Problem 1. Use Euler Theorem to find the remainder upon division of n by m, where

a) $n = 29^{202}$, $m = 13$;

b) $n = 99^{999999}$, $m = 23$

c) $n = 29^{198}$, $m = 20$

d) $n = 3^{1000000}$, $m = 14$

Solution: a) Note that $29 \equiv 3 \pmod{13}$. Thus $29^{202} \equiv 3^{202} \pmod{13}$. It suffices then to find remainder upon division of 3^{202} by 13.

By Euler's theorem (or its special case Fermat's Little Theorem) we have $3^{12} \equiv 1 \pmod{13}$. Now $202 = 12 \cdot 16 + 10$. Thus

$$3^{202} = 3^{12 \cdot 16 + 10} = (3^{12})^{16} \cdot 3^{10} \equiv 3^{10} \pmod{13}.$$

Now $3^{10} = 9^5$ and $9 \equiv -4 \pmod{13}$. Thus

$$3^{10} \equiv (-4)^5 = (-4) \cdot 16^2 \equiv (-4) \cdot 3^2 = (-4) \cdot 9 \equiv (-4)^2 = 16 \equiv 3 \pmod{13}.$$

Thus the remainder is 3.

Note: The solution can be simplified by observing that $3^3 \equiv 1 \pmod{13}$.

b) Note that $99 \equiv 7 \pmod{23}$, so $99^{999999} \equiv 7^{999999} \pmod{23}$. By Euler's theorem, $7^{22} \equiv 1 \pmod{23}$. Now we want to find r such that $999999 = 22 \cdot k + r$ and $0 \leq r < 22$. Note that both 999999 and 22 are divisible by 11 and therefore so is r. Thus $r = 0$ or $r = 11$. Since r must be odd, we have $r = 11$ (alternatively, you can find r by performing division algorithm). It follows that

$$7^{999999} \equiv 7^{11} = 7 \cdot 49^5 \equiv 7 \cdot 3^5 = 21 \cdot 81 \equiv (-2) \cdot 12 = -24 \equiv 22 \pmod{23}.$$

Thus the remainder is 22.

c) Note that $29 \equiv 9 = 3^2 \pmod{20}$, so $29^{198} \equiv 3^{396} \pmod{20}$. Now $\phi(20) = \phi(4 \cdot 5) = \phi(4)\phi(5) = 2 \cdot 4 = 8$, so $3^8 \equiv 1 \pmod{20}$. Now $396 = 8 \cdot 49 + 4$. Thus

$$3^{396} \equiv 3^4 = 81 \equiv 1 \pmod{20}.$$

Thus the remainder is 1.

d) Note that $\phi(14) = \phi(2 \cdot 7) = \phi(2)\phi(7) = 6$. Also, $1000000 = 6k + 4$ for some k. Thus

$$3^{1000000} \equiv 3^4 = 81 \equiv 11 \pmod{14} .$$

Thus the remainder is 11.

Problem 2. Prove that if n is relatively prime to 72 then $n^{12} \equiv 1 \pmod{72}$.

Solution: Note that $72 = 8 \cdot 9$. Since $\phi(8) = 4$, we have $n^4 \equiv 1 \pmod{8}$ for any n relatively prime to 8. It follows that $n^{12} \equiv 1 \pmod{8}$ for any n such that $\gcd(8, n) = 1$.

Similarly, $\phi(9) = 6$ so $n^6 \equiv 1 \pmod{9}$ for any n relatively prime to 9. It follows that if $\gcd(n, 9) = 1$ then $n^{12} \equiv 1 \pmod{9}$.

Suppose that $\gcd(n, 72) = 1$. Then both $\gcd(n, 8) = 1 = \gcd(n, 9)$. Thus $n^{12} \equiv 1 \pmod{8}$ and $n^{12} \equiv 1 \pmod{9}$. In other words, $8|n^{12} - 1$ and $9|n^{12} - 1$. Since 8 and 9 are relatively prime, we have $8 \cdot 9 = 72|n^{12} - 1$, i.e. $n^{12} \equiv 1 \pmod{72}$.

Remark. Note that what we proved is stronger than what Euler's theorem implies for 72. In fact, $\phi(72) = \phi(8)\phi(9) = 4 \cdot 6 = 24$, so we only get $n^{24} \equiv 1 \pmod{72}$ from Euler's theorem for 72.