Some Related Functions to Integer GCD and Coprimality

S. M. Sedjelmaci
LIPN, CNRS UPRES-A 7030
Université Paris-Nord,
Av. J.B.-Clément, 93430 Villetaneuse, France.
sms@lipn.univ-paris13.fr

December 15, 2009

Abstract: We generalize a formula of B. Litow [7] and propose several new formula linked with the parallel Integer Coprimality, Integer GCD and Modular Inverse problems as well. Particularly, we find a new trigonometrical definition of the GCD of two integers $a, b \geq 1$:

$$\gcd(a,b) = \frac{1}{\pi} \int_0^{\pi} \cos[\,(b-a)x\,]\ \frac{\sin^2(abx)}{\sin(ax)\,\sin(bx)}\ dx.$$

We also suggest a generalization of the GCD function to real numbers.

Keywords: Integer GCD, Coprimality, Modular Inverse, Parallel Complexity.

1 Introduction

1.1 Parallel Complexity of Integer GCD

The problems of the parallel computation of the Integer GCD (Greatest Common Divisor), coprimality and modular inverse of integers are still open: we do not know if they belong to the NC class [6]. As far as we know, there are only a few works dealing with these questions, since first being stated by A. Borodin et al. [1] in 1982. Although the sequential case is satisfactory (subquadratic GCD algorithm [8, 3]), the parallel case is still resistant. It seems to be hard to find a fast parallel GCD algorithm. The best presently known parallel performance is $O(n/\log n)_\epsilon$ time with $O(n^{1+\epsilon})$ processors on the CRCW PRAM model, for any $\epsilon > 0$, by Chor and Goldriech [2], Sorenson [11] and the author [9], where n is the the number of bits of the larger integer. All the presently known GCD algorithms are based on reduction steps which reduce the size of the pair of integers until they reach 0, the previous one being the GCD. It seems that this approach has reached its limit and new ideas must be explored to improve the parallel complexity of the Integer GCD and its related problems.

1.2 A new Approach

Throughout the paper, a and b are two positive integers, their GCD is denoted by $d = \gcd(a, b)$. The pair of integers a and b are said to be coprime if and only if $\gcd(a, b) = 1$. The Kronecker symbol δ of two reals x, y is defined as follows: $\delta_x^y = 1$ if $x = y$ and 0 otherwise. The expression $\exp(z)$ means the exponential of a complex z, i.e.: $\exp(z) = e^z$. The ceil and floor functions of a real x are defined by $\lceil x \rceil = \min\{\text{ integer } k \mid k \geq x\}$ and $\lfloor x \rfloor = \max\{\text{ integer } k \mid k \leq x\}$.

B. Litow [7] suggested a sieve function related to the coprimality problem. It is defined as follows ($0 < \rho < 1$):

$$S(a, b) = \int_0^1 \frac{ds}{z(1 - \rho^a z^a)(1 - \rho^b / z^b)} \ , \tag{1}$$

where $z = \exp(2\pi\iota s)$, ι is the complex number such that $\iota^2 = -1$ and $\rho = 1 - 1/ab$. It is easy to prove (see Lemma 2.3) that, if a and b are coprime and $\rho = \exp(-1/2ab)$, then $S(a, b) > 0.58$, otherwise $S(a, b) = 0$ when $\gcd(a, b) \geq 2$.

In this paper we present a closed formula of $S(a, b)$ as well as tight lower bound. Moreover, we prove that the sieve function defined in (1) can be used to compute Bézout coefficients and modular inverse as well. We generalize this formula and propose several new formula linked with these problems. Particularly, we find a new trigonometrical definition of the GCD of two integers $a, b \geq 1$:

$$\gcd(a, b) = \frac{1}{\pi} \int_0^\pi \cos[\,(b - a)x\,] \ \frac{\sin^2(abx)}{\sin(ax)\ \sin(bx)} \ dx. \tag{2}$$

This definition shows that the GCD of two integers $a, b \geq 1$ is nothing but the $|b - a|$-th coefficient of the cosine Fourier series for the function

$$P(x) = \ \frac{\sin^2(abx)}{\sin(ax)\ \sin(bx)}.$$

Moreover, we also show that the $|b - a - 2|$-th coefficient of the cosine Fourier series for the same function $P(x)$ gives a coprimality sieve function.

Our aim is not to compute exactly the GCD by the trigonometrical integral (Eq. 2), but rather to find a parallel algorithm which approximate its value with a good error control. As a matter of fact, if such approximation can be done by an NC algorithm, i. e.: a parallel algorithm running in a polylogarithmic time with a polynomial number of processors, then we will prove simultaneously that Integer GCD, Coprimality and Modular Inverse problems will be all in the NC class.

1.3 The main idea:

Let n be an integer. The starting point is the following orthogonality formula:

$$I_n = \int_0^1 z^n \ ds = \begin{cases} 0 & \text{if } n \neq 0, \\ 1 & \text{if } n = 0, \end{cases} \quad \text{where } z = \exp(2\pi\iota s).$$

This formula is the basis for the residue theorem, Cauchy formula for complex function and Fourier analysis as well. Moreover, if instead of n, we use any discrete function $F(n_1, \ldots, n_p)$, then it may be used to give the number of solutions of the Diophantine equation $F(n_1, \ldots, n_p) = 0$. As a matter of fact, it was successfully used to attack the Goldbach conjecture first by Ramanujan and Hardy [4], then by Hardy-Littlewood [5] early in 1918-1919 and later on by Vinogradov [12] for a weak version of Goldbach conjecture. The aim of this paper is to apply this approach to some open questions in parallel computation problems like, integer GCD, modular inverse and coprimality.

This paper is organized as follows: Section 2 deals with weighted series related to coprimality and integer GCD. Section 3 is devoted to finite sums approach following Vinogradov's ideas [12]. We conclude with some remarks and open questions.

2 Weighted Series

First, we give two Lemmas which are frequently used throughout the paper:

Lemma 2.1 *Let $a, b \geq 1$ be two integers and let $d = \gcd(a, b)$, then the equation*

$$\begin{cases} pa - qb = 0 \\ 0 \leq p < b \quad \text{and} \quad 0 \leq q < a. \end{cases}$$

have exactly d solutions given by

$$\begin{cases} p = \lambda \times (b/d) \\ q = \lambda \times (a/d) \quad \text{with} \quad \lambda = 0, 1, 2, \ldots, d-1. \end{cases}$$

Proof: Let $a_1 = a/d$ and $b_1 = b/d$, then $\gcd(a_1, b_1) = 1$ and since $d \geq 1$ we obtain $pa_1 = qb_1$. Since $\gcd(a_1, b_1) = 1$, b_1 must divides p, so we let $p = \lambda b_1 = \lambda \times (b/d)$ for some integer λ and $q = \lambda a_1 = \lambda \times (a/d)$. Moreover, $0 \leq p = \lambda b_1 = \lambda \times (b/d) < b$, then $0 \leq \lambda \leq d - 1$. *QED*

Lemma 2.2 *Let $a, b \geq 2$ be two integers and let $d = \gcd(a, b)$, then the equation*

$$\begin{cases} pa - qb = 1 \\ 0 \leq p < b \quad \text{and} \quad 0 \leq q < a. \end{cases}$$

have no solution if $\gcd(a, b) \geq 2$ and a unique solution if $\gcd(a, b) = 1$.

Proof: Let $d = \gcd(a, b)$, then $d \mid (pa - qb) = 1$ so $d = 1$, since d is positive. Thus, there is no solution if $d \geq 2$. We assume $d = 1$. There exists, by Bézout theorem, a pair (p_1, q_1) of integers such that $p_1 a - q_1 b = 1$. Moreover, for every integer λ, we have $(p_1 - \lambda b)a - (q_1 - \lambda a)b = p_1 a - q_1 b = 1$, so there is an infinity pair of integers (p, q) satisfying $pa - qb = 1$. We may assume $p_1, q_1 > 0$, otherwise just consider $\lambda = -\lceil -p_1/b \rceil$ and the pair $(p', q') = (\ (p_1 - \lambda b)a, (q_1 - \lambda a)b\ )$. Moreover, for $\lambda = \lfloor p_1/b \rfloor$, we obtain the pair $(p_1 - (\lfloor p_1/b \rfloor)b,\ q_1 - (\lfloor p_1/b \rfloor)a) = (p_0, q_0)$ satisfying $p_0 a - q_0 b = 1$. But $0 < p_0 = p_1 \bmod b < b$ and $q_0 = (1/b)(p_0 a - 1) < (1/b)(ab - 1) = a - 1/b < a$. *QED*

2.1 A Coprimality Sieve:

We assume that $a \geq 3$ and $b \geq 3$ are coprime, i.e.: $\gcd(a,b) = 1$, so there exists a pair of integer $p, q \geq 1$ such that: $pa - qb = 1$ (called Bézout relation). If we consider $F(p,q) = pa - qb - 1$, for any pair of integers (p,q) and $z = \exp(2\pi\imath s)$, then

$$J(p,q) = \int_0^1 z^{pa-qb-1}\, ds = \begin{cases} 0 & \text{if } pa - qb \neq 1, \\ 1 & \text{if } pa - qb = 1. \end{cases}$$

In order to interchange integrals and series, it is convenient to consider the associated weighted series which are uniformly convergent on the circle $|z| = 1$:

$$\frac{1}{1-(\rho z)^a} = \sum_{p\geq 0} (\rho z)^{pa} \quad \text{and} \quad \frac{1}{1-(\lambda/z)^b} = \sum_{q\geq 0} \lambda^{qb} z^{-qb},$$

where ρ and λ are any real numbers such that $0 < \rho, \lambda < 1$, so that

$$\frac{1}{z\ (1-(\rho z)^a)\ (1-(\lambda/z)^b)} = \sum_{p\geq 0}\sum_{q\geq 0} \rho^{pa}\lambda^{qb} z^{pa-qb-1}, \tag{3}$$

and, if we choose $\lambda = \rho$, we obtain the coprimality sieve function studied by B. Litow [7]:

$$S(a,b) = \int_0^1 \frac{ds}{z(1-\rho^a z^a)(1-\rho^b/z^b)}\ .$$

This sieve function S enjoys some interesting properties

Lemma 2.3 *If $a, b \geq 3$ and $0 < \rho < 1$, then we have*

$$S(a,b) = 0, \qquad \text{if } \gcd(a,b) \geq 1$$
$$S(a,b) = \frac{\rho^{ap_0+bq_0}}{1-\rho^{2ab}} = \frac{\rho^{2ap_0-1}}{1-\rho^{2ab}}, \quad \text{if } \gcd(a,b) = 1$$
$$S(a,b) > \frac{1}{e-1} \sim 0.58 \qquad \text{if } \gcd(a,b) = 1 \text{ and } \rho = exp(-1/2ab),$$

where (p_0, q_0) is the unique pair of integers such that $1 \leq p_0 < b$ and $1 \leq q_0 < a$, satisfying $ap_0 - bq_0 = 1$.

Proof: Since all the expansions in Eq.(3) are uniformly convergent for $|z| = 1$, then

$$S(a,b) = \sum_{p\geq 0}\sum_{q\geq 0} \int_0^1 \rho^{ap+bq}\ z^{ap-bq-1}\ ds\ ,$$

where $z = \exp(2\pi\imath s)$, but $\int_0^1 z^n\ ds = 0$ for every integer $n \neq 0$ and equal to 1 if $n = 0$, so

$$S(a,b) = \sum_{p,q\geq 1 \text{ with } ap-bq=1} \rho^{ap+bq}\ .$$

If $\gcd(a,b) \geq 2$, then, by Lemma 2.2, there is no pair (p,q) such that $ap - bq = 1$ and $S(a,b) = 0$. Otherwise, if $\gcd(a,b) = 1$ then there exists an infinity of pairs (p,q) such that $p, q \geq 1$ and $pa - bq = 1$ (see Proof of Lemma 2.2), namely

$$\begin{cases} p = p_0 + k \times b \\ q = q_0 + k \times a \quad \text{with} \quad k \geq 0. \end{cases}$$

with $1 \leq p_0 < b$ and $1 \leq q_0 < a$, hence

$$S(a,b) = \sum_{k \geq 0} \rho^{a(p_0+kb)+b(q_0+ka)} = \frac{\rho^{ap_0+bq_0}}{1-\rho^{2ab}} = \frac{\rho^{2ap_0-1}}{1-\rho^{2ab}}.$$

Moreover, if $\rho = \exp(-1/2ab)$, then

$$S(a,b) > \frac{\rho^{2ab}}{1-\rho^{2ab}} = \frac{1}{e-1} \sim 0.58.$$

QED

REMARK: As noticed in Section 1.2, if one can approximate the value of $S(a,b)$ in Eq. (1), not only the function S is a coprimality sieve, but it also allows to compute the modular inverse of a, modulo b, namely p_0, in case a and b are coprime. Moreover, if such approximation can be done by an NC algorithm, i. e.: a parallel algorithm running in a polylogarithmic time with polynomial number of processors, then we will prove simultaneously that both Coprimality and Modular Inverse problems will be in the NC class.

2.2 A GCD formula:

One can follow the same idea with the function $F(p,q) = pa - qb$ and obtain the following result:

Theorem 2.1 *Let a, b be two integer such that $a, b \geq 2$ and $\rho = exp\ (\frac{-1}{2ab})$. Let T be the function defined by*

$$T(a,b) = \int_0^1 \frac{ds}{(1-\rho^a z^a)(1-\rho^b/z^b)}, \qquad \text{where } z = \exp(2\pi\iota s)\,,$$

then

$$\lfloor T(a,b) \rfloor = \gcd(a,b).$$

Proof : As for Lemma 2.3, we have

$$T(a,b) = \sum_{p,q \geq 0} \rho^{pa+qb} \int_0^1 z^{pa-qb}\ ds\ ,$$

and

$$T(a,b) = \sum_{p,q \geq 0,\ \text{with}\ pa=qb} \rho^{pa+qb}\ .$$

Let $d = \gcd(a,b)$, then the solutions of the equation $pa = qb$ are

$$\begin{cases} p = & k \times (b/d) \\ q = & k \times (a/d), \text{ for } k \geq 0. \end{cases}$$

So

$$T(a,b) = \sum_{k \geq 0 \text{ s.t.: } p=k\times(b/d)} \rho^{2pa} = \sum_{k \geq 0} \rho^{2kab/d} = \frac{1}{1-\rho^{2ab/d}}\ .$$

For $\rho = \exp\,(\frac{-1}{2ab})$, we obtain

$$T(a,b) = \frac{1}{1-e^{-1/d}}\ ,$$

hence the result since

$$\forall\ d \geq 1, \qquad d\ <\ \frac{1}{1-e^{-1/d}}\ <\ d+1.$$

QED

REMARK: The residu theorem gives

$$T(a,b) = \frac{1}{\rho b}\sum_{k=0}^{b-1}\frac{1}{1-\rho^{2a}\tau^{ak}}.$$

3 The Finite Sums Approach

Following Vinogradov's idea [12], instead of using series, one may consider finite sum of exponentials. We prove that the GCD and a coprimality sieve function are respectively the first and the second non negative coefficients in the expansion series of a same rational function.

Theorem 3.1 *Let a, b be two positive integers and $z = z(s) = exp\,(2\pi\iota s)$, with $0 \leq s < 1$. Let G be the complex function defined by*

$$G(z) = \frac{1}{z^{b(a-1)}}\ (\sum_{p=0}^{b-1} z^{pa})\ (\sum_{q=0}^{a-1} z^{qb}) = \sum_{n=-b(a-1)}^{a(b-1)} g(n)\, z^n$$

Then we have

$$1)\quad g(0) = \int_0^1 G(z)\ ds = \gcd(a,b) \qquad \forall a,b \geq 1.$$

$$2)\quad g(1) = \int_0^1 \frac{G(z)}{z}\ ds = \begin{cases} 1 & \textit{if}\ \ \gcd(a,b) = 1, \\ 0 & \textit{if}\ \ \gcd(a,b) \geq 2, \end{cases} \quad \forall a,b \geq 2.$$

Proof: Consider the polynomials

$$f_a(z) = \sum_{p=0}^{b-1} z^{pa}, \quad f_b(z) = \sum_{q=0}^{a-1} z^{qb},$$

and the polynomial F defined by

$$F(z) = f_a(z) \times f_b(z) = \sum_{n=0}^{2ab-a-b} c(n)\, z^n.$$

So

$$G(z) = \frac{F(z)}{z^{b(a-1)}} = \frac{1}{z^{b(a-1)}}\ (\sum_{p=0}^{b-1} z^{pa})\ (\sum_{q=0}^{a-1} z^{qb}) = \sum_{n=-b(a-1)}^{a(b-1)} g(n)\, z^n.$$

If we set $k = (a-1) - q$, then $0 \leq k \leq a-1$, and

$$G(z) = \sum_{p=0}^{b-1} \sum_{q=0}^{a-1} z^{pa+qb-b(a-1)} = \sum_{p=0}^{b-1} \sum_{k=0}^{a-1} z^{pa-kb},$$

so, for any integer n, such that $-b(a-1) \leq n \leq a(b-1)$, we obtain (with q instead of k)

$$g(n) = \sum_{0 \leq p < b,\ 0 \leq q < a\ ;\ pa-qb=n} 1.$$

Two special cases are important:
From Lemma 2.1, for $a, b \geq 1$,

$$g(0) = \sum_{0 \leq p < b,\ 0 \leq q < a\ ;\ pa=qb} 1 = \gcd(a,b),$$

and, from Lemma 2.2, for $a, b \geq 2$,

$$g(1) = \sum_{0 \leq p < b,\ 0 \leq q < a\ ;\ pa-qb=1} 1\ , \quad \text{so}$$

$$g(1) = \begin{cases} 1 & \text{if } \gcd(a,b) = 1, \\ 0 & \text{if } \gcd(a,b) \geq 2, \end{cases}$$

since $g(0)$ and $g(1)$ represent respectively, the number of solution for the equations $pa - qb = 0$ and $pa - qb = 1$, with $0 \leq p < b$ and $0 \leq q < a$. On the other hand, the coefficient $c(n)$ can be obtained by the Cauchy formula

$$\forall n \geq 0, \quad c(n) = \frac{1}{2\pi\iota} \int_{|z|=1} \frac{F(z)}{z^{n+1}}\, dz = \int_0^1 \frac{F(z)}{z^n}\, ds, \quad \text{with} \quad z = e^{2\pi\iota s}.$$

It is easy to see that the coefficient $c(n)$ and $g(n)$ are linked with the relation $g(n) = c(\ n + b(a-1)\ )$, so $g(0) = c(\ b(a-1)\ ) = d = \gcd(a,b)$ and $c(\ b(a-1)+1\ ) = g(1) = \delta_d^1$, where $\delta_n^m = 1$ if $m = n$, and equal to 0 otherwise. Consequently, $\forall a, b \geq 2$ and $z = \exp(2\pi\iota s)$:

$$\int_0^1 \frac{(\sum_{p=0}^{b-1} z^{pa})\ (\sum_{q=0}^{a-1} z^{qb})}{z^{b(a-1)}}\, ds = \gcd(a,b) \tag{4.1}$$

$$\int_0^1 \frac{(\sum_{p=0}^{b-1} z^{pa})\ (\sum_{q=0}^{a-1} z^{qb})}{z^{b(a-1)+1}}\, ds = \begin{cases} 1 & \text{if } \gcd(a,b) = 1, \\ 0 & \text{if } \gcd(a,b) \geq 2. \end{cases} \tag{4.2}$$

QED

Examples:

1) If $(a,b) = (5,3)$, then $G(z) = z^{-12}\,(1 + z^5 + z^{10})(1 + z^3 + z^6 + z^9 + z^{12})$, so the constant term of $G(z)$ is $g(0) = 1 = \gcd(5,3)$.

2) If $(a,b) = (6,2)$, then $G(z) = z^{-10}\,(1 + z^6)(1 + z^2 + z^4 + z^6 + z^8 + z^{10})$, so the constant term of $G(z)$ is $g(0) = 2 = \gcd(6,2)$.

3.1 A Trigometrical Formula for the Integer GCD

Using the relation (for any real θ)

$$e^{\iota\theta} - 1 = e^{\iota\theta/2}(\ e^{\iota\theta/2} - \ e^{-\iota\theta/2}\ ) = e^{\iota\theta/2} \times 2\ \iota\ \sin(\theta/2)\ ,$$

we obtain (if $z^a \neq 1$ and $z^b \neq 1$)

$$G(z) = z^{-b(a-1)}\ \frac{z^{ab}-1}{z^a-1}\ \frac{z^{ab}-1}{z^b-1} = z^{(b-a)/2}\ \frac{\sin(\pi abs)}{\sin(\pi as)}\ \frac{\sin(\pi abs)}{\sin(\pi bs)}.$$

So,

$$\int_0^1 G(z)\ ds = I + \iota\ J = \int_0^1 e^{\pi\iota s(b-a)}\ \frac{\sin^2(\pi abs)}{\sin(\pi as)\ \sin(\pi bs)}\ ds = \gcd(a,b).$$

Since $\gcd(a,b)$ is a real number, then

$$I = \int_0^1 \cos[\pi s(b-a)]\ \frac{\sin^2(\pi abs)}{\sin(\pi as)\ \sin(\pi bs)}\ ds = \gcd(a,b), \qquad (5.1)$$

or (Formula (2), proposed in the introduction)

$$I = \frac{1}{\pi}\int_0^\pi \cos[(b-a)x)]\ \frac{\sin^2(abx)}{\sin(ax)\ \sin(bx)}\ dx\ = \gcd(a,b), \qquad (5.2)$$

$$\text{and}\ \ J = \int_0^1 \sin[\pi s(b-a)]\ \frac{\sin^2(\pi abs)}{\sin(\pi as)\ \sin(\pi bs)}\ ds = 0.$$

This last result can be obtained straightforward. Let

$$H(s) = \sin[\pi s(b-a)]\ \frac{\sin^2(\pi abs)}{\sin(\pi as)\ \sin(\pi bs)},$$

then $H(1-s) = -H(s)$ for $0 < s < 1$ and $J = \int_0^1 H(s)\ ds = 0$.
Similarly, we also obtain a new coprimality sieve ($d = \gcd(a,b)$):

$$\int_0^1 \cos[\ (b-a-2)\pi s\ ]\ \frac{\sin^2(\pi abs)}{\sin(\pi as)\ \sin(\pi bs)}\ ds = \delta_d^1\,, \qquad (6.1)$$

$$\text{or}\ \ \frac{1}{\pi}\int_0^\pi \cos[\ (b-a-2)x\ ]\ \frac{\sin^2(abx)}{\sin(ax)\ \sin(bx)}\ ds = \delta_d^1\ . \qquad (6.2)$$

Example: If $a = b = n \geq 1$, then we obtain:

$$\gcd(n,n) = \frac{1}{\pi}\int_0^\pi \frac{\sin^2(n^2x)}{\sin^2(nx)}\ dx = \frac{1}{n\pi}\int_0^{n\pi} \frac{\sin^2(ny)}{\sin^2(y)}\ dy = \frac{1}{n\pi}(n^2\pi) = n.$$

Remark:
We observe that Formula (5.2) and (6.2) show that $\gcd(a,b)$ and the integer comprimality functions are, respectively, the $|b-a|$-th and the $|b-a-2|$-th coefficients of the cosine Fourier series for the function

$$P(x) = \ \frac{\sin^2(abx)}{\sin(ax)\ \sin(bx)}\ .$$

Note that all the integrals are well defined since $P(x)$ can be extended to a continuous function P^* in all the interval $[0, \pi]$. Actually, P^* is analytic for all reals, since P^* is the product of two Dirichlet kernels which are finite sums of trigonometrical cosine functions (see formula (8)).

Other equivalent formula for the GCD: $(\forall a, b \geq 1)$

$$\gcd(a,b) = 1/2 \ + \int_0^1 \cot(\pi as) \ \cot(\pi bs) \ \sin^2(\pi abs) \ ds \tag{7.1}$$

$$\gcd(a,b) = 1/2 \ + \frac{1}{\pi} \ \int_0^\pi \cot(ax) \ \cot(bx) \ \sin^2(abx) \ dx \tag{7.2}$$

3.2 Link with Dirichlet kernels:

Let $n \geq 1$ be an integer and x be a real number. The Dirichlet kernel function D_n is defined by

$$D_n(x) = \sum_{k=-n}^{n} e^{ikx} = 1 + 2\sum_{k=1}^{n} \cos(kx) = \frac{\sin[\ (2n+1)(x/2)\ ]}{\sin(x/2)} \ ,$$

where the last equality is valid only for $x \neq 0 \bmod 2\pi$, but we have $D_n(2k\pi) = 2n+1$, for any integer k. Hence, for all odd integers $a, b \geq 3$:

$$\gcd(a,b) = \frac{1}{\pi} \int_0^\pi \cos[\ (b-a)x)\ ] \ \times D_{(a-1)/2}(2bx) \quad \times D_{(b-1)/2}(2ax) \ dx. \tag{8}$$

Note that Dirichlet D_n kernels are linked with Chebyshev polynomials of second order U_n:

$$D_n(x) = 1 + 2\sum_{k=1}^{n} \cos(kx) = \frac{\sin[\ (2n+1)(x/2)\ ]}{\sin(x/2)}$$

$$= U_{2n}(\cos(x/2)) \quad \text{with} \quad U_n(\cos(x)) = \frac{\sin[(n+1)x]}{\sin(x)}.$$

3.3 A GCD function for real numbers:

We observe that the integral of formula (2) may be well defined for some pairs of real numbers. We suggest to extend the definition of the GCD to the pairs of reals for which the integral formula is well defined.

Examples:

$$\gcd(1/2, 1/2) = \frac{1}{\pi} \int_0^\pi \frac{\sin^2(x/4)}{\sin^2(x/2)} \ dx = \frac{4}{\pi} \int_0^{\pi/4} \frac{\sin^2(t)}{\sin^2(2t)} \ dt = \frac{1}{\pi}.$$

$$\gcd(1, 1/2) = \frac{1}{\pi} \int_0^\pi \cos(x/2) \ \frac{\sin(x/2)}{\sin(x)} \ dx = \frac{1}{\pi} \int_0^\pi \frac{1}{2} \ dx = \frac{1}{2}.$$

More generally, the GCD function is well defined for all pairs $(a, b) \in]0, 1[^2$, since the only singularity in formula (2) will be $x = 0$.

4 Conclusion

- If our integral definition of GCD given in (2) (or one of the others equivalent to it) can be evaluated numerically in NC, with a good error control, then the GCD and its related problems will belong to the NC class. So our next step of research is to find numerical approximation algorithms for our formula.
- Another way to address this issue is to consider an adapted fast parallel computation of Fourrier coefficients.
- One may try to prove that, at least, the Integer GCD is in RNC (random NC class) by random computations methods for integrals.

References

[1] **A. Borodin., J. von zur Gathen, J. Hopcroft.** Fast Parallel Matrix and GCD Computations, *Information and Control*, 52, 3, 241-256, 1982.

[2] **B. Chor and O. Goldreich.** An improved parallel GCD, *Algorithmica*, 5, 1990, 1-10.

[3] **J. von zur Gathen, J. Gerhard.** *Modern Computer Algebra*, 1st ed., Cambrige University Press, 1999.

[4] **G.H. Hardy, S. Ramanujan.** Asymptotic formulae in combinatorial analysis, *in Proc. London Math. Soc.*, 17, 75-115, 1918.

[5] **G.H. Hardy, J.E. Littlewood.** A new solution of Waring's problem, *Q. J. Math.*, 48, 272-293, 1919.

[6] **R. Karp, V. Ramachandran.** *Parallel Algorithms for Shared-memory Machines*, in J. Van Leeuwen Editor, Algorithms and Complexity, Elsevier and MIT Press, 1990, Handbook of Theoretical Computer Science, Vol. A.

[7] **B. Litow.** Parallel Complexity of Integer Coprimality, *in Electronic Colloquium on Computational Complexity*, Report No.9, 1998.

[8] **A. Schönhage.** Schnelle Berechnung von Kettenbruchentwicklugen, *Acta Informatica*, 1, 1971, 139-144.

[9] **S.M. Sedjelmaci.** A Parallel Extended GCD Algorithm, *Journal of Discrete Algorithms*, 6, (2008) 526-538.

[10] **S.M. Sedjelmaci.** On a Sieve Function for Coprimality and Modular Inverse, *Pre-print, LIPN, University of Paris 13, Villetaneuse*, France, (2005) .

[11] **J. Sorenson.** Two Fast GCD Algorithms, *J. of Algorithms*, 16, 1994, 110-144.

[12] **I.M. Vinogradov.** Method of Trigonometrical Sums in the Theory of Numbers, *Mineola, NY: Dover Publications*, 2004.