Problem 1 (Zeta functions, 11P)
Consider the elliptic curve $E : y^2 = x^3 + 3x$ over $\mathbb{F}_5$. Find the zeta function $\zeta_E(s)$ of $E$ and compute $\#E(\mathbb{F}_{5^7})$.

Problem 2 (MOV Attack, 12P)
Let $B' := z \mod 701$ and $B := \max(2, B')$ where $z$ is the numerical part of your Z-number. Consider the supersingular curve $E : y^2 = x^3 + 2$ over $\mathbb{F}_{701}$ and let $P$ be the unique point in $E(\mathbb{F}_{701})$ of the form $(\cdot, 1)$ and $Q$ the unique point in $E(\mathbb{F}_{701})$ of the form $(\cdot, B)$. Use the MOV attack to find a $\lambda \in \{0, \ldots, 701\}$ with $Q = \lambda \cdot P$.

You can use a computer algebra system for the necessary computations, but the individual steps of the MOV attack have to be documented.

Problem 3 Non-interactive key establishment (12P)
Consider the curve $y^2 = x^3 + 1$ over $\mathbb{F}_{1234554329}$, which is cyclic of order $n = 1234554330$. We use the non-interactive key establishment scheme of Sakai et al. discussed in class. Suppose Alice’s secret key corresponds to the point $(182284254, 1234) \in E(\mathbb{F}_{1234554329})$ and Bob’s identity corresponds to the point $(z, \sqrt{z^2 - 1}) \in E(\mathbb{F}_{1234554329})$, where $z$ is the numerical part of your Z-number. Compute the common secret between Alice and Bob resulting from Sakai et al.’s protocol.

Hint: To evaluate the Weil Pairing, you can use a computer algebra system. E.g., consider the curve $y^2 = x^3 + 1$ over $\mathbb{F}_5$ with 6-torsion points $P = (4, 0)$ and $Q = (4w, 0)$ where $w$ is a primitive 3rd root of unity in $\mathbb{F}_{25}$. In Magma (see http://magma.maths.usyd.edu.au/calc/ for an online calculator), the value of the Weil pairing $e_6(P, Q)$ can be computed as follows.

```python
w:=RootOfUnity(3,GF(5));
E:=EllipticCurve([GF(25)|0,1]);
P:=E![4,0]; Q:=E![4*w,0];
WeilPairing(P,Q,6);
```