1. (a) [3 marks] Prove that no integer in the sequence $11, 111, 1111, \ldots$ is a perfect square.

Solution. We first show that all numbers in the sequence are of the form $4k+3$ for $k \in \mathbb{Z}$: clearly $11 = 4 \cdot 2 + 3$, and every successive number is 10^n more than the previous (for $n \geqslant 2$) in the sequence. Since $10^n \equiv 0 \pmod 4$ for $n \geqslant 2$, this establishes the claim that all numbers in the sequence are of the form $4k+3$. Now note that if a number is a perfect square, then it cannot be written in the form $4k+3$ for $k \in \mathbb{Z}$: indeed, we have

$$\begin{aligned} (4m)^2 &\equiv 0 \pmod 4 \\ (4m+1)^2 &\equiv 1 \pmod 4 \\ (4m+2)^2 &\equiv 0 \pmod 4 \\ (4m+3)^2 &\equiv 1 \pmod 4. \end{aligned}$$

[S] Three marks, distributed as follows:

- 2 marks for showing that all numbers in the sequence are congruent to $3 \pmod 4$
- 1 mark for showing that all squares are congruent to 0 or $1 \pmod 4$.

(b) [5 marks] State and prove Fermat's Little Theorem.

Solution. Statement: Let p be a prime and let $x \in \mathbb{Z}$ such that $p \nmid x$. Then $x^{p-1} \equiv 1 \mod p$.
Proof: Let G be the group $(\mathbb{Z}/p\mathbb{Z})^\times$, so that $\#G = p-1$. Apply Lagrange's Theorem from group theory, which implies that if G is a finite group and $g \in G$ then $g^{\#G} = i_G$. In our case we take $g = x + p\mathbb{Z}$, which gives

$$(x+p\mathbb{Z})^{p-1} = 1 + p\mathbb{Z} \implies x^{p-1} + p\mathbb{Z} = 1 + p\mathbb{Z} \implies x^{p-1} \equiv 1 \mod p.$$

[B] This is standard material from the lecture notes:

- 1 mark for the statement of Fermat's Little Theorem
- 4 marks for the proof

(c) [5 marks] Let n be an odd positive integer. Prove that $n | (2^{n!} - 1)$.

Solution. We first show that for positive integers n, that $\phi(n) | n!$. Indeed, it is true for $n = 1$; if $n > 1$ and if $n = p_1^{a_1} \cdots p_k^{a_k}$ is the prime factorization of n, where $p_1 < \cdots < p_k$, then

$$\phi(n) = p_1^{a_1 - 1} \cdots p_k^{a_k - 1}(p_1 - 1) \cdots (p_k - 1),$$

and we have $(p_1^{a_1-1} \cdots p_k^{a_k-1}) | n$, while $p_1 - 1 < p_k \leqslant n$, which implies that $p_k - 1 < n$ and $p_1 - 1 < \cdots < p_k - 1$ are different positive integers smaller than n. Thus

$$((p_1 - 1) \cdots (p_k - 1)) | (n-1)!,$$

and it follows that $\phi(n) | ((n-1)!n) = n!$.
If n is odd, then by Euler's Theorem, $n | (2^{\phi(n)} - 1) | (2^{n!} - 1)$, hence $n | (2^{n!} - 1)$, as desired.

[N] 5 marks distributed as follows:

- 3 marks for showing that $\phi(n) \mid n!$
- 2 marks for finishing the proof

(d) [5 marks] Find all solutions to the equation $x^2 - 1 \equiv 0 \pmod{35}$.

Solution. Solving $x^2 - 1 \equiv 0 \pmod{35}$ means we must find $n, x \in \mathbb{Z}$ such that $x^2 - 1 = 35n$. One way to do this is to consider the equation mod 5 and 7:

$$\begin{aligned} x^2 - 1 &\equiv 0 \pmod{5} \Rightarrow x \equiv \pm 1 \pmod{5} \\ x^2 - 1 &\equiv 0 \pmod{7} \Rightarrow x \equiv \pm 1 \pmod{7}. \end{aligned}$$

Then carrying out the Chinese Remainder Theorem on the four possible combinations of signs gives the results. Alternatively, one can say that the first condition gives as our candidates

$$x \equiv 1, 4, 6, 9, 11, 14, 16, 19, 21, 24, 26, 29, 31, 34 \pmod{35},$$

while the second condition gives

$$x \equiv 1, 6, 8, 13, 15, 20, 22, 27, 29, 34 \pmod{35},$$

so putting things together, we find

$$x \equiv 1, 6, 29, 34 \pmod{35}.$$

[S] 5 marks distributed as follows:

- 1 mark for a solving strategy
- 4 marks for the solutions themselves: 1 mark for each solution

(e) [7 marks] Prove that for any $n \in \mathbb{Z}$, the integer $n^2 + n + 1$ does not have any divisors of the form $6k - 1$, for $k \in \mathbb{Z}$.

Solution. We first reduce to the case that $n^2 + n + 1$ has no *prime* divisors of the form $6k-1$, by using the observation that if p, q are primes not of the form $6k-1$, then neither is their product: $(6k+1)(6j+1) \equiv 1 \pmod{6}$.
Then note that if $p = 6k-1$ divides n^2+n+1, it divides $4(n^2+n+1) = (2n+1)^2+3$, so -3 must be a quadratic residue modulo p. We compute the corresponding Legendre symbol, using some properties of the symbol developed in the course and quadratic reciprocity:

$$\begin{aligned} \left(\frac{-3}{p}\right) &= \left(\frac{-1}{p}\right)\left(\frac{3}{p}\right) \\ &= (-1)^{\frac{p-1}{2}}\left(\frac{3}{p}\right) \\ &= (-1)^{\frac{p-1}{2}}(-1)^{\frac{p-1}{2}\cdot\frac{3-1}{2}}\left(\frac{p}{3}\right) \\ &= \left(\frac{p}{3}\right) \\ &= \left(\frac{6k-1}{3}\right) \\ &= \left(\frac{-1}{3}\right) \\ &= -1. \end{aligned}$$

So -3 is not a quadratic residue mod p, and we have reached a contradiction.

Alternate solution (provided by R. Knight). If p is a prime such that $p \equiv -1 \pmod 6$, then $|(\mathbb{Z}/p\mathbb{Z})^\times| \equiv 4 \pmod 6$, so $(\mathbb{Z}/p\mathbb{Z})^\times$ contains no cube roots of 1 other than 1 itself. Hence $n^2 + n + 1 \not\equiv 0 \pmod p$.

[N] 7 marks distributed as follows:

- 2 marks for reducing to the case of prime divisors
- 5 marks for a complete worked strategy showing that primes of the form $6k - 1$ don't divide $n^2 + n + 1$, such as showing -3 is a quadratic nonresidue modulo p