5.2 | 3 For any integer $n \geq 0$, $13 \mid 11^{12n+6} + 1$:

Fermat $\Longrightarrow$ $11^{12} \equiv 1 \pmod{13} \Longrightarrow 11^{12n} \equiv 1 \pmod{13}$ $\forall\ n \geq 0$.

Note that $11 \equiv -2 \pmod{13} \Longrightarrow 11^6 \equiv (-2)^6 \equiv -1 \pmod{13}$.

Multiply these congruences to get $11^{12n+6} \equiv -1 \pmod{13}$.

∎

---

7 If $7 \nmid a$, then either a^3+1 or a^3-1 is divisible by 7 :

$7 \nmid a \Longrightarrow a^6 \equiv 1 \pmod{7}$ (Fermat)

$\Longrightarrow a^6 - 1 \equiv 0 \pmod{7}$,

$\Longrightarrow 7 \mid (a^3+1)(a^3-1) \Longrightarrow 7 \mid a^3+1$ or

$7 \mid a^3-1$.

∎

12 p an odd prime, $1 \le k \le p-1 \Rightarrow \binom{p-1}{k} \equiv (-1)^k \pmod p$:

Note that $p-1 \equiv -1$, $p-2 \equiv -2$, ..., $p-k \equiv -k \pmod p$,

so $(p-1)(p-2)\cdot\ldots\cdot(p-k) \equiv (-1)^k k! \pmod p$.

Dividing through by $k!$ yields $\binom{p-1}{k} \equiv (-1)^k \pmod p$. ∎

5.3 11a) Fermat $\Rightarrow 16! \equiv -1 \pmod{17}$

$\Rightarrow 16! \equiv 16 \pmod{17}$

$\Rightarrow 15! \equiv 1 \pmod{17}$ by cancellation.

11b) Fermat $\Rightarrow 28! \equiv -1 \equiv 28 \pmod{29} \Rightarrow 27! \equiv 1 \pmod{29}$.

If $26! \equiv r \pmod{29}$, then $27! \equiv 27r$ & $27r \equiv 1 \pmod{29}$.

The unique solution of this congruence is $r = 14$, so

$26! \equiv 14 \pmod{29} \Rightarrow 2(26!) \equiv 28 \pmod{29}$. ∎

5(a) $n > 1$ prime iff $(n-2)! \equiv 1 \pmod{n}$:

By Wilson's Thm., $(n-1)! \equiv -1 \pmod{n}$ iff n is prime

$$\iff (n-1)! \equiv (n-1) \pmod{n}$$

$$\iff (n-2)! \equiv 1 \pmod{n}.$$

∎

5(b) If n is composite and $n \neq 4$, $(n-1)! \equiv 0 \pmod{n}$:

There are 2 cases:

(1) $n = ab$ for divisors a, b with $1 < a < b < n$.

Then a and b appear in $(n-1)!$ and $n \mid (n-1)!$.

(2) n cannot be written as the product of distinct divisors.

In this case, $n = a^2$ for some prime a. Since $n > 4$, $a > 2 \implies a^2 > 2a \implies n > 2a$. Thus, a appears at least twice in the factorization of $(n-1)!$ and $n \mid (n-1)!$. ∎

7 p prime, a an integer $\Rightarrow p \mid a^p + (p-1)!\,a$, $p \mid (p-1)!\,a^p + a$:

Fermat $\Rightarrow$ $a^p \equiv a \pmod p$

Wilson $\Rightarrow$ $(p-1)! \equiv -1 \pmod p$

$\Rightarrow a^p \equiv a$, $(p-1)!\,a \equiv -a$ $\Rightarrow a^p + (p-1)!\,a \equiv 0 \pmod p$

Similarly, $a^p (p-1)! \equiv -a^p \equiv -a \Rightarrow a^p (p-1)! + a \equiv 0 \pmod p$.

---

9 For any odd prime p, $1^2 \cdot 3^2 \cdot 5^2 \cdot \ldots \cdot (p-2)^2 \equiv (-1)^{\frac{p+1}{2}} \pmod p$:

$(p-1)! = \underbrace{(p-1)}_{\equiv -1} \cdot (p-2) \cdot \underbrace{(p-3)}_{\equiv -3} \cdot \ldots \cdot 5 \cdot \underbrace{4}_{\equiv -(p-4)} \cdot 3 \cdot \underbrace{2}_{\equiv -(p-2)} \cdot 1$

(This is $2(\frac{p-1}{2}) - 1$)

Thus, $(p-1)! \equiv (p-2)^2 (p-4)^2 \cdot \ldots \cdot 5^2 \cdot 3^2 \cdot 1^2 \cdot (-1)^{\frac{p-1}{2}}$

and $(p-2)^2 \cdot (p-4)^2 \cdot \ldots \cdot 5^2 \cdot 3^2 \cdot 1^2 \cdot (-1)^{\frac{p-1}{2}} \equiv -1 \pmod p$ (Wilson)

$\Rightarrow 1^2 \cdot 3^2 \cdot 5^2 \cdot \ldots \cdot (p-4)^2 \cdot (p-2)^2 \equiv (-1)(-1)^{\frac{p-1}{2}} = (-1)^{\frac{p+1}{2}} \pmod p$.

∎