Modular Arithmetic Problems 1, M366

Problem 1 a) Find the quotient and remainder if we divide 108 by 3.

b) Find the quotient and remainder if we divide 129 by 7.

c) Find the remainder if we divide $13475657841492 + 4058760856705731$ by 5.

d) If today is Friday, what day of the week will it be in 779 days?

Problem 2 a) Calculate $(81 * 13) \mod 10$.

b) $(14 + 3 * 26) \mod 3$.

c) Find an x such that $(17 + x) \equiv 0 \pmod 4$.

d) If $x \equiv 5 \pmod 8$ and $y \equiv 6 \pmod 8$ then find $(x + y) \mod 8$ and $(xy) \mod 8$.

Problem 3 a) Calculate $3^{100} \mod 11$

b) Calculate $5^{12345} \mod 12$

Problem 4 Let $n \geq 0$ be an integer. Show that $(3^{2n+1} + 2^{n+2}) \equiv 0 \pmod 7$.

Problem 5 Let $\phi(n)$ denote the Euler Totient function applied to n.

a) Find $\phi(7)$

b) Find $\phi(49)$

c) Find $\phi(35)$

d) Find $\phi(100)$

a) Divide 108 by 3, find the quotient and remainder

$108 = 3m + r \quad m = 36 \quad r = 0$

b) 129 by 7

$129 = 7m + r \quad m = 18 \quad r = 3$

c) mod 5 is easy just look at the last digit

$\ldots 9\underline{2} + \ldots 3\underline{1} = \ldots \underline{3} \qquad 3 \bmod 5 = 3$

$1\underline{0} \to 0 \quad 1\underline{5} \to 0$
$1\underline{2} \to 2 \quad 1\underline{7} \to 2$
$1\underline{4} \to 4 \quad 1\underline{9} \to 4$

d) week = 7 days

$779 = 7m + r \quad m = 111 \quad r = 2$

friday + 2 = Sunday

day name	mod 7
friday	0
saturday	1
sunday	2
⋮	⋮

Problem 2

a) $81 \bmod 10 = 1$, $13 \bmod 10 = 3$ $\Big\} \; 3 \times 1 = 3$ OR $81 \times 13 = 1053$

$1053 \bmod 10 = 3$

$3 = 3$ ✓

b) $(14 + 3 * 26) \bmod 3 \stackrel{?}{=} 14 \bmod 3 + 3 \bmod 3 * 26 \bmod 3$

$= 2 + 0 * 2 = 2$

$92 \bmod 3 = 2$

c) $(17+x) \equiv 0 \bmod 4$

$1 + x \equiv 0 \bmod 4$

$17 + 3 = 20 \equiv 0$

$17 - 1 = 16 \equiv 0$

$x \equiv -1 \equiv 3 \bmod 4$ $\quad$ $\underline{x = 3 \bmod 4}$

OR $\longrightarrow$ We can deduce 17 (mod 4) to 1

d) $x+y \bmod 8 = 5+6 = 11 \bmod 8 \equiv 3$

$(xy) \bmod 8 \equiv 5 \cdot 6 = 30 \bmod 8 \equiv 6$

Problem 3

a) $3^{100} \bmod 11$

11 is prime

$3^{100} = (3^{10})^{10} \equiv 1 \bmod 11$

$$\boxed{\begin{array}{l}\text{Fermat's little theorem} \\ a^{p-1} = 1 \bmod p\end{array}}$$

b) $5^{12345} \bmod 12 =$ $\quad 5^1 \equiv 5 \bmod 12$ $\quad 5^2 \equiv 1 \bmod 12$

$5^{12345} \equiv 5^1 \equiv 5$

Problem 4

$3^{2n+1} + 2^{n+2} \equiv 0 \bmod 7$

(a) $3^{2n+1} \equiv 0 \bmod 7$?

(b) $2^{n+2} \equiv 0 \bmod 7$? $\quad$ or $\quad$ (a) + (b) $\equiv 0 \bmod 7$?

$3^k \bmod 7$ follows the cycle

k $3^1 \equiv 3 \bmod 7$

l $3^2 \equiv 2 \bmod 7$

m $3^3 \equiv 6 \bmod 7$

n $3^4 \equiv 4 \bmod 7$

o $3^5 \equiv 5 \bmod 7$

p $3^6 \equiv 1 \bmod 7$

$2^k \bmod 7$ follows the cycle

q $2^1 \equiv 2 \bmod 7$

r $2^2 \equiv 4 \bmod 7$

s $2^3 \equiv 1 \bmod 7$

$n=0$

$3^1 + 2^2 \pmod 7 \equiv 3+4 \pmod 7$

$3+4 = 7 \equiv 0$ ✓

$n=1$

$3^3 + 2^3 \pmod 7 \equiv 6+1 = 7$

$7 \bmod 7 \equiv 0$ ✓

$n=2$

$3^5 + 2^4 \pmod 7 \equiv 5+2 = 7$ ✓

There are 18 total combinations

(k, r): $2n+1 = 1$ $n+2 = 2$

(m, s): $2n+1 = 3$ $n+2 = 3$

(o, q): $2n+1 = 5$ $n+2 = 1$

repeats (mod 3)

Satisfies

$(2n+1 + n+2) \equiv 0 \bmod 3$

$2n+1+n+2 \longrightarrow 3n+3 \rightarrow 3(n+1) \equiv 0 \bmod 3$

$2n+1 \equiv 1 \bmod 2$, always odd & $3^{2n+1} \bmod 7 \not\equiv 2^{n+2} \bmod 7$

$\forall n \in \mathbb{Z}, n \geq 0 \quad (3^{n+1} + 2^{n+2}) \equiv 0 \bmod 7$

$3^{2n+1} \rightarrow (3^2)^n \cdot 3$ and $2^{n+2} \longrightarrow 2^n \cdot 2^2$

$2^n \cdot 3 + 2^n \cdot 4 \equiv 2^n(3+4) \equiv 0 \bmod 7$

Problem 5

$\Phi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right)$

a) $\Phi(7) = 7\left(1-\frac{1}{7}\right) = 7 \cdot \frac{6}{7} = 6$

b) $\Phi(49) = 49\left(1-\frac{1}{7}\right) = 49 \cdot \frac{6}{7} = 42$

c) $\Phi(35) = 35\left(1-\frac{1}{5}\right)\left(1-\frac{1}{7}\right) = 35 \cdot \frac{4}{5} \cdot \frac{6}{7} = 24$

5 7

d) $\Phi(100) = 100\left(1-\frac{1}{2}\right)\left(1-\frac{1}{5}\right) = 100 \cdot \frac{1}{2} \cdot \frac{4}{5} = 40$

10 10

2 5