Problem 1

1. $14^{27} \bmod 5$

$14^4 \bmod 5 = 1$

$\therefore 14^{24} \bmod 5 = 1$

$\therefore 14^{27} \bmod 5 = 5$

2. $\sum_{i=1}^{100} i! \bmod 7$

$\sum_{i=1}^{100} i! = 1 + 2! + 3! + 4! + \cdots + 100!$

$= 1 + 2 + 3\times2 + 4\times3\times2 + \cdots + 100!$

$\because 7! \bmod 7,\ 8! \bmod 7,\ \cdots,\ 100! \bmod 7 = 0$

$\therefore \sum_{i=1}^{100} i! = (1 \bmod 7) + (2 \bmod 7) + (6 \bmod 7) + (24 \bmod 7) + (120 \bmod 7) + (720 \bmod 7) + 0$

$= 1 + 2 + 6 + 3 + 1 + 6$

$= 19$

3. $8x \bmod 13 = 1$

$13y = 8x + 1$

$13 = 8\times1 + 5$ $\quad 5 = 13 - 8\times1$ $\quad 5 = m - x$

$8 = 5\times1 + 3$ $\quad 3 = 8 - 5\times1$ $\quad 3 = x - 5\times1 = x - (m - x) = 2x - m$

$5 = 3\times1 + 2$ $\quad 2 = 5 - 3\times1$ $\quad 2 = m - x - 2x + m = 2m - 3x$

$3 = 2\times1 + 1$ $\quad 1 = 3 - 2\times1$ $\quad 1 = 2x - m - 2m + 3x = 5x - 3m$

$2 = 2\times1 + 0$

$\therefore 5$ is multiplicative inverse of 8 in $\mathbb{Z}_{13}$

4. $83x \bmod 191 = 1$

$191y = 83x + 1$

$191 = 83\times2 + 25$ $\quad 25 = 191 - 83\times2$ $\quad 25 = m - 2x$

$83 = 25\times3 + 8$ $\quad 8 = 83 - 25\times3$ $\quad 8 = x - 3m + 6x = 7x - 3m$

$25 = 8\times3 + 1$ $\quad 1 = 25 - 8\times3$ $\quad 1 = m - 2x - 21x + 9m$

$8 = 1\times8$ $\quad = 10m - 23x$

$-23 = 168 \bmod 191$

$\therefore 168$ is multiplicative inverse of 83 in $\mathbb{Z}_{191}$

5. $56x + 26y = \gcd(56, 26)$

$2 \mid 56$ $\quad 2 \mid 26$

$\gcd(56, 26) = 2$

6. Proof: $\because p \equiv 1 \bmod 5$

$\therefore p - 1$ divides 5

$\because p$ is a prime and $2 \not\equiv 1 \bmod 5$

$\therefore p$ is odd

$\therefore p \equiv 1 \bmod 2$ $\quad \therefore p - 1$ divides 2

$\because LCM(5, 2) = 10$

$\therefore p - 1$ divides 10

$\therefore p \equiv 1 \bmod 10$