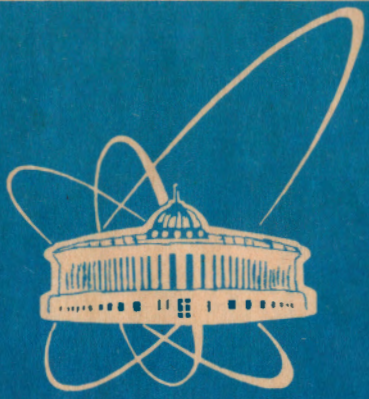

сообщения
объединенного
института
ядерных
исследований
дубна

E10-94-450

V.I.Ilyushchenko

REVERSIBLE ARITHMETIC — ADDITION, SUBTRACTION, MULTIPLICATION AND DIVISION

1994

Илющенко В.И.
E10-94-450

Реверсивная арифметика — сложение, вычитание, умножение и деление

Известно, что стандартная операция деления обеспечивает наиболее общее представление целых чисел, $n = q * d + r$. За счет существенного изменения алгоритма деления автору удалось разработать новый реверсивный алгоритм индуцированного деления (ID), реализуемый в виде большого числа разных версий и обладающий необычными свойствами. Версия декрементного ID $n \oslash b \Leftrightarrow q_b(n)$ дает, например, для $n = 23$ и $b = 2$ индуцированное частное (с $r = 0$) $23 \oslash 2 \Leftrightarrow 7$ вместо стандартного $23:2 = 11$ (с $r = 1$). Последовательное применение аксиомы реверсивности обеспечивает реверсивные операции индуцированного умножения, сложения и вычитания, что позволяет сформировать базис новой реверсивной арифметики.

Работа выполнена в Лаборатории высоких энергий ОИЯИ.

Сообщение Объединенного института ядерных исследований. Дубна, 1994

Ilyushchenko V.I.
E10-94-450

Reversible Arithmetic — Addition, Subtraction, Multiplication and Division

The standard arithmetic operation of division is known to provide the most general representation of integer numbers, $n = q * d + r$. By a drastic change in the division algorithm the author deduced and tested the novel reversible Induced Division (ID) algorithm allowing for many specific versions and possessing uncommon properties. The decremented ID version $n \oslash b \Leftrightarrow q_b(n)$ yields e.g. for $n = 23$ and $b = 2$ induced quotient (with $r = 0$) $23 \oslash 2 \Leftrightarrow 7$ instead of the standard $23:2 = 11$ (with $r = 1$). The consecutive use of the reversibility axiom allows to deduce the reversible operations of induced multiplication, addition and subtraction, thus forming the basis of the novel reversible arithmetic.

The investigation has been performed at the Laboratory of High Energies, JINR.

Communication of the Joint Institute for Nuclear Research. Dubna, 1994

Die ganze Zahl schuf der liebe Gott,
alles uebrige ist Menschenwerk.
L.Kronecker (1823 – 1891)
(The integer number was created by the beloved Lord,
the rest is a man's work. - VII.)

1 Introduction

The novel techniques developed for the general solution of unstable inverse problems [1] are based on the mathematical axiom of reversibility between the left–hand side, L, and the right–hand side, R, of any equivalence relation

$$L \Longleftrightarrow R \tag{1}$$

The consistent implementation of this axiom (1), however seemingly quite trivial, results in robust solution techniques of Systems of Linear Algebraic Equations (SLAE) [2], robust Least SQuares (LSQ) techniques [3] etc.

Here we describe the first version of reversible arithmetic based on the above reversibility axiom.

2 Standard Arithmetic

The basic four arithmetic operations – addition, subtraction, multiplication and division – are known to be classified into two main categories. These correspond to direct operations, i.e. addition and multiplication, and their inverse counterparts, subtraction and division, respectively. On the other hand, addition and subtraction can be called operations of the first order, while multiplication and division, those of the second order. The last classification reflects the fact that the arithmetic operations of the second order can be reduced, at least on computer, to the arithmetic operations of the first order [4].

The basic properties of addition and multiplication are as follows [5].

2.1 Addition

1. $a + b$ is always a number or, in other words, the operation of addition is always, without any exceptions, executable (as opposed to subtraction being not always executable in the domain of positive numbers).
2. The sum $a + b$ is always defined in a unique way.
3. There is valid an associative law: $(a + b) + c = a + (b + c) = a + b + c$.
4. There is valid a commutative law: $a + b = b + a$
5. There is valid a law of monotonicity: if $b > c$, then $a + b > a + c$.

2.2 Multiplication

1. $a * b$ is always a number.
2. The product $a * b$ is always unique.

3. The associativity law: $a * (b * c) = (a * b) * c = a * b * c$.
4. The commutativity law: $a * b = b * a$
5. The monotonicity law: if $b > c$, then $a * b > a * c$.

2.3 Distributivity etc

Finally, there is valid a combined distributivity law: $a * (b + c) = a * b + a * c$.

It is also important for our subsequent analysis that the standard arithmetic deals only with the numbers of a certain single type, e.g. integers,n. Positive integers are known to form the natural scale $0, 1, 2, ...N$, with $N \to \infty$.

Another important point concerns the most general representation of numbers. One can easily see that it is provided by division:

$$n = q * d + r \tag{2}$$

where q – a quotient, d – a divisor and r – a residue. If $r = 0$, $q = 1$ and $d = n$, then n is called a prime number, if $r = 0$, $q \neq 1$ and $d \neq n$, then n is called a composite number [6].

Generally, with $r = 0$, the inverse (divisibility) problem cannot be solved for a large scalar n composed of 100 and more digits even by means of the biggest modern supercomputers. This simple fact forms the basis of the second absolute cryptographic system, i.e. the so–called public–key (RSA) cryptography [7].

However, the operation of division was till now not used in information coding, data compression and other similar scientific and technological domains of interest.

3 Reversible Arithmetic

The standard operation of division is essentially a single–step one – we divide a given dividend n by a given divisor d and obtain a quotient q and a residue r, e.g. 23 = 11*2 + 1 ($n = 23$, $q = 11$, $d = 2$, $r = 1$) or 23 = 7*3 + 2 ($n = 23$, $q = 7$, $d = 3$, $r = 2$).

3.1 Examples of Induced Division (ID)

Now we will drastically change the logic of division algorithm:

23:2 -to made $n = 23$ dividable by $d = 2$
let us subtract from 23 a unity (1)
11:2 -let us subtract from 11 a unity (1)
5:2 - let us subtract from 5 a unity (1)
2:2 - let us subtract from 2 a zero (0)

so that the final partial quotient $q = 1$.

We call this algorithm the Decremented Induced Division (DID) to be written down as $23 \oslash 2 \Longleftrightarrow 7$ (where $\oslash$ is the ID sign), i.e. to result in an induced DID quotient (inquot) $q_b(n) = (0111)_2 = 7$.

Here $d = b = 2$ is called a dibasor so that $n = 23 \Longleftrightarrow 7 \otimes 2$ with $r = 0$ (where $\otimes$ is the Induced Multiplication (IM) sign).

In short, in the new arithmetic the operation of division becomes a multistep one to be specified by the final partial quotient $q = 1$ and the final residue $r = 0$. As a net result, the inverse IM operation of can be completely described by the bit structure of the inquot, $q_2(n)$.

The Incremented Induced Division (IID) for the same $n = 23$ and $d = b = 2$ looks like:

23:2 -to made $n = 23$ dividable by $d = 2$
let us add to 23 a unity (1)
12:2 -let us add a zero (0)
6:2 - let us add a zero (0)
3:2 - let us add a unity (1)
2:2 - let us add a zero (0)

so that the final partial quotient $q = 1$.
Here again the induced quotient (inquot) $Q_b(n) = (01001)_2 = 9$.

Now let us consider once again the patterns of binary DID and IID inquots by starting from below, i.e. the ciphers in the above r.h.s. parenthized columns. For the DID algorithm we obtain

$$23 = 2^4 + (0111)_2 = 16 + 7 \tag{3}$$

while for the IID algorithm we obtain

$$23 = 2^5 - (01001)_2 = 32 - 9 \tag{4}$$

3.2 Generalized formulations

The above induced division algorithm allows such versions as InterMittent Induced Division (IMID), Randomized Induced Division (RID) etc, thus producing a series of cryptographic codes with the relevant cryptographic keys in the form of specific division patterns (inquots). In addition, each such algorithm can be iterated or recursed since input and output of the induced division have identical numerical forms.

Furthermore, the above algorithms can be easily generalized for any dibasor $d = b$. However, for $b > 2$ instead of BITs (Binary digiITs) we deal with DITs

(Decimal digITs) forming the explicit digital structure of inquots, e.g. $q_3(23) = 23 - 3^2 = n - z = (112)_3 = 14$ (DID) or $Q_3(23) = 3^3 - 23 = Z - n = (011)_3 = 4$ (IID).

The first scale limit, z, is called a lower zero, while the second scale limit, Z, is called an upper zero, with $R = (Z - z)$ being an inquot range. Thus, instead of the single natural scale $N = 0, 1, 2, ...$ used in the standard arithmetic, here we have the quantized natural scale, $N_b = N_2 = 0, 1; 0, 1, 2, 3; 0, 1, 2, 3, 4, 5, 6, 7; ...$ etc specified by many partial zeroes.

Thus, in the reversible arithmetic all numbers are quite naturally subdivided into two fundamental classes corresponding to inquots and dibasors.

4 Induced Addition and Subtraction

4.1 Induced Subtraction (IS)

The reversible operation of division

$$n : b \Longleftrightarrow q_b(n) \tag{5}$$

can be considered as an equivalent of the reversible operation of subtraction

$$n \cdot \frac{b-1}{b} n \Longleftrightarrow q_b(n) \tag{6}$$

where $\cdot$ is the IS sign.

4.2 Induced Addition (IA)

The reversible IM operation

$$q_b(n) \cdot b \Longleftrightarrow n \tag{7}$$

where $\cdot$ is the IM sign, can be used for deducing an exact form of reversible addition.

However, the reversible operation of addition can be more simply deduced from the relevant operation of subtraction as

$$q_b(n) \oplus \frac{b-1}{b} n \Longleftrightarrow n \tag{8}$$

where $\oplus$ is the IA sign.

5 Conclusion

Thus, the novel arithmetic possesses the following main properties within the natural scale:

1. All integers are subdivided into two main classes - inquots and dibasors.
2. Reversible Induced Division allows a set of different versions (DID, IID, IMID etc) to be formulated and specified by a common feature of $q = 1$, where q is a final partial quotient.

As a net result, all integers become composite within the reversible arithmetic - there is no primes at all.

3. The "continuous" natural scale with the single zero point is changed for a quantized natural scale with multiple zeroes.
4. As opposed to the standard arithmetic operations of addition and multiplication, their reversible counterparts do not possess such properties as commutativity, associativity etc.
5. The reversible arithmetic can be effectively used for information coding, data compression, cryptographic applications, calculations by means of computers etc.
6. The problems to be solved deal with extensions of the reversible arithmetic into rational, irrational, transcendental etc numeric domains as well as with algebraic extensions of different kind, e.g. modular, polynomial etc.
7. The reversibility axiom results not only in a novel arithmetic but also in the robust techniques for solving LSQ, SLAE and many other fundamental problems of data processing.

6 Acknowledgments

The author would like to thank late Prof. L.Kronecker for his deep insight into the problem under study. The author also acknowledges the generous support provided by Prof.A.I.Malakhov within the SPHERE collaboration.

References

[1] V.I.Ilyushchenko,
Reversible Mathematics - an Artificial Science or a Scientific Art ?,
JINR Preprint E10-92-343, JINR, Dubna (1992).

[2] V.I.Ilyushchenko,
The Novel Approach to Solving Systems of Linear Algebraic Equations (SLAE),
JINR Preprint E10-93-403, JINR, Dubna (1993).

[3] V.I.Ilyushchenko,
The Reversible Robust Least Squares Techniques,

JINR Preprint, JINR, Dubna (1994)(to be published).

[4] D.E.Knuth,
The Art of Computer Programming, v.2,
Addison Wesley, Reading (1969).

[5] F.Klein,
Elementarmathemtik von hoheren Standpunkte, B.1,
Springer, Berlin (1924).

[6] H.Riesel,
En Bok om Primtal,
Studentlitteratur, Stockholm (1968) (in Swedish).

[7] Rivest R.L., Shamir A. and Adleman A.,
Comm. ACM, 21, 120 (1978).

Received by Publishing Department
on November 23, 1994.