

MOD Theory

SADI KHAN

(30 December, 1999)

Theorem 1

$A \in \mathbb{N}, B \in \mathbb{N}$ and $C \in \mathbb{N}$

If $A < C$ then $A \% C = A$,

For any value of A , $A \% C$ must be less than C

so, $(A \% C) \% C = (A \% C)$

$$(A \% C) \% C = (A \% C)$$

If $A \% C = K$, that means, when we divide A by C then there will be a gap of length K . So,

$\Rightarrow m.(A \% C) = mK$

Again, if we divide mA by mC then length of the gap must be mK

That means,

$\Rightarrow m.(A \% C) = mA \% mC$

$$m.(A \% C) = mA \% mC$$

Theorem 2

Let $Z = (A \times B) \% C$

Suppose $A \% C = m$, that means if we divide A by C then m will be the remainder that is there will be a gap of length m .

For $2A$ then gap will be $2m$ (if $2m < C$)

In the same way for nA , the gap will be nm .

if $nm > C$ then we have to divide it by C in order to get the actual remainder.

So, $Z = nm \% C$

As, $m = A \% C$, $Z = \{n \times (A \% C)\} \% C$

If we put B instead of n then the expression looks like,

$$(A \times B) \% C = \{ (A \% C) \times B \} \% C$$

Corollary: $(A + B) \% C = \{ (A \% C) + (B \% C) \} \% C$

Theorem 3

Again let $A \% C = m$.

So, $Z = (m \times B) \% C$

$= (B \times m) \% C$

$= \{(B \% C) \times m\} \% C$

$= \{(A \% C) \times (B \% C)\} \% C$

$$(A \times B) \% C = \{(A \% C) \times (B \% C)\} \% C$$

Theorem 4

If $A=B$ then $Z = \{(A \% C) \times (A \% C)\} \% C$

so, $A^2 \% C = (A \% C)^2 \% C$

$$A^2 \% C = (A \% C)^2 \% C$$

Author: Masudur Rahman Khan (Sadi)

<http://www.sadi-khan.com>

Theorem 5

$A^n \% C = (A \% C)^n \% C$ is true if $n = 1$

Suppose, it is also true for $n=m$.

According to this we can write, $A^{m+1} \% C = (A \% C)^{m+1} \% C$

Again,

$A^{m+1} \% C$

$= (A \cdot A^m) \% C$

$= \{(A^m \% C) \times (A \% C)\} \% C$

$= \{[(A \% C)^m \% C] \times (A \% C)\} \% C$

$= \{(X \% C) \times Y\} \% C$ [Taking $X = (A \% C)^m$ and $Y = (A \% C)$]

$= XY \% C$

$= (A \% C)^{m+1} \% C$

so $A^{m+1} \% C = (A \% C)^{m+1} \% C$

This statement is true for $n=1$, so it will be true for $n+1$ if it is true for n . (Theory of induction)

$$\boxed{A^n \% C = (A \% C)^n \% C}$$

Theorem 6

Let, $ABC \% D = K$

$\Rightarrow A(BC) \% D$

$\Rightarrow [(A \% D)(BC \% D)] \% D$ [See theorem : 3]

$\Rightarrow [(A \% D)\{(B \% D)(C \% D)\} \% D] \% D$

$\Rightarrow [P.(MN \% D)] \% D$ [let $M = B \% D$ and $N = C \% D, P = A \% D$]

$\Rightarrow [(MN \% D).P] \% D$

$\Rightarrow MNP \% D$ [See theorem : 2 ($MN = A, P = B, D = C$, that is, $\{(A \% C).B\} \% C$]

$\Rightarrow \{(A \% D)(B \% D)(C \% D)\} \% D$

$$\boxed{(ABC) \% D = \{(A \% D)(B \% D)(C \% D)\} \% D}$$