Practice Problems from Section 3.6. Exercises 3.6.1–3.6.13 except for: 2, 10, 13.
These *Practice Problems* are a sampling of the type of problems which could be on the exam.
These *Practice Problem* are, in no way, meant as a comprehensive review for the exam.

Math is not a spectator sport.
Often we learn more from our failed attempts at a proof rather than
immediately looking at the hints or reading a clean proof.
So give these problems a solid attempt before seeking help, e.g.:
looking through your notes and/or book, looking at the below hints, or looking at Piazza.
Since these problems are not to hand in, on Piazza you may share:
hints and/or an attempt at a solution for others to comment on.

Some hints are very generous. Do not except such generous hints on the exam.

1. Prove that each point on or inside the circle whose equation is

$$(x-1)^2 + (y-2)^2 = 4$$

is also inside the circle whose equation is

$$x^2 + y^2 = 26\ .$$

hint. **Definition**. The point $(x_0, y_0) \in \mathbb{R}^2$ is:

- inside the circle whose equation is $(x-h)^2 + (y-k)^2 = r^2$ provided $(x_0-h)^2 + (y_0-k)^2 < r^2$
- on the circle whose equation is $(x-h)^2 + (y-k)^2 = r^2$ provided $(x_0-h)^2 + (y_0-k)^2 = r^2$
- outside the circle $(x-h)^2 + (y-k)^2 = r^2$ provided $(x_0-h)^2 + (y_0-k)^2 > r^2$.

hint. Symbolically looks: $\left(\forall (x,y) \in \mathbb{R}^2\right)\ [\ P(x,y) \implies Q(x,y)\ ]$ where $P(x,y)$ and $Q(x,y)$ are open senences in the variable x and y.

SW. $\left(\forall (x,y) \in \mathbb{R}^2\right)\ \left[\ (x-1)^2 + (y-2)^2 \le 4 \implies x^2 + y^2 < 26\ \right].$

Proof. Let $(x,y) \in \mathbb{R}^2$ satisfy

$$(x-1)^2 + (y-2)^2 \le 4. \tag{1.1}$$

We shall show that $x^2 + y^2 < 26$.

Since the square of a real number is nonnegative, the inequality (1.1) gives

$$0 \le (x-1)^2 \le 2^2 \qquad \text{and} \qquad 0 \le (y-2)^2 \le 2^2. \tag{1.2}$$

The following inequalities follow from (1.2) by algebra.

$$\begin{aligned} |x-1| &\le 2 &\quad \text{and} \quad & |y-2| \le 2 \\ -2 \le x-1 &\le 2 &\quad \text{and} \quad & -2 \le y-2 \le 2 \\ -1 \le x &\le 3 &\quad \text{and} \quad & 0 \le y \le 4 \\ 0 \le x^2 &\le 9 &\quad \text{and} \quad & 0 \le y^2 \le 16 \end{aligned} \tag{1.3}$$

Using (3) we now see that

$$x^2 + y^2 \le 9 + 16 = 25 < 26.$$

We have just shown that if $(x-1)^2 + (y-2)^2 \le 4$ then $x^2 + y^2 < 26$.

This completes the proof that each point on or inside the circle with equation $(x-1)^2 + (y-2)^2 = 4$ is also inside the circle whose equation is $x^2 + y^2 = 26$. □

3. Are the following statements true or false? Justify your answer.

3.1. For each integer a, if 3 does not divide a, then 3 divides $2a^2 + 1$.

3.2. For each integer a, if 3 divides $2a^2 + 1$, then 3 does not divide a.

3.3. For each integer a, we have 3 does not divide a if and only if 3 divides $2a^2 + 1$.

hint. Each one is true.

TL. 3.1: use cases with a and mod 3. 3.2: use contrapositive and modulo arithmetic. 3.3: follows from 3.1 and 3.2.

4. Prove that if $x \in \mathbb{R}$ and y is a irrational number then $x + y$ is irrational or $x - y$ is irrational.

hint. Since being irrational does not give us much of *a bird in the hand*, can we somehow work with the rational numbers, which give us *some birds in the hand*? When symbolically write, note we can get a conditional open sentence by using $\mathbb{R}^2$ as the universe. Think about all them nice closure properties of $\mathbb{Q}$ (to help avoid algebra). Proof is very similar to proof of book's Prop. 3.19 (§3.3, p123).

SW. Symbolically written:

$$\left(\forall\,(x,y)\in\mathbb{R}^2\right)\left[\, y\notin\mathbb{Q} \implies \{\ (x+y)\notin\mathbb{Q}\vee(x-y)\notin\mathbb{Q}\ \}\,\right]. \tag{4.1}$$

TL. Knowing a real number is irrational does not give us much of a *bird in the hand*. On the other hand, knowing a real number is rational give us some *bird in the hand* (e.g., nice closure properties, a numerator, and a denominator). As stated, all the real numbers in open sentence in (4.1) are irrational. So let's look at some negations of the open sentence in (4.1) in attempt to get some rational numbers ⟨as so to get some birds in the hand⟩. Below are some negations (4.1) ⟨some more useful than others⟩.

$$\sim\ \left[\ \left(\forall\,(x,y)\in\mathbb{R}^2\right)\left[\, y\notin\mathbb{Q} \implies \{\ (x+y)\notin\mathbb{Q}\vee(x-y)\notin\mathbb{Q}\ \}\,\right]\ \right]$$

$$\left(\exists\,(x,y)\in\mathbb{R}^2\right)\ \sim\ \left[\, y\notin\mathbb{Q} \implies \{\ (x+y)\notin\mathbb{Q}\vee(x-y)\notin\mathbb{Q}\ \}\,\right]$$

⟨Recall think of $P\Rightarrow Q$ as a *promise*. So the negation of $P\Rightarrow Q$ is to *break our promise*. Thus $\sim[P\Rightarrow Q]\equiv[P\wedge(\sim Q)]$.⟩

$$\left(\exists\,(x,y)\in\mathbb{R}^2\right)\ \left[\, y\notin\mathbb{Q}\ \wedge\ \sim\{\ (x+y)\notin\mathbb{Q}\vee(x-y)\notin\mathbb{Q}\ \}\,\right]$$

$$\left(\exists\,(x,y)\in\mathbb{R}^2\right)\ \left[\, y\notin\mathbb{Q}\ \wedge\ (x+y)\in\mathbb{Q}\ \wedge\ (x-y)\in\mathbb{Q}\,\right]$$

$$\left(\exists\,(x,y)\in\mathbb{R}^2\right)\ \left[\, (x+y)\in\mathbb{Q}\ \wedge\ (x-y)\in\mathbb{Q}\ \wedge\ y\notin\mathbb{Q}\,\right] \tag{4.2}$$

The statement in (4.2) gives us more to work with ⟨more of a bird in the hand⟩ than (4.1). So let's try a proof by contradiction and assume (4.2) holds ⟨i.e., the negation of what we want to show holds⟩ and go looking for a contradition. Our birds in the hand are: $x+y\in\mathbb{Q}$ and $x-y\in\mathbb{Q}$. Can we somehow use that $x+y\in\mathbb{Q}$ and $x-y\in\mathbb{Q}$ to find a contradition to $y\notin\mathbb{Q}$? The key observations are: $(x+y)-(x-y)=2y$ and $y=\frac{1}{2}(2y)$.

⚠. Compare Problem 4's ThinkingLand to book's Prop. 3.19's ThinkingLand (p123). Do you see the two TL's are basically the same?

Proof. We shall show Problem 4 by contradiction. Thus let $x,y\in\mathbb{R}$ satisfy that

$$x+y\in\mathbb{Q}\qquad\text{and}\qquad x-y\in\mathbb{Q}\qquad\text{and}\qquad y\notin\mathbb{Q}. \tag{4.3}$$

We shall find a contradiction ⟨to our above assumption in (4.3)⟩.

Since both $x+y$ and $x-y$ are rational, $\mathbb{Q}$ is closed under subtraction, and

$$(x+y)-(x-y)=2y$$

we have that $2y\in\mathbb{Q}$. Since $\frac{1}{2}$ is also rational, $\mathbb{Q}$ is closed under multiplication, and

$$y=\frac{1}{2}\,(2y)$$

we get that $y\in\mathbb{Q}$. However we assumed that $y\notin\mathbb{Q}$. So we have a contradiction.

This completes the proof by contradiction of Problem 4. □

---

5. Prove that there exist irrational numbers x and y such that x^y is a rational number.

hint. We know $\sqrt{2}$ is irrational (by Thm. 3.20, p124). Try cases. Consider the number $\left(\sqrt{2}\right)^{\sqrt{2}}$, which is either rational or irrational (who knows, but who cares since ...) Case 1: The $\left(\sqrt{2}\right)^{\sqrt{2}}$ is rational. Case 2: The $\left(\sqrt{2}\right)^{\sqrt{2}}$ is irrational.

TL. Case $\left(\sqrt{2}\right)^{\sqrt{2}}$ is rational, take $x=\sqrt{2}=y$. Case $\left(\sqrt{2}\right)^{\sqrt{2}}$ is irrational, take $x=\left(\sqrt{2}\right)^{\sqrt{2}}$ and $y=\sqrt{2}$.

---

6. Let a and b be natural numbers such that

$$a^2\ =\ b^3\,. \tag{6}$$

6.1. Prove that if a is even, then 4 divides a.

6.2. Prove that if 4 divides a, then 4 divides b.

6.3. Prove that if 4 divides b, then 8 divides a.

6.4. Prove that if a is even, then 8 divides a.

6.5. Give an example of natural numbers a and b such that a is even and $a^2=b^3$, but b is not divisible by 8.

hint. Helpful. If $n\in\mathbb{N}$ then $\left[\ n\text{ is even}\ \overset{\text{Thm 3.10}}{\Longleftrightarrow}\ n^2\text{ is even}\ \right]$ and $\left[\ n\text{ is even}\ \overset{\text{ER 3.2.1}}{\Longleftrightarrow}\ n^3\text{ is even}\ \right]$.

TL. Let $a,b\in\mathbb{N}$ satisfy

$$a^2\ =\ b^3. \tag{6.1}$$

From class (Thm 3.10 and ER 3.2.1).

Theorem S. An integer z is even if and only if z^2 is even.

Theorem C. An integer z is even if and only if z^3 is even.

6.1. Let a be even. Then

$$a\text{ even}\xrightarrow{\text{Thm. S}}a^2\text{ even}\xrightarrow{(6.1)}b^3\text{ even}\xrightarrow{\text{Thm. C}}b\text{ even}.$$

So $\exists j, k \in \mathbb{Z}$ s.t. $a = 2k$ and $b = 2j$. So

$$a^2 = b^3 \xRightarrow{\text{Alg}} 2^2k^2 = 2^3j^3 \xRightarrow{\text{Alg}} k^2 = 2j^3 \xRightarrow[\text{even}]{\text{def.}} k^2 \text{ even} \xRightarrow{\text{Thm. S}} k \text{ even} \xRightarrow[\text{even}]{\text{def.}} \exists n \in \mathbb{Z} \text{ s.t. } k = 2n.$$

Know $a = 2k$ so get

$$a \;=\; 2k \;=\; 2\,(2n) \;=\; 4n \xRightarrow[\text{divides}]{\text{def.}} 4 \mid a.$$

6.2. Let 4 divide a. Then

$$\begin{aligned}4 \mid a &\xRightarrow[\text{divides}]{\text{def.}} \exists n \in \mathbb{Z} \text{ s.t. } a = 4n \xRightarrow{(6.1)} b^3 = (4n)^2 = 2\left(8n^2\right) \xRightarrow[\text{even}]{\text{def.}} b^3 \text{ even} \xRightarrow{\text{Thm. C}} b \text{ even}\\ &\xRightarrow[\text{even}]{\text{def.}} \exists k \in \mathbb{Z} \text{ s.t. } b = 2k \xRightarrow{(6.1)} (2k)^3 = (4n)^2 \xRightarrow[4=2^2]{\text{Alg}} 2^3k^3 = 2^4n^2 \xRightarrow{\text{Alg}} k^3 = 2n^2\\ &\xRightarrow[\text{even}]{\text{def.}} k^3 \text{ even} \xRightarrow{\text{Thm. C}} k \text{ even} \xRightarrow[\text{even}]{\text{def.}} \exists j \in \mathbb{Z} \text{ s.t. } k = 2j \xRightarrow[\text{together}]{\text{put}} b = 2k = 2(2j) = 4j \xRightarrow[\text{divides}]{\text{def.}} 4 \mid b.\end{aligned}$$

6.3. Let 4 divide b. Then

$$\begin{aligned}4 \mid b &\xRightarrow[\text{divides}]{\text{def.}} \exists k \in \mathbb{Z} \text{ s.t. } b = 4k = 2(2k) \xRightarrow[\text{even}]{\text{def.}} b \text{ even} \xRightarrow{\text{Thm. C}} b^3 \text{ even} \xRightarrow{(6.1)} a^2 \text{ even}\\ &\xRightarrow{\text{Thm. S}} a \text{ even} \xRightarrow[\text{3a.}]{\text{part}} 4 \mid a \xRightarrow[\text{divides}]{\text{def.}} \exists j \in \mathbb{Z} \text{ s.t. } a = 4j.\end{aligned}$$

So now have $j, k \in \mathbb{Z}$ s.t. $a = 4j$ and $b = 4k$. So get

$$\begin{aligned}a^2 = b^3 &\implies (4j)^2 = (4k)^3 \xRightarrow{\text{Alg}} 4^2j^2 = 4^3k^3 \xRightarrow{\text{Alg}} j^2 = 4k^3 = 2(2k^3) \xRightarrow[\text{even}]{\text{def.}} j^2 \text{ even}\\ &\xRightarrow{\text{Thm. S}} j \text{ even} \xRightarrow[\text{even}]{\text{def.}} \exists n \in \mathbb{Z} \text{ s.t. } j = 2n \xRightarrow{\text{Alg}} a = 4j = 4(2n) = 8n \xRightarrow[\text{divides}]{\text{def.}} 8 \mid a.\end{aligned}$$

6.4. Follows from parts: 6.1, 6.2, 6.3.

6.5. Think prime fractorizations: $a = \prod_{i=1}^{n} (p_i)^{k_i}$ and $b = \prod_{i=1}^{m} (q_i)^{j_i}$. Since a is even we know $\boxed{p_1 = 2}$.

$$\prod_{i=1}^{n} (p_i)^{2k_i} \overset{\text{by}}{\underset{(6.1)}{=}} \prod_{i=1}^{m} (q_i)^{3j_i} \xRightarrow[\text{prime factoriz.}]{\text{uniqueness of}} n = m \text{ and } \forall i \in \{1, 2, \ldots, n\} : p_i = q_i \text{ and } 2k_i = 3j_i.$$

So try $n = m = 1$ and $p_1 = q_1 = 2$ and $\langle$for $2k_i = 3j_i\,\rangle$ $k_1 = 3$, and $j_1 = 2$. So take $a = (p_1)^{k_1} = 2^3$ and $b = (q_1)^{j_1} = 2^2$. So $a = 8$ and $b = 4$ will do it.

---

7. Prove Theorem 7.

Theorem 7. Let a and b be integers with $a \neq 0$. If a does not divide b, then the equation

$$ax^3 + bx + (b + a) \;=\; 0 \tag{7.1}$$

does not have a solution that is a natural number.

hint. Proof by contrapositive. So assume there exists $n \in \mathbb{N}$ that is a solution to equation in (7.1), i.e., $an^3 + bn + (b + a) = 0$. Note $ax^3 + bx + (b + a) = 0$ when $x = -1$ so $x - (-1) \overset{\text{i.e.}}{=} x + 1$ is a factor of $x^3 + bx + (b + a)$. Now use long division of polynomials to get $n^3 + 1 \;=\; (n + 1)\left(n^2 - n + 1\right)$.

SW. Symbolically, the original (7-O) is

$$\left(\forall\,(a, b) \in \mathbb{Z}^{\neq 0} \times \mathbb{Z}\right)\ \left[\ a \nmid b \implies \{\ (\forall n \in \mathbb{N})\ \left[\ an^3 + bn + (b + a) \neq 0\ \right]\ \}\ \right]. \tag{7-O}$$

Symbolically, using the contrapositive, (7-O) is (logically) equivalent to

$$\left(\forall\,(a, b) \in \mathbb{Z}^{\neq 0} \times \mathbb{Z}\right)\ \left[\ \{\ (\exists n \in \mathbb{N})\ \left[\ an^3 + bn + (b + a) = 0\ \right]\ \} \implies a|b\ \right]. \tag{7-CP}$$

TL. Proof by contrapositive. So assume there exists $n \in \mathbb{N}$ that is a solution to equation in (7.1). Thenwe have

$$\begin{gathered}an^3 + bn + (b + a) = 0\\ an^3 + a = -bn - b\\ a\,(n + 1)\left(n^2 - n + 1\right) - -b\,(n + 1)\\ a\left(n^2 - n + 1\right) = -b\\ a\left(-n^2 + n - 1\right) = b.\end{gathered}$$

The last equation imples $a \mid b$,

---

def. A **Pythagorean triple** is a 3-tuple (a, b, c) such that $a, b, c \in \mathbb{N}$ with $a < b < c$ and $a^2 + b^2 = c^2$.

8. Are the following propositions true or false? Justify your conclusions.

8.1. If (a, b, c) form a Pythagorean triple, then 3 divides a or 3 divides b.

8.2. If (a,b,c) form a Pythagorean triple, then 5 divides a or 5 divides b or 5 divides c.

hint. Both are true. Helpful Facts. Lemma 8.1: if $a \in \mathbb{Z}$, then $[a \not\equiv 0 \pmod 3] \Leftrightarrow [a^2 \equiv 1 \pmod 3]$. Pf: $\boxed{\Rightarrow}$ is proof by cases. $\boxed{\Leftarrow}$ is proof by contrapositive. Look over your class notes. Lemma 8.2. If $c \in \mathbb{Z}$, then $c^2 \equiv 0 \pmod 3$ or $c^2 \equiv 1 \pmod 3$. Pf: use Lemma 8.1. Proposition 3.33. If $a \in \mathbb{Z}$ and $a \not\equiv 0 \pmod 5$, then $a^2 \equiv 1 \pmod 5$ or $a^2 \equiv 4 \pmod 5$. Pf: by cases, book §3.5 (p151).

SW. $\left(\forall (a,b,c) \in \mathbb{N}^3\right)$ [(a,b,c) is a Pyth. triple $\implies (3|a \vee 3|b)$] .
$\left(\forall (a,b,c) \in \mathbb{N}^3\right)$ [(a,b,c) is a Pyth. triple $\implies (5|a \vee 5|b \vee 5|c)$] .

TL. We will use the following facts from class and book.
Lemma 8.1. If $a \in \mathbb{Z}$, then $[a \not\equiv 0 \pmod 3] \Leftrightarrow [a^2 \equiv 1 \pmod 3]$.
Lemma 8.2. If $c \in \mathbb{Z}$, then $c^2 \equiv 0 \pmod 3$ or $c^2 \equiv 1 \pmod 3$.
Proposition 3.33. If $a \in \mathbb{Z}$ and $a \not\equiv 0 \pmod 5$, then $a^2 \equiv 1 \pmod 5$ or $a^2 \equiv 4 \pmod 5$.

8.1. Proof by contradication. Let (a,b,c) be a Pythagorean triple. By way of contradiction, assume $3 \nmid a$ and $3 \nmid b$.
Then $a \not\equiv 0 \pmod 3$ and $b \not\equiv 0 \pmod 3$.
Thus Lemma 8.1 gives $a^2 \equiv 1 \pmod 3$ and $b^2 \equiv 1 \pmod 3$.
Since $c^2 = a^2 + b^2$, mod. arithmetic gives $c^2 \equiv 2 \pmod 3$.
Since there is a unique number $r \in \{0,1,2\}$ such that $c^2 \equiv r \pmod 3$
we get $c^2 \not\equiv 0 \pmod 3$ and $c^2 \not\equiv 1 \pmod 3$. This contradicts Lemma 8.2.

8.2. Proof by contradication. Let (a,b,c) be a Pythagorean triple. BWOC, assume $5 \nmid a$ and $5 \nmid b$ and $5 \nmid c$.
Then $a \not\equiv 0 \pmod 5$ and $b \not\equiv 0 \pmod 5$ and $c \not\equiv 0 \pmod 5$. Thus Prop. 3.33 gives

(A) $a^2 \equiv 1 \pmod 5$ or $a^2 \equiv 4 \pmod 5$
(B) $b^2 \equiv 1 \pmod 5$ or $b^2 \equiv 4 \pmod 5$
(C) $c^2 \equiv 1 \pmod 5$ or $c^2 \equiv 4 \pmod 5$.

Since $c^2 = a^2 + b^2$, by mod arithmetic, now use (A) and (B) to argue that c^2 can be congruent to 0, 2, or 3 (mod 5). This contradicts (C), using the fact that there exists a unique $r \in \{0,1,2,3,4\}$ such that $c^2 \equiv r \pmod 5$.

9. More on Pythagorean triples.

9.1. Prove that there exists a Pythagorean triple (a,b,c) where $a = 5$ and b and c are consecutive natural numbers.

9.2. Prove that there exists a Pythagorean triple (a,b,c) where $a = 7$ and b and c are consecutive natural numbers.

9.3. Prove that there exists a Pythagorean triple (a,b,c) where a is odd and b and c are consecutive natural numbers.

TL. **Def.** If $b, c \in \mathbb{R}$ with $b < c$, then b and c are said to be **consecutive** if $c = b + 1$.
Lemma 9a. Let $a,b,c \in \mathbb{R}$. Then $a^2 + b^2 = (b+1)^2$ if and only if $b = \frac{a^2-1}{2}$.

Why? $a^2 + b^2 = (b+1)^2 \overset{\text{algebra}}{\Longleftrightarrow} a^2 = 2b + 1 \overset{\text{algebra}}{\Longleftrightarrow} b = \dfrac{a^2-1}{2}$.

Lemma 9b. If $a, b \in \mathbb{N}$ and $b = \frac{a^2-1}{2}$, then $a < b$ if and only if $2 < a$.

Why? $a < \frac{a^2-1}{2} \overset{\text{algebra}}{\Longleftrightarrow} 0 < a^2 - 2a - 1$. The zeros of the concave up parabola $f(x) = x^2 - 2x - 1$ are $1 \pm \sqrt{2}$.

9.1. Use Lemma 9a with $a = 5$. So $b = \frac{25-1}{2} = 12$ and so $c = 13$.

9.2. Use Lemma 9a with $a = 7$. So $b = \frac{49-1}{2} = 24$ and so $c = 25$.

9.3. Yes, lots of them. By Lemma 9a and Lemma 9b, any triple of the form $\left(a, \frac{a^2-1}{2}, \frac{a^2+1}{2}\right)$ where a is odd and $a > 2$ would do.

11. Definition. Two prime numbers that differ by 2 are called **twin primes**.

Conjecture 11. If p and q are twin primes other than 3 and 5, then $pq + 1$ is a perfect square and 36 divides $pq + 1$.
Is Conjecture 11 true or false? Justify your answer.

hint. Let p and q be twin primes. Without loss of generality, $p < q$. So $q = p + 2$. Now express $pq + 1$ in terms of only p (i.e., get rid of q). Note 36 divides a perfect square k^2 if and only if 6 divides k. Cases with p and mod 6.

TL. Let p and q be twin primes other than 3 and 5. Without loss of generality $p < q$ (given what we need to show it does not matter which of the 2 primes we think of as the smaller prime of the two). So $q = p + 2$ since p and q are twin prime. Since p and q are twin primes but not the twin primes 3 and 5, we also have $p > 3$. Since, by algebra,

$$pq + 1 = p(p+2) + 1 = p^2 + 2p + 1 = (p+1)^2 \tag{11.1}$$

we get $pq + 1$ is a perfect square. Next we want to show $36 | (pq+1)$. Note

$$36 | (pq+1) \Leftrightarrow 36 | (p+1)^2 \Leftrightarrow 6 | (p+1)\,. \tag{11.2}$$

Let's do cases with p mod 6. There exists a unique $r \in \{0,1,2,3,4,5\}$ such that $p \equiv r \pmod 6$, which leads to 6 cases.
Cases 1–3. $p \equiv 0 \pmod 6$ or $p \equiv 2 \pmod 6$ or $p \equiv 4 \pmod 6$. Cases 1 –3 cannot occur since p is prime and $p > 3$ and so p is odd. Being odd, p cannot be congruent, mod 6, to an even number.

Case 4. $p \equiv 3 \pmod 6$. If r is a prime and $r \equiv 3 \pmod 6$ then $r = 6k+3 \overset{\text{i.e.}}{=} 3(2k+1)$ for some $k \in \mathbb{Z}$ and so $3|r$ and so the prime $r = 3$. Taking r to be our given prime p gives that $p = 3$ but we know $p > 3$. So Case 2 cannot occur.
Case 5. $p \equiv 1 \pmod 6$. If $p \equiv 1 \pmod 6$ then by mod arithmetic $p+2 \equiv 3 \pmod 6$. By the observation in Case 2, taking r to be our given prime $p+2$ gives that $p+2 = 3$. But $p+2 > 5$. So Case 3 cannot occur.
Case 6. $p \equiv 5 \pmod 6$. By def. of congrence, there exists $k \in \mathbb{Z}$ such that $p = 6k+5$. Thus

$$pq+1 = (p+1)^2 = ((6k+5)+1)^2 = (6k+6)^2 = 36\,(k+1)^2\,. \tag{11.3}$$

Note $k+1 \in \mathbb{Z}$ by closure properties of $\mathbb{Z}$ since $k \in \mathbb{Z}$. Thus $36\,(())\,pq+1$ by def. of divides.

Since we have exhausted all possible cases, this finishes the proof.

12. Are the following statements true or false? Justify your conclusions.

12.1. If a and b are integers, then $(a+b)^2 \equiv (a^2+b^2) \pmod 2$.

12.2. If a and b are integers, then $(a+b)^3 \equiv (a^3+b^3) \pmod 3$.

12.3. If a and b are integers, then $(a+b)^4 \equiv (a^4+b^4) \pmod 4$.

12.4. If a and b are integers, then $(a+b)^5 \equiv (a^5+b^5) \pmod 5$.

hint. Parts 12.1, 12.2, 12.4 are true. Part 12.3 is false. Algebra gives: $(a+b)^2 - (a^2+b^2) = (a^2+2ab+b^2) - (a^2+b^2) = 2ab$. For the higher powers, if needed, review (the linked) Pascal's Triangle.

Recall. Let $n \in \mathbb{N}$ and $a, b \in \mathbb{Z}$. The following are equivalent (TFAE).

(1) a is congruent to b modulo n
(2) $a \equiv b \pmod n$
(3) n divides $a-b$, i.e., $n|(a-b)$
(4) $(\exists k \in \mathbb{Z})\,[a-b = nk]$
(5) $(\exists k \in \mathbb{Z})\,[a = nk+b]$

$\xLeftrightarrow[\text{take } j=-k]{\text{to see } (4)\Leftrightarrow(4')}$

(1′) b is congruent to a modulo n
(2′) $b \equiv a$ (mod n)
(3′) n divides $b-a$, i.e., $n|(b-a)$
(4′) $(\exists j \in \mathbb{Z})\,[b-a = nj]$
(5′) $(\exists j \in \mathbb{Z})\,[b = nj+a]$

Note $(1) \xLeftrightarrow{\text{notation}} (2) \xLeftrightarrow[\text{congruence}]{\text{def. of}} (3) \xLeftrightarrow[\text{divides}]{\text{def. of}} (4) \xLeftrightarrow{\text{algebra}} (5)$. Similiarly, $(1') \Leftrightarrow (2') \Leftrightarrow (3') \Leftrightarrow (4') \Leftrightarrow (5')$.

▷. As def. of $a \equiv b \pmod n$ we can use (unless otherwise indicated) any of the above equivalent formations: (3), (4), (5), (3′), (4′), (5′).

▷. If needed, review (the linked) Pascal's Triangle.

12.1. Algebra gives $(a+b)^2 - (a^2+b^2) = (a^2+2ab+b^2) - (a^2+b^2) = 2ab$. Thus 2 divides $(a+b)^2 - (a^2+b^2)$ by def. of divides since $a, b \in \mathbb{Z}$. So by def. of congruent mod 2 (see (3) above) we get $(a+b)^2 \equiv (a^2+b^2) \pmod 2$.

12.2. Similar to 12.1. For help with algebra, use Pascal's triangle.

12.3. Algebra (with help from Pascal's triangle) gives

$$\begin{aligned}(a+b)^4 - (a^4+b^4) &= (a^4+4a^3b+6a^2b^2+4ab^3+b^4) - (a^4+b^4) = 4a^3b+6a^2b^2+4ab^3 \\ &= 2\left[ab\left(2a^2+3ab+2b^2\right)\right].\end{aligned}$$

Opps, algebra was not so friendly in this problem. Maybe it is not true. In order for $(a+b)^4 \equiv (a^4+b^4) \pmod 4$, the above computaations shows we would need $\left[ab\left(2a^2+3ab+2b^2\right)\right]$ to be even. But Lemma POO and friends give us that if a and b are both odd, then $\left[ab\left(2a^2+3ab+2b^2\right)\right]$ will be odd. So, for a counterexample, take your two favorite odd numbers. To make life easy, how about $a = 1 = b$. Then

$$(a+b)^4 \equiv (1+1)^4 \equiv 16 \equiv 4\,(4) + 0 \equiv 0 \pmod 4$$

but

$$a^4 + b^4 \equiv 1^4 + 1^4 \equiv 2 \pmod 4.$$

12.4. Similar to 12.1. For help with algebra, use Pascal's triangle.