Problem 1. ***Week 5 - 1.)***

Let E be an elliptic curve over $\mathbb{Q}$ and let $P \in E$ be a point. Let f and g be rational functions on E. Show that $ord_P(fg) = ord_P(f) + ord_P(g)$.

Solution.
Let u_P be a uniformizer at P. From the definition of $ord_P(f)$, we know that $f = u_P^{ord_P(f)} f_1$, such that f_1 is some rational function which is non-vanishing at point P. Similarly, for $g = u_P^{ord_P(g)} g_1$.

Let's consider function fg over E.
We know that fg is a rational function, as both f and g are rational functions. Also we have that

$$fg = u_P^{ord_P(f)} f_1 u_P^{ord_P(g)} g_1 = u_P ord_P(f) + ord_P(g) f_1 g_1$$

. We can see that $f_1 g_1$ is also a rational function, which is also non-vanishing at point P. Applying the same definition from before on fg, gives us $ord_P(fg) = ord_P(f) + ord_P(g)$. $\square$

Problem 2. ***Week 6 - 1.)***
Suppose that $T \in E[m]$ is a point and $T' \in E[m^2]$ satisfies $mT' = T$.
Show that the divisor

$$\sum_{R \in E[m]} [T' + R] - \sum_{R \in E[m]} [R]$$

is principal on E.

Solution.
Checking if the divisor is principal consists of calculating the sum of points and comparing it to a point at infinity.

$$\sum_{R \in E[m]} [T' + R] - \sum_{R \in E[m]} [R] = \sum_{R \in E[m]} T' + R - R = \sum_{R \in E[m]} T' = T' \sum_{R \in E[m]} 1 = m^2 T'$$

The last equation comes from the fact that there are n^2 elements in $E[m]$. As $T' \in E[m^2]$, we know that $m^2 T' = \infty$.
This implies that a given divisor is a principal divisor on E. $\square$

Problem 3. ***Week 7 - 3.)***
If $E/\mathbb{F}_{29}$ is $y^2 = x^3 - x$ and $P = (17, 13)$, $Q = (17, 16)$, use the MOV attack to reduce this to the discrete log problem over $\mathbb{F}_{29}$. Then use this to find k such that $Q = kP$. (Note that P has order $N = 4$.)

Solution.
We start by choosing a random point T from $E[N]$, such that points P and T generate $E[N]$. One such point is $T = (12, 11)$.

Now, we calculate the 'roots of unity' from the Weil pairing for P, T and Q, T respectively. With the help of Sage, we get:

$$e_4(P,T) = 28$$

$$e_4(Q,T) = 28$$

. These values are elements of $\mathbb{F}_{29}$. Now, let's evaluate the following equation:

$$\frac{e_4(P,T)}{e_4(Q,T)} = e_4(P-Q,T) = e_4(P-kP,T) = e_4(P,T)^(1-k)$$

This gives us: $1 = \frac{28}{28} = 28^{(1-k)}$, in field $\mathbb{F}_{29}$. Obivously, $28 = -1 \mod 29$, so this limit options for k down to either 1 or 3. Since P and Q are not the same point, we get the solution $k = 3$.

Appendix: Sage code that was used for this solution:

```
E = EllipticCurve(GF(29),[-1,0])
E(0).division_points(4)

P = E(17,13)
Q = E(17,16)
z1=P.weil_pairing(T,4)
z2=Q.weil_pairing(T,4)
```

□