موضوع الدرس: _____ التاريخ: / /

Diophantine Equation

↳ only integer solution

Linear Diophantine equ.

$ax + by = c$

(x, y) → variables.

* Has a solution IFF $c \% \gcd(a,b) = 0$.

first → If we assume that $g = \gcd(a,b)$

$\therefore ax + by = g$ (Extended euclidean) solve by →

Generally, if $c \% g = 0 \rightarrow t = c/g$ *

$\therefore ax*t + by*t = g*t = c$

موضوع الدرس: ——— التاريخ: / /

Congruence

$$a \equiv b \pmod{n}$$

* a and b congruent modulo n.

* It means $a \% n = b \% n = x$

∴ $(a - b) \bmod n = \text{Zero}$

$37 \equiv 57 \pmod{10}$

∴ $37 \% 10 = 57 \% 10 = 7$

$(\overbrace{57 - 37}^{20}) \bmod 10 = \text{Zero}$

* More Importantly $a - b = q \cdot n$

$\frac{20}{10} = 2 \leftarrow \frac{(a-b)}{n}$

∴ $20 = 2 \times 10$, $a = b + qn$

$(a-b)$, q , n

موضوع الدرس: _____ التاريخ: / /

$\therefore a \equiv b \pmod n$

$= a = b + qn$

* IF $ax \equiv ay \pmod n$

$\therefore x \equiv y \left(\mod \left(\frac{n}{\gcd(a,n)} \right) \right)$

$\therefore$ If $ax \equiv ay \pmod n$

Same $x \equiv y \pmod n$

$\therefore \gcd(a,n) = 1$

1) * IF $a \equiv b \pmod m$, $b \equiv c \pmod m$

$\therefore a \equiv c \pmod m$

$16 \equiv 13 \mod 3$, $13 \equiv 22 \pmod 3$

$\therefore 16 \equiv 22 \pmod 3$

$3 \cdot 37 \equiv 357 \pmod{10}$

$-20 \equiv -10 \in \mathbb{Z}$ → ∴ gcd(3, 10) = 1

$111 \equiv 171 \pmod{10}$

$-60 \equiv 0 \pmod{10}$

~~$16 \equiv 13 \pmod{3}$~~

$16 \equiv 13 \pmod{3}$

$256 \equiv 169$

$(16)^2 \equiv (13)^2 \pmod{3}$

∴ If $a \equiv b \pmod{p}$ → $a^n \equiv b^n \pmod{p}$, $n \geq 1$

$(15 + 13)^2 \equiv 15^2 + 13^2 \pmod{2}$

$784 \equiv 394 \pmod{2}$

$390 \pmod{2} = \text{zero}$

∴ If p is prime ∴

$(x + y)^p \equiv x^p + y^p \pmod{p}$

4) If $a \equiv b \pmod m$,
$c \equiv d \pmod m$
$\therefore a \pm c \equiv b \pm d \pmod m$

* $16 \equiv 13 \pmod 3$ ⊕ $\therefore 38 \equiv 38 \pmod 3$
$22 \equiv 25 \pmod 3$ ⊖ $-6 \equiv -12 \pmod 3$

5) If $a \equiv b \pmod m$,
$c \equiv d \pmod m$
$\therefore ac \equiv bd \pmod m$
$16 \equiv 13 \pmod 3$ $\therefore 352 \equiv 325 \pmod 3$
$22 \equiv 25 \pmod 3$

6) If $a \equiv b \pmod m$
$\therefore a + c \equiv b + c \pmod m$

7) If $a \equiv b \pmod m$
$\therefore ac \equiv bc \pmod m$
$16 \equiv 13 \pmod 3$
$16 * 2 \equiv 13 * 2 \pmod 3$

* from Rule 7 $\rightarrow ax \equiv b \pmod m$
same as $x \equiv \frac{b}{a} \pmod m$
$\rightarrow x \equiv ba^{-1} \pmod m$

* Congruence and large power :-

* Find answer of 3^{5555} % 80

$3^4 \equiv 1 \pmod{80}$

$3^{5555} = (3^4)^{1388} + 3^3$ 5555 = 4*1388 + 3

∴ 3^3 % 80 = 27

* Find answer (3^{1000} + 3) % 28

$3^3 \equiv -1 \pmod{28}$

1000 = (3 * 333) + 1

$(3^3)^{333} \rightarrow -1$

∴ $(-1 * 3^1) + 3$ % 28 = 6

* ∴ عكسي نقلل الباور في المود بحيث ان نفكر في ال ≡ ل 1 أو -1

موضوع الدرس:—— التاريخ / / ٢٠

⊛ Linear Modular Equation :-

Solve $ax \equiv b \ (\%\ m)$

$ax = b + q_1 m$

$\therefore ax + (-q_1) m = b$ → linear Diophantine

y

Ex $258x \equiv 369 \pmod{147}$

$\therefore 258x = 369 + q_1 147$

$\therefore 258x + 147y = 369$

Solve by Euclides

$\gcd(a,b) = 3$

$369 \% 3 = 0$

$\therefore 258x + 147y = 3$

$\therefore 258(x * 123) + 147(y * 123) = 3 * 123$

$\therefore$ % should impose some restrictions

We take % m to any ax → m solution max!

However we can prove only gcd unique solution

∴ linear Diophantine → Infinite ∈

∴ linear Modular Eqn → gcd (a, b) → ∈