(1) Use Fermat’s Little Theorem to verify that 17 divides $11^{104} + 1$.

Solution:
Working modulo 17, we have that
\[
11^{104} \equiv (11^2)^{52} \pmod{17} \\
\equiv 2^{52} \pmod{17} \\
\equiv (2^5)^{10} \cdot 2^2 \pmod{17} \\
\equiv (-2)^{10} \cdot 4 \pmod{17} \\
\equiv 4 \cdot 4 \pmod{17} \\
\equiv 16 \pmod{17}.
\]

(2) Show that for any integer $n \geq 0$, $13 \mid (11^{12n+6} + 1)$.

Solution:
Working modulo 13, we have that
\[
1 + 11^{12n+6} \equiv 1 + (11^2)^n \cdot 11^6 \pmod{13} \\
\equiv 1 + 1 \cdot (-2)^6 \pmod{13} \\
\equiv 0 \pmod{13}.
\]

(3) Let $a$ be any integer. Show that $a$ and $a^5$ have the same last digit.

Solution:
Since $a^5 \equiv a \pmod{5}$ and $a^5 \equiv a \pmod{2}$, it follows that $a^5 \equiv a \pmod{10}$. Hence $a$ and $a^5$ have the same last digit.

(4) Use Fermat’s Little Theorem to show that, if $p$ is an odd prime, then
(i) $1^{p-1} + 2^{p-1} + 3^{p-1} + \cdots + (p-1)^{p-1} \equiv -1 \pmod{p}$;
(ii) $1^p + 2^p + 3^p + \cdots + (p-1)^p \equiv 0 \pmod{p}$.

Solution:
First observe that, since $(a, p) = 1$ for all integers $1 \leq a \leq p - 1$, it follows from Fermat’s Little Theorem that $a^{p-1} \equiv 1$ for all such $a$. 

(i) Working modulo $p$, we have
\[
1^{p-1} + \cdots + (p-1)^{p-1} \equiv 1 + \cdots + 1 \pmod{p}
\equiv p - 1 \pmod{p}
\equiv -1 \pmod{p}.
\]

(ii) Again working modulo $p$ gives
\[
1^p + 2^p + \cdots + (p-1)^p \equiv 1 + 2 + \cdots + p - 1 \pmod{p}
\equiv \frac{(p-1)p}{2} \pmod{p}
\equiv 0 \pmod{p}.
\]

(5) Prove each of the following assertions:
(i) If $n$ is an odd integer, then $\phi(2^n) = \phi(n)$.
(ii) If $n$ is an even integer, then $\phi(2n) = 2\phi(n)$.
(iii) $\phi(3n) = 3\phi(n)$ if and only if $3 \mid n$.
(iv) $\phi(3n) = 2\phi(n)$ if and only if $3 \nmid n$.
(v) $\phi(n) = n/2$ if and only if $n = 2^k$ for some $k \geq 0$. [Hint: Write $n = 2^k N$, where $N$ is odd, and use the condition $\phi(n) = n/2$ to show that $N = 1$.]

Solution:
(i) If $n$ is odd, then
\[
\phi(2n) = \phi(2)\phi(n) = 1 \cdot \phi(n) = \phi(n).
\]

(ii) Suppose that $n$ is an even integer, with $n = 2^k m$, where $m$ is odd. Then
\[
\phi(2n) = \phi(2^{k+1} m)
= \phi(2^{k+1})\phi(m)
= 2^k \phi(m)
= 2(2^{k-1} \phi(m))
= 2\phi(2^k m)
= 2\phi(n).
\]

(iii) Suppose that $3 \nmid n$. Then $(3, n) = 1$, and we have that
\[
\phi(3n) = \phi(3)\phi(n) = 2\phi(n).
\]
Hence it follows that if $\phi(3n) = 3\phi(n)$, then $3 \mid n$. 
Suppose conversely that $3 \mid n$. Then we may write $n = 3^k m$, where $(3, m) = 1$. Therefore
\[
\phi(3n) = \phi(3^{k+1} m) \\
= \phi(3^{k+1})\phi(m) \\
= (3^{k+1} - 3^k)\phi(m) \\
= 3(3^k - 3^{k-1})\phi(m) \\
= 3\phi(3^k m) \\
= 3\phi(n),
\]

(iv) We have shown in (iv) above that, if $3 \mid n$, then $\phi(3n) = 3\phi(n)$. It therefore follows that if $\phi(3n) = 2\phi(n)$, then $3 \nmid n$.

Suppose conversely that $3 \nmid n$. Then $(3, n) = 1$, and so
\[
\phi(3n) = \phi(3)\phi(n) = 2\phi(n).
\]

(v) Suppose that $\phi(n) = n/2$, and write $n = 2^k N$, where $N$ is odd. Then
\[
n/2 = \phi(n) \\
= \phi(2^k N) \\
= \phi(2^k)\phi(N) \\
= 2^{k-1}\phi(N).
\]
This implies that $n = 2^k\phi(N)$. Hence $2^k N = 2^k\phi(N)$, and so we have that $\phi(N) = N$. It therefore follows that $\phi(N)$ is odd. Since $N$ is odd, this in turn implies that $N = 1$.

(Exercise: Show that if $n > 2$, then $\phi(n)$ is even!)

Suppose conversely that $n = 2^k$. Then
\[
\phi(n)\phi(2^k) = 2^k - 2^k = n/2.
\]

(6) Use Euler’s Theorem to establish the following:

(i) For any integer $a$, $a^{37} \equiv a \pmod{37}$. [Hint: $1729 = 7 \times 13 \times 19$.]

(ii) For any integer $a$, $a^{33} \equiv a \pmod{4080}$. [Hint: $4080 = 15 \times 26 \times 17$.]

**Solution:** (i) Suppose that $(a, 1729) = 1$, where $1729 = 7 \cdot 13 \cdot 19$. Then $(a, 19) = 1$, and so $a^{19} \equiv 1 \pmod{19}$, i.e. $a^{18} \equiv 1 \pmod{19}$. This in turn implies that $a^{36} \equiv 1 \pmod{19}$.

Also, $(a, 13) = 1$, and so $a^{12} \equiv 1 \pmod{13}$, or $a^{12} \equiv 1 \pmod{13}$. As a result, we see also that $a^{36} \equiv 1 \pmod{13}$.

Finally, $(a, 7) = 1$ implies that $a^{6} \equiv 1 \pmod{7}$, or $a^{36} \equiv 1 \pmod{7}$. Hence $a^{36} \equiv 1 \pmod{37}$.

It now follows that $a^{37} \equiv a \pmod{7}$, $a^{37} \equiv a \pmod{13}$, and $a^{37} \equiv a \pmod{19}$. Furthermore, each of these congruences is also valid if $7 \mid a$, $13 \mid a$, or $19 \mid a$. Hence we deduce that
\[
a^{37} \equiv a \pmod{7 \cdot 13 \cdot 19}
\]
for any $a$.

(ii) Suppose that $a$ is an odd integer with $(a, 4080) = 1$. We are given that $4080 = 15 \times 26 \times 17$.

From Euler’s theorem, and the observation that $\phi(15) = 8, \phi(16) = 8,$ and $\phi(17) = 16$, it follows that $a^8 \equiv 1 \pmod{15}, a^8 \equiv 1 \pmod{16},$ and $a^{16} \equiv 1 \pmod{16},$ and $a^{32} \equiv 1 \pmod{17}$.

It therefore follows that $a^{33} \equiv a \pmod{15}, a^{33} \equiv a \pmod{16},$ and $a^{33} \equiv a \pmod{17}$. Furthermore, each of these congruences is in fact valid for any odd $a$. Hence we deduce that

$$a^{33} \equiv a \pmod{15 \cdot 16 \cdot 17}$$

for any odd $a$.

(7) (a) Use Fermat’s Little Theorem to find the last digit of $3^{100}$.

(b) Let $a$ be any positive integer. Show that $a$ and $a^5$ have the same last digit.

**Solution:**

(a) We have that $3^4 \equiv 1 \pmod{5}$ and $3^4 \equiv 1 \pmod{2}$; hence $3^4 \equiv 1 \pmod{10}$. As a result, we have

$$3^{100} = (3^4)^{25} \equiv 1^{25} \equiv 1 \pmod{10},$$

and so the last digit of $3^{100}$ is equal to 1.

(b) Since $a^5 \equiv a \pmod{5}$ and $a^5 \equiv a \pmod{2}$, we have that $a^5 \equiv a \pmod{10}$; thus $a^5$ and $a$ have the same last digit.

(8) (a) Find the remainder when $15!$ is divided by 17.

(b) Find the remainder when $2(26!)$ is divided by 29.

**Solution:**

(a) We have $16! \equiv -1 \pmod{17}$ and so

$$15!\cdot 16 \equiv 15!(-1) \equiv -1 \pmod{17}.$$ 

Thus $15! \equiv 1 \pmod{17}$.

(b) We have $28! \equiv -1 \pmod{29}$, and so

$$26! \cdot 27 \cdot 28 \equiv 26!(-2)(-1) \equiv -1 \pmod{29}.$$ 

Thus

$$2(26!) \equiv -1 \equiv 28 \pmod{29}.$$ 

(9) Show that $18! \equiv -1 \pmod{437}$. [Hint: $437 = 19 \times 23$.]

**Solution:**

Observe that $18! \equiv -1 \pmod{19}$ and $22! \equiv -1 \pmod{23}$. Thus

$$22! \equiv 18!4! \equiv 18! \equiv -1 \pmod{23}.$$

It follows that $18! \equiv -1 \pmod{19 \cdot 23}$. 