T 10.1

$E: y^2 = f(x)$, where $f \in k[x]$ is a cubic polynomial

To count the number of points of $E(k)$:
$\forall x \in k$ check if $f(x) \in k$ is a square in k.

Detecting squares in FF is easy. Namely, we have:

Th: Given k finite field with q elements,
if q is odd, then $\forall$ element $t \in k^\times$ we have:

$$t \text{ is a square} \Leftrightarrow t^{\frac{q-1}{2}} = 1 \in k$$

$\Rightarrow$) If t is a square

$\Rightarrow \exists\ v \in k$ s.t. $v^2 = t$

$\Rightarrow v^{2 \cdot (q-1)} = t^{q-1}$

$\Rightarrow v^{q-1} = t^{\frac{q-1}{2}}$ (1)

Theorem 3.4.2 implies that k^* is a cyclic group of order $q-1$

$\Rightarrow$ (Lagrange's theorem) $v^{q-1} = 1$ (2)

Therefore, from (1) and (2) we have

$t^{\frac{q-1}{2}} = 1 \in k$ the neutral element of k^*, that is an element of k.

$\Leftarrow$) Theorem 3.4.2 implies that k^* is a cyclic group of order $q-1$

Let $k^* = \langle g \rangle$ (g is a generator of k^*)

$\Rightarrow \exists\ e$ s.t. $g^e = t$

$\Rightarrow g^{e \cdot \frac{q-1}{2}} = t^{\frac{q-1}{2}} = 1 \quad \Rightarrow \quad g^{e \cdot \frac{q-1}{2}} = 1$ (3)

But g is a generator of the cyclic group.
That means that $\operatorname{ord}(g) = q-1$

From (3) it's clear that $2 \mid e$.

Indeed, we should have that $e \cdot \frac{q-1}{2} = \xi \cdot (q-1)$, $\exists \xi \in \mathbb{Z}$
$\Rightarrow \frac{e}{2} = \xi \Rightarrow 2 \mid e$.

So now let $e' = \frac{e}{2} \Rightarrow e = 2e'$

$$\Rightarrow t = g^e = g^{2e'} = (g^{e'})^2$$

Since g is a generator, $g^{e'} = v \in k$

$$\Rightarrow t = v^2$$

This means that t is a square. $\square$

T 10.3

Let $E: y^2 = x^3 + ax + b$ be defined over k $(a, b \in k)$.

Assume $P = (x_P, y_P)$, $Q = (x_Q, y_Q) \in E(k) \setminus \{O\}$ (i.e. $x_P, y_P, x_Q, y_Q \in k$)
s.t. $x_P \neq x_Q$

Let $L_{P,Q}$ be the line through P, Q.

Th: $L_{P,Q}$ intersects E in a third point $R = (x_R, y_R) \in E(k)$.

Find a formula for x_R in terms of x_P, y_P, x_Q, y_Q, a, b.

We have that the line $L_{P,Q}$ is given by

$$y - y_P = \frac{y_Q - y_P}{x_Q - x_P}(x - x_P) \iff y = \frac{y_Q - y_P}{x_Q - x_P} x + y_P - \frac{y_Q - y_P}{x_Q - x_P} x_P$$

Let $m := \frac{y_Q - y_P}{x_Q - x_P}$, $q := y_P - \frac{y_Q - y_P}{x_Q - x_P} x_P$

The intersection between E and $L_{P,Q}$ will be given by the solutions of the following system of equations:

$$\begin{cases} y = mx+q \\ y^2 = x^3+ax+b \end{cases} \quad (4) \quad \iff (mx+q)^2 = x^3+ax+b$$

$$\iff (mx)^2 + q^2 + 2mqx = x^3+ax+b$$

$$\iff x^3 - m^2x^2 + (a-2mq)x + b - q^2 = 0$$

Using Viète's formulas with $n=3$, we can compute the $n=3$ roots r_1, r_2, r_3 by solving the following system:

$$\begin{cases} r_1 + r_2 + r_3 = m^2 \\ r_1r_2 + r_1r_3 + r_2r_3 = a-2mq \\ r_1r_2r_3 = -(b-q^2) \end{cases}$$

Two of these three roots will be x_P and x_Q, so let's say $r_1 = x_P$, $r_2 = x_Q$ (that we already know).

From the 1st equation of the system we can compute

$$r_3 = m^2 - r_1 - r_2 = m^2 - x_P - x_Q$$

So we have that $R = (x_R, y_R) \in E(k)$ is the 3rd point of intersection and it is such that:

$$x_R = m^2 - x_P - x_Q, \quad y_R = m x_R + q.$$

So in conclusion

$$x_R = \left(\frac{y_Q - y_P}{x_Q - x_P}\right)^2 - x_P - x_Q \qquad \square$$