1. Find an integer $n \in \mathbb{Z}$ such that $|n^3 - 5|_2 < 2^{-3}$. Show that there is no integer n for which $|n^3 - 5|_5 < 5^{-3}$.

Let K be a field, complete with respect to a non-Archimedean valuation $|\ |$, with valuation ring $R = \{x \in K : |x| \leq 1\}$. Prove that if $f(x) \in R[x]$ and $a_0 \in R$ satisfies the inequality $|f(a_0)| < |f'(a_0)|^2$, then one can produce an infinite sequence $(a_n)_0^\infty$ in R, starting at a_0, such that

(i) $|a_{i+1} - a_i| \leq |f(a_i)|/|f'(a_i)|$ for $i \geq 0$;

(ii) $|f'(a_0)| = |f'(a_1)| = |f'(a_2)| = \dots$; and

(iii) $|f(a_0)| > |f(a_1)| > \dots$

Deduce that there exists an element $a \in R$ such that $|a - a_0| \leq |f(a_0)|/|f'(a_0)|$ and $f(a) = 0$.

Show that the above conclusion remains true if $|f(a_0)| = |f'(a_0)|^2$, providing that one has $0 < |f'(a_0)| < 1$ and $|\frac{1}{2}f''(b)| < 1$ for all $b \in R$.

For which values $n \in \mathbb{Z}$ does the equation $x^3 + 3x + y^3 + 3y = n$ have solutions $x, y \in \mathbb{Z}_3$?

2. Let $\mathcal{E} : y^2 = x^3 + Ax + B$, be an elliptic curve, where $A, B \in \mathbb{Z}_p$. Show that any $(x, y) \in \mathcal{E}_{\text{tors}}(\mathbb{Q}_p)$ satisfies $|x|_p \leqslant 1, |y|_p \leqslant 1$.

[You may assume that if $F(X,Y)$ is a formal group defined over $\mathbb{Z}_p$, and that if $z \in p\mathbb{Z}_p$ is a non-trivial torsion point for the group operation $x \oplus y = F(x, y)$ on $p\mathbb{Z}_p$, then it has order p^n, and $|z|_p \geq p^{-1/(p^n - p^{n-1})}$.]

Let $\widetilde{\mathcal{E}}$ denote the reduction of $\mathcal{E}$ modulo p. If $\widetilde{\mathcal{E}}$ is non-singular, show that $\mathcal{E}_{\text{tors}}(\mathbb{Q}_p)$ is isomorphic to a subgroup of $\widetilde{\mathcal{E}}(\mathbb{F}_p)$.

Let $y^2 = x^3 + ax + b$ be an elliptic curve defined over $\mathbb{Z}$. Show that if $(x_1, y_1) \in \mathbb{Q}^2$ is a non-trivial torsion point, then $x_1, y_1 \in \mathbb{Z}$, and either $y_1 = 0$ or $y_1^2 | 4a^3 + 27b^2$.

[You may use without proof the polynomial identity

$$\phi_1(X)\psi_1(X) + \phi_2(X)\psi_2(X) = 4a^3 + 27b^2,$$

where $\phi_1(X) = 3X^2 + 4a$, $\psi_1(X) = (3X^2 + a)^2$, $\phi_2(X) = -27(X^3 + aX - b)$ and $\psi_2(X) = X^3 + aX + b$.]

(a) If $b = a^2$, find a point of infinite order on $\mathcal{E}(\mathbb{Q})$.

(b) Find the torsion elements over $\mathbb{Q}$, and their group structure, in the case $a = 1, b = 2$.

(c) Prove that if $a \equiv 1 \pmod{10}$ and $b \equiv 5 \pmod{10}$ then the point at infinity is the only rational torsion point.

3. Let $\mathcal{E} : y^2 = x(x^2 + ax + b)$ be an elliptic curve, with $a, b \in \mathbb{Z}$, and let $\mathcal{C} = \mathcal{E}(\mathbb{Q})$. Define the map $q : \mathcal{C} \to \mathbb{Q}^\times/(\mathbb{Q}^\times)^2$ by setting $q(x, y) = x(\mathbb{Q}^\times)^2$ if $x \neq 0$ and $q(x, y) = b(\mathbb{Q}^\times)^2$ otherwise. Show that the image of q is finite.

Now let $\mathcal{E}'$ be the elliptic curve $y^2 = x(x^2 + a_1x + b_1)$, with $a_1 = -2a$ and $b_1 = a^2 - 4b$, and let $\mathcal{D} = \mathcal{E}'(\mathbb{Q})$. Stating clearly any properties you may require concerning the 2-isogeny $\phi : \mathcal{E} \to \mathcal{E}'$ and its dual $\hat{\phi}$, show that $\mathcal{C}/2\mathcal{C}$ is finite.

[You may assume that the map q above is a homomorphism, with kernel $\hat{\phi}(\mathcal{D})$.]

In the special case $\mathcal{E} : y^2 = x(x^2 - p^2)$, where p is an odd prime, show that the rank is at most 2.

[You may use without proof the fact that the order of $\mathcal{C}/2\mathcal{C}$ is 2^{R+s} where R is the rank of $\mathcal{C}$ and 2^s is the order of its rational 2-torsion subgroup.]

Show that if $x^4 + p^2y^4 = 2z^2$ has a non-trivial integer solution, then $(\frac{2}{p}) = +1$, so that $p \equiv \pm 1 \pmod 8$.

Deduce that, for $\mathcal{E} : y^2 = x(x^2 - p^2)$ as before, the rank is at most 1 if $p \equiv 3$ or $5 \pmod 8$. For $p = 5$ display a non-integral point (x, y) on the curve. [It may help to consider points for which x is a square.] Deduce that for $p = 5$ the rank is exactly 1.