Do not turn this page until you are told that you may do so

1. (i) Find an $x \in \mathbb{Z}$ such that $|x^2 + 6|_5 < 5^{-3}$. **[2 marks]**

(ii) Let $\alpha = 12, \overline{14} = 1 \cdot 5^{-1} + 2 \cdot 5^0 + 1 \cdot 5^1 + 4 \cdot 5^2 + 1 \cdot 5^3 + 4 \cdot 5^4 + \ldots \in \mathbb{Q}_5$. Express α in the form a/b, where $a, b \in \mathbb{Z}$. **[2 marks]**

(iii) Let $p \neq 2$ be prime and let $b \in \mathbb{Z}_p$, with $|b|_p = 1$. Show that there exist $x, y \in \mathbb{Z}_p$ such that $x^2 + y^2 = b$. **[4 marks]**

(iv) Determine the primes p for which there exist $x, y \in \mathbb{Z}_p$ such that $y^2 = x^3 + 2x + 2$. Are there $x, y \in \mathbb{Z}$ such that $y^2 = x^3 + 2x + 2$? **[5 marks]**

(v) Construct examples of elliptic curves $y^2 = x^3 + f_2x^2 + f_1x + f_0$, where $f_0, f_1, f_2 \in \mathbb{Z}$, which are satisfied by some $x, y \in \mathbb{Z}_p$ with $|y|_p = 1$, for all primes p except $3, 5, 7$. Find other examples of similar types, and explain what method you are using to construct your examples.

[7 marks]

2. (i) Find the torsion group over $\mathbb{Q}$ for the elliptic curve: $Y^2 = X(X + 1)(X + 4)$.

[6 marks]

(ii) Find the torsion group over $\mathbb{Q}$ for the elliptic curve: $\mathcal{E} : Y^2 = X(X - 1)(X - 4)$. Are you able to compute this using only reductions modulo p? Are you able to compute this using only the fact that the order of $\mathcal{E}_{\text{tors}}(\mathbb{Q})$ divides the order of every $\widetilde{\mathcal{E}}(\mathcal{F}_p)$? Find other examples of a similar type, explaining how you construct them. **[14 marks]**

3. (i) Show that any elliptic curve over $\mathbb{Q}$ with a rational point of order 5 is birationally equivalent to: $Y^2 + (1 + v)XY + vY = X^3 + vX^2$, for some $v \in \mathbb{Q}$. **[7 marks]**

(ii) Discuss variations of the same idea, for different values of order N. Find elliptic curves over $\mathbb{Q}$ with a point of order N, for various choices of N; for each such curve, compute the whole of the torsion group over $\mathbb{Q}$. **[13 marks]**

4. (i) Find the rank of the elliptic curve $Y^2 = X(X^2 + 6X + 1)$. **[7 marks]**

(ii) Compute the rank, of an elliptic curve $Y^2 = X(X^2 + aX + b)$, with $a, b \in \mathbb{Z}$, of your own choosing, but where b is divisible by at least three distinct primes. Also compute the rank of an example for which the rank is at least 2. **[9 marks]**

(iii) For an elliptic curve $Y^2 = X(X^2 + aX + b)$, suppose that $b(a^2 - 4b)$ is divisible by precisely k distinct primes. Give an upper bound on the rank. Are there any conditions on the sign of a, b which allow this bound to be improved? Can you describe any other conditions on a, b which allow the bound to be improved? **[9 marks]**

5. (i) Let $\mathcal{C} : Y^2 = X(X + \lambda_1)(X + \lambda_2)$, where $\lambda_1, \lambda_2 \in \mathbb{Q}^*$ and $\lambda_1 \neq \lambda_2$. Determine $\mu_1, \mu_2 \in \left(\mathbb{Q}(\sqrt{\lambda_1}, \sqrt{\lambda_2})\right)$ such that there is a 2-isogeny defined over $\mathbb{Q}$ from $\mathcal{C}$ to the curve $\mathcal{D} : Y^2 = X(X - \mu_1)(X - \mu_2)$. Suppose that $(0, 0) \in \mathcal{C}(\mathbb{Q})$; show that $\lambda_1, \lambda_2, \mu_1, \mu_2 \in (\mathbb{Q}^*)^2$. **[7 marks]**

(ii) Let $\mathcal{E}$ be any elliptic curve, defined over $\mathbb{Q}$. Find the best bound you can on the possible number of $\mathbb{Q}$-rational points of order 4 on $\mathcal{E}$. **[8 marks]**

End of Last Page