addition and subtraction tables to play the same game as with the Calendar Tables.

j) For multiplication tables, this is also true provided selected entries are multiplied instead of being added up.

k) For multiplication tables, both diagonals are palindromic, i.e. each is the same in both directions.

l) If an addition table has an odd number of rows, then every remainder occurs on the main diagonal.

m) In subtraction tables with an odd number of rows, the second diagonal is a permutation of the first row.

n) In addition tables with an even number of rows, the main diagonal contains only a half of all the remainders. The remainders on the diagonal appear twice each.

o) In multiplication tables with a number of rows **N** where **(N+1)** is prime, the same is also true: the main diagonal contains only a half of all the remainders. The remainders on the diagonal appear twice each.

p) In the table of multiplication by **N**, rows corresponding to the numbers coprime with **N** consist of permutations of the first row. The reverse does not hold.

III. CHINESE REMAINDER THEOREM

According to D.Wells [10-14], the following problem was posed by Sun Tsu Suan-Ching (4th century AD): There are certain things whose number is unknown. Repeatedly divided by 3, the remainder is 2; by 5 the remainder is 3; and by 7 the remainder is 2. What is the number?

Oystein Ore [9] mentions another puzzle with a dramatic element from *Brahma-Sphuta-Siddhanta* (Brahma's Correct System) by Brahmagupta (born 598 AD):

An old woman goes to market and a horse steps on her basket and crashes the eggs. The rider offers to pay for the damages and asks her how many eggs she had brought. She does not remember the exact number, but when she had taken them out two at a time, there was one egg left. The same happened when she picked them out three, four, five, and six at a time, but when she took them seven at a time they came out even. What is the smallest number of eggs she could have had?

Problems of this kind are all examples of what universally became known as the *Chinese Remainder Theorem*. In

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 4, Issue 6, December 2014

mathematical parlance the problems can be stated as finding **n**, given its remainders of division by several numbers $m_1,m_2,...,m_k$:

$n = n_1 \pmod{m_1}$
$n = n_2 \pmod{m_2}$
...
$n = n_k \pmod{m_k}$

The modern day theorem is best stated with a couple of useful notations. For non-negative integers $m_1,m_2,...,m_k$, their *greatest common divisor* is defined as:

$gcd(m_1,m_2,...,m_k) = max\{s: s|m_i, \text{ for } i=1,...,k\}$,

Where, as usual, **"s|m"** means that **s** divides **m** exactly. The *least common multiple* of **k** numbers is defined as

$lcm(m_1,m_2,...,m_k) = min\{s: s>0 \text{ and } m_i|s, \text{ for } i=1,...,k\}$,

Both **gcd()** and **lcm()** are **symmetric functions** of their arguments. They are complementary in the sense that, for **k = 2**, $gcd(m_1,m_2)lcm(m_1,m_2) = m_1m_2$.

However, for **k>2** a similar identity does not in general hold. For an example, consider two triplets: {2,4,16} and {2,8,16}. Both have exactly the same gcd and lcm but obviously different products. On the other hand, both **gcd** and **lcm** are *associative*:

$gcd(m_1, (gcd(m_2, m_3)) = gcd(gcd(m_1, m_2), m_3)$

and, both equal $gcd(m_1, m_2, m_3)$.

Similarly,

$lcm(m_1, (lcm(m_2, m_3)) = lcm(lcm(m_1, m_2), m_3)$

Associativity allows one to proceed a step at a time with an inductive argument without putting all eggs into a basket at once. Jumping at the opportunity we will prove the most basic case of **k=2**.

Theorem
Two simultaneous congruences $n \equiv n_1 \pmod{m_1}$ and $n \equiv n_2 \pmod{m_2}$ are only solvable when $n_1 \equiv n_2 \pmod{gcd(m_1,m_2)}$. The solution is unique modulo $lcm(m_1,m_2)$.

When m_1 and m_2 are **coprime** their **gcd is 1**. By convention, $a \equiv b \pmod 1$ is simply understood as the usual **equality a = b**.

Proof

The first congruence is equivalent to $n = tm_1 + n_1$, the second to $n = sm_2 + n_2$, for some integers **t** and **s**.

Equating we obtain

(1) $tm_1 - sm_2 = n_2 - n_1$.

The left-hand side is divisible by $gcd(m_1,m_2)$. So, unless the right-hand side is also divisible by $gcd(m_1,m_2)$, there could not possibly exist **t** and **s** that satisfy the identity.

Now let's assume that $gcd(m_1,m_2)|(n_2 - n_1)$ and denote $n_0 = (n_2 - n_1)/gcd(m_1,m_2)$. Then, **(1)** can be written as

(2) $t(m_1/gcd(m_1,m_2)) = n_0 \pmod{(m_2/gcd(m_1,m_2))}$

By definition, $m_1/gcd(m_1,m_2)$ and $m_2/gcd(m_1,m_2)$ are coprime; since we are dividing m_1 and m_2 by their largest common factor. Therefore, by a generalization of Euclid's Proposition, **(2)** has a solution. Given **t**, we can determine $n = tm_1 + n_1$. This proves the existence part.

To prove the uniqueness part, assume **n** and **N** satisfy the two congruences. Taking the differences we see that

(3) $N-n = 0 \pmod{m_1}$ and $N-n = 0 \pmod{m_2}$

which implies $N-n = 0 \pmod{lcm(m_1,m_1)}$.
Let's now solve the two problems we started this section with.

Problem # 1

Solve

p1: $x = 2 \pmod 3$
p2: $x = 3 \pmod 5$
p3: $x = 2 \pmod 7$

From **p1**, $x = 3t + 2$, for some integer **t**. Substituting this into **p2** gives $3t = 1$. Looking up **1/3** in the division table **modulo 5**, this reduces to a simpler equation

p4: $t = 2 \pmod 5$

which, in turn, is equivalent to $t = 5s + 2$ for an integer **s**. Substitution into $x = 3t + 2$ yields $x = 15s + 8$. This now goes into **p3:** $15s + 8 = 2 \pmod 7$. *Casting out 7* gives $s = 1 \pmod 7$. From here, $s = 7u + 1$ and, finally, $x = 105\,u + 23$.

Note that $105 = lcm(3,5,7)$. Thus we have solutions **23, 128, 233**, ...

Problem # 2

Solve

q1: $x = 1 \pmod 2$
q2: $x = 1 \pmod 3$
q3: $x = 1 \pmod 4$
q4: $x = 1 \pmod 5$
q5: $x = 1 \pmod 6$
q6: $x = 0 \pmod 7$

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 4, Issue 6, December 2014

With the experience we acquired so far, the combination of q1-q5 is equivalent to

q7: x = 1 (mod 60)

x = 60t + 1. Plugging this into **q6** gives **60t = -1 (mod 7)**. *Casting out* 7 yields **4t = 6 (mod 7)** and then **2t = 3 (mod 7)**. From division tables modulo 7, **3/2 = 5 (mod 7).** Therefore, **t = 7u + 5**. Finally, **x = 420u + 301**. Allowing for an average size farmer, the most likely number of eggs she might expect to be compensated for is **301**.

IV. A RESIDUE SYSTEM OF EQUATIONS

Consider the linear algebraic system of equations $Ax = b$. Even if **A** and **b** are required to be integral there is no guarantee that **x**, the solution vector, will be integral. On the other hand, when we write the residue system of equations $|A\bar{x}|_M = |b|_M$ with **A** and **b** integral, we seek an integral vector $|\bar{x}|_M$ which satisfies it. In general, then, **x** and $|\bar{x}|_M$ are different and it would appear that $|\bar{x}|_M$ would not aid us in finding **x**; however, it turns out that this is not the case. We can use residue arithmetic in solving it and this will lead us to a solution of $Ax = b$, where **A** and **b** are integral.

It is more practical in a general situation to select a set of moduli $m_1, m_2, ..., m_s$, with $M = m_1 m_2 ... m_s$ because, this enables us to obtain results modulo **M** by doing most of the arithmetic modulo m_i, for $i = 1,2,\ldots,s$. To be more specific, we select a set of moduli $m_1, m_2, ..., m_s$, with $(m_i, m_j) = 1$ for $i \neq j$. Let $d = \det A$ and $y = A^{adj} b$. We shall assume there are sufficient moduli (large enough) so that **M** satisfies $(d, M) = 1$ and $M > 2\max\left(|d|, \max_i |y_i|\right)$.

We solve the residue systems $|A\bar{x}|_{m_i} = |b|_{m_i}$ for $i = 1,2,\ldots,s$, (for each of the moduli) and obtain the residue representations $d \sim \{|d|_{m_1}, |d|_{m_2}, \ldots, |d|_{m_s}\}$ and $y \sim \{|y|_{m_1}, |y|_{m_2}, \ldots, |y|_{m_s}\}$. From these two s-tuples we can determine $|d|_M = |y|_M$ and if **M** is large enough, we can determine **d** and **y** and, ultimately, $x = A^{-1} b$.

There are various algorithms for obtaining $|d|_M$ and $|y|_M$. Perhaps the best known procedure makes use of a classic theorem from the theory of numbers called the Chinese Remainder Theorem.

Theorem. Let $m_1, m_2, ..., m_s$ be the base for a residue number system with $(m_i, m_j) = 1$ for $i \neq j$, and let $M = m_1 m_2 ... m_s$. Also, let $\hat{m}_j = \frac{M}{m_j}$. Now, if **q** has the residue representation $q \sim \{r_1, r_2, ..., r_s\}$ where $r_i = |q|_{m_i}$ $i = 1,2,...,s$ then $|q|_M = \left| \sum_{j=1}^{s} \hat{m}_j \left| r_j \hat{m}_j^{-1} (m_j) \right|_{m_j} \right|_M$.

Obtaining **x** from $|\bar{x}|_M$.

Fortunately, we can obtain **x** if we are willing to do the additional work. Obviously, we need to compute $|d|_M$ and $|y|_M$ since **x** is obtained from **y** by dividing the components of **y** by **d**. It should be pointed out that only at this point do we leave residue arithmetic, and so only at this point do we introduce rounding errors. Actually, if the division is merely indicated, but never carried out, then there will be no errors introduced.

Theorem. If the modulus **M** is chosen so that

i) $M > 2|d|_M$

And if d' is formed from $|d|_M$ so as to satisfy

ii) $|d'|_M = |d|_M$

iii) $|d'|_M < M/2$

Then d'=d.

In addition, the modulus **M** is chosen so that

iv) $M > 2\max_i |y_i|_M$

And if y' is formed from $|y|_M$ so as to satisfy

v) $|y'|_M = |y|_M$

vi) $\max_i |y'|_M < M/2$

Then y'=y.

Briefly, these conditions are satisfied for $M > 2\max\left(|d|, \max_i |y_i|\right)$

In practice, the moduli are chosen as large prime numbers. This choice increases the probability that $(d, m_i) = 1$ and that $|d|_{m_i} \neq 0$. We recall that if these two conditions are

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 4, Issue 6, December 2014

satisfied, then **A** is nonsingular modulo m_i, and the residue system $\left|A\bar{x}\right|_{m_i} = \left|b\right|_{m_i}$ can be solved for $\left|d\right|_{m_i}$ and $\left|y\right|_{m_i}$. If the two conditions are not satisfied, then we simply select another prime for a modulus. Furthermore, by choosing prime numbers for the moduli, we guarantee that $\left(m_i, m_j\right) = 1$ for $i \neq j$, and hence, there is a unique integer in the interval (0,m-1) with the given residue representation.

V. RESULTS

As an illustration we use the matrix [15-16]:

$$A = \left(y + \delta_{ij} x\right); \quad \delta_{ij} = 1 \quad \forall \quad i = j;$$

$$\delta_{ij} = 0 \quad \forall \quad i \neq j \; ; \quad b = \begin{pmatrix} ny + x \\ . \\ . \\ . \\ ny + x \end{pmatrix} ;$$

The value of the determinant and the adjugate matrix are known

$$|A| = x^{n-1}(x + ny)$$

$$A^{+} = \begin{pmatrix} x^{n-2}\left[x + (n-1)\right] & -x^{n-2}y & . \; . \; . & -x^{n-2}y \\ -x^{n-2}y & x^{n-2}\left[x + (n-1)\right] & . \; . \; . & -x^{n-2}y \\ . & . & . \; . \; . & . \\ . & . & . \; . \; . & . \\ . & . & . \; . \; . & . \\ -x^{n-2}y & -x^{n-2}y & . \; . \; . & x^{n-2}\left[x + (n-1)\right] \end{pmatrix}.$$

The program we used was written in the style of **CUDA-C** using some intrinsic subroutines of this language. The code was tested on a **TESLA 2070-Q** at high performance computing area of the UNISON (ACARUS).

We choose $x = 1, y = 1$ and we conducted experiments for four numbers **N** of equations, namely: **N=1000,5000,10000** and **25530** and we used 448 cores with 5.375 Gb in RAM Memory.

The following table and graphic shown the times in usual **Integer Arithmetic** and overhead times for the solutions using **Uni-Modular Arithmetic**.

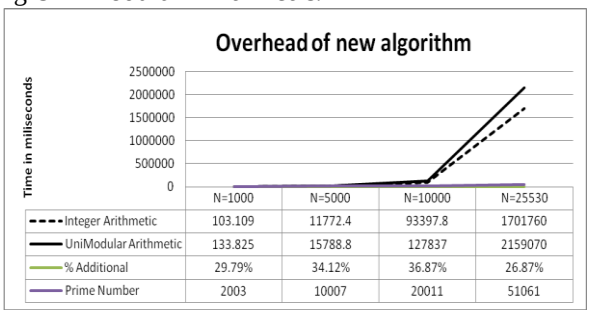

Fig. 1 Obtained results

VI. CONCLUSIONS

The traditional user of scientific computing prefers to use well proven routines that are recognized by the international scientific community. Among the well known collections are IMSL, NAG, and LINPACK. However, a direct solution method should be used in the case of dense non structured matrices. If, in addition the coefficients and the right hand side are integers and an exact solution is desired, the most affordable alternative is to use residual arithmetic on hybrid GPU-Accelerated Multi-core Systems.

ACKNOWLEDGMENT

The authors would like to thank their colleague at the University of Sonora, María del Carmen Heras Sánchez, she has been a director of the high performance computing area of the UNISON (ACARUS).

REFERENCES

[1] González, H.E., **"**Método Cramer–LU aplicado al Algoritmo Simplex**"**. Tesis Doctoral. DEPFI-UNAM. 2005.

[2] González, H.E., Carmona L., J.J., Computación y Sistemas Vol. 17 No. 3, 2013 pp. 413-422. ISSN 1405-5546.

[3] González, H.E., Cruz, M., E., Investigación Operacional Vol. 23 No. 2, 2002 pp. 175-184. ISSN 0257-4306.

[4] J.H.Conway and R.K.Guy, The Book of Numbers, Springer-Verlag, NY, 1996.

[5] H.Davenport, The Higher Arithmetic, Harper&Brothers, NY.

[6] K.Devlin. Mathematics: The Science of Patterns, Scientific American Library, 1997.

[7] R.Graham, D.Knuth, O.Potashnik, Concrete Mathematics, 2nd edition, Addison-Wesley, 1994.

[8] P.Hilton, D.Holton, J.Pederson, Mathematical Reflections, Springer Verlag, 1997.

[9] Oystein Ore, Number Theory and Its History, Dover Publications, 1976.

[10] S.K.Stein, Mathematics: The Man-Made Universe, 3rd edition, Dover, 2000.

[11] H.Davenport, The Higher Arithmetic, Harper&Brothers, NY.

[12] P.J.Davis and R.Hersh, The Mathematical Experience, Houghton Mifflin Company, Boston, 1981.

[13] R.Graham, D.Knuth, O.Potashnik, Concrete Mathematics, 2nd edition, Addison-Wesley, 1994.

[14] D.Wells, The Penguin Book of Curious and Interesting Puzzles, Penguin Books, 1992**.**

[15] Young, David M.; Gregory, Robert Todd. A Survey of Numerical Mathematics. Volume II. Dover Publications, Inc., 1972.

[16] http://www.nvidia.com/object/cuda_home_new.html.

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 4, Issue 6, December 2014

AUTHOR BIOGRAPHY

H. E. González. He received the PhD in Operations Research at the National Autonomous University of Mexico (UNAM) in 2005. He has been working in research activities for more than twenty years. He has published a book and more than ten scientific papers. Presently, he is a full-time researcher at the National Institute of Nuclear Research (ININ) at the Department of Systems.

J.J. Carmona L., He received his B.S. in Electronic Engineering from UAM. Presently, he is a full-time researcher at the National Institute of Nuclear Research (ININ) at the Department of Systems.