A functional technique based on the Euclidean algorithm with applications to 2-D acoustic diffractal diffusers

Luis Cortés-Vega
Mathematics Department, Antofagasta University, Casilla 170, Antofagasta, Chile
E-mail: luis.cortes@uantof.cl, luisvega@vtr.net

Abstract. We built, based on the Euclidean algorithm, a functional technique, which allows to discover a direct proof of Chinese Remainder Theorem. Afterwards, by using this functional approach, we present some applications to 2-D acoustic diffractal diffusers. The novelty of the method is their functional algorithmic character, which improves ideas, as well as, other results of the author and his collaborators in a previous work [2].

1. Introduction
In a historical context, the Chinese remainder theorem, CRT, was proposed to solve some astronomical problems. Now, is one of the main theorems of number theory [10]. Over the years, CRT has been played a prominent role due to its applicability in diverse fields of science and engineering, as photo radar [6], cryptography and code theory [1,4], circuits on systems [7], technology of diffusers [3] and matrix theory [8], among others.

The aim of this paper is twofold: 1) The first one, is to exploit some functionals expressions based on the Euclidean algorithm in order to describe a direct proof of CRT. It should be stressed that the origins of this approach appear in [2], however, there no analysis of the CRT has been considered, so far. In this context, the results of this paper are new and they complement previous theoretical results given in [2]. 2) Second one, we are interested in to characterize functionally the depths \(d_{h,k}\) of a 2-D acoustic diffractal diffuser, which have the following form

\[
d_{h,k} = \left\{ \left\lfloor \frac{h}{N} \right\rfloor^2 + \left\lfloor \frac{k}{N} \right\rfloor^2 \right\}_{\mod M} \frac{\lambda_M}{2M} + \left\{ \left(\frac{h}{\mod M}\right)^2 + \left(\frac{k}{\mod M}\right)^2 \right\}_{\mod N} \frac{\lambda_N}{2N}. \tag{1}
\]

Here, \(M \in \mathbb{N}^*\) and \(N \in \mathbb{N}^*\) are prime numbers associated with low and high frequency; \(\lambda_M\) and \(\lambda_N\) are the wavelengths of the low frequency diffusser and high frequency diffusser, respectively. Also in the same formula, the expression \(\lfloor \cdot \rfloor\) denotes the integer floor function, and the expression \((a)_{\mod N}\) is the usual modular representation of \(a\). It is important to emphasize that the \(d_{h,k}\) depths are associated to the \((h, k)\)th position of a series of wells separated by thin fins, all inside of a 2-D acoustic diffractal diffuser. We address in this part of paper to answer the next two questions: 1) Which is the minimum amount of information needed in order to accelerate the computation of the \(d_{h,k}\) numbers ? - This is certainly an interesting question, since it plays a
role in many facets associated to the building of diffractal for industrial use, see [3]-, and 2) It plays some role, in the answer to this first question the CRT?

In all of our discussion, N will designate the set of natural numbers, \( a \in \mathbb{N}^* \) if \( a \in \mathbb{N} \cup \{0\} \). Furthermore, it will be used the simbol \( \gcd(b, d) \) to denote the greatest common divisor between \( b \) and \( d \) (not both zero). In this notation, if \( \gcd(a, b) = 1 \), we say that \( a \) and \( b \) are relatively prime.

2. Preliminaries

We present first given some basic facts about the representation of natural number. Indeed, the Euclidean algorithm implies that

\[
a = r_0 + r_1 b + r_2 b^2 + \ldots + r_{n-1} b^{n-1} + r_n b^n, \quad 0 \leq r_i \leq b - 1, \text{ for all } i = 0, 1, 2, \ldots, n.
\]

(2)

Here, \( a, b \in \mathbb{N}^* \) and \( b \geq 2 \), additional details can be found in [10]. From here, we can define on \( \mathbb{N}^* \) the following functions

\[
\phi_b : \mathbb{N}^* \to \mathbb{N}^*, \quad \phi_b(a) = \begin{cases} a, & \text{if } 0 \leq a \leq b - 1, \\ r_0, & \text{if } a \geq b. \end{cases}
\]

Definition 1 Let \( b, d \in \mathbb{N}^* \) with \( b, d \geq 2 \). We define the composition of \( C_d \) with \( C_b \), and of \( \phi_d \) with \( \phi_b \) by a usual way, that is: \( C_d \circ C_b : \mathbb{N}^* \to \mathbb{N}^* \), such that \( (C_d \circ C_b)(a) \overset{\text{def}}{=} C_d(C_b(a)) \) and \( \phi_d \circ \phi_b : \mathbb{N}^* \to \mathbb{N}^* \) such that \( (\phi_d \circ \phi_b)(a) \overset{\text{def}}{=} \phi_d(\phi_b(a)) \), for all \( a \in \mathbb{N}^* \).

We begin by establishing the following

Theorem 2 Let \( a, b, d \in \mathbb{N}^* \), with \( b \geq 2 \). Then the following properties are valid:

\[\begin{align*}
\phi(0) &= 0, \\
\phi_{b \cdot d}(a) &= 0, \text{ for all } d \in \mathbb{N}^*, \\
\phi_{b \cdot b} &= \phi_{b \cdot d}, \\
\phi_{b \cdot (a + d)} &= \phi_{b \cdot (a) + \phi_b(d)} = \phi_{b \cdot (a) + d}, \\
\phi_{b \cdot (a \times d)} &= \phi_{b \cdot (a) \times d} = \phi_{b \cdot (a \times d)}, \\
\phi_{b \cdot (a + b)} &= \phi_{b \cdot b} (\text{"periodicity" of } \phi_b). \\
C_b(0) &= 0, \\
C_b(b) &= a, \text{ in particular } C_b(b) = 1, \\
C_b(b^n) &= b^{n-1}, \\
C_b(\phi_b(a)) &= 0, \text{ (} C_b \text{ is a "annihilator" of } \phi_b \text{),} \\
C_b(a + d) &= C_b(a) + C_b(d) = C_b(\phi_b(a) + \phi_b(d)), \\
C_b(a \times d) &= C_b(a \times d) = C_b(\phi_b(a) \times \phi_b(d)), \\
C_b(a + b) &= C_b(a) + 1 \text{ (} C_b \text{ is "quasi-periodic"),} \\
\phi_{b \cdot b}(a) &= \phi_{b \cdot d}(a) (a < b) \text{ if and only if } C_b(a) = 0, \\
C_b(\phi_b(a)) &= C_b(\phi_b(a)).
\end{align*}\]

Proof. In order to prove the Theorem 2, we have that \((\phi_1), (\phi_2), (c1), (c2), (c3)\) and \((c1)\) are direct. The proof of \((\phi_3), (\phi_4), (\phi_5)\) and \((\phi_6)\) can be found in [2]. In the same lines of reasoning as in [2], one can also check that the rest of the items are straightforward from the definition of \(\phi_b\) and \(C_b\), respectively. Note that in particular, the identity \((c5)\) follows from definition of \(C_b(a)\) and the property \((\phi_4)\). Also, \((c6)\) follows direct from the extension of the property \((c5)\) for "d" summands, \((c2)\) follows of definitions of \(C_b\) and \(\phi_b\). Finally, the proof of property \((c3)\) follows by using all previous properties. This last property will be key in the proof of CRT. ■
3. A direct proof of CRT via a functional approach

As a first step, we start with the following

**Definition 3** In our approach, if $a$ and $b$ are relatively prime, henceforth the symbol $i_b(a)$ will be denoted the moduli multiplicative inverse of $a$. That is, $i_b(a) \in \{0, 1, 2, \ldots, b - 1\}$ and

$$\phi_b \left( a \times i_b(a) \right) = 1.$$

Note that if $a$ and $b$ are relatively prime, the number $i_b(a)$ always exists and verifies the following additional identity:

$$i_b(a) = i_b(\phi_b(a)).$$

Now, we will center on the following Theorem:

**Theorem 4** Assume $b, d \in \mathbb{N}^*$, with $b, d \geq 2$. Then, for all $a \in \mathbb{N}^*$ we have

$$\phi_{d \times b}(a) = \phi_d(a) + d \times \phi_b(C_d(a)).$$

**Proof.** Is direct, by applying $C_d$ to the numerical value of $C_b(a)$, together with the definitions of $C_d$ and $C_{d \times b}$ and the properties (e1) and (e3) of Theorem 2, respectively.

**Remark 5** Our first observation is that, once established the expression (4), one can proof the validity of the expression (5), given below:

$$\phi_{d \times b}(a) = \phi_d(a) + b \times \phi_d(C_b(a)),$$

for all $a \in \mathbb{N}^*$. With the following Theorem, we reached our first goal.

**Theorem 6** Let $b_1$ and $b_2$ relatively prime in $\mathbb{N}$, with $b_1$, $b_2 \geq 2$. Let $\gamma$ and $\beta$ be two arbitrary numbers such that $\gamma \in \{0, 1, \ldots, (b_1 - 1)\}$ and $\beta \in \{0, 1, \ldots, (b_2 - 1)\}$, respectively. Then we can find in the set $\{0, 1, 2 \ldots, (b_1 \times b_2 - 1)\}$ one unique element $\hat{a}$ that satisfies the system:

$$\begin{cases}
\phi_{b_1}(a) = \gamma, \\
\phi_{b_2}(a) = \beta.
\end{cases}$$

**Proof.** We shall prove that the expression $\hat{a} = \phi_{b_1 \times b_2}(a)$, obtained from the expression (4)-(5), is the unique solution of system (6) in $\{0, 1, 2 \ldots, (b_1 \times b_2 - 1)\}$. In fact, we first note that $\hat{a} = \phi_{b_1 \times b_2}(a) < b_1 \times b_2$, follows direct by the definition of $\phi_{b_1 \times b_2}(a)$. By applying $\phi_{b_1}$ to $\hat{a}$, plus the aid of Theorem 4, we get $\phi_{b_1}(\hat{a}) = \phi_{b_1}(\phi_{b_1 \times b_2}(a)) = \phi_{b_1}(\phi_{b_1}(a) + b_1 \times \phi_{b_2}(C_{b_1}(a)))$.

Then by property $(\phi 4)$ of Theorem 2 we find that

$$\phi_{b_1}(\hat{a}) = \phi_{b_1}(\phi_{b_1}(a)) + \phi_{b_2}(b_1 \times \phi_{b_2}(C_{b_1}(a))).$$

So, by the property $(\phi 2)$, from this equality we get: $\phi_{b_1}(\hat{a}) = \phi_{b_1}(\phi_{b_1}(a)) = \gamma$. Now, by a similar argument, and the aid of the Remark 5, we get the other identity, that is, $\phi_{b_2}(\hat{a}) = \phi_{b_2}(\phi_{b_1 \times b_2}(a)) = \phi_{b_2}(a) = \beta$. The uniqueness is direct. Now, it is important to count in applications with an explicit version of the solution. Indeed, if the min $\{b_1, b_2\} = b_1$ the solution $\hat{a}$ of (6) can be expressed by the formula:

$$\hat{a} = \beta + b_2 \times \phi_{b_1}(\phi_{b_2}(b_2)) \times [\gamma + \beta \times (b_1 - 1)].$$

(7)
If on the contrary, min \( \{b_1, b_2\} = b_2 \) the the form explicit to consider, it must be

\[
\hat{a} = \gamma + b_1 \times \phi_{b_2} \{i_{b_2} (\phi_{b_2} (b_1)) \times [\beta + \gamma \times (b_2 - 1)]\}. \tag{8}
\]

Note that in both expressions (7) and (8), it is important the fact that both \( b_1 \) and \( b_2 \) are relatively prime in \( \mathbb{N} \).

Finally, we shall given an example to illustrate an application of (7) and (8). In fact, for the system

\[
\begin{align*}
\phi_7(a) &= 3, \\
\phi_9(a) &= 7.
\end{align*}
\tag{9}
\]

all the conditions of Theorem 6 can be verified. Now, \( \min \{7, 9\} = 7 \). As we have already mentioned, the expression (7) yields to: \( \hat{a} = 7 + 9 \times \phi_7 \{i_7 (\phi_7 (9)) \times [3 + 7 \times (7 - 1)]\} \). Hence, \( \hat{a} = 7 + 9 \times \phi_7 \{i_7 (2) \times [3 + 7 \times 6]\} \).

As, \( i_7 (2) = 4 \), we get \( \hat{a} = 7 + 9 \times \phi_7 \{4 \times [3 + 7 \times 6]\} \). Now, by the properties \( (\phi_5), (\phi_4) \) and \( (\phi_2) \) of Theorem 2, we get \( \phi_7 \{4 \times [3 + 7 \times 6]\} = 5 \). Therefore, \( \hat{a} = 52 < 63 \).

4. About Diffractional diffusers
A diffuser is a technology to obtain a pleasant sound atmosphere for one or more receivers. To appreciate the importance of the study of this type of technology, see e.g., the book by Cox and D’Antonio [3]. Here, the mathematical expression vital in the building of 2-D acoustic diffractional diffuser is:

\[
d_{h,k} = \left\{ \frac{h}{N} \right\}^2 + \left\{ \frac{k}{N} \right\}^2 \mod M \times \frac{\lambda_M}{2M} + \left\{ (h \mod M)^2 \mod N + (k \mod M)^2 \mod N \right\} \times \frac{\lambda_N}{2N}, \tag{10}
\]

where \( d_{h,k} \) denotes the depth of the \((h,k)^{th}\) well of 2-D diffractional, also \( N \in \mathbb{N}^* \) and \( M \in \mathbb{N}^* \) are two prime numbers, \( \lambda_N \) and \( \lambda_M \) denote the wavelengths of the low frequency diffuser and high frequency diffuser, respectively. In the next Theorem we give one response to the two questions posed in the introduction. Before, we need some preliminaries Lemmas.

**Lemma 7** Assume \( b \in \mathbb{N}^* \), with \( b \geq 2 \). Then for all \( a \in \mathbb{N}^* \) we have that:

\[
\text{(I) } \phi_b(a) = \begin{cases} a, & \text{if } 0 \leq a \leq b - 1, \\
(a \mod b), & \text{if } a \geq b \end{cases} \quad \text{and (II) } C_b(a) = \begin{cases} a, & \text{if } 0 \leq a \leq b - 1, \\
\lfloor \frac{a}{b} \rfloor, & \text{if } a \geq b. \end{cases}
\]

**Proof.** In the last section of [2], we prove that under these hypotheses the identity (I) above is valid. On the other hand, the identity (II) follows direct of the property (e2) on Theorem 2, together with the identity (I), the definition of \( C_b(a) \) and the equality \( a = (a \mod b) + b \lfloor \frac{a}{b} \rfloor \), as shown in [5].

Of this form, by using the Lemma 7, we can rewrite the \( d_{h,k} \) numbers in a transparent functional way. More precisely we have

\[
d_{h,k} = \phi_M \left( C_N^2(h) + C_N^2(k) \right) \times \frac{\lambda_M}{2M} + \left\{ \phi_N \left( \phi_M^2(h) \right) + \phi_N \left( \phi_M^2(k) \right) \right\} \times \frac{\lambda_N}{2N}. \tag{11}
\]

**Remark 8** In (11), we have that \( h, k \in \mathbb{N}^* \) are arbitrary, \( C_N^2(h) = C_N(h) \times C_N(h) \), \( \phi_M^2(k) = \phi_M(k) \times \phi_M(k) \), and the other variables have the same Physical significance than in (10).
Lemma 9 Assume $b, d \in \mathbb{N}^*$, with $b, d \geq 2$. Then for all $a \in \mathbb{N}^*$ we have
\[
\phi_d (\phi_b (a)) = \phi_d [\phi_b (\phi_{b \times d} (a))]
\]
and
\[
\phi_d (C_b (a)) = C_b (\phi_{b \times d} (a)).
\]

Proof. The proof of (12) and (13) follows direct by of the expressions (4) and (5), and properties of Theorem 2.

Theorem 10 Assume $M, N \in \mathbb{N}^*$, with $M, N \geq 2$ are primes numbers. Then for all $h, k \in \mathbb{N}$ we have
\[
d_{h,k} = F_{h,k} \times \frac{\lambda_M}{2M} + G_{h,k} \times \frac{\lambda_N}{2N},
\]
where
\[
F_{h,k} = \phi_M \left[ C_N^2 (\phi_{M \times N} (h)) + C_N^2 (\phi_{M \times N} (k)) \right]
\]
and
\[
G_{h,k} = \left\{ \phi_N \left( \phi_M^2 (\phi_{M \times N} (h)) \right) + \phi_N (\phi_M^2 (\phi_{M \times N} (k))) \right\}.
\]

Proof. The proof follows direct by of (11) and the equalities given in Lemma 9 given above, together with the properties of Theorem 2.

Theorem 10, from a computational point of view, it is exactly what we need, since rather than using natural numbers $h$ and $k$ on direct way, the arguments of functions $C_N$ and $\phi_M$ in formula (11) can be used their residual representations on $M \times N$, and so to make a fast computation on a residual number system. This is transparent, since the functional expressions $\phi_{M \times N} (h)$ and $\phi_{M \times N} (k)$ are intrisic to the $d_{h,k}$ depths. It is interesting to note that here, the CRT plays a role important to convert the computation of $\phi_N (h)$, $\phi_M (h)$, $\phi_N (k)$ and $\phi_M (k)$ into $\phi_{M \times N} (h)$ and $\phi_{M \times N} (k)$, respectively. Theorem 10 then, answers the two questions posed at the beginning of this section. Numerical simulations will be presented in a future work.

5. Conclusions
We considered a technique based on the Euclidean algorithm, where the novel scenario is their functional algorithmic character. We obtained a direct proof of Chinese Remainder Theorem, CRT, and then it is shown that the functional expressions $\phi_{M \times N} (h)$ and $\phi_{M \times N} (k)$ are intrisic to the $d_{h,k}$ depths, this is in order to accelerate their computation. Here it is a key to note that the diffuser diffractal combines the property of self-similarity of fractals [9] with uniform scattering exhibiting Schroeder diffuser, and producing an an extended bandwidth of sound. Results, related with the theoretical part of this paper, are a complement of those given in [2], which, with appropriate modifications, can be extended to general Euclidean domains. Finally, with our exposition, we seek to motivate and to familiarize the reader with this type of approach and with the technology of diffusers.

Acknowledgments
I am especially indebted to professor Dr. Pablo Martín de Julian, academic of Department of Physics at the University of Antofagasta, who went through the whole paper and recommended several valuable modifications and corrections.

Work supported by Decanatura de la Facultad de Ciencias Básicas, Universidad de Antofagasta, and Grant FONDECYT N° 1121103, Chile.
6. References
[1] Asmuth, C. A. and Bloom J., A modular approach to key safeguarding, IEEE Transactions on Information Theory IT-29, 208-210, (1983).
[2] Cortés–Vega L. A., Rojas-Castro D. E., Santiago–Ayala Y. S. and Rojas–Romero S. C., “A technique based on the Euclidean algorithm and its applications to Cryptography and Nonlinear Diophantine Equations”, Proyecciones. J. Math., 26, 309–333 (2007).
[3] Cox T. J. and D’Antonio P., “Acoustic Absorbers and Diffusers: Theory, Design and Application”, 2nd ed. Abington, Oxfordshire: Taylor & Francis, (2009).
[4] Ding C., Pei D. and Salomaa A., “Chinese remainder theorem: applications in computing, coding, cryptography, World Scientific Publishing Co., Inc., (1996).
[5] Knuth, D. E., “The Art of Computer Programming”, Addison-Wesley, (1972).
[6] Sullivan R. J., “Microwave Radar Imaging and Advanced Concepts”, 2nd ed. Scitech Pub Inc, (2004).
[7] Wang Y., Residue to binary converters based on net Chinese remainder theorems. IEEE Trans Circuits Syst II, 47, 197-204. (2000).
[8] Fiol M.A., Congruences in Z”, finite Abelian groups and the Chinese remainder theorem. Discrete Math. 67,101-105 (1987).
[9] Mandelbrot B. B., “The fractal Geometry of Nature”, Freeman, San Fransisco (1983).
[10] Niven I., Zuckerman S. H. and Montgomery H., “An introduction to the theory of numbers”, 5nd ed. Jhon Wiley & Sons, Inc., (1991).