3.1/ #8 If $p \geq q \geq 5$ and p, q are primes, then $24 \mid p^2 - q^2$.

pf.: Since $24 = 2^3 \cdot 3$, we have to show that 2^3 and 3 divide $p^2 - q^2$.

First, note that $p = 4n \pm 1$ and $q = 4m \pm 1$ for $n, m \in \mathbb{Z}$ (in fact, for $n, m \in \mathbb{N}$!)

so that $p^2 - q^2 = (4n \pm 1)^2 - (4m \pm 1)^2 = (16n^2 \pm 8n + 1) - (16m^2 \pm 8m + 1)$

$= 8(2n^2 - 2m^2 \pm (n - m))$. Thus, $8 \mid p^2 - q^2$.

Next, note that $p = 3n \pm 1$ and $q = 3m \pm 1$ for (different!) integers n, m. Then $p^2 - q^2 = (3n \pm 1)^2 - (3m \pm 1)^2$

$= 9n^2 - 9m^2 \pm 6(n - m)$,

so $3 \mid p^2 - q^2$.

■

10 If $p \neq 5$ is an odd prime, then either p^2-1 or p^2+1 is divisible by 10.

pf.: Since p^2-1 and p^2+1 are obviously even, we just have to show that 5 divides one of them. Consider cases:

$p = 5m \pm 1$, some $m \in \mathbb{N}$ **OR** $p = 5m \pm 2$, some $m \in \mathbb{N}$

$\Rightarrow p^2 = 25m^2 \pm 10m + 1$

$\Rightarrow p^2 - 1 = 25m^2 \pm 10m$

$\Rightarrow 5 \mid p^2 - 1.$

$\Rightarrow p^2 = 25m^2 \pm 20m + 4$

$\Rightarrow p^2 + 1 = 25m^2 + 20m + 5$

$\Rightarrow 5 \mid p^2 + 1.$

(Note: All that really matters is that $5 \nmid p$; p need not be prime!)

3.2 #12 $p_n = n^{\text{th}}$ prime

(a) $p_n \geq 2n-1$ for $n \geq 5$:

Since $p_5 = 11$, the base case holds: $11 \geq 2(5)-1 = 9$. ✓

Induction hypothesis: suppose that $p_n \geq 2n-1$ for some $n \geq 5$.

Then $p_{n+1} \geq p_n + 2 \underbrace{\geq}_{\text{IH}} 2n-1+2 = 2(n+1)-1$,

s. the inequality holds for p_{n+1}. By induction, it therefore holds $\forall\, n \geq 5$.

∎

(b) None of the integers $P_n = p_1 p_2 \cdots p_n + 1$ is a perfect square.

<u>pf.</u>: Note that $P_n = 2p_2 p_3 \cdots p_n + 1$ and that every odd prime is either of the form $4m+1$ or $4m+3$. The product $p_2 \cdots p_n$ is therefore either of the form $4m+1$ or $4m+3$ (see the proofs on page 54, for example), so

$$P_n = 2(4m+1) + 1 = 8m + 3 = 4M + 3$$

<u>or</u> $$P_n = 2(4m+3) + 1 = 8m + 7 = 4N + 3 \text{ , some } M, N \in \mathbb{N}.$$

As we know from earlier problems, a number of the form $4m+3$ cannot be a perfect square.

∎

(c) The sum $\frac{1}{p_1} + \dots + \frac{1}{p_n}$ is never an integer.

pf.: Suppose, to the contrary, that

$$\frac{1}{p_1} + \frac{1}{p_2} + \dots + \frac{1}{p_n} = M \in \mathbb{N} .$$

Multiply both sides by $P := p_2 p_3 \cdot \dots \cdot p_n$:

$$\frac{P}{p_1} + \underbrace{\frac{P}{p_2} + \dots + \frac{P}{p_n}}_{\text{each of them } \in \mathbb{N}} = \underbrace{MP}_{\in \mathbb{N}}$$

This forces $\frac{P}{p_1} \in \mathbb{N}$, i.e., $p_1 \mid p_2 \cdot \dots \cdot p_n$, which cannot happen!

∎

4.2 **4(a)** $2^2 \equiv 4 \pmod 7$ and $2^3 \equiv 1 \pmod 7$

$$\Rightarrow (2^3)^{16} = 2^{48} \equiv 1 \pmod 7 \Rightarrow 2^2 \cdot 2^{48} = 2^{50} \equiv \underline{4} \pmod 7$$

$$41 \equiv -1 \pmod 7 \Rightarrow 41^{65} \equiv -1 \pmod 7 \Rightarrow 41^{65} \equiv \underline{6} \pmod 7.$$

4(b) Consider the sum $1^5 + 2^5 + \ldots + 99^5 + 100^5$.

All of the even terms are divisible by 4; eliminating them leaves the sum $1^5 + 3^5 + 5^5 + 7^5 + \ldots + 97^5 + 99^5$

$$\underbrace{\equiv 1 \quad \equiv -1}_{\equiv 0} \quad \underbrace{\equiv 1 \quad \equiv -1}_{\equiv 0} \quad \underbrace{\equiv 1 \quad \equiv -1}_{\equiv 0} \pmod 4$$

$\Rightarrow$ The original sum is divisible by 4!

5 Note that $53^2 \equiv 1 \pmod{39} \Rightarrow (53)^{102} \equiv 1 \pmod{39}$

$\Rightarrow (53)^{103} \equiv 14 \pmod{39}$

Similarly, $103^2 \equiv 1 \pmod{39} \Rightarrow (103)^{53} \equiv 1 \pmod{39}$

$\Rightarrow (103)^{53} \equiv 25 \pmod{39}$

$\equiv -14 \pmod{39}$

Thus, $(53)^{103} + (103)^{53} \equiv 0 \pmod{39}$.

$111 \equiv -1 \pmod{7} \Rightarrow 111^{333} \equiv -1 \pmod{7}$, and

$333 \equiv -3 \pmod{7} \Rightarrow (333)^3 \equiv 1 \pmod{7} \Rightarrow (333)^{111} \equiv 1 \pmod{7}$.

Thus, $111^{333} + 333^{111} \equiv 0 \pmod{7}$.

8(a) If a is an odd integer, then $a^2 \equiv 1 \pmod 8$.

pf.: a odd $\Rightarrow$ $a = 4m \pm 1$, some $m \in \mathbb{Z}$

$\Rightarrow$ $a^2 = 16m^2 \pm 8m + 1$ $\Rightarrow$ $a^2 - 1 = 16m^2 \pm 8m$

$\Rightarrow$ $8 \mid a^2 - 1$ $\Rightarrow$ $a^2 \equiv 1 \pmod 8$. ∎

8(b) For any integer a, $a^3 \equiv 0, 1,$ or $6 \pmod 7$.

$\longrightarrow$ This is problem #6, section 2.2. (HW #2)

8(c) For any integer a, $a^4 \equiv 0$ or $1 \pmod 5$.

$\longrightarrow$ problem 3(c), 2.2 (HW #2)

8(d) If a is not divisible by 2 or 3, then $a^2 \equiv 1 \pmod{24}$.

pf.: Must show that $2^3 \mid a^2 - 1$ and $3 \mid a^2 - 1$.

8(a) proves that $2^3 \mid a^2 - 1$.

Since $a = 3m \pm 1$. $a^2 = 9m^2 \pm 6m + 1$ and $a^2 - 1 = 9m^2 \pm 6m \Rightarrow 3 \mid a^2 - 1$. ∎

15 If a is an odd integer, then $a^{2^n} \equiv 1 \pmod{2^{n+2}}$, $n \geq 1$.

pf.: a odd $\Rightarrow a = 4m \pm 1$, some $m \in \mathbb{Z}$

$\Rightarrow a^2 = 16m^2 \pm 8m + 1 \Rightarrow a^2 - 1 = 16m^2 \pm 8m$

$\Rightarrow 8 \mid a^2 - 1 \Rightarrow a^2 \equiv 1 \pmod{8}$.

This establishes the base case.

IH: Suppose that $a^{2^n} \equiv 1 \pmod{2^{n+2}}$ for some $n \geq 1$.

This means that $2^{n+2} \mid a^{2^n} - 1$; since a^{2^n} must be odd, $2 \mid a^{2^n} + 1$. It follows that

$2 \cdot 2^{n+2} \mid (a^{2^n} + 1)(a^{2^n} - 1)$, i.e.,

$2^{n+3} \mid a^{2^{n+1}} - 1$. Thus, $a^{2^{n+1}} \equiv 1 \pmod{2^{n+3}}$.

∎

16 $2^{44} \equiv 1 \pmod{89}$: compute a bunch of stuff:

$2^4 \equiv 16 \pmod{89}$

$\Rightarrow 2^8 \equiv 256 \equiv -11 \pmod{89}$

$2^{12} \equiv -176 \equiv 2 \pmod{89}$

$\Rightarrow 2^{36} \equiv 8 \pmod{89}$

Then $2^8 \cdot 2^{36} \equiv -88 \equiv 1 \pmod{89}$. ✓

$2^{48} \equiv 1 \pmod{97}$: compute more stuff:

$2^7 \equiv 31 \pmod{97}$

$2^8 \equiv 62 \pmod{97}$

$2^9 \equiv 124 \equiv 27 \pmod{97}$

$2^{10} \equiv 54 \pmod{97}$

$2^{11} \equiv 108 \equiv 11 \pmod{97}$

$2^{12} \equiv 22 \pmod{97}$

$2^{24} \equiv 484 \equiv 96 \equiv -1 \pmod{97}$

$\Rightarrow 2^{48} \equiv 1 \pmod{97}$. ✓