

Q: There exists an integer  $x$ , such that  
 $3x \equiv 347 \pmod{453}$ .

Sol:

$ax \equiv b \pmod{m}$  has a solution  
iff  $(a, m) \mid b$

$$a = 3, b = 347, m = 453$$

$$(a, m) = 3$$

$$3 \nmid 347$$

$\therefore$  No such  $x$  exists.

Q: Find the remainder of  $7^{2012}$  upon division by 2011

Sol: 2011 is prime.

Fermat's Theorem,  $7^{2010} \bmod 2011 = 1$

$$7^{2012} = \underline{7^{2010}} * \underline{7^2} \bmod 2011 = 49$$

Q: Find last two decimal digits of  $413^{402}$ .

Hint: The last two decimal digits of a positive integer  $n$  are given by the least non-negative residue of  $n \bmod 100$ .

Sol:  $413 = 13 \pmod{100}$

$$13^{402} \pmod{100}$$

$$13^{\phi(100)} = 1 \pmod{100}$$

$$\begin{aligned} 13^{402} &= (13^{40})^{10} \times 13^2 \pmod{100} \\ &= 69 \end{aligned}$$

$$100 = 2^2 \times 5^2$$

$$\begin{aligned} \phi(100) &= 2^1(2-1) \times 5^1(5-1) \\ &= 40 \end{aligned}$$

$$402 = 40 \times 10 + 2$$

Q: Find all integer solutions  $(x, y)$  of the equation  $13x + 11y = 7$ .

Hint: first find solution for  $13x + 11y = 1$   
then generalize.

Sol: By Euclidean algorithm, we will get  $x = -5, y = 6$ .

Let  $(x_0, y_0) = (-5, 6)$  for  $13x + 11y = 1$ .

$(x_1, y_1) = 7(x_0, y_0) = (-35, 42)$  is solution for  $13x + 11y = 7$ .

$$(x, y) = (-35 + 11k, 42 - 13k), k \in \mathbb{Z}$$

Q: prove that, for all integers  $n \geq 2$ , the number  $n^{40} + 1$  is composite.  
and find a non-trivial divisors of this number.

Hint: try modulo  $n^8 + 1$  ,  $40 = 8 \times 5$

$$n^8 \equiv -1 \pmod{n^8 + 1}$$

$$(n^8)^5 \equiv (-1)^5 \pmod{n^8 + 1}$$

$$n^{40} \equiv -1 \pmod{n^8 + 1}$$

$$n^{40} + 1 \equiv 0 \pmod{\underline{n^8 + 1}}$$

Q: prove that, for any integer  $n$ , the number  $n^3 - n$  is divisible by 35.

fill ??

$$\begin{aligned} a^{p-1} &\equiv 1 \pmod{p}, \\ p &\nmid a \end{aligned}$$

$$35 = 7 \times 5$$

$$\begin{aligned} p=5, & \quad 5 \nmid n \quad \left. \begin{array}{l} 5 \nmid n \\ 5 \mid n \end{array} \right\} \end{aligned}$$

$$\begin{aligned} p=7, & \quad 7 \nmid n \quad \left. \begin{array}{l} 7 \nmid n \\ 7 \mid n \end{array} \right\} \end{aligned}$$