Barret Modular Multiplication Algorithm

Akshay Hajare (SID 45756503)

ELEC8860 Engineering Unit

Macquarie University, NSW 2109 Australia

E-mail: akshay.hajare@students.mq.edu.au

18 MAY 2020

Abstract

The sole ideal being the solving is to make relevancy in the interleaved modular multiplication algorithms basing on the theories and the leman in the Barrett and Montgomery modular reduction. With the simple algorithms, especially in the suitable situation of multiplication. Ideally, get the proper way of the choosing of alpha(α) and beta (β), to minimize the error of the solution *q*. Furthermore, get the scrutiny of the selection of the bounding limits between the α and β to get soluble and relevant output. In some cases, the multiplication output in the modular multiplier times some to be alike or, moreover, alike critical criterion is necessary to keep consistency and soluble loop of iterative. The problems and formula in support of this from theories and lemma of relevant reference.

Key words: Barrett, Montgomery, Modular Multiplier, Alpha (α), Beta (β)

1. Preliminaries

The notation of the document is variable. Multiplication of the n-bit integer. That integer A is representing radix r representation as $A = (A_{n-1}\ldots A_0)_r$ where $r = 2^w$; n_w representing the [2] numbers in the digits integers and of equilibrium to $[n/w]$ where w is the digit size; A_i is the digit A_i and elements are $[0,r-1]$ [6].

2. A criterion for Choosing Alpha (α) And Beta (β)

The multiplication criteria of the Barret modular have the assumption of choosing the alpha and beta in the integers to minimize the error, assuming the results are q [6]. There furthermore, in the division in the integer. With the power of 2 is a simple shift operation with the looping sequence. They are an arbitrary value in the estimation of the situation q. At the last solution at the very end in the modular algorithm of multiplication has been evidence [1]. The arbitrary and more skillful sporting of the determination of α and β in which the modular multiplication classical on the background of the Barret rection proved the lemmas algorithm. Following the parameter: $\alpha = w + 3$ and $\beta = -2$. The parameters give the certainty of a clear sequence in the variable of w in the alpha [4].

3. Output Bound of The Selection of α and β

$X*Y = XYR^{-1} \bmod M$

The resulting solution needs to be converted back after the process. For the necessity of implementation to be effective usual $R=r^{nw}$ where $r = 2^{w}$ [7] each repeated digit similar to a multiplication of the precompute algorithm $M' = -M^{-1} \bmod r = -M_0^{-1} \bmod r$ in the algorithm solution final result [8].

4. The Inputs Likely Being the Same as The Output

In the algorithm calculation, the tendency of the repetitive solution of output being the same as the output: Algorithm of points multiplication in the Montgomery.

Input: G, K

Output

; Q= kG

initialize P_0=G; P_1 = 2G:

For (i=1-2; i> or = 0; i..)

If (k[i]==1) $P_0 = P_0 = P_1$;P_1=2P1; end for.

Q =P_0;

5. The Choice for Maintaining Good Iteration in Inputs and Outputs

The **input** is set to the $X = (X_{nw-1}\ldots X_0)_r$, $Y = (Y_{nw-1}\ldots Y_0)_r$,

$M = (M_{nw-1}\ldots M_0)_r$ Having 0 less or equal to $X,Y < M$, 2^{n-1} less or equal to $M < 2^n$, $r = 2^w$ with $nw = [n/w]$. The **output**: $Z = XY \bmod M$. with the for $i = n_w - 1$ down to 0 do Z implying $Zr = XY_i$ and the qc implying $[Z/M]$ and then Z implying $Z - qcM$ [3] **end for** return and continues with the iteration [5].

Applications

- The binary summation is using the technique Barret modular multiplication.
- Used in the pseudocode calculation for an algorithm in the prediction of multiplication with powers.
- The Montgomery require this skill in the Karatsuba modular multiplication of large digits

Conclusion

It is evident mathematical that the multiplication algorithm Barret modular is a tool that is very necessary for the multiplication. Moreover, the results of the error are contracts to the selection of α and β. Despite having the output and the input is the same, the modular multiplication algorithm givers explicit iteration to give correct output to a specific output.

References

[1] R. Liu and S. Li, "Implementation of VLSI Architecture for Montgomery Modular Multiplier", *International Journal of Innovative Technology and Exploring Engineering*, vol. 9, no. 1, pp. 218-221, 2019. Available: 10.35940/ijitee.a1045.1191s19.

[2] J. Ding and S. Li, "A Modular Multiplier Implemented with Truncated Multiplication", *IEEE Transactions on Circuits and Systems II: Express Briefs*, vol. 65, no. 11, pp. 1713-1717, 2018. Available: 10.1109/tcsii.2017.2771239.

[3] C. Negre and T. Plantard, "Efficient regular modular exponentiation using multiplicative half-size splitting", *Journal of Cryptographic Engineering*, vol. 7, no. 3, pp. 245-253, 2016. Available: 10.1007/s13389-016-0134-5.

[4] L. Meng, "Automatic Timetable Generation Using Genetic Algorithm", *Journal of Information Engineering and Applications*, 2019. Available: 10.7176/jiea/8-1-03.

[5] D. Thiyam, S. Cruces, J. Olias and A. Cichocki, "Optimization of Alpha-Beta Log-Det Divergences and their Application in the Spatial Filtering of Two Class Motor Imagery Movements", *Entropy*, vol. 19, no. 3, p. 89, 2017. Available: 10.3390/e19030089.

[6] L. Ibanez et al., "Parkinson disease polygenic risk score is associated with Parkinson disease status and age at onset but not with alpha-synuclein cerebrospinal fluid levels", *BMC Neurology*, vol. 17, no. 1, 2017. Available: 10.1186/s12883-017-0978-z.

[7] T. Tan and H. Lee, "Efficient-Scheduling Parallel Multiplier-Based Ring-LWE Cryptoprocessors", *Electronics*, vol. 8, no. 4, p. 413, 2019. Available: 10.3390/electronics8040413.

[8] W. Severa, C. Vineyard, R. Dellana, S. Verzi and J. Aimone, "Training deep neural networks for binary communication with the Whetstone method", *Nature Machine Intelligence*, vol. 1, no. 2, pp. 86-94, 2019. Available: 10.1038/s42256-018-0015-y.