A NOTE ON EXTENDED BASED ON GENERALIZED HARRIS ALGORITHM USING SGN FUNCTION

Anton Iliev, Nikolay Kyurkchiev,
Asen Rahnev, Todorka Terzieva

Abstract. *In this note we present new working extended algorithm which enhance the results obtained in [28]. The algorithm works well for every integers* a *and* b*, for which* $a \neq 0$ *and* $b \neq 0$*.*

Key words: Key words: Extended Euclidean algorithm, Hybrid extended algorithm, sgn function, Least absolute remainder.

Mathematics Subject Classification: 11A05, 68W01

Acknowledgments

This work has been accomplished with the financial support by the Grant No BG05M2OP001-1.001-0003, financed by the Science and Education for Smart Growth Operational Program (2014–2020) and co-financed by the European Union through the European structural and Investment funds.

References

[1] T. Moore, On the Least Absolute Remainder Euclidean Algorithm, *Fibonacci Quarterly*, (1992), **30**, 161–165.

[2] Th. Cormen, Ch. Leiserson, R. Rivest, Cl. Stein, *Introduction to Algorithms*, 3rd ed., The MIT Press, Cambridge, (2009).

[3] J. Tembhurne, S. Sathe, New Modified Euclidean and Binary Greatest Common Divisor Algorithm, *IETE Journal of Research*, (2016), 62, No. 6, 852–858.

[4] 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).

[5] A. Golev, *Textbook on algorithms and programs in C#*, University Press "Paisii Hilendarski", Plovdiv, (2012), (in Bulgarian).

[6] T. Terzieva, *Introduction to web programming*, University Press "Paisii Hilendarski", Plovdiv, (2021), ISBN: 978-619-202-623-3, (in Bulgarian).

[7] T. Terzieva, *Development of algorithmic thinking in the Informatics Education*, University Press "Paisii Hilendarski", Plovdiv, (2021), ISBN: 978-619-202-622-6, (in Bulgarian).

[8] T. Terzieva, *Educational tools for teaching in digital environment*, University Press "Paisii Hilendarski", Plovdiv, (2021), (in Bulgarian).

[9] S. Enkov, *Programming in Arduino Environment*, University Press "Paisii Hilendarski", Plovdiv (2017), (in Bulgarian).

[10] A. Iliev, N. Kyurkchiev, A Note on Knuth's Implementation of Euclid's Greatest Common Divisor Algorithm, *International Journal of Pure and Applied Mathematics*, (2017), **117**, 603–608.

[11] 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*, (2018), **118**, 31–37.

[12] 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*, (2018), **118**, 713–721.

[13] 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*, (2018), **4**, No. 3, 26–29.

[14] A. Iliev, N. Kyurkchiev, *New Trends in Practical Algorithms: Some Computational and Approximation Aspects*, LAP LAMBERT Academic Publishing, Beau Bassin, (2018).

[15] A. Iliev, N. Kyurkchiev, The faster extended Euclidean algorithm, *Collection of scientific works from conference*, Pamporovo, Bulgaria, 28–30 November 2018, (2019), 21–26.

[16] A. Iliev, N. Kyurkchiev, A. Rahnev, A New Improvement of Least Absolute Remainder Algorithm for Greatest Common Divisor. III, *Neural, Parallel, and Scientific Computations*, (2019), **27**, No. 1, 1–9.

[17] A. Iliev, N. Kyurkchiev, A. Rahnev, *Nontrivial Practical Algorithms: Part 2*, LAP LAMBERT Academic Publishing, Beau Bassin (2019).

[18] 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)

[19] A. Iliev, N. Kyurkchiev, A. Rahnev, New Extended Algorithm for Finding Greatest Common Divisor, *Neural, Parallel, and Scientific Computations*, (2020), 28, No. 1, 89–95.

[20] A. Iliev, N. Kyurkchiev, A. Rahnev, Efficient Binary Algorithm for Kronecker Symbol, *Communications in Applied Analysis*, (2021), 25, No. 1, 11–21.

[21] A. Iliev, N. Kyurkchiev, A. Rahnev, Efficient Algorithm for Kronecker Symbol, *International Electronic Journal of Pure and Applied Mathematics*, (2021), 15, No. 1, 23–30.

[22] A. Iliev, N. Kyurkchiev, A. Rahnev, New Extended Algorithm Using Least Absolute Remainder, *International Journal of Differential Equations and Applications*, **21** No. 1 (2022), 85–92.

[23] A. Iliev, N. Kyurkchiev, A. Rahnev, T. Terzieva, Efficient Binary Extended Algorithm Using SGN Function, *International Journal of Differential Equations and Applications*, (2021), **20**, No. 2, 179–186.

[24] A. Iliev, N. Kyurkchiev, A. Rahnev, A Refinement of the Knuth's Extended Euclidean Algorithm for Computing Modular Multiplicative Inverse, *Communications in Applied Analysis*, (2021), 25, No. 1, 23–37.

[25] A. Iliev, N. Kyurkchiev, A. Rahnev, T. Terzieva, New Hybrid Extended Algorithm, *Communications in Applied Analysis*, (2023), **27**, No. 1, 15–25.

[26] A. Iliev, N. Kyurkchiev, A. Rahnev, T. Terzieva, New Refined Enhanced Hybrid Extended Algorithm, *Communications in Applied Analysis*, (2022), 26, No. 1, 99–109.

[27] A. Iliev, N. Kyurkchiev, A. Rahnev, V. Kyurkchiev, New Extended Based on Generalization of Harris Algorithm, *Communications in Applied Analysis*, (2022), **26**, No. 1 , 61–73.

[28] A. Iliev, N. Kyurkchiev, A. Rahnev, T. Terzieva, Extended Based on Generalized Harris Algorithm Using SGN Function, *Communications in Applied Analysis*, (2023), **27**, No. 1, 1–14.

[29] A. Iliev, N. Kyurkchiev, A. Rahnev, A Refinement of the Extended Euclidean Algorithm, (2021), *International Electronic Journal of Pure and Applied Mathematics*, (2021), 15, No. 1, 33–44.

[30] D. Knuth, *The Art of Computer Programming, Vol. 2, Seminumerical Algorithms*, 3rd ed., Addison-Wesley, Boston, (1998).

[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] 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.

[36] J. Erho, J. Consul, B. Japheth, Juggling Versus Three-Way-Reversal Sequence Rotation Performance Across Four Data Types, *International Journal of Scientific Research in Computer Science and Engineering*, (2019), **7**, No. 6, 10–18.

[37] J. Butar-butar, F. Sinuhaji, Faktorisasi Polinomial Square-Free dan bukan Square-Free atas Lapangan Hingga Zp, *Jurnal Teori dan Aplikasi Matematika*, (2019), **3**, No. 2, 132–142.

[38] L. Akcay, B. Ors, Comparison of RISC-V and transport triggered architectures for a post-quantum cryptography application, *Turk J Elec Eng & Comp Sci*, (2021), **29**, 321–333.

[39] C. Falcon Rodriguez, M. Cruz, C. Falcon, Full Euclidean Algorithm by Means of a Steady Walk, *Applied Mathematics*, (2021), **12**, 269–279.

[40] 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)*, (2022), **10**, No. 2, 335–340.

[41] N. Fatma, M. Hassan, D. Akhtar, J. Zaman, Diminution of Extended Euclidean Algorithm for Finding Multiplicative Inverse in Galois Field, *Science and Engineering Journal*, (2023), **11**, No. 1, 1222–1240.

[42] 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)*, (2023), **4**, No. 1, 48–57.

[43] J. Butar-Butar, Y. Siringoringo, Kode Siklik Berulang Dari Kode Linear Fp Atas Lapangan Hingga F Pl Dengan L Bilangan Prima Tertentu, *Barekeng: J. Il. Mat. & Ter.*, (2021), **15**, No. 02, 231–240.

[44] 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.

[45] H. Gyulyustan, A Note on Euclidean Sequencing Algorithm, Proc. 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.

[46] P. Kyurkchiev, V. Matanski, The Faster Euclidean Algorithm for Computing Polynomial Multiplicative Inverse, Proc. 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.

[47] V. Matanski, P. Kyurkchiev, The Faster Lehmer's Greatest Common Divisor Algorithm, Proc. 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.

[48] Z. Ibran, E. Aljatlawi, A. Awin, On Continued Fractions and Their Applications, *Journal of Applied Mathematics and Physics*, (2022), **10**, 142–159.

[49] Y. Fan, G. Chen, M. Cui, Formalization of Finite Field GF(2^n) Based on COQ, *Computer Science*, (2020), **47** No. 12, 311–318.

Anton Iliev[1,*], Nikolay Kyurkchiev[2], Asen Rahnev[3], Todorka Terzieva[4]
[1,2,3,4] Faculty of Mathematics and Informatics,
University of Plovdiv Paisii Hilendarski,
24, Tzar Asen Str., 4000 Plovdiv, Bulgaria,
[1,2] Institute of Mathematics and Informatics,
Bulgarian Academy of Sciences,
Acad. G. Bonchev Str., Bl. 8, 1113 Sofia, Bulgaria
Corresponding author: `aii@uni-plovdiv.bg`