HOMEWORK

For this week, please answer the following questions from the text. I've copied the problem itself below and the question numbers for your convenience.

(1) (6.3) Suppose that the cubic polynomial $X^3 + AX + B$ factors as

$$X^3 + AX + B = (X - e_1)(X - e_2)(X - e_3)$$

Prove that $4A^3 + 27B^2 = 0$ if and only if two (or more) of e_1, e_2, and e_3 are the same. (Hint: Multiply out the right-hand side and compare coefficients to relate A and and B to e_1, e_2, e_3.)

Suppose that instead we start with the cubic $X^3 + AX^2 + BX + C$. What is the formula, in terms of A, B, and C for its discriminant?

(2) (6.6) Make an addition table for E over $\mathbb{F}_p$, as we did in Table 6.1.
  (a) $E : Y^2 = X^3 + X + 2$ over $\mathbb{F}_5$.
  (b) $E : Y^2 = X^3 + 2X + 3$ over $\mathbb{F}_7$.
  (c) $E : Y^2 = X^3 + 2X + 5$ over $\mathbb{F}_{11}$.

(3) (6.9) Let E be an elliptic curve over $\mathbb{F}_p$ and let P and Q be points in $E(\mathbb{F}_p)$. Assume that Q is a multiple of P and let $n_0 > 0$ be the smallest solution to $Q = nP$. Also let $s > 0$ be the smallest solution to $sP = \mathcal{O}$. Prove that every solution to $Q = nP$ looks like $n_0 + is$ for $i \in \mathbb{Z}$. (Hint: Write $n = is + r$ for some $0 \leq r < s$ and determine the value of r.)

(4) (6.10) Let $\{P_1, P_2\}$ be a basis for $E[m]$. The *Basis Problem* for $\{P_1, P_2\}$ is to express an arbitrary point $P \in E[m]$ as a linear combination of the basis vectors, i.e, to find n_1 and n_2 so that $P = n_1P_1 + n_2P_2$. Prove that an algorithm that solves the basis problem for $\{P_1, P_2\}$ can be used to solve the ECDLP for points in $E[m]$.

(5) (6.11) Use the double-and-add algorithm (Table 6.3) to compute nP in $E(\mathbb{F}_p)$ for each of the following curves and points, as we did in Fig. 6.4.
  (a) $E : Y^2 = X^3 + 23X + 13, p = 83, P = (24, 14), n = 19$
  (b) $E : Y^2 = X^3 + 143X + 367, p = 613, P = (195, 9), n = 23$
  (c) $E : Y^2 = X^3 + 1828X + 1675, p = 1999, P = (1756, 348), n = 11$
  (d) $E : Y^2 = X^3 + 1541X + 1335, p = 3221, P = (2998, 439), n = 3211$