International Electronic Journal of Pure and Applied Mathematics
Volume 15 No. 1 2021, 45-53
ISSN: 1314-0744
url: https://www.e.ijpam.eu
doi: 10.12732/iejpam.v15i1.5

A REFINEMENT OF THE BÖH'S ALGORITHM FOR COMPUTING MODULAR MULTIPLICATIVE INVERSE

Anton Iliev[1,2], Nikolay Kyurkchiev[1,2],
Asen Rahnev[1], Todorka Terzieva[1]

[1]Faculty of Mathematics and Informatics
University of Plovdiv Paisii Hilendarski
24, Tzar Asen Str., 4000 Plovdiv, BULGARIA

[2]Institute of Mathematics and Informatics
Bulgarian Academy of Sciences
Acad. G. Bonchev Str., Bl. 8, 1113 Sofia, Bulgaria

Abstract: In this note we redesign and decrease number of operations in the algorithm [59]. Our benefit from this reduction is the faster calculation of modular multiplicative inverse for the approach from [59].

AMS Subject Classification: 11A05, 68W01
Key Words: modular multiplicative inverse, Böh's algorithm, reduced number of operations

1. Introduction

Let a and b be a natural numbers. We set our task to reorganize the algorithm in [59] and provide more effective in comparison to [59] recursively and iteratively ways for computation of the modular multiplicative inverse of a modulo b (eeacmi1 := $a^{-1} \pmod{b}$) as well as simultaneously eeacmi2 := $b^{-1} \pmod{a}$. For the practical importance and implementations which concern Euclidean algorithm, see [1]–[6] and [45]–[60]. New results also are presented in [10]–[44], [53]–[58].

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.

In [32] using other boundary conditions we optimize the classical Stein's binary algorithm for calculating greatest common divisor:

Received: April 10, 2021
Revised: May 28, 2021
Published: June 6, 2021

International Electronic Journal of Pure and Applied Mathematics – IEJPAM, Volume 15, No. 1 (2021)

```
k = 0; j = 0;
while ((a & 1) == 0) { a >>= 1; j++; }
while ((b & 1) == 0) { b >>= 1; k++; }
if (j < k) min = j; else min = k;
while (a != b)
if (a > b) { a -= b;
do a >>= 1; while ((a & 1) == 0); }
else { b -= a;
do b >>= 1; while ((b & 1) == 0); }
gcd = a <<= min;
```

The approach in [32] keen us to develop series of effective algorithms in [33]–[44].

2. Main Results.

Based on results in [59] we propose the following optimized iterative

Algorithm 1.

```
if ((a & 1) == 0 && (b & 1) == 0) eeacmi1 = eeacmi2 = 0;
else
{
a0 = a; b0 = b; iter = 0;
x1 = 1; x2 = 0; y1 = 0; y2 = 1;
while ((a & 1) == 0)
{ iter++; a >>= 1; y1 <<= 1; y2 <<= 1; }
while ((b & 1) == 0)
{ iter++; b >>= 1; x1 <<= 1; x2 <<= 1; }
while (a != b)
if (a < b)
{
b -= a; y1 += x1; y2 += x2;
do
{ iter++; b >>= 1; x1 <<= 1; x2 <<= 1; }
while ((b & 1) == 0);
}
else
{
a -= b; x1 += y1; x2 += y2;
do
{ iter++; a >>= 1; y1 <<= 1; y2 <<= 1; }
while ((a & 1) == 0);
```

International Electronic Journal of Pure and Applied Mathematics – IEJPAM, Volume 15, No. 1 (2021)

```
}
if (b > 1) eeacmi1 = eeacmi2 = 0;
else
{
while (iter > 0)
{
if ((y1 & 1) == 1 ||(y2 & 1) == 1) { y1 += b0; y2 += a0; }
iter--; y1 >>= 1; y2 >>= 1;
}
while (y1 > 0) y1 -= b0; while (-b0 >= y1) y1 += b0; eeacmi1 = -y1;
while (y2 < 0) y2 += a0; while (y2 >= a0) y2 -= a0; eeacmi2 = y2;
}
}
```

and its recursive version as

Algorithm 2.

```
static long Euclid(long a, long b, ref long x,
ref long y, ref long iter, long x1, long x2, long y1, long y2)
{
if ((a & 1) == 0)
{
iter++;
return Euclid(a >> 1, b, ref x, ref y, ref iter, x1, x2, y1 << 1, y2 << 1);
}
if ((b & 1) == 0)
{
iter++;
return Euclid(a, b >> 1, ref x, ref y, ref iter, x1 << 1, x2 << 1, y1, y2);
}
if (a == b) { x = y1; y = y2; return a; }
else
if (a > b)
return Euclid(a - b, b, ref x, ref y, ref iter, x1 + y1, x2 + y2, y1, y2);
else
return Euclid(a, b - a, ref x, ref y, ref iter, x1, x2, y1 + x1, y2 + x2);
}
```

and its calling:

```
if ((a & 1) == 0 && (b & 1) == 0) eeacmi1 = eeacmi2 = 0;
```

International Electronic Journal of Pure and Applied Mathematics – IEJPAM, Volume 15, No. 1 (2021)

```
else
{
iter = 0;
x1 = 1; x2 = 0; y1 = 0; y2 = 1;
gcd = Euclid(a, b, ref x, ref y, ref iter, x1, x2, y1, y2);
if (gcd > 1) eeacmi1 = eeacmi2 = 0;
else
{
while (iter > 0)
{
if ((x & 1) == 1 ||(y & 1) == 1) { x += b; y += a; }
x >>= 1; y >>= 1; iter--;
}
while (x > 0) x -= b; while (-b >= x) x += b; eeacmi1 = -x;
while (y < 0) y += a; while (y >= a) y -= a; eeacmi2 = y;
}
}
```

Numerical Example.

Below is the source code of the main function, which we have used for our testing purposes:

```
long a, b, iter, d = 0, eeacmi1, eeacmi2, d1 = 0, d2 = 0;
long gcd, b0, a0, x1, x2, x = 0, y = 0, y1, y2;
int min, j, k;
for (int i = 1; i < 100000001; i++) { a = i; b = 200000002 - i;
//here is placed the source code of every one of algorithm 1,
//calling of recursive algorithm 2
//and optimized classical Stein's binary algorithm
//from Introduction of the present paper
d1 += eeacmi1; d2 += eeacmi2;
}
Console.WriteLine(d1); Console.WriteLine(d2);
```

CPU time results are:

CPU time of Algorithm 1 is: **47.285 seconds.**

International Electronic Journal of Pure and Applied Mathematics – IEJPAM, Volume 15, No. 1 (2021)

CPU time of Algorithm 2 is: **107.739 seconds.**

3. Conclusion

Again we give an approach for betterment the numerical procedures, which are connected to the class of so called Euclidean algorithms.

Acknowledgements

This paper is supported by the National Scientific Program "Information and Communication Technologies for a Single Digital Market in Science, Education and Security (ICTinSES)", financed by the Ministry of Education and Science.

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

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

[9] T. Terzieva, *Educational tools for teaching in digital environment*, University Press "Paisii Hilendarski", Plovdiv (2021). (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*, **117** (2017), 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*, **118** (2018), 31–37.

[12] 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.

[13] 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.

[14] 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.

[15] 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.

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

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

[18] 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)

[19] 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.

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

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

[22] 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.

[23] 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.

[24] 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.

[25] 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.

[26] 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.

[27] 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.

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

[29] 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)

[30] 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.

[31] A. Iliev, N. Kyurkchiev, A. Rahnev, New Algorithm for Finding Greatest Common Divisor, *Neural, Parallel, and Scientific Computations*, 28 No. 1 (2020), 69–74.

International Electronic Journal of Pure and Applied Mathematics – IEJPAM, Volume 15, No. 1 (2021)

[32] A. Iliev, N. Kyurkchiev, A. Rahnev, A New Improvement of Stein's Binary Algorithm for Finding Greatest Common Divisor, *Neural, Parallel, and Scientific Computations*, 28 No. 1 (2020), 75–80.

[33] A. Iliev, N. Kyurkchiev, A. Rahnev, New Algorithms for Finding Modular Multiplicative Inverse, *Neural, Parallel, and Scientific Computations*, 28 No. 1 (2020), 81–88.

[34] 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.

[35] A. Iliev, N. Kyurkchiev, A. Rahnev, A New Improvement of Modular Multiplicative Inverse Binary Algorithm, *International Electronic Journal of Pure and Applied Mathematics*, 14 No. 1 (2020), 37–44.

[36] A. Iliev, N. Kyurkchiev, A. Rahnev, Recursive Extended Stein's Binary Algorithm, *International Electronic Journal of Pure and Applied Mathematics*, 14 No. 1 (2020), 31–36.

[37] A. Iliev, N. Kyurkchiev, A. Rahnev, A new improvement of Jacobi symbol algorithm, *International Electronic Journal of Pure and Applied Mathematics*, 15 No. 1 (2020), 13–22.

[38] A. Iliev, N. Kyurkchiev, A. Rahnev, A new improvement of Jacobi symbol binary algorithm, *International Electronic Journal of Pure and Applied Mathematics*, 15 No. 1 (2020), 1–11.

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

[40] 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.

[41] A. Iliev, N. Kyurkchiev, A. Rahnev, T. Terzieva, A Refinement of the Extended Euclidean Algorithm using SGN Function, (2021), preprint.

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

[43] 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.

[44] A. Iliev, N. Kyurkchiev, A. Rahnev, A New Improvement of Extended Stein's Binary Algorithm, *Proceedings of the Anniversary International Scientific Conference "Synergetics and Reflection in Mathematics Education"*, Pamporovo, 16–18 October 2020, Plovdiv University Press, (2020), 259–264.

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

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

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

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

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

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

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

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

[53] 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.

[54] 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.

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

[56] 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.

International Electronic Journal of Pure and Applied Mathematics – IEJPAM, Volume 15, No. 1 (2021)

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

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

[59] F. Böh, Verfahren zur Berechnung der modularen Inversen zweier Zahlen, *European Patent Office*, EP 1 271 304 A2, (2003), 11 pp.

[60] V. Strassen, Gaussian Elimination is not Optimal, *Numer. Math.* **13**, (1969), 354–356.

International Electronic Journal of Pure and Applied Mathematics – IEJPAM, Volume 15, No. 1 (2021)