5.2.3 From Fermat's theorem deduce that, for any integer $n \geq 0$, $13 \mid 11^{12n+6} + 1$.

Let $n \geq 0$. By Fermat's theorem,

$$11^{12} \equiv 1 \pmod{13}.$$

So

$$11^{12n+6} = (11^{12})^n \cdot 11^6 \equiv 1^n \cdot 11^6 \equiv (121)^3 \equiv 4^3 \equiv -1 \pmod{13}.$$

Therefore

$$11^{12n+6} + 1 \equiv -1 + 1 \equiv 0 \pmod{13}.$$

Thus

$$13 \mid 11^{12n+6} + 1.$$

5.2.4 (d) Derive $a^9 \equiv a \pmod{30}$ for all a.

Let $a \in \mathbb{Z}$. Then note that $30 = 5 \cdot 3 \cdot 2$. It is enough to show that $5 \mid a^9 - a$, $3 \mid a^9 - a$, and $2 \mid a^9 - a$. So by Fermat's theorem $a^5 \mid a \pmod{5}$ for any a. Then

$$a^9 - a = a^4 a^5 - a \equiv a^4 a - a \equiv a^5 - a \equiv a - a \equiv 0 \pmod{5}.$$

So $5 \mid a^9 - a$. We want to show $3 \mid a^9 - a$. So by Fermat's theorem $a^3 \equiv a \pmod{3}$ for any a. So

$$a^9 - a = a^3 a^3 a^3 \equiv a^3 - a \equiv a - a \equiv 0 \pmod{3}.$$

So $3 \mid a^9 - a$. We now want to show $2 \mid a^9 - a$. So by Fermat's theorem $a^2 \equiv a \pmod{2}$ for any a. Then

$$a^9 - a = (a^2)^4 a - a \equiv a^4 a - a \equiv a^2 - a \equiv a - a \equiv 0 \pmod{2}.$$

So $2 \mid a^9 - a$. Putting each case together gives that $a^9 \equiv a \pmod{30}$ for all a.

5.2.13 Assume that p and q are distinct odd primes such that $p-1 \mid q-1$. If $\gcd(a, pq) = 1$, show that $a^{q-1} \equiv 1 \pmod{pq}$.

Assume that p and q are distinct odd primes such that $p-1 \mid q-1$, i.e. $q-1 = n(p-1)$ for some $n \in \mathbb{Z}$. Let a be an integer with the property that $\gcd(a, pq) = 1$, i.e. $\gcd(a, p) = 1$ and $\gcd(a, q) = 1$. Then we want to show $a^{q-1} \equiv 1 \pmod{pq}$, i.e. $pq \mid a^{q-1} - 1$. It is enough to show

$$p \mid a^{q-1} - 1 \text{ and } q \mid a^{q-1} - 1.$$

By Fermat's theorem, since $\gcd(a, p) = 1$ and $\gcd(a, q) = 1$,

$$a^{q-1} \equiv 1 \pmod{q}.$$

and

$$a^{p-1} \equiv 1 \pmod{p}.$$

Then

$$a^{q-1} = a^{n(p-1)} = (a^{p-1})^n \equiv 1^n \equiv 1 \pmod{p}.$$

Therefore

$$a^{q-1} - 1 \equiv 1 - 1 \equiv 0 \pmod{p}.$$

So

$$p \mid a^{q-1} - 1 \text{ and } q \mid a^{q-1} - 1.$$

Thus $pq \mid a^{q-1} - 1$ implying $a^{q-1} \equiv 1 \pmod{pq}$.

5.2.20 Show that $561 \mid 3^{561} - 3$.

We want to show $3^{561} \equiv 3 \pmod{561}$. Note that $561 = 3 \cdot 11 \cdot 17$. It is enough to show $3 \mid 3^{561} - 3$, $7 \mid 3^{561} - 3$, and $11 \mid 3^{561} - 3$. Notice that $3 \mid 3^{561} - 3$ as 3 is common to both terms. For the next case, Fermat's theorem gives

$$3^{10} \equiv 1 \pmod{11}.$$

Then

$$3^{561} = 3^{560}3 \equiv 1 \cdot 3 \pmod{11}.$$

Therefore

$$3^{561} - 3 \equiv 3 - 3 \equiv 0 \pmod{11}.$$

So $11 \mid 3^{561} - 3$. Then by Fermat's theorem

$$3^{16} \equiv 1 \pmod{17}.$$

So

$$3^{561} = 3^{560}3 \equiv 1 \cdot 3 \pmod{17}.$$

Therefore

$$3^{561} - 3 \equiv 3 - 3 \equiv 0 \pmod{17}.$$

So $17 \mid 3^{561} - 3$. Putting each case together gives that $561 \mid 3^{561} - 3$.