

NEW ALGORITHM FOR FINDING GREATEST COMMON DIVISOR

Anton Iliev¹, Nikolay Kyurkchiev², Asen Rahnev³

^{1,2,3}Faculty of Mathematics and Informatics

University of Plovdiv Paisii Hilendarski

24, Tzar Asen Str., 4000 Plovdiv, BULGARIA

ABSTRACT: In recent articles and books [7]–[27] we present techniques for optimizing various algorithms for finding the greatest common divisor. Here we are developing a new algorithm with potential for application for long as well as regular numbers. The approach that we use is based on a combination of "remainder" and "difference" operations. This will be especially useful when dealing with long numbers, because just using a "remainder" operation would take too much CPU time. Once again we note that our algorithms do not depend on both the hardware computer system and the software environment, those mentioned in the paper are only to illustrate the power of the new algorithms.

AMS Subject Classification: 11A05, 68W01

Key Words: greatest common divisor, reduced number of operations

Received: April 10, 2020; **Accepted:** October 2, 2020;

Published: October 17, 2020 **doi:** 10.12732/npsc.v28i1.7

Dynamic Publishers, Inc., Acad. Publishers, Ltd.

<https://acadsol.eu/npsc>

1. INTRODUCTION

For two natural numbers a and b , we set ourselves the task of constructing a new sequence of numbers that ends with a number that is the greatest common divisor. Our approach is different with comparison to sources [1]–[6] and [28]–[34], etc. that have used not so well organized in computational point of view Knuth's interpretation [28], [21] of Euclidean algorithm.

For testing purposes for new algorithm we will use the following computer: processor – Intel(R) Core(TM) i7-6700HQ CPU 2.60GHz, 2592 Mhz, 4 Core(s), 8 Logical Processor(s), RAM 16 GB, Microsoft Windows 10 Enterprise x64, Microsoft Visual C# 2017 x64.

2. Main Results.

We propose the following:

Algorithm 1.

```
do
if (a > b) { if ((a % b) == 0) { gcd = b; break; } else b -= a; }
else { if ((b % a) == 0) { gcd = a; break; } else a -= b; }
while ((gcd = a) != b);
```

and its recursive implementation as

Algorithm 2.

```
static long Euclid(long a, long b)
{ if (a == b) return a; else
if (a > b) { if ((a % b) == 0) return b; else b -= a; }
else { if ((b % a) == 0) return a; else a -= b; }
return Euclid(a, b); }
```

Numerical Example.

We will compare the proposed here algorithm with Knuth's iterative and recursive [21] implementations respectively.

```
long a, b, gcd, ob, d = 0;
for (int i = 1; i < 100000001; i++) { a = i; b = 200000002 - i;
//here is the source code of every one of algorithms 1 and Knuth's
//iterative, and calling of algorithms 2 and Knuth's recursive
d += gcd; }
Console.WriteLine(d);
```

Both recursive implementations (Algorithm 2 and Knuth's) can be called by:

$\text{gcd} = \text{Euclid}(a, b)$;

CPU time of Algorithm 1 is: **21.385 seconds.**

CPU time of Knuth's iterative is: **24.709 seconds.**

CPU time of Algorithm 2 is: **34.198 seconds.**

CPU time of Knuth's recursive is: **45.898 seconds.**

3. Conclusion

The numerical experiments show that Algorithms 1 and 2 presented here are quite effective from computational point of view and in particular they are comparable to our best realizations, see [7]–[27].

The proposed algorithms resurrect one old idea of Strassen [35] related to minimizing the number of operations "multiplication" and "division" at the expense of operations "addition" and "subtraction" which finds serious application when working by block matrices with large dimensions. In the future, a very serious study is planned related to the study of the asymptotics in terms of the number of operations.

Acknowledgement

The work of the first author has been accomplished with the financial support of the MES by the Grant No. D01-271/16.12.2019 for NCDSC part of the Bulgarian National Roadmap on RIs.

The work of the second and third authors is supported by the Project FP19-FMI-002 "Innovative ICT for Digital Research Area in Mathematics, Informatics and Pedagogy of Education" of the Scientific Fund of the University of Plovdiv Paisii Hilendarski, Bulgaria.

REFERENCES

- [1] A. Akritas, A new method for computing polynomial greatest common divisors and polynomial remainder sequences, *Numerische Mathematik*, **52** (1988), 119–127.
- [2] S. Enkov, *Programming in Arduino Environment*, University Press "Paisii Hilendarski", Plovdiv (2017). (in Bulgarian)
- [3] F. Chang, Factoring a Polynomial with Multiple-Roots, *World Academy of Science, Engineering and Technology*, **47** (2008), 492–495.
- [4] Th. Cormen, Ch. Leiserson, R. Rivest, Cl. Stein, *Introduction to Algorithms*, 3rd ed., The MIT Press, Cambridge (2009).

- [5] K. Garov, A. Rahnev, *Textbook-notes on programming in BASIC for facultative training in mathematics for 9.–10. Grade of ESPU*, Sofia (1986). (in Bulgarian)
- [6] A. Golev, *Textbook on algorithms and programs in C#*, University Press "Paisii Hilendarski", Plovdiv (2012). (in Bulgarian)
- [7] A. Iliev, N. Kyurkchiev, A Note on Knuth's Implementation of Euclid's Greatest Common Divisor Algorithm, *International Journal of Pure and Applied Mathematics*, **117** (2017), 603–608.
- [8] A. Iliev, N. Kyurkchiev, A. Golev, A Note on Knuth's Implementation of Extended Euclidean Greatest Common Divisor Algorithm, *International Journal of Pure and Applied Mathematics*, **118** (2018), 31–37.
- [9] A. Iliev, N. Kyurkchiev, A. Rahnev, A Note on Adaptation of the Knuth's Extended Euclidean Algorithm for Computing Multiplicative Inverse, *International Journal of Pure and Applied Mathematics*, **118** (2018), 281–290.
- [10] A. Iliev, N. Kyurkchiev, A Note on Euclidean and Extended Euclidean Algorithms for Greatest Common Divisor for Polynomials, *International Journal of Pure and Applied Mathematics*, **118** (2018), 713–721.
- [11] A. Iliev, N. Kyurkchiev, A Note on Least Absolute Remainder Euclidean Algorithm for Greatest Common Divisor, *International Journal of Scientific Engineering and Applied Science*, **4** No. 3 (2018), 31–34.
- [12] A. Iliev, N. Kyurkchiev, A Note on Knuth's Algorithm for Computing Extended Greatest Common Divisor using SGN Function, *International Journal of Scientific Engineering and Applied Science*, **4** No. 3 (2018), 26–29.
- [13] A. Iliev, N. Kyurkchiev, *New Trends in Practical Algorithms: Some Computational and Approximation Aspects*, LAP LAMBERT Academic Publishing, Beau Bassin (2018).
- [14] A. Iliev, N. Kyurkchiev, 80th Anniversary of the birth of Prof. Donald Knuth, *Biomath Communications*, **5** (2018), 7 pp.
- [15] A. Iliev, N. Kyurkchiev, New Realization of the Euclidean Algorithm, *Collection of scientific works of Eleventh National Conference with International Participation Education and Research in the Information Society*, Plovdiv, ADIS, June 1–2, (2018), 180–185. (in Bulgarian)
- [16] A. Iliev, N. Kyurkchiev, New Organizing of the Euclid's Algorithm and one of its Applications to the Continued Fractions, *Collection of scientific works from conference "Mathematics. Informatics. Information Technologies. Application in Education"*, Pamporovo, Bulgaria, 10–12 October 2018, (2019), 199–207.

- [17] A. Iliev, N. Kyurkchiev, The faster Euclidean algorithm, *Collection of scientific works from conference*, Pamporovo, Bulgaria, 28–30 November 2018, (2019), 15–20.
- [18] A. Iliev, N. Kyurkchiev, The faster extended Euclidean algorithm, *Collection of scientific works from conference*, Pamporovo, Bulgaria, 28–30 November 2018, (2019), 21–26.
- [19] P. Kyurkchiev, V. Matanski, The faster Euclidean algorithm for computing polynomial multiplicative inverse, *Collection of scientific works from conference*, Pamporovo, Bulgaria, 28–30 November 2018, (2019), 43–48.
- [20] V. Matanski, P. Kyurkchiev, The faster Lehmer’s greatest common divisor algorithm, *Collection of scientific works from conference*, Pamporovo, Bulgaria, 28–30 November 2018, (2019), 37–42.
- [21] A. Iliev, N. Kyurkchiev, A. Rahnev, A New Improvement Euclidean Algorithm for Greatest Common Divisor. I, *Neural, Parallel, and Scientific Computations*, **26** No. 3 (2018), 355–362.
- [22] A. Iliev, N. Kyurkchiev, A. Rahnev, A New Improvement of Harris–Stein Modification of Euclidean Algorithm for Greatest Common Divisor. II, *International Journal of Pure and Applied Mathematics*, **120** No. 3 (2018), 379–388.
- [23] A. Iliev, N. Kyurkchiev, A. Rahnev, A New Improvement of Least Absolute Remainder Algorithm for Greatest Common Divisor. III, *Neural, Parallel, and Scientific Computations*, **27** No. 1 (2019), 1–9.
- [24] A. Iliev, N. Kyurkchiev, A. Rahnev, A New Improvement of Tembhurne–Sathe Modification of Euclidean Algorithm for Greatest Common Divisor. IV, *Dynamic Systems and Applications*, **28** No. 1 (2019), 143–152.
- [25] A. Iliev, N. Kyurkchiev, A. Rahnev, *Nontrivial Practical Algorithms: Part 2*, LAP LAMBERT Academic Publishing, Beau Bassin (2019).
- [26] A. Iliev, N. Valchanov, T. Terzieva, Generalization and Optimization of Some Algorithms, *Collection of scientific works of National Conference "Education in Information Society"*, Plovdiv, ADIS, 12–13 May 2009, (2009), 52–58. (in Bulgarian)
- [27] H. Gyulyustan, A Note on Euclidean Sequencing Algorithm, *Proceedings of the Scientific Conference "Innovative ICT for Digital Research Area in Mathematics, Informatics and Pedagogy of Education"*, Pamporovo, 7–8 November 2019, Plovdiv University Press, 2020, 57–64.
- [28] D. Knuth, *The Art of Computer Programming, Vol. 2, Seminumerical Algorithms*, 3rd ed., Addison-Wesley, Boston (1998).

- [29] Hr. Krushkov, A. Iliev, *Practical programming guide in Pascal, Parts I and II*, Koala press, Plovdiv (2002). (in Bulgarian)
- [30] P. Nakov, P. Dobrikov, *Programming=++Algorithms*, 5th ed., Sofia (2015). (in Bulgarian)
- [31] A. Rahnev, K. Garov, O. Gavrailov, *Textbook for extracurricular work using BASIC*, MNP Press, Sofia (1985). (in Bulgarian)
- [32] A. Rahnev, K. Garov, O. Gavrailov, *BASIC in examples and tasks*, Government Press "Narodna prosveta", Sofia (1990). (in Bulgarian)
- [33] N. Kasakliev, *C# Programming Guide*, University Press "Paisii Hilendarski", Plovdiv (2016). (in Bulgarian)
- [34] A. Rahnev, N. Pavlov, N. Valchanov, T. Terzieva, *Object Oriented Programming*, Lightning Source UK Ltd., London (2014).
- [35] V. Strassen, Gaussian Elimination is not Optimal, *Numer. Math.* **13**, (1969), 354–356.