81. When $F_{16} = F_2[x]/(x^4 + x^3 + x^2 + x + 1)$, then one can brute force to find all primitive elements. You can also do some cheating. Since we already know that $x^4 + x^3 + 1$ is primitive polynomial, any $\beta$ s.t. $\beta^4 + \beta^3 + 1 = 0$ is a primitive element. Look at my trick in the singular file "find-primitive,sing", where I find 4 PEs.

$\beta = \alpha + 1$, or $\alpha^2 + 1$, $\alpha^3 + 1$, $\alpha^3 + \alpha^2 + \alpha$

82. This is easy. Note that the only irreducible polynomial of degree 2 is $x^2 + x + 1 = p(x)$

$P(\beta) = 0$.

If $\beta \in F_4 = \{0, 1, \alpha^5, \alpha^{10}\}$, where $\alpha = PE \notin F_{16}$.

$P(\beta) = 0 \Rightarrow \beta^2 + \beta + 1$. If $\beta = \alpha^5$

$(\alpha^5)^2 + \alpha^5 + 1 = \alpha^{10} + \alpha^5 + 1 = 0 \pmod{\alpha^4 + \alpha^3 + 1}$

When $\beta = \alpha^{10}$.

$\beta^2 + \beta + 1 = \alpha^{20} + \alpha^{10} + 1 = 0 \pmod{\alpha^4 + \alpha^3 + 1}$. 
The expression is given in the HW for $P=2$

$$(\alpha_1 + \cdots + \alpha_t)^2 = \alpha_1^2 + \cdots + \alpha_t^2$$

but it is actually true for any prime power

$$(\alpha_1 + \cdots + \alpha_t)^{pk} = \alpha_1^{pk} + \cdots + \alpha_t^{pk}$$

for any field of characteristic $p$, i.e., for $\mathbb{F}_{pk}$

Proof: put $t=2$:

$$(\alpha_1 + \alpha_2)^{pk} = \alpha_1^{pk} + \alpha_2^{pk} \hspace{1cm} \text{(1)}$$

Set $k=1$. As I gave in the hint

$$(\alpha_1 + \alpha_2)^p = \alpha_1^p + (\binom{p}{1})\alpha_1^{p-1}\alpha_2 + \cdots + (\binom{p}{p-1})\alpha_1\alpha_2^{p-1} + \alpha_2^p$$

Since the binomial coefficients $\binom{p}{i}$ are multiples of $p$, they are $=0 \pmod{p}$. So,

$$(\alpha_1 + \alpha_2)^p = \alpha_1^p + \alpha_2^p \hspace{1cm} \text{(2)}$$

Raise Eqn (1) to the $p^m$ power:

$$\left[(\alpha_1 + \alpha_2)^{pk}\right]^p = (\alpha_1^{pk})^p + (\alpha_2^{pk})^p$$

$$\Rightarrow \quad (\alpha_1 + \alpha_2)^{pk+1} = \alpha_1^{pk+1} + \alpha_2^{pk+1} \hspace{1cm} \text{(3)}$$

\(\Rightarrow\) Eqn. (1) being true for $k$, Eqn (3) makes it true for $k=k+1$, hence Eqn (1) is true by induction.

Now

$$\alpha_1 + \alpha_2 + \alpha_3 = \left[(\alpha_1 + \alpha_2) + \alpha_3\right] \ldots \text{and so on...}$$
Design of a 3-bit Maslovito Multiplier.

\[ f_8 = F_3(x^3 \mod p(x) = x^3 + x + 1) \]

\[ x^3 + x + 1 = 0 \Rightarrow x^3 = x + 1 \]
\[ x^4 = x^2 + x \]

\[ Z = A \cdot B \]
\[ A = a_0 + a_1 x + a_2 x^2 \]
\[ B = b_0 + b_1 x + b_2 x^2 \]

\[ A \cdot B = \left( \sum_{i=0}^{2} a_i x^i \right) \cdot \left( \sum_{i=0}^{2} b_i x^i \right) = (a_0 + a_1 x + a_2 x^2)(b_0 + b_1 x + b_2 x^2) \]
\[ = a_0 b_0 + a_0 b_1 x + a_0 b_2 x^2 + a_1 b_0 x + a_1 b_1 x^2 + a_1 b_2 x^3 + a_2 b_0 x^2 + a_2 b_1 x^3 + a_2 b_2 x^4 \]

\[ = \left( \begin{array}{c}
    a_0 b_0 \\
    a_1 b_0 \\
    a_2 b_0 \\
  \end{array} \right) + \left( \begin{array}{c}
    a_0 b_1 \\
    a_1 b_1 \\
    a_2 b_1 \\
  \end{array} \right) x + \left( \begin{array}{c}
    a_0 b_2 \\
    a_1 b_2 \\
    a_2 b_2 \\
  \end{array} \right) x^2 \]

\[ = 3_0 + 3_1 x + 3_2 x^2 \]

[See the singular file of the design]
05 Just apply the lagrangian interpolation formula and make use of Singular to compute the polynomial. In fact, the "interpolate.sing" file that I had uploaded on the website can be easily modified to update the function values @ \( \frac{N_i}{D_i} f(x_i) \) for \( i = 1 \ldots 8 \).

Interpolated polynomial is:

\[
F(A) = (\alpha^2+\alpha+1)A^7 + (\alpha^2+1)A^6 + \alpha A^5 + (\alpha+1)A^4 \\
+ (\alpha^2+\alpha+1)A^3 + (\alpha^2+1)A
\]

Note, for random logic abstraction in F9, the polynomial is of degree 9-1, \( \alpha \) is quite dense. Random logic is better dealt by ABC.

See singular file "hw3-95-lagrange.sing" on the website.