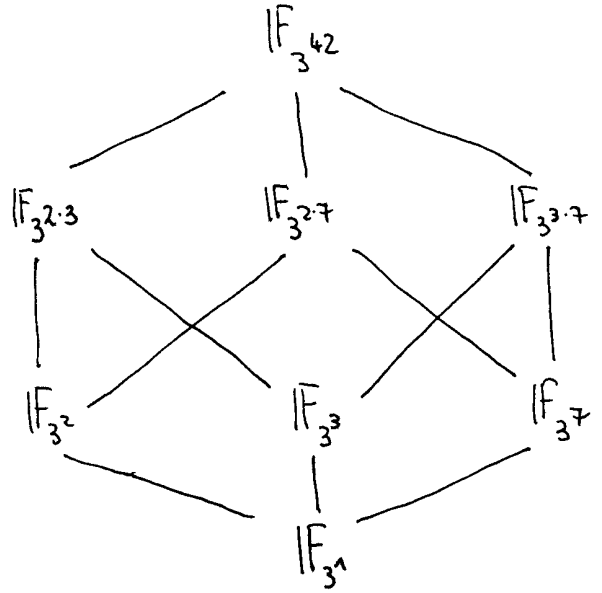
1. F has $8 = 2^3$ elements. If F had a subfield E with $4 = 2^2$ elements then F would be an E-vectorspace and thus 8 would have to be a power of 4, which it is not. Thus F does not have a subfield with 4 elements.

2. By the subfield criterion every subfield of $\mathbb{F}_{3^{42}}$ must have 3^d elements where d is a divisor of 42 and for each such divisor there is exactly one such subfield. Subfield inclusion is the same as being a divisor for the exponents. Thus the subfield diagram looks like this ($42 = 2 \cdot 3 \cdot 7$):



3. The polynomial $x^2 + 1$ is irreducible in $\mathbb{F}_3[x]$, thus $\mathbb{F}_9 \cong \mathbb{F}_3[x]/(x^2+1)$
Set Θ be the coset $x + (x^2+1)$, thus $\Theta^2 = -1$

(a) $\mathbb{F}_9 = \{0, 1, 2, \Theta, \Theta+1, \Theta+2, 2\Theta, 2\Theta+1, 2\Theta+2\}$

(b) A primitive root has order 8, $\mathbb{F}_9^*$ is a cyclic group of order 8, it has $\phi(8) = 4$ generators. 1 and 2 and Θ and 2Θ are no generators since they have orders 1, 2, 4 and 4 respectively, thus $\{\Theta+1, \Theta+2, 2\Theta+1, 2\Theta+2\}$ are primitive roots. Note: $(\Theta+1)^3 = \Theta^3 + 1 = \Theta \cdot (-1) + 1 = 2\Theta + 1$
$(\Theta+1)^5 = (2\Theta+1) \cdot (\Theta^2 + 2\Theta + 1) = (2\Theta+1) \cdot 2\Theta = \Theta^2 + 2\Theta = 2\Theta + 2$
$\Rightarrow (\Theta+1)^7 = \Theta + 2$ (indeed: $(\Theta+1)(\Theta+2) = \Theta^2 + 2 = -1 + 2 = 1$)

(c) NO.

5. If either m or n is divisible by a square of a prime, so is mn and thus $\mu(mn) = 0 = \mu(m) \cdot \mu(n)$. Assume now that both m and n are products of distinct primes and $\gcd(m,n) = 1$. Then no prime occurs in both, thus $\mu(mn) = \mu(m) \cdot \mu(n)$ since mn is also a product of distinct primes and the number of prime divisors of mn is the sum of the number of m and n.

4. Assume $f = a_n + a_{n-1}x + \dots + a_0 x^n = p \cdot q$ for $p, q \in F[x]$, $\deg p < n$, $\deg q < n$.
(assume $a_0 \neq 0 \neq a_n$)

Let $p = \sum_{i=0}^{d} b_i x^i$, $q = \sum_{j=0}^{n-d} c_j x^j$, set $b_i = 0$ for $i < 0$ or $i > d$
and $c_j = 0$ for $j < 0$ or $j > n-d$.

$\Rightarrow a_k = \sum_{\substack{i,j \in \mathbb{Z} \\ i+j = n-k}} b_i c_j$ for $0 \leq k \leq n$. because $f = p \cdot q$.

Now set: $\hat{p} := \sum_{i=0}^{d} b_{d-i} x^i$ and $\hat{q} := \sum_{j=0}^{n-d} c_{n-d-j} x^j$

Claim: $\hat{f} := a_0 + a_1 x + \dots + a_n x^n = \hat{p} \cdot \hat{q}$

Indeed: The coefficient at x^k of $\hat{p} \cdot \hat{q}$ is $\sum_{\substack{i,j \in \mathbb{Z} \\ i+j=k}} b_{d-i} \cdot c_{n-d-j} = \sum_{\substack{i',j' \in \mathbb{Z} \\ i'+j' = n-k}} b_{i'} c_{j'}$

$i' = d - i$
$j' = n - d - j$

$= a_{n-k}$ for $0 \leq k \leq n$.

$\Rightarrow$ If f is reducible then $\hat{f}$ is reducible as well.
$\Rightarrow$ If $\hat{f}$ is irreducible then f is irreducible.
$\Rightarrow$ By symmetry: f irreducible iff $\hat{f}$ irreducible.

Note: We need $a_0 \neq 0 \neq a_n$, otherwise $\hat{f}$ not well-defined.

6. Use Lemma: $\sum_{d \mid n} \mu(d) = \begin{cases} 1 & n = 1 \\ 0 & \text{otherwise} \end{cases}$

Assume $h, H : \mathbb{N} \to G$ (additively written abelian group)
and $h(n) = \sum_{d \mid n} \mu(n/d) \cdot H(d) = \sum_{d \mid n} \mu(d) \cdot H(n/d)$ for all n.

Then: $\sum_{d \mid n} h(d) = \sum_{d \mid n} \sum_{c \mid d} \mu(\underbrace{d/c}_{=d'}) H(\underbrace{c}_{=c})$

$= \sum_{c \mid n} \sum_{\substack{d \mid n \\ c \mid d}}$ (we run over all pairs (c,d) with $c \mid d \mid n$)

$= \sum_{c \mid n} H(c) \sum_{d' \mid n/c} \mu(d') = H(n)$, since $\sum_{d' \mid n/c} \mu(d') = \begin{cases} 1 & n/c = 1 \\ 0 & \text{otherwise} \end{cases}$.

7. $N_q(n) = \frac{1}{n} \sum_{d|n} \mu\left(\frac{n}{d}\right) q^d = \frac{1}{n} \sum_{d|n} \mu(d)\, q^{n/d}$

(a) $n = 18$ Divisors d: 1 2 3 6 9 18

$\mu(d)$: 1 −1 −1 1 0 0

$\Rightarrow N_q(18) = \frac{1}{18}\left(q^{18} - q^9 - q^6 + q^3\right)$

(b) $n = 70$ Divisors d: 1 2 4 5 10 20

$\mu(d)$: 1 −1 0 −1 1 0

$\Rightarrow N_q(70) = \frac{1}{20}\left(q^{70} - q^{10} - q^4 + q^2\right)$

8. $I(q,n;x) = \prod_{d|n} \left(x^{q^d} - x\right)^{\mu\left(\frac{n}{d}\right)} = \prod_{d|n} \left(x^{q^{n/d}} - x\right)^{\mu(d)}$

(a) $n = 4$, $q = 3$ Divisors d: 1 2 4

$\mu(d)$ 1 −1 0

$\Rightarrow I(3,4,x) = \left(x^{3^4} - x\right) / \left(x^{3^2} - x\right) = \frac{x^{80} - 1}{x^8 - 1} = x^{72} + x^{64} + x^{56} + x^{48} + x^{40} + x^{32} + x^{24} + x^{16} + x^8 + 1$

$= \sum_{i=0}^{9} x^{8i}$

(b) $n = 6$, $q = 2$ Divisors d: 1 2 3 6

$\mu(d)$ 1 −1 −1 1

$\Rightarrow I(6,2,x) = \frac{\left(x^{2^6} - x\right)\left(x^{2^1} - x\right)}{\left(x^{2^3} - x\right)\left(x^{2^2} - x\right)} = \frac{\left(x^{63} - 1\right)\left(x - 1\right)}{\left(x^7 - 1\right)\left(x^3 - 1\right)} = \frac{\sum_{i=0}^{8} x^{7i}}{x^2 + x + 1}$

$= x^{54} + x^{53} + x^{51} + x^{50} + x^{48} + x^{46} + x^{45} + x^{43} + x^{42} + x^{33} + x^{32} + x^{30} +$

$x^{29} + x^{27} + x^{25} + x^{24} + x^{22} + x^{21} + x^{12} + x^{11} + x^9 + x^8 + x^6 + x^4 + x^3 + x + 1$

I used a computer to compute this!