A NEW IMPROVEMENT OF EXTENDED STEIN’S BINARY ALGORITHM

Anton Iliev[1,*], Nikolay Kyurkchiev[2], Asen Rahnev[3]

[1,2,3] *Faculty of Mathematics and Informatics,*
University of Plovdiv “P. Hilendarski”, 24, Tzar Asen Str., 4000 Plovdiv, Bulgaria

[1,*] *Corresponding author: aii@uni-plovdiv.bg*

[2] *nkyurk@uni-plovdiv.bg*

[3] *assen@uni-plovdiv.bg*

Abstract. In this paper our aim is to receive extended Stein’ binary algorithm with better computational characteristics. In this connection we give other boundary condition and reorganize the classical extended Stein’ algorithm.

Key Words: *greatest common divisor, extended binary algorithm, reduced number of operations*

Introduction

For two arbitrary natural numbers *a* and *b*, we search for natural number *gcd* and integer numbers *x* and *y* such that $x*a+y*b=gcd$, where *gcd* is the greatest common divisor. We will optimize extended Stein’ iterative algorithm, which is presented in the book by Menezes, Oorschot and Vanstone [37] (on page 608). This algorithm is specialized for dealing with long numbers. In our previously published papers and two books [7]–[29] we present various of tasks and different effective from computational point of view new implementations of this classical task. In many other sources the approach to these tasks (see, [1]–[6] and [30]–[37]) is based on Knuth’ interpretations [30].

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.

Main Results

We propose the following extended:

Algorithm 1.

```
int g = 0;

if ((a & 1) == 0 && (b & 1) == 0)
    do { a >>= 1; b >>= 1; g++; }
    while ((a & 1) == 0 && (b & 1) == 0);

u = a; v = b; x1 = 1; x2 = 0; y1 = 0; y2 = 1;

while ((u & 1) == 0)
   { u >>= 1;
   if ((x1 & 1) == 0 && (x2 & 1) == 0) { x1 >>= 1; x2 >>= 1; }
   else { x1 = (x1 + b) >> 1; x2 = (x2 - a) >> 1; } }

while ((v & 1) == 0)
   { v >>= 1;
   if ((y1 & 1) == 0 && (y2 & 1) == 0) { y1 >>= 1; y2 >>= 1; }
   else { y1 = (y1 + b) >> 1; y2 = (y2 - a) >> 1; } }

while (u != v)
    if (u > v)
      { u -= v; x1 -= y1; x2 -= y2;
      while ((u & 1) == 0)
      { u >>= 1;
       if ((x1 & 1) == 0 && (x2 & 1) == 0) { x1 >>= 1; x2 >>=
1; }
       else { x1 = (x1 + b) >> 1; x2 = (x2 - a) >> 1; } }
      }
    else
    { v -= u; y1 -= x1; y2 -= x2;
       while ((v & 1) == 0)
      { v >>= 1;
```

```
        if ((y1 & 1) == 0 && (y2 & 1) == 0) { y1 >>= 1; y2 >>=
1; }
        else { y1 = (y1 + b) >> 1; y2 = (y2 - a) >> 1; } }
      }
  x = y1; y = y2; gcd = v << g;
```

Numerical Example

We will compare the proposed here algorithm with extended Stein' iterative [37].

```
 long a, b, x, y, y1, y2, d = 0, u, v;
 long x1, x2, gcd;
 for (int i = 1; i < 100000001; i++) { a = i; b = 200000002 -
i;
 //here is the source code of every one of algorithm 1 and
 //extended Stein' iterative [37]
 d += gcd; }
Console.WriteLine(d);
```

CPU time of Algorithm 1 is: **69.701 seconds.**

CPU time of Stein' iterative is: **75.568 seconds.**

Conclusion

We demonstrate how the extended Stein' algorithm can be optimized. We believe that these results will be useful for the specialists in computer science and computational mathematics which want to make the computational processes to work faster.

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] Akritas, A., A new method for computing polynomial greatest common divisors and polynomial remainder sequences, *Numerische Mathematik*, 52 (1988), 119–127.

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

[3] Chang, F., Factoring a Polynomial with Multiple-Roots, *World Academy of Science, Engineering and Technology*, 47 (2008), 492–495.

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

[5] Garov, K., A. Rahnev, *Textbook-notes on programming in BASIC for facultative training in mathematics for 9.–10. Grade of ESPU*, Sofia (1986). (in Bulgarian)

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

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

[14] Iliev, A., N. Kyurkchiev, 80th Anniversary of the birth of Prof. Donald Knuth, *Biomath Communications*, 5 (2018), 7 pp.

[15] Iliev, A., 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] Iliev, A., 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] Iliev, A., N. Kyurkchiev, The faster Euclidean algorithm, *Collection of scientific works from conference*, Pamporovo, Bulgaria, 28–30 November 2018, (2019), 15–20.

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

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

[26] Iliev, A., 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] Gyulyustan, H., 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] Iliev, A., N. Kyurkchiev, A. Rahnev, New Algorithm for Finding Greatest Common Divisor, *preprint*.

[29] Iliev, A., N. Kyurkchiev, A. Rahnev, A New Improvement of Stein’s Binary Algorithm for Finding Greatest Common Divisor, *preprint*.

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

[31] Krushkov, Hr., A. Iliev, *Practical programming guide in Pascal, Parts I and II*, Koala press, Plovdiv (2002). (in Bulgarian)

[32] Nakov, P., P. Dobrikov, *Programming=++Algorithms*, 5th ed., Sofia (2015). (in Bulgarian)

[33] Rahnev, A., K. Garov, O. Gavrailov, *Textbook for extracurricular work using BASIC*, MNP Press, Sofia (1985). (in Bulgarian)

[34] Rahnev, A., K. Garov, O. Gavrailov, *BASIC in examples and tasks*, Government Press "Narodna prosveta", Sofia (1990). (in Bulgarian)

[35] Kasakliev, N., *C# Programming Guide*, University Press “Paisii Hilendarski”, Plovdiv (2016). (in Bulgarian)

[36] Rahnev, A., N. Pavlov, N. Valchanov, T. Terzieva, *Object Oriented Programming*, Lightning Source UK Ltd., London (2014).

[37] Menezes, A., P. Oorschot, S. Vanstone, *Handbook of Applied Cryptography*, 5th ed., CRC Press LLC, New York (2001).