Algologic Technical Report #9/2012

An interesting property of Multiplicative inverse in mod(m)

S. Parthasarathy
drpartha@gmail.com

Ref.: euclid3.tex
Version : 20121225a

Abstract

This report examines an interesting aspect of modular arithmetic. A companion paper [1] studies the basic properties of modular multiplicative inverses.

1 Basic definitions

This Technical Report is a sequel to [1]. In the text that follows, we use the symbols "*" and "." (ignore the quote signs) to denote traditional arithmetic multiplication.

$\mathbb{Z}$ Denotes the set of integers {..., -2, -1, 0, 1,2,3,4,....}

$\mathbb{Z}^+$ Denotes the set of positive integers {1,2,3,4,....}

$\mathbb{Z}_m$ Denotes the set of residues (remainders) {0,1,2,3,4,5,.....m-1} when $z \in \mathbb{Z}$ is divided by m.

2 The modular multiplicative inverse problem – an interesting observation

Given $P,\ find\ Q\ such\ that\ P*Q = 1$ is a trivially simple problem in elementary arithmetic. e.g. Given $P = 5, P * Q = 1 \Longrightarrow Q = 1/5$

Q is said to be the *multiplicative inverse of P*, and vice-versa.

This same problem may be restated in modular arithmetic as :

Problem statement :: Given $P, m\ ,\ find\ Q\ such\ that\ P * Q \equiv 1 * mod(m)$

Q is said to be the *modular multiplicative inverse of P*, and vice-versa. Computing Q in mod(m) arithmetic is not as stratightforward as in elementary arithmetic.

We now report an interesting observation concerning modular multiplicative inverses.

We observe that the modular multiplicative inverse of 5 mod 6 is 5 ($1\ \equiv 5 * 5\ mod\ 6$). The modular multiplicative inverse of 5 mod 4 is 5 ($1\ \equiv\ 5{*}5\ mod\ 4$). *We notice the incredible property that the multiplicative inverse of n is n, under a certain modulo arithmetic.*

We can generalise this observation as:

- The modular multiplicative inverse of n mod (n+1) is n
- The modular multiplicative inverse of n mod (n-1) is n

2.1 Proof

By defifinition, P is the modular multiplicative inverse of Q mod m if P*Q mod m = 1.

This implies that
$\exists k : k \in \mathbb{Z}\ and\ k * m + 1 = P * Q$

We use this definition to prove that : *The modular multiplicative inverse of n mod (n+1) is n*

If n*n mod (n+1) = 1

$$
\begin{aligned}
then\ k * (n+1) + 1 &= n * n && (1)\\
k * (n+1) &= n * n - 1 && (2)\\
&= n^2 - 1 && (3)\\
&= (n+1) * (n-1) && (4)\\
\therefore k &= (n-1) && (5)
\end{aligned}
$$

Since $n \in \mathbb{Z}$, $k \in \mathbb{Z}$. QED
Similarly, we can prove that : *The modular multiplicative inverse of n mod (n-1) is n*. In this case, k = (n+1)

3 Concluding Remarks

This report was typeset in LaTeX by the author (using Kile, on a Suse Linux system). The LaTeX source can be obtained from the author, by sending a request to `drpartha@gmail.com`. Please quote the reference code and the version code given in the beginning of this report (below the title line).

Writing a mathematically rich document, and typesetting it using LaTeX , is a perilous task. The author welcomes comments, suggestions and remarks (about this article). Please report any flaws, inconsistencies, and ambiguities you may find, to `drpartha@gmail.com`. The author thanks you in advance, for this gesture. Every such communication will also be personally acknowledged by the author, and taken into account in the next version of this report.

The author will be happy to answer any questions you may have on this subject.

References

[1] `S. Parthasarathy`, *Multiplicative inverse in mod(m)*, Algologic Technical Report #1/2012, Feb. 2012.

* * *$_{\text{end}}$