Problem 6.11 (Solution)

(1) A better way to do it than the text suggests.

The polynomial \( x^3 + Ax + B \) has a repeated root \( \iff \) its gcd with its derivative \( 3x^2 + A \) is not 1. Now

\[
(3x^2 + A, x^3 + Ax + B) = (2, 3x^2 + A)
\]

divide into, take remainder

\[
= (A + \frac{27B^2}{4A^2}, \frac{27B}{4A})
\]

divide into, take remainder

\[
= (A + \frac{27B^2}{4A^2}, \frac{27B}{4A}) \iff A + \frac{27B^2}{4A} \neq 0
\]

\[
\text{expected root case: } \quad 4A^2 + 27B^2 \neq 0
\]

(2) \( E: y^2 = x^3 + x + 1 \)

\[
|E(F_3)| = 3 + 1 + \sum_{x \in F_3} (x^3 + x + 1) = 4 + \left( \frac{1}{3} \right) + \left( \frac{0}{3} \right) + \left( \frac{2}{3} \right) = 4 + 1 + 0 + (-1) = 4
\]

\[
|E(F_5)| = 5 + 1 + \sum_{x \in F_5} (x^3 + x + 1) = 6 + \left( \frac{1}{5} \right) + \left( \frac{1}{5} \right) + \left( \frac{4}{5} \right) + \left( \frac{4}{5} \right) = 6 + 1 + (-1) = 6 + 1 + 1 + 1 = 9
\]

\[
|E(F_{11})| = 14
\]

\[
a_3 = -3, \quad a_{11} = 2
\]

In each case, \( |a| 
eq 2\sqrt{p} \).
(3) \( E : y^2 = x^3 + x + 1 \) / \#5
\[ P = (4, 2), \quad Q = (0, 1) \]
\[ 2P = (3, 4) \]
\[ 3P = P + 2P = (2, 4) \]
\[ 4P = 3P + P = (0, 0) \]
\[ 5P = 4P + P = (0, 1) = Q \]

(4) \( E / F_p, \quad P, Q \in E(F_p) \)

\( n_0 > 0 \) since \( \#E = nP \).
\( s > 0 \) then \( sP = \emptyset \)

So \( Q = nP \) \( \Leftrightarrow \) write (Elec. alg.) \( n = ts + r, \ 0 \leq r < s \).
Then \( Q : hP = \overline{t(sP)} + rP = rP \).

Clearly \( (s > t \geq n_0) \) (by minimality of \( n_0 \)),
and so writing \( j = r - n_0 \) we have \( s > j \geq 0 \),
and \( jP = rP - n_0P = Q - Q = \emptyset \).
By minimality of \( s, \ j = 0 \). Hence \( r = n_0 \)
and \( n = is + n_0 \).
Problem 5. In section 4.5, we gave an abstract description of Pollard's $\rho$ method, and in Section 1.5, we gave an explicit function to solve the discrete logarithm problem $\mathbb{F}_p^*$. Adapt this method to create a Pollard $\rho$-algorithm to solve the ECDLP.

Suppose we have an elliptic curve $E$ with $|E(\mathbb{F}_p)| = N$, and points $P, Q \in E(\mathbb{F}_p)$, and we want to find $n$ s.t. $nP = Q$. We shall use the function

$$f(Z) = \begin{cases} 
Z + P & \text{if } 0 \leq Z < p/3 \\
Z + Z & \text{if } p/3 \leq Z < 2p/3 \\
Z + Q & \text{if } 2p/3 \leq Z < p
\end{cases}$$

If we let $X_0 = Y_0 = \varnothing \in E(\mathbb{F}_p)$, and define the sequences $X_{k+1} = f(X_k)$ and $Y_{k+1} = f(f(Y_k))$, we should eventually find a match $X_i = y_i$, for some $i$. By keeping track of which cases of $f$ we follow, as in the version for $\mathbb{Z}/p\mathbb{Z}^*$, we can write $X_i = \alpha P + \beta Q$ and $Y_i = \gamma P + \delta Q$, giving us

$$\alpha P + \beta Q = \gamma P + \delta Q \implies (\alpha - \gamma)P = (\beta - \delta)Q$$

Let us write $u = \alpha - \gamma$ and $v = \beta - \delta$. Then we have $nP = uQ$, or equivalently $vn \equiv u \pmod{N}$. If GCD($u, N$) = 1, then we can multiply both sides by $v^{-1}$ to find a solution

$$n \equiv \frac{v^{-1}u}{(N)}$$

In general, if GCD($u, N$) = $d$, we can use the Euclidean algorithm to find $s$ s.t. $st \equiv d \pmod{N}$, which we can multiply to both sides of $vn \equiv u$ to get

$$dn \equiv du$$

Then, as with the algorithm for $\mathbb{Z}/p\mathbb{Z}^*$, we need only search for the solution

$$n \in \{u + k \cdot Nd \mid k = 0, 1, 2, \ldots, N\}$$

Problem 6. Let $E$ be the elliptic curve $y^2 = x^3 - x$. Find the group structure of $E(\mathbb{F}_5)$ and $E(\mathbb{F}_{11})$.

As with the example in class, we have

$$(-x)^3 - (-x) = -(x^3 - x)$$

$-1$ is a square in $E(\mathbb{F}_5)$, so we have $\left(\frac{x^3-x}{5}\right) = \left(\frac{-1}{5}\right) = 1$, so we need only check half of the values to find $|E(\mathbb{F}_5)| = 5 + 1 + 2 = 8$. More simply, however, $-1$ is not a square in $\mathbb{F}_{11}$, so like in class we have $|E(\mathbb{F}_{11})| = 11 + 1 = 12$.

Now, since $E(\mathbb{F}_5)$ is Abelian, we have that $E(\mathbb{F}_5)$ is $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ or $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ or $\mathbb{Z}/8\mathbb{Z}$. As in class, we shall distinguish between these by counting the 2-torsion points. Our candidate groups for $E(\mathbb{F}_5)$ have 1, 3, and 7 2-torsion points respectively. $x^3 - x$ has three roots over $\mathbb{F}_5$, namely 0, 1, and -1. So $E(\mathbb{F}_5)$ has the three 2-torsion points $(0, 0)$, $(1, 0)$, and $(-1, 0)$. Thus, we have

$$E(\mathbb{F}_5) = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$$

Next, $E(\mathbb{F}_{11})$ must be one of $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ or $\mathbb{Z}/12\mathbb{Z}$. The former has the three 2-torsion points $(1, 0)$, $(0, 3)$, and $(1, 3)$, while the latter has the single 2-torsion point 6. $x^3 - x$ still has three roots over $\mathbb{F}_{11}$, namely 0, 1, and -1, so $E(\mathbb{F}_{11})$ must have three 2-torsion points, and

$$E(\mathbb{F}_{11}) = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$$
Problem 7. Alice and Bob agree to use elliptic Diffie-Hellman key exchange with the prime, elliptic curve, and point
\[ p = 2671, \quad E : y^2 = x^3 + 171x + 853, \quad P = (1980, 431) \in E(\mathbb{F}_{2671}). \]
(a) Alice sends Bob the point \( Q_A = (2110, 543) \). Bob decides to use the secret multiplier \( n_B = 1943 \).
What point should Bob send to Alice?
Bob should send \( 1943(1980, 431) = (1432, 667) \).

(b) What is their secret shared value?
Their secret shared value is \( 1943(2110, 543) = (2424, 911) \).

(c) How difficult is it for Eve to figure out Alice’s secret multiplier \( n_A \)? If you know how to program, use a computer to find \( n_A \).
Figuring out \( n_A \) is equivalent to solving the ECDLP \( n_A P = Q_A \), which is thought to be exponential. In this case, we have either \( n_A = 726 \) or \( n_A = 2045 \).

(d) Alice and Bob decide to exchange a new piece of secret information using the same prime, curve, and point. This time Alice sends Bob only the \( x \)-coordinate \( x_A = 2 \) of her point \( Q_A \). Bob decides to use the secret multiplier \( n_B = 875 \). What single number module \( p \) should Bob send to Alice, and what is their secret shared value?
We have \( 875(1980, 431) = (161, 2040) \), so Bob would send \( x_B = 161 \). We have \( 2^x + 171(2) + 853 = 1203 \), which has a square root 96. We have \( 875(2, 96) = (1708, 1252) \), so the shared secret would be 1708.