3336

Office Hour

11:00 am

A (direct) proof for a Proposition is presented below. Read through the proof and then determine which Proposition was proven.

Undefined control sequence \square

a) ○ Technically no proposition was proven true since there is an algebraic mistake in Line (3).

b) ○ If you add up six consecutive integers, then the result is equivalent to ~~1~~ 3 mod 6.

c) ○ If $x \in \mathbb{Z}$ then $\sum_{i=0}^{5} x + i \not\equiv 0 \bmod 6$.

d) ○ The sum of 6 consecutive integers is never congruent to 0 mod 6.

Proposition.

(1) Let $x \in \mathbb{Z}$ and consider the 6 consecutive integers $x, x+1, x+2, x+3, x+4, x+5$.
(2) The sum of these integers equals $6x + 15$.
(3) This expression reduces to a non-zero integer mod 6: $6x + 15 \equiv \overset{3}{1} \bmod 6$. ✓
(4) Therefore the sum of any 6 consecutive integers can never be a multiple of 6. □

Recall $a \equiv b \bmod n$ means:

1) $a$ + $b$ have the same remainder when divided by $n$

2) $a - b$ is a multiple of $n$

$x \in \mathbb{Z}$, the expression $6x + 15$ is NOT cong. to 1 mod 6

$6x + 15 - 1 = 6x + 14 = \underbrace{6(x+2)}_{\checkmark} + 2 \neq$ mult. of 6

not a multi of 6

faster: $6x + 15 \equiv 15 \bmod 6 \equiv 3 \bmod 6 \not\equiv 1 \bmod 6$

$a \equiv b \bmod n$

means:

2) a & b differ by a multiple of n

ex) $27 \equiv 67 \bmod 5$

$27 - 67 = -40 = (-8) \cdot 5$ ✓

1) a & b have the same remainder when divided by n

ex) $27 \div 5$ : $27 = 5 \cdot 5 + 2$

$67 \div 5$ : $67 = 5 \cdot 13 + 2$

Note:

$a = q_1 n + r$

$b = q_2 n + r$

$$a - b = q_1 n + r - (q_2 n + r)$$
$$= q_1 n - q_2 n$$
$$= \underbrace{(q_1 - q_2) n}_{\text{multi. of } n}$$

if a & b have same remainder when dividing by n, then $a - b =$ multi of n mod = "modular" = "modulo"

means "ignoring"

ex| lets work in $\underbrace{\mathbb{Z} \text{ mod } 7}$

"ignoring multiples of 7"

||

"only care about remainders"

$17 \equiv 3 \text{ mod } 7$

$17 + 3 = 20 \equiv 6 \text{ mod } 7$

$17 + 3 \equiv 3 + 3 \text{ mod } 7 = 6 \text{ mod } 7$

ex| $3 \cdot 3 = 9 \equiv 2 \text{ mod } 7$

ex| work mod 6

$3 \cdot 3 = 9 \equiv 3 \text{ mod } 6$

$4 \cdot 9 = 36 \equiv 0 \text{ mod } 6$

in many programming languages: the percent sign is used

ex) $27 \% 5 \longrightarrow 2$

$27 \equiv 2 \mod 5$

$$\underbrace{2 \bmod 5 = 7 \bmod 5}_{2 \equiv 7 \mod 5}$$

Use the Euclidean Algorithm to find a solution to the congruence equation $-18x \equiv 1 \mod 49$ (if a solution exists).

to solve an equation

$ax \equiv b \mod n$

1) $\gcd(a, n) \mid b$ ?

if yes, there are solutions

if no, there are no solutions

$-18x \equiv 1 \mod 49$

$a = -18$

$n = 49$

$b = 1$

1) $\gcd(-18, 49)$

use Euclid's Algorithm

note $-18 \equiv 31 \mod 49$

$\boxed{-18 + 49 = 31}$

$31x \equiv 1 \mod 49$

$a = 31$

$n = 49$

$b = 1$

$49 = 1 \cdot 31 + 18$

$31 = 1 \cdot 18 + 13$

$18 = 1 \cdot 13 + 5$

$13 = 2 \cdot 5 + 3$

$5 = 1 \cdot 3 + 2$

$3 = \underline{1} \cdot 2 + \boxed{1}$

$2 = \underline{2} \cdot 1 + 0$

first step: $\gcd(-18, 49) = \gcd(31, 49) = 1$

$-18x \equiv 1 \mod 49$

$31x \equiv 1 \mod 49$

$\gcd(31, 49) = 1$ this divides 1 so there are solutions!

---

Second step

$ax \equiv b \mod n$

if $\gcd(a, n) = 1$, then we use Bezout's Id to find an inverse of a !

$49 = \underline{1} \cdot 31 + 18$

$31 = \underline{1} \cdot 18 + 13$

$18 = \underline{1} \cdot 13 + 5$

$13 = \underline{2} \cdot 5 + 3$

$5 = \underline{1} \cdot 3 + 2$

$3 = \underline{1} \cdot 2 + \boxed{1}$

to get to Bezout's Id, rewrite these equations solving for remainders:

$18 = 49 - 31$

$13 = 31 - 18$

$5 = 18 - 13$

$3 = 13 - 2 \cdot 5$

$2 = 5 - 3$

$\boxed{1} = 3 - 2$

now, back substitute:

$1 = 3 - 2 = 3 - (5 - 3) = 2 \cdot 3 - 5$

$1 = 2(13 - 2\cdot 5) - 5 = 2\cdot 13 - 5\cdot 5$

$1 = 2\cdot 13 - 5(18 - 13) = 2\cdot 13 - 5\cdot 18 + 5\cdot 13$

$1 = 7\cdot 13 - 5\cdot 18$

$1 = 7\cdot(31 - 18) - 5\cdot 18$

$1 = 7\cdot 31 - 7\cdot 18 - 5\cdot 18$

$= 7\cdot 31 - 12\cdot 18$

$= 7\cdot 31 - 12\cdot(49 - 31)$

$1 = \underline{7\cdot 31} - 12\cdot 49 + \underline{12\cdot 31}$

$$\boxed{1 = 19\cdot 31 - 12\cdot 49}$$

original equation: $-18x \equiv 1 \mod 49$

$31x \equiv 1 \mod 49$

$19\cdot 31 = 1 + 12\cdot 49$

$19\cdot 31 \equiv 1 \mod 49$

19 is the inverse of 31 (mod 49)

$\underbrace{19\cdot 31}\, x \equiv 1 \mod 49$ (19·)

$1\cdot x \equiv 19 \mod 49$

$$\boxed{x \equiv 19 \mod 49}$$

$$\boxed{x = 19}$$

idea

$$a^{-1} a x = b \cdot a^{-1}$$

$$x = a^{-1} b$$

$\longrightarrow$

$ax \equiv b \mod n$

find $a^{-1}$ $\longleftarrow$ $a^{-1}$ may not exist !!

$\downarrow$

Bezout

$\downarrow$

Euclid Alg

$\downarrow$

Division Algorithm

---

$ax \equiv b \mod n$

$\gcd(a, n) \nmid b \longrightarrow$ no solutions

$\gcd(a, n) \mid b$

1) $\gcd(a, n) = 1 \longrightarrow$ exactly one solution

2) $\gcd(a, n) > 1 \longrightarrow$ multi solutions