4. Cartesian Elimination

let $A\times B=\{(a,b): a\in A, b\in B\}$

$A\times C=\{(a,c): a\in A, c\in C\}$

Suppose $A\times B=A\times C$, which means

$\forall x(x\in A\times B \leftrightarrow x\in A\times C)$

let $P(m,n)$ be an arbitrary point in $A\times B$

$\therefore$ it is also a point in $A\times C$

$\therefore m\in A \quad n\in B \quad n\in C$

$\therefore$ for every n, if it is in B, than it is in C

$\forall x(x\in B\rightarrow x\in C)$

vise versa $\forall x(x\in C\rightarrow x\in B)$

$\therefore B=C$

$\therefore A\times B=A\times C\rightarrow B=C$

If A is empty

than $A\times B=\varnothing$ $A\times B=A\times C$

$A\times C=\varnothing$

but the Cartesian Product of empty set with every sets is $\varnothing$

So we cannot tell how is B and C

$A=\varnothing\rightarrow A\times B=A\times C$

but $A\times B=A\times C\not\rightarrow B\times C$

5. Modular Numerology

$c=a \bmod p$ $d=b \bmod p$	Division: ①②③⑤⑥ Congruence: ④⑦

$\therefore$ there exists unique quotient integer x, y

enables $a=xp+c$ ①

$b=yp+d$ ②

Suppose $m\mid p$ and $a\equiv b \pmod m$

$\therefore$ exist integer k $p=km$ ③ $m\mid(a-b)$ ④

$a-b=(xp+c)-(yp+d)$

$=(x-y)p+(c-d)$

$=k(x-y)m+c-d$

$\because m\mid a-b$

$\therefore (a-b) \bmod m=0$ ⑤

$\therefore (k(x-y)m+c-d) \bmod m=0$

$\therefore (c-d) \bmod m=0$ ⑥

$\therefore m\mid c-d$

$\therefore c\equiv d \pmod m$ ⑦

$\therefore m\mid p\wedge a\equiv b \pmod m \rightarrow c\equiv d \pmod m$

(Direct proof rule)

6. Prime Examples

p is prime, so it has just two positive factors: p and 1

let $n=p \bmod 6$ $0\le n<6$

$\therefore$ there exist unique quotient m for $p=6m+n$

for $0\le n<6$, n might be 0, 1, 2, 3, 4, 5

① if n is 0
$p=6m$
$6\mid p$
p is not prime

② if n is 1
$p=6m+1$
p can be prime

③ if $n=2$
$p=6m+2$
$=2(3m+1)$
$2\mid p$ not prime

④ $n=3$
$p=6m+3$
$=3(2m+1)$
$3\mid p$ not prime

⑤ $n=4$
$p=6m+4$
$=2(3m+2)$
$2\mid p$ not prime

⑥ $n=5$
$p=6m+5$
can be prime

$\therefore$ n might be 1 or 5

$\therefore p=6m+1$ or $p=6m+5$

$6\mid(p-1)$ or $6\mid(p-5)$

$\therefore p\equiv 1 \pmod 6$ or $p\equiv 5 \pmod 6$