

Modular Arithmetic

Simply Looking at the Face of Clock

10/13/2015

www.doorsteptutor.com

1

Why Bother?- Shortcuts to Several Problems

- Remainder Problems (Simple)
 - LCM
 - Chinese Remainder Theorem
- Remainders of Exponentiations: $\frac{3^{53}}{4}$?
- Last Digit Problems: 7^{17}
 - Modular Arithmetic
 - Euler's and Fermat's Little Theorem
 - Wilson's Theorem

10/13/2015

www.doorsteptutor.com

2

More Motivations – Reducing Big Numbers

•Time Problems

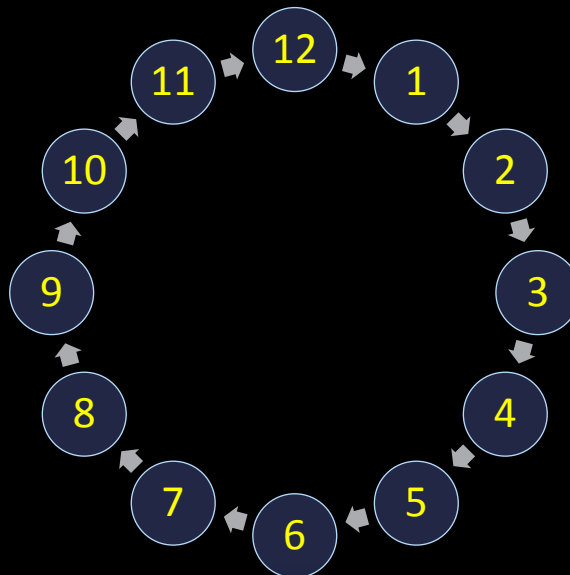
- A train coming at 3 pm is delayed 16 hours, what time will it come?

10/13/2015

www.doorsteptutor.com

3

Face of a Clock

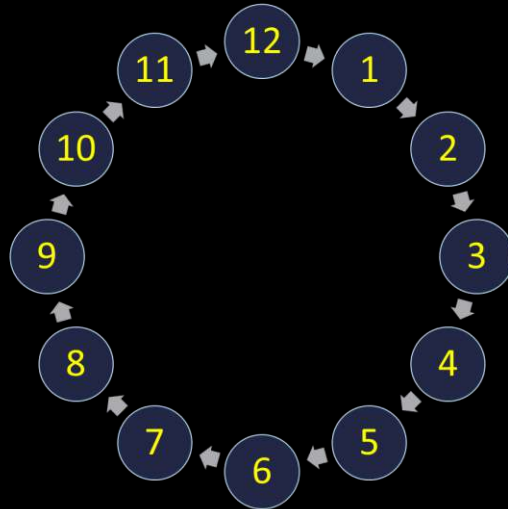


10/13/2015

www.doorsteptutor.com

4

Numbers in Clock World- Concept of Congruence

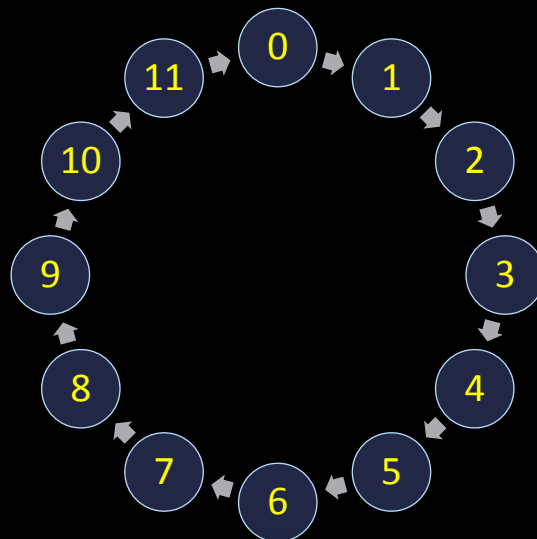


10/13/2015

www.doorsteptutor.com

5

Face of a Clock Replace 12 with 0- Modulo 12

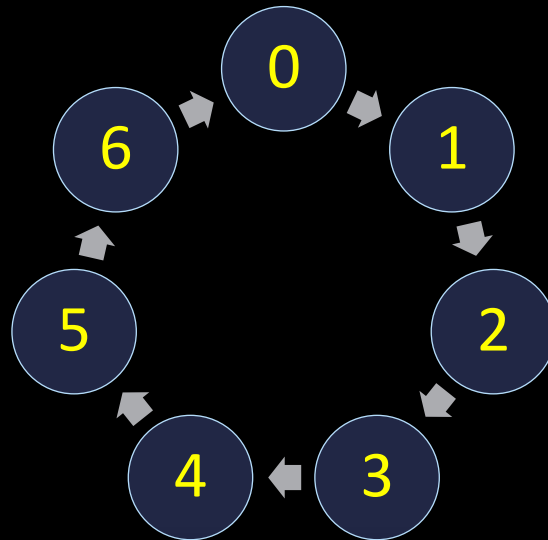


10/13/2015

www.doorsteptutor.com

6

What happens With 7 Days?

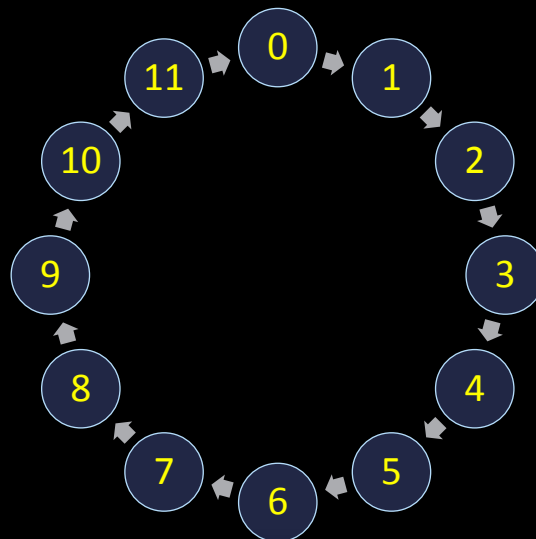


10/13/2015

www.doorsteptutor.com

7

Running the Clock Backwards



10/13/2015

www.doorsteptutor.com

8

Addition and Subtraction of Congruence's

10/13/2015

www.doorsteptutor.com

9

Application of Addition- Example-1

• Find last digit of: $2403 + 791 + 688 + 4339$

• Remainder of $\frac{60002 - 601}{6}$

10/13/2015

www.doorsteptutor.com

10

Multiplication in Congruence's

10/13/2015

www.doorsteptutor.com

11

Application of Multiplication- Example-2/3

- Find the remainder of $\frac{124 \times 134 \times 23}{3}$
- There are 44 boxes of chocolates with 113 chocolates in each box. If you sell the chocolates by dozens, how many will be leftover?

10/13/2015

www.doorsteptutor.com

12

Exponentiation in Congruence's

10/13/2015

www.doorsteptutor.com

13

Application of Exponentiation Example – 4/5

• Find the last digit of 17^{16} .

• Find the remainder $\frac{6^{666}}{7}$

10/13/2015

www.doorsteptutor.com

14

Division of Congruence's: Never Divide, Think from Basics

• $10 \equiv 2 \pmod{8}$ – Divide by 2

• $24 \equiv 4 \pmod{5}$ (5 and 2 are coprime) - Divide by 2

Combining Congruence's

Example - 6

- 3 professors begin courses of lectures on Monday, Tuesday, Wednesday and announce their intentions of lecturing at intervals of 2, 3, 4 days respectively. If there are no lectures on Saturday, after how many days will all professors omit a lecture together?

10/13/2015

www.doorsteptutor.com

17

Concept of Multiplicative Inverse

- $ab \equiv 1 \pmod{N}$
 - b is multiplicative inverse of a mod N
 - a is multiplicative inverse of b mod N

10/13/2015

www.doorsteptutor.com

18

Summary

- $a + c \equiv (b + d) \pmod{N}$
 - *Remainder of Sum \equiv Sum of Remainders*
- $a - c \equiv (b - d) \pmod{N}$
 - *Remainder of Different \equiv Difference of Remainders*
- $ac \equiv (bd) \pmod{N}$
 - *Remainder of Product \equiv Product of Remainders*
- $\frac{a}{e} \equiv \frac{b}{e} \left(\pmod{\left(\frac{N}{\gcd(N,e)} \right)} \right)$
 - Don't do division without writing out basic equation
- $a^e \equiv b^e \pmod{N}$
 - *Remainder of Exponent \equiv Exponent of Remainders*

10/13/2015

www.doorsteptutor.com

19

Next - Faster Solutions to Exponent Problems

- Find the remainder $\frac{2^{1606}}{1607}$
- Euler and Fermat's Little Theorem
- Wilsons Theorem

10/13/2015

www.doorsteptutor.com

20