Math 418/818
Assignment 10 - Solutions

1. (a) Since $|E(F_{13})| = 12 = 2^23$, we have that $n_2 = 2$ and $n_3 = 1$. Thus, $(\alpha_3, \beta_3) = (1, 0)$ and $(\alpha_2, \beta_2) = (1, 1)$ or $(2, 0)$. Since $-1$ is a root of $f(x) = x^3 + 1$, we see that $f(x) = (x + 1)g(x)$ with $g(x) = x^2 - x + 1$. Now $g(-3) = 13 \equiv 0 \pmod{13}$, so $g(x) \equiv (x + 3)(x + 9) \pmod{13}$. Thus, $f(x)$ has 3 roots in $F_{13}$, viz. $x_1 = -1 = 12$, $x_2 = -3 = 10$ and $x_3 = -9 = 4$, and so $|E(F_{13})|2| = 4$. Thus, by Observation 3 in class we have that $\beta_2 \geq 1$ and so $(\alpha_2, \beta_2) = (1, 1)$. This means that $A = 2^23^3 = 24^3 = 6$ and $B = 2^23^3 = 2^13^0 = 2$. Thus, $E(F_{13})$ has type $(6, 2)$, i.e., $E(F_{13}) \simeq \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

(b*) Since again $|E'(F_{13})| = 12 = 2^23$, we have the same possibilities for the $(\alpha_\ell, \beta_\ell)$ as in part (a). Since $-1$ is a root of $f(x) = x^3 + x + 2$, we have that $f(x) = (x + 1)g(x)$, where $g(x) = x^2 - x + 2$. Now since $\text{disc}(g) = (-1)^2 - 4(2) = -7$, and since $(\frac{7}{13}) = (\frac{7}{13}) = (\frac{4}{7}) = (\frac{-1}{7}) = -1$, we see that $\text{disc}(g)$ is not a square in $F_{13}$, and so $g(x)$ has no roots in $F_{13}$. Thus, $f(x)$ has only 1 root in $F_{13}$ and so $|E'(F_{13})|2| = 2$. This means by Observation 3 that $\beta_2 = 0$ and so $\alpha_2 = 2$. Thus, $A = 2^23^3 = 24^3 = 12$ and $B = 2^23^3 = 2^33^0 = 1$, so $E'(F_{13})$ has type $(12, 1)$, which means that $E'(F_{13}) \simeq \mathbb{Z}/12\mathbb{Z}$ is cyclic.

Note: Both parts of this question must be done without using Maple.

2. (See the MAPLE solution on the course web-site.)

3. (See the MAPLE solution on the course web-site.)

4. (See the MAPLE solution on the course web-site.)