Elliptic Curves
Example Sheet 4

1. Determine the rank and a set of coset representatives for $E(\mathbb{Q})/2E(\mathbb{Q})$ for the following elliptic curves:
(a) $y^2 = x(x-3)(x+4)$
(b) $y^2 = x(x-1)(x+3)$
(c) $y^2 = x(x+1)(x-14)$

2. (Fibonacci) By an appropriate transformation, show that common solutions to the pair of equations
$$u^2 + v^2 = z^2, \qquad u^2 - v^2 = w^2$$
lead to points on a certain elliptic curve E. Determine $E(\mathbb{Q})$ and use it solve the equations (remember the solution $u = v = z = w = 0$ is not allowed).

3. Is 219 a quadratic residue modulo 383?

4. You know that -1 is a quadratic residue modulo p if and only $p \equiv 1 \pmod 4$ and that 2 is a quadratic residue modulo p if and only if $p \equiv \pm 1 \pmod 8$. For which primes p is -2 a quadratic residue? For which primes p is 3 a quadratic residue?

5. Suppose p, q are primes with $p = 2q + 1$ and $q \equiv 1 \pmod 4$. Show that 2 is a primitive root modulo p.
Hint: Think about the structure of the group $\mathbb{F}_p^*$.