On Computing Modular Multiplicative Inverse

Yiu-Kwong Man, *Member, IAENG*

***Abstract* — A simple efficient method for computing modular multiplicative inverse is presented. This approach has the advantage that the backward substitutions commonly adopted for the Extended Euclidean Algorithm (EEA) can be avoided. The modular multiplicative inverse can be computed effectively by the successive quotients obtained in the Euclidean Algorithm (EA). Some illustrative examples are provided.**

***IndexTerms*—modular multiplicative inverse, Euclidean Algorithm, Extended Euclidean Algorithm, Chinese Remainder Theorem.**

I. Introduction

THE Euclidean Algorithm (EA) and the Extended Euclidean Algorithm (EEA) have important applications in number theory, discrete mathematics, computer sciences and cryptography [1-7], etc. In this paper, we present a simple efficient approach for computing modular multiplicative inverse via EA. However, the backward substitutions commonly involved in the EEA can be avoided, The modular multiplicative inverse can be computed effectively by the successive quotients obtained by EA [3, 4, 6]. This new approach is based on the author's recent works on solving linear Diophantine equations in two variables [8, 9] and it is highly suitable for either hand calculation or computer programming.

The whole paper is organized like this. The mathematical background is described in section 2. Then, the new approach is introduced in section 3, followed by some examples in section 4. Finally, some concluding remarks are described in section 5.

II. Mathematical Background

Consider two positive integers a, b such that $a < b$. Their greatest common divisor GCD (a, b) can be computed by the Euclidean Algorithm as follows:

$$\begin{aligned} b &= aq_1 + r_1 \\ a &= r_1 q_2 + r_2 \\ r_1 &= r_2 q_3 + r_3 \\ &\vdots \\ r_{n-3} &= r_{n-2} q_{n-1} + r_{n-1} \\ r_{n-2} &= r_{n-1} q_n \end{aligned}$$

where q_i, r_i are the successive quotients and remainders obtained by the divisions involved in the Euclidean Algorithm, and r_{n-1} is equal to GCD (a, b). Moreover, if we are required to solve the Diophantine equation $ax + by = c$, where c is divisible by GCD (a, b), then backward substitutions can be adopted for finding a particular solution, which is known as the Extended Euclidean Algorithm. In particular, if a and b are coprime, namely GCD(a, b) = 1, the linear Diophantine equation $ax + by = 1$ is solvable, which is equivalent to the problem of finding the multiplicative inverse such that it satisfies $ax \equiv 1 \pmod{b}$. Here is an example for illustrating how the backward substitution approach works.

The author is working at the Department of Mathematics and Information Technology, EdUHK and a member of *IAENG*. (E-mail: ykman@eduhk.hk).

Example 1. Solve $8x \equiv 1 \pmod{11}$.

Solution. This problem is equivalent to solving the Diophantine equation $8x + 11y = 1$. Using the Euclidean Algorithm, we obtain

$$\begin{aligned} 11 &= 1 \times 8 + 3 \\ 8 &= 2 \times 3 + 2 \\ 3 &= 1 \times 2 + 1 \\ 2 &= 2 \times 1. \end{aligned}$$

Starting from the second last equation and working backward, we have

$$\begin{aligned} 1 &= 3 - 2 \\ &= 3 - (8 - 2\times 3) \\ &= 3 \times 3 - 8 \\ &= 3 \times (11 - 8) - 8 \\ &= 3 \times 11 - 4 \times 8. \end{aligned}$$

Hence, $x \equiv -4 \equiv 7 \pmod{11}$ is a particular solution of $8x \equiv 1 \pmod{11}$ and the general solution is $x = 7 + 11k$, where k is an arbitrary integer.

From this example, we can see that backward substitutions involve the tasks of removing brackets and collecting the integer multiples of the given numbers in order to find the modular multiplicative inverse. Can we compute it by an alternative approach without using backward substitutions? In the next section, we will introduce such an approach for finding modular multiplicative inverse.

III. Alternative Approach

Using the above notations, we have

$$\begin{aligned} r_1 &= b - aq_1 \\ r_2 &= a - r_1q_2 = a - (b - aq_1)q_2 = -bq_2 + a\,(1 + q_1q_2) \\ r_3 &= r_1 - r_2q_3 = (b - aq_1) - q_3[-bq_2 + a\,(1 + q_1q_2)] \\ &= b\,(1 + q_2q_3) - a\,[q_1 + q_3\,(1 + q_1q_2)] \\ r_4 &= r_2 - r_3q_4 \\ &= -bq_2 + a\,(1 + q_1q_2) - q_4[b\,(1 + q_2q_3) - a(q_1 + q_3\,(1 + q_1q_2))] \\ &= -b\,[q_2 + q_4\,(1 + q_2q_3)] + a\,[q_1\,q_4 + (1 + q_1q_2)\,(1 + q_3q_4)] \end{aligned}$$

ISBN: 978-988-14049-2-3
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

and so on. According to the pattern of the coefficients, we can deduce the recurrence relations (see [8, 9]) for finding a solution of $ax + by = 1$ or the multiplicative inverse of $ax \equiv 1 \pmod{b}$ as follows:

$$x_0 = 1,\ x_1 = q_1 \text{ and } x_i = x_{i-2} + q_i x_{i-1} \text{ for } 1 < i < n,$$
$$y_0 = 0,\ y_1 = 1 \text{ and } y_i = y_{i-2} + q_i y_{i-1} \text{ for } 1 < i < n.$$

Let $x' = (-1)^n x_{n-1}$ and $y' = (-1)^{n-1} y_{n-1}$. Then, (x', y') is a particular solution of $ax + by = 1$ and x' mod b is the multiplicative inverse of $ax \equiv 1 \pmod{b}$.

We can see that the tedious task of backward substitutions can be avoided and the alternative procedure only involves the successive quotients obtained by the Euclidean algorithm. Thus, it is very convenient for hand calculation or computer programming.

IV. EXAMPLES

Example 2. Solve $8x \equiv 1 \pmod{11}$ by the alternative approach described above.

Solution. According to Example 1, the successive quotients (except the last one) obtained by the Euclidean algorithm are 1, 2 and 1 respectively. Following the alternative procedure described above, we obtain:

i	0	1	2	3
q_i		1	2	1
x_i	1	1	3	4

Hence, $x \equiv -4 \equiv 7 \pmod{11}$ is a solution of $8x \equiv 1 \pmod{11}$.

Example 3. Find the multiplicative inverse of 797 mod 15936.

Solution. Consider $797x \equiv 1 \pmod{15936}$. Applying the Euclidean algorithm, the successive quotients (except the last one) obtained are 19, 1 and 198 respectively.

i	0	1	2	3
q_i		19	1	198
x_i	1	19	20	3979

Hence, $x \equiv -3979 \equiv 11957 \pmod{15936}$, which is the multiplicative inverse required.

The following example shows this approach can also be used to solve a system of linear congruences via the use of the Chinese Remainder Theorem (CRT).

Theorem (Chinese Remainder Theorem). Let $n_1, n_2, \ldots, n_k$ be positive integers such that GCD $(n_i, n_j) = 1$ for $i \neq j$. Then the system of linear congruences

$$\begin{aligned} x &\equiv a_1 \pmod{n_1} \\ x &\equiv a_2 \pmod{n_2} \\ &\vdots \\ x &\equiv a_k \pmod{n_k} \end{aligned}$$

has a simultaneous solution, which is unique modulo the product of $n_1, n_2, \ldots, n_k$.

Reader can refer to [2] for the proof of this important theorem in number theory. We now illustrate how to apply the alternative approach described in this paper for solving a system of linear congruences by means of the Chinese Reminder Theorem.

Example 4. Solve the following system of linear congruences

$$\begin{aligned} x &\equiv 4 \pmod{5} \\ x &\equiv 3 \pmod{7} \\ x &\equiv 5 \pmod{11} \end{aligned}$$

Solution. First, let us compute the followings:

$$\begin{aligned} n &= \text{lcm}\,(5, 7, 11) = 385 \\ N_1 &= n / 5 = 77 \\ N_2 &= n / 7 = 55 \\ N_3 &= n / 11 = 35 \end{aligned}$$

Next, consider the linear congruences $77y \equiv 1 \pmod{5}$, $55y \equiv 1 \pmod{7}$ and $35y \equiv 1 \pmod{11}$. Applying the alternative approach, we can easily obtain their solutions, namely $y_1 = 3$, $y_2 = 6$ and $y_3 = 6$ respectively. Thus, we can obtain the following solution for the given system of linear congruences:

$$x = 77(3)(4) + 55(6)(3) + 35(6)(5) = 2964.$$

Hence, $x = 2964 \equiv 269 \pmod{385}$ is the unique solution of the given system modulo 385.

V. CONCLUDING REMARKS

In this paper, we have introduced a simple efficient approach for computing modular multiplicative inverse, which can avoid using backward substitutions. This approach can be used to solve a system of linear congruences via the Chinese Remainder Theorem (CRT). Since the latter has wide applications in various areas such as scientific computing, number theory, coding theory and cryptography, we anticipate that this new approach will be found useful for reference by researchers in related disciplines, as well as lecturers involved in teaching number theory, discrete mathematics or computer programming, etc.

REFERENCES

[1] B. Anjanadevi, P. S. Sitharama Raju, V. Jyothi and V. Kumari, "A Novel approach for privacy preserving in video using Extended Euclidean algorithm based on Chinese Remainder Theorem", *Int. J. Communication & Network Security*, vol. 1, pp. 45-49, 2011.

[2] D. M. Burton, *Elementary Number Theory*, Boston: Allyn and Bacon, 1980.

[3] J. Gathen and J. Gerhard, *Modern Computer Algebra*, Cambridge: Cambridge University Press, 1999.

[4] V. Keerthika, "Role of Chinese Reminder Theorem in cryptography", International Journal of Engineering and Advanced Technology, vol. 8, pp. 256-258, 2019.

[5] J. A. M. Naranjo, J. A. Lopez-Ramos and L. G. Casado, "Applications of the Extended Euclidean Algorithm to privacy and secure communications", *Proceedings of the 10th International Conference*

ISBN: 978-988-14049-2-3
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

on Computational and Mathematical Methods in Science and Engineering, CMMSE 2010, pp. 27-30, 2010.
[6] O. Ore, *Number Theory and Its History*, NY: Dover, 1988.
[7] M. Syafiq Johar, "Minimal number of steps in the Euclidean algorithm and its application to rational tangles", *Rose-Hulman Undergraduate Mathematics Journal*, vol. 16, article 3, 2015.
[8] Y.K. Man, "A top-down approach for solving linear Diophantine equation", *Proceedings of the World Congress on Engineering 2019, WCE2019, Lecture Notes in Engineering and Computer Science, 3-5 July 2019, London, U.K.*, pp. 11-13.
[9] Y.K. Man, "A simple approach for solving linear Diophantine equation in two variables", In S.I. Ao, L. Gelman, H.K. Kim (Eds.), *Transactions on Engineering Technologies*, pp. 83-87, Singapore: Springer, 2021.

ISBN: 978-988-14049-2-3
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)