5.3.1b Find the remainder when $2(26!)$ is divided by 29.
By Wilson's Theorem,

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

Then, we have

$$\begin{aligned} (28)! &\equiv -1 \pmod{29} \\ 28 \cdot 27 \cdot (26!) &\equiv -1 \pmod{29} \\ -1 \cdot -2 \cdot (26!) &\equiv -1 \pmod{29} \\ 2(26!) &\equiv 28 \pmod{29} \end{aligned}$$

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

5.3.04 Show that $18! \equiv -1 \pmod{437}$.
Notice, $437 = 19 \cdot 23$ and $\gcd(19, 23) = 1$. Then, by Wilson's Theorem

$$18! \equiv -1 \pmod{19}$$

Also, by Wilson's Theorem

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

Then, we have

$$\begin{aligned} 22! &\equiv -1 \pmod{23} \\ 22 \cdot 21 \cdot 20 \cdot 20 \cdot 18 \cdot 18! &\equiv -1 \pmod{23} \\ 24 \cdot 18! &\equiv -1 \pmod{23} \\ 18! &\equiv -1 \pmod{23} \end{aligned}$$

Thus, from the two resultants, we have

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

$$18! \equiv -1 \pmod{437}$$

Thus, $18! \equiv -1 \pmod{437}$.

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 $3|(a^2 + b^2)$ implies that $3|a$ and $3|b$, a contradiction.

Suppose $\sqrt{2} = a/b$, with $\gcd(a, b) = 1$. Then $a^2 = 2b^2$, so that $a^2 + b^2 = 3b^2$.

$$3|(a^2 + b^2) \Rightarrow a^2 + b^2 \equiv 0 \pmod{3}$$

Using the results from 5.3.12, if for some $k \in \mathbb{Z}, p = 4k + 3$ is prime and $a^2 + b^2 \equiv \pmod{p}$, then $a \equiv b \equiv 0 \pmod{p}$
But $3 = 0 \cdot k + 3$
Thus, $a \equiv b \equiv 0 \pmod{3}$
Then, $3|a$ and $3|b$, contradicts $\gcd(a, b) = 1$
Therefore, $\sqrt{2}$ is irrational.

5.3.17 If p and q are distinct primes, prove that for any integer a,

$$pq|a^{pq} - a^p - a^q + a$$

By Fermat's corollary,
$a^p \equiv a \pmod{p}$. Then,
$(a^p)^q \equiv a^{pq} \equiv a^q \pmod{p}$
Thus,

$$a^{pq} \equiv 0 + a^q \equiv (a^p - a) + a^q \equiv a^p + a^q - a \pmod{\text{p}}$$

Similarly for q,

$$a^{pq} \equiv 0 + a^p \equiv (a^q - a) + a^p \equiv a^p + a^q - a \pmod{\text{q}}$$

Therefore,

$$p|a^{pq} - a^p - a^q + a$$
$$q|a^{pq} - a^p - a^q + a$$

Thus, $pq|a^{pq} - a^p - a^q + a$