# Elliptic Curves
## Example Sheet 3

For the first exercise you need the Hasse-Weil Theorem:

**Hasse-Weil Theorem.** Let $C$ be a non-singular curve of genus $g$ over $\mathbb{F}_p$. Then

$$|\#C(\mathbb{F}_p) - (p+1)| \leq 2g\sqrt{p}.$$

1. Let $g \geq 0$ be a fixed integer. Show that there is a constant $P(g)$ such that if $p$ is prime, $p \geq P(g)$ and $C/\mathbb{F}_p$ is non-singular of genus $g$, then $C(\mathbb{F}_p) \neq \emptyset$.

2. Let $a$, $b$ be non-zero integers. Consider the curve

   $$C : y^2 = ax^{100} + b.$$

   Show (with the help of Q1) that there is a constant $P_0$ (depending on $a$, $b$) such that $C(\mathbb{Q}_p) \neq \emptyset$ for all primes $p \geq P_0$.

3. Find the torsion subgroups of the following elliptic curves:
   (i) $Y^2 = X^3 + X + 1$,
   (ii) $Y^2 = X^3 - 7$,
   (iii) $Y^2 = X^3 + 1$,
   (iv) $Y^2 = X^3 + 4X$,
   (v) $Y^2 = X^3 - X$.