

## EXTENDED BASED ON GENERALIZED DAYKIN-HARRIS ALGORITHM

Anton Iliev<sup>1,2</sup>, Nikolay Kyurkchiev<sup>1,2</sup>,  
Asen Rahnev<sup>1</sup> and Svetoslav Enkov<sup>1</sup>

<sup>1</sup>Faculty of Mathematics and Informatics  
University of Plovdiv Paisii Hilendarski  
24, Tzar Asen Str., 4000 Plovdiv, BULGARIA

<sup>2</sup>Institute of Mathematics and Informatics  
Bulgarian Academy of Sciences  
Acad. G. Bonchev Str., Bl. 8, 1113 Sofia, BULGARIA

**ABSTRACT:** In this paper we generalize Daykin-Harris algorithm [6] in the way that now our new algorithm can calculate coefficients  $x$  and  $y$  in Bezout's identity [1] i.e. for arbitrary but given natural numbers  $a$  and  $b$ , so that  $x * a + y * b = gcd$ , where  $gcd$  is greatest common divisor of  $a$  and  $b$ . This algorithm will be useful for long numbers. It uses basically "addition" and "subtraction" operations.

**AMS Subject Classification:** 11A05, 68W01

**Key Words:** extended Euclidean algorithm, extended Daykin-Harris algorithm, Bezout's identity, long numbers

**Received:** April 17, 2024

**Revised:** May 21, 2024

**Published:** May 24, 2024

**doi:** 10.12732/ijdea.v23i1.4

Academic Publications, Ltd.

<https://acadpubl.eu>

---

## 1. INTRODUCTION

The reason of interest to these algorithms is because they are naturally used in cryptography for computing modular multiplicative inverse [7]. Many algorithmic problems lead to computation of greatest common divisor of two natural numbers  $a$  and  $b$ , see [4], [15]–[51]. New algorithms in this research field can be found in [15]–[30].

Our new algorithm extends the results of Daykin [2], Harris [3] and our recent paper [6].

The Euclidean algorithm and its modifications and generalizations are studied by many authors in [8]-[14], [31]-[51].

For testing purposes 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 extended algorithm, which generalizes regular Daykin-Harris algorithm [6]:

### Algorithm 1.

```

x1 = 1; x2 = 0; y1 = 0; y2 = 1;
if (a > b)
{
z = a;
while (a > b) { a -= b; x1 -= y1; x2 -= y2; }
a1 = z - b;
if (a + a1 < z)
do
{
do { a1 += a; y1 -= x1; y2 -= x2; } while (a + a1 < z);
if (a + a1 > z) do { a += a1 - z; x1 -= y1; x2 -= y2; } while (a + a1 > z);
}
while (a + a1 != z);
else if (a + a1 > z)
do
{
do { a += a1 - z; x1 -= y1; x2 -= y2; } while (a + a1 > z);
if (a + a1 < z) do { a1 += a; y1 -= x1; y2 -= x2; } while (a + a1 < z);
}
while (a + a1 != z);
gcd = a; x = x1; y = x2;

```

```

}
else
{
z = b;
while (b > a) { b -= a; y1 -= x1; y2 -= x2; }
b1 = z - a;
if (b + b1 < z)
do
{
do { b1 += b; x1 -= y1; x2 -= y2; } while (b + b1 < z);
if (b + b1 > z) do { b += b1 - z; y1 -= x1; y2 -= x2; } while (b + b1 > z);
}
while (b + b1 != z);
else if (b + b1 > z)
do
{
do { b += b1 - z; y1 -= x1; y2 -= x2; } while (b + b1 > z);
if (b + b1 < z) do { b1 += b; x1 -= y1; x2 -= y2; } while (b + b1 < z);
} while (b + b1 != z);
gcd = b; x = y1; y = y2;
}

```

and we will compare the speed of newly Algorithm 1. to extended Euclidean algorithm [31] (Algorithm 2.):

**Algorithm 2.**

```

x1 = 1; x2 = 0; y1 = 0; y2 = 1;
while (a != b)
if (a > b) { a -= b; x1 -= y1; x2 -= y2; }
else { b -= a; y1 -= x1; y2 -= x2; }
gcd = a; x = y1; y = y2;

```

### 3. NUMERICAL EXAMPLE

For testing purposes of Algorithms 1. and 2. we will use the following main function:

```
long a, b, gcd, d1 = 0, a1, b1, z, x1, x2, y1, y2;
for (int i = 1; i < 100000001; i++) { a = i; b = 200000002 - i;
//here are placed the source code of algorithms 1. and 2.
d1 += gcd;
}
Console.WriteLine(d1);
```

CPU time results are:

CPU time of Algorithm 1. is: **98.178 seconds.**

CPU time of Algorithm 2. is: **109.508 seconds.**

Algorithm 1. considerably overtakes speed of Algorithm 2.

### 4. CONCLUSION

By this paper we enrich the theory of so-called extended Euclidean algorithm showing new way of realization of computational process.

### ACKNOWLEDGEMENTS

This study is financed by the project No FP23-FMI-002 “Intelligent software tools and applications in research in Mathematics, Informatics, and Pedagogy of Education” of the Scientific Fund of the Paisii Hilendarski University of Plovdiv, Bulgaria.

## REFERENCES

- [1] E. Bezout, *Theorie generale des equations algebriques*, Paris, France: Ph.-D. Pierres, (1779).
- [2] D. Daykin, An Addition Algorithm for Greatest Common Divisor, *Fibonacci Quarterly*, 8, No. 3 (1970), 347–349.
- [3] V. Harris, On Daykin’s algorithm for finding the g.c.d., *Fibonacci Quarterly*, 12 (1974), 80.
- [4] E. Bach, J. Shallit, *Algorithmic Number Theory, Vol. 1: Efficient Algorithms*, MA: MIT Press, Cambridge (1996).
- [5] V. Harris, An algorithm for finding the greatest common divisor, *Fibonacci Quarterly*, 8 (1970), 102–103.
- [6] A. Iliev, N. Kyurkchiev, A. Rahnev, S. Enkov, An Effective Realization of Daykin-Harris Algorithm, preprint, (2024).
- [7] A. Iliev, N. Kyurkchiev, A. Rahnev, New Algorithms for Finding Modular Multiplicative Inverse, *Neural, Parallel, and Scientific Computations*, 28 No. 1 (2020), 81–88.
- [8] Th. Cormen, Ch. Leiserson, R. Rivest, Cl. Stein, *Introduction to Algorithms*, 3rd ed., The MIT Press, Cambridge (2009).
- [9] 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)
- [10] A. Golev, *Textbook on algorithms and programs in C#*, University Press ”Paisii Hilendarski”, Plovdiv (2012). (in Bulgarian)
- [11] T. Terzieva, *Introduction to web programming*, University Press ”Paisii Hilendarski”, Plovdiv (2021), ISBN 978-619-202-623-3. (in Bulgarian)
- [12] T. Terzieva, *Development of algorithmic thinking in the Informatics Education*, University Press ”Paisii Hilendarski”, Plovdiv (2021), ISBN 978-619-202-622-6. (in Bulgarian)
- [13] T. Terzieva, *Educational tools for teaching in digital environment*, University Press ”Paisii Hilendarski”, Plovdiv (2021). (in Bulgarian)
- [14] S. Enkov, *Programming in Arduino Environment*, University Press ”Paisii Hilendarski”, Plovdiv (2017). (in Bulgarian)

- [15] 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.
- [16] 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.
- [17] 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.
- [18] 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.
- [19] 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.
- [20] 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.
- [21] A. Iliev, N. Kyurkchiev, *New Trends in Practical Algorithms: Some Computational and Approximation Aspects*, LAP LAMBERT Academic Publishing, Beau Bassin (2018).
- [22] A. Iliev, N. Kyurkchiev, The faster extended Euclidean algorithm, *Collection of scientific works from conference*, Pamporovo, Bulgaria, 28–30 November 2018, (2019), 21–26.
- [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, *Nontrivial Practical Algorithms: Part 2*, LAP LAMBERT Academic Publishing, Beau Bassin (2019).
- [25] 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)

- [26] A. Iliev, N. Kyurkchiev, A. Rahnev, New Extended Algorithm for Finding Greatest Common Divisor, *Neural, Parallel, and Scientific Computations*, 28 No. 1 (2020), 89–95.
- [27] A. Iliev, N. Kyurkchiev, A. Rahnev, Efficient Binary Algorithm for Kronecker Symbol, *Communications in Applied Analysis*, 25 No. 1 (2021), 11–21.
- [28] A. Iliev, N. Kyurkchiev, A. Rahnev, Efficient Algorithm for Kronecker Symbol, *International Electronic Journal of Pure and Applied Mathematics*, 15 No. 1 (2021), 23–30.
- [29] A. Iliev, N. Kyurkchiev, A. Rahnev, V. Kyurkchiev, New Extended Based on Generalization of Harris Algorithm, *Communications in Applied Analysis*, **26** No. 1 (2022), 61–73.
- [30] A. Iliev, N. Kyurkchiev, A. Rahnev, A Refinement of the Extended Euclidean Algorithm, (2021), *International Electronic Journal of Pure and Applied Mathematics*, 15 No. 1 (2021), 33–44.
- [31] D. Knuth, *The Art of Computer Programming, Vol. 2, Seminumerical Algorithms*, 3rd ed., Addison-Wesley, Boston (1998).
- [32] A. Rahnev, K. Garov, O. Gavrailov, *Textbook for extracurricular work using BASIC*, MNP Press, Sofia (1985). (in Bulgarian)
- [33] A. Rahnev, K. Garov, O. Gavrailov, *BASIC in examples and tasks*, Government Press "Narodna prosveta", Sofia (1990). (in Bulgarian)
- [34] N. Kasakliev, *C# Programming Guide*, University Press "Paisii Hilendarski", Plovdiv (2016). (in Bulgarian)
- [35] A. Rahnev, N. Pavlov, N. Valchanov, T. Terzieva, *Object Oriented Programming*, Lightning Source UK Ltd., London (2014).
- [36] D. Rachmawati, M. Budiman, On Using The First Variant of Dependent RSA Encryption Scheme to Secure Text: A Tutorial, *J. Phys.: Conf. Ser.*, (2020), 1542 012024.
- [37] J. A. Erho, J. I. Consul, B. R. Japheth, Juggling Versus Three-Way-Reversal Sequence Rotation Performance Across Four Data Types, *International Journal of Scientific Research in Computer Science and Engineering*, **7** No. 6 (2019), 10–18.
- [38] J. L. Butar-butur, F. Sinuhaji, Faktorisasi Polinomial Square-Free dan bukan Square-Free atas Lapangan Hingga  $Z_p$ , *Jurnal Teori dan Aplikasi Matematika*, **3** No. 2 (2019), 132–142.

- [39] L. Akcay, B. Ors, Comparison of RISC-V and transport triggered architectures for a post-quantum cryptography application, *Turk J Elec Eng & Comp Sci*, **29**, (2021), 321–333.
- [40] C. Falcon Rodriguez, M. Cruz, C. Falcon, Full Euclidean Algorithm by Means of a Steady Walk, *Applied Mathematics*, **12** (2021), 269–279.
- [41] P. Thapar, U. Batra, Implementation of Elliptical Curve Cryptography Based Diffie-Hellman Key Exchange Mechanism in Contiki Operating System for Internet of Things, *International Journal of Electrical and Electronics Research (IJEER)*, **10** No. 2 (2022), 335–340.
- [42] N. Fatma, M. R. Hassan, D. Akhtar, J. K. M. S. Zaman, Diminution of Extended Euclidean Algorithm for Finding Multiplicative Inverse in Galois Field, *Science and Engineering Journal*, **11** No. 1 (2023), 1222–1240.
- [43] H. Qausar, M. Absa, A. T. Hidayat, Z. Mujtahid, Penerapan Pecahan Bersambung Dalam Melakukan Aproksimasi Bilangan Irasional Menuju Bilangan Rasional, *Jurnal Ilmiah Matematika Realistik (JI-MR)*, **4**, No. 1 (2023), 48–57.
- [44] J. L. Butar-Butar, Y. B. P. Siringoringo, Kode Siklik Berulang Dari Kode Linear Fp Atas Lapangan Hingga F Pl Dengan L Bilangan Prima Tertentu, *Barekeng: J. Il. Mat. & Ter.*, **15**, No. 02 (2021), 231–240.
- [45] V. Matanski, An Efficient Binary Algorithm for Solving Equation  $GCD * 2^{|J-K|} = X * A0 + Y * B0$ , Proceedings of Anniversary International Scientific Conference “Computer Technologies and Applications”, 15-17 September 2021, Pamporovo, Bulgaria, *Plovdiv University Press*, 79–86, ISBN: 978-619-202-702-5.
- [46] H. Gyulyustan, A Note on Euclidean Sequencing Algorithm, Proceedings of the Scientific Conference “Innovative ICT for Digital Research Space in Mathematics, Informatics and Educational Pedagogy”, Pamporovo, 7-8.11.2019, *Plovdiv University Press*, (2020), 57–63, ISBN 978-619-202-572-4.
- [47] P. Kyurkchiev, V. Matanski, The Faster Euclidean Algorithm for Computing Polynomial Multiplicative Inverse, Proceedings of the Scientific Conference Innovative ICT in Research and Education: Mathematics, Informatics and Information Technologies, Pamporovo, 29-30 November 2018, (2019), 43–48, ISBN: 978-619-202-439-0.
- [48] V. Matanski, P. Kyurkchiev, The Faster Lehmer’s Greatest Common Divisor Algorithm, Proceedings of the Scientific Conference Innovative ICT in Research and Education: Mathematics, Informatics and Information Technologies, Pamporovo, 29-30 November 2018, (2019), 37–42, ISBN: 978-619-202-439-0.



- [49] D. J. Zhu, P. M. May, B. W. E. Norris, Z. M. Aman, E. F. May, Cage-Specific Hydrate Equilibrium Electrolyte Model, *Energy & Fuels*, (2024), doi: 10.1021/acs.energyfuels.3c05110
- [50] Z. Ibran, E. Aljatlawi, A. Awin, On Continued Fractions and Their Applications, *Journal of Applied Mathematics and Physics*, **10** (2022), 142–159.
- [51] Y. Fan, G. Chen, M. Cui, Formalization of Finite Field  $\text{GF}(2^n)$  Based on COQ, *Computer Science*, **47** No. 12 (2020), 311–318.