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

By Wilson's theorem, $28! \equiv -1 \pmod{29}$. So

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

Then

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

So

$$2 \cdot 26! \equiv -1 \pmod{29}.$$

Therefore

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

Thus the remainder when $2(26!)$ is divided by 29 is 28.

5.3.4 Show that $18! \equiv -1 \pmod{437}$.

Note that $437 = 19 \cdot 23$. Wilson's theorem gives that $18! \equiv -1 \pmod{19}$. Then it is enough to show that $23 \mid 18! + 1$ or $18 \equiv -1 \pmod{23}$ **because** $\gcd(19, 23) = 1$. Wilson's theorem gives

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

Then

$$22 \cdot 21 \cdot 20 \cdot 19 \cdot 18! \equiv -1 \pmod{23}$$

or

$$(-1) \cdot (-2) \cdot (-3) \cdot (-4) \cdot 18! \equiv -1 \pmod{23}$$

So

$$24 \cdot 18! \equiv -1 \pmod{23}$$

Then

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

Thus

$$18! \equiv -1 \pmod{23}$$

as desired.

5.3.13 Supply any missing details in the following proof of the irrationality of $\sqrt{2}$: Suppose $\sqrt{2} = a/b$, with $\gcd(a, b) = 1$. Then $a^2 = 2b^2$, so that $a^2 + b^2 = 3b^2$. But $3 \mid (a^2 + b^2)$ implies that $3 \mid a$ and $3 \mid b$.

We know that $a^2 + b^2 = 3b^2$ implies that $3 \mid a^2 + b^2$, i.e., $a^2 + b^2 \equiv 0 \pmod 3$. Now we discuss the following two cases.

Case I: $3 \mid a$**.** Then $3 \mid a^2$. By $3 \mid a^2 + b^2$, $3 \mid b^2$ which implies $3 \mid b$ because 3 is a prime. So 3 is a common divisor of a and b, contradicting that $\gcd(a, b) = 1$.

Case II: $3 \nmid a$**.** So $3 \nmid a^2$. It also follows that $3 \nmid b^2$ because $3 \mid a^2 + b^2$. So $3 \nmid b$. Then by Fermat's theorem, $a^2 \equiv 1 \pmod 3$ and $b^2 \equiv 1 \pmod 3$. So $a^2 + b^2 \equiv 2 \pmod 3$, which contradicts that $a^2 + b^2 \equiv 0 \pmod 3$.

Above all, we conclude the proof.

5.3.17 If p and q are distinct primes, prove that for any $a \in \mathbb{Z}$,

$$pq \mid a^{pq} - a^p - a^q + a.$$

We need only show that $p \mid a^{pq} - a^p - a^q + a$ and $q \mid a^{pq} - a^p - a^q + a$ because $\gcd(p, q) = 1$. Corollary to Fermat's theorem gives $(a^p)^q \equiv a^p \pmod q$. So $q \mid (a^p)^q - a^p$. Corollary to Fermat's theorem also gives $a^q \equiv a \pmod q$. So $q \mid a^q - a$. Putting these together gives

$$q \mid (a^p)^q - a^p - (a^q - a) = a^{pq} - a^p - a^q + a.$$

Similarly Corollary to Fermat's theorem gives that

$$(a^q)^p \equiv a^q \pmod p \text{ and } a^p \equiv a \pmod p.$$

Therefore

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

So

$$p \mid (a^q)^p - a^q - (a^p - a) = a^{pq} - a^p - a^q + a.$$

Thus

$$pq \mid a^{pq} - a^p - a^q + a.$$