Chapter 2 Arithmetic of Finite Fields

1. We adopt the convention that the degree of the zero polynomial is $-\infty$. For any two polynomials $f(x), g(x)$, we then have $\deg(f(x)g(x)) = \deg f(x) + \deg g(x)$. Moreover, we can include the case $r(x) = 0$ in the case $\deg r(x) < \deg g(x)$.

(a) Let $m = \deg f(x)$ and $n = \deg g(x)$. Since the result is trivial for $n = 0$ (constant non-zero polynomials $g(x)$), we assume that $n \geqslant 1$, and proceed by induction on m. If $m < n$, we take $q(x) = 0$ and $r(x) = f(x)$. So consider $m \geqslant n$, and assume that the result holds for all polynomials $f_1(x)$ of degrees $< m$. If a and b are the leading coefficients of f and g, we construct the polynomial $f_1(x) = f(x) - (a/b)x^{m-n}g(x)$. Clearly, $\deg f_1(x) < m$, and so by the induction hypothesis, $f_1(x) = q_1(x)g(x) + r_1(x)$ for some polynomials q_1 and r_1 with $\deg r_1 < \deg g$. But then, $f(x) = (q_1(x) + (a/b)x^{m-n})g(x) + r_1(x)$, that is, we take $q(x) = q_1(x) + (a/b)x^{m-n}$ and $r(x) = r_1(x)$.

In order to prove the uniqueness of the quotient and the remainder polynomials, suppose that $f(x) = q(x)g(x) + r(x) = \bar{q}(x)g(x) + \bar{r}(x)$ with both r and $\bar{r}$ having degrees less than $\deg g$. But then, $(q(x) - \bar{q}(x))g(x) = \bar{r}(x) - r(x)$. If $r \neq \bar{r}$, then the right side is a non-zero polynomial of degree less than n, whereas the left side, if non-zero, is a polynomial of degree $\geqslant n$. This contradiction indicates that we must have $q = \bar{q}$ and $r = \bar{r}$.

(b) Since $r(x) = f(x) - q(x)g(x)$, any common divisor of $f(x)$ and $g(x)$ divides $r(x)$ and so $\gcd(g(x), r(x))$ too. Likewise, $f(x) = q(x)g(x) + r(x)$ implies that any common divisor of $g(x)$ and $r(x)$ divides $f(x)$ and so $\gcd(f(x), g(x))$ too. In particular, $\gcd(f, g) \mid \gcd(g, r)$ and $\gcd(g, r) \mid \gcd(f, g)$. If both these gcds are taken as monic polynomials, they must be equal.

(c) We follow a procedure similar to the Euclidean gcd of integers. We generate three sequences $r_i(x), u_i(x), v_i(x)$ maintaining the invariance $u_i(x)f(x) + v_i(x)g(x) = r_i(x)$ for all $i \geqslant 0$. We initialize the sequences as $r_0(x) = f(x)$, $u_0(x) = 1$, $v_0(x) = 0$, $r_1(x) = g(x)$, $u_1(x) = 0$, $v_1(x) = 1$. Subsequently, for $i = 2, 3, 4, \ldots$, we compute the quotient $q_i(x)$ and $r_i(x)$ of Euclidean division of $r_{i-2}(x)$ by $r_{i-1}(x)$. We also update the u and v sequences as $u_i(x) = u_{i-2}(x) - q_i(x)u_{i-1}(x)$ and $v_i(x) = v_{i-2}(x) - q_i(x)v_{i-1}(x)$. The algorithm terminates, since the r sequence consists of polynomials with strictly decreasing degrees. If j is the smallest index for which $r_j(x) = 0$, then $\gcd(f(x), g(x)) = r_{j-1}(x) = u_{j-1}(x)f(x) + v_{j-1}(x)g(x)$.

(d) Let $d(x) = \gcd(f(x), g(x)) = u(x)f(x) + v(x)g(x)$ for some polynomials u, v. For any polynomial $q(x)$, we have $d(x) = (u(x) - q(x)g(x))f(x) + (v(x) + q(x)f(x))g(x)$. In particular, we can take $q(x) = u(x) \operatorname{quot} g(x)$, and assume that $\deg u < \deg g$ in the Bézout relation $d = uf + vg$. But then, $\deg vg = \deg v + \deg g = \deg(d - uf) \leqslant \max(\deg d, \deg uf) = \deg uf = \deg u + \deg f < \deg g + \deg f$, that is, $\deg v < \deg f$.

2. The statement is false: $x^5 + x + 1 = (x^2 + x + 1)(x^3 + x^2 + 1)$.

3. Let θ be a root of $x^4 + 1$, that is, $\theta^4 + 1 = 0$, that is, $\theta^4 = -1$. But then, $x^4 + 1 = x^4 - \theta^4 = (x^2 - \theta^2)(x^2 + \theta^2) = (x - \theta)(x + \theta)(x^2 + \theta^2) = (x - \theta)(x + \theta)(x^2 - \theta^6) = (x - \theta)(x + \theta)(x - \theta^3)(x + \theta^3)$. Therefore, $x^4 + 1$ splits in $\mathbb{Q}(\theta)$.

4. **(a)** $x, x+1, x^2+x+1, x^3+x+1, x^3+x^2+1, x^4+x+1, x^4+x^3+1, x^4+x^3+x^2+x+1$.

(b) $x, x+1, x+2, x^2+1, x^2+x+2, x^2+2x+2, x^3+2x+1, x^3+2x+2, x^3+x^2+2, x^3+x^2+x+2, x^3+x^2+2x+1, x^3+2x^2+1, x^3+2x^2+x+1, x^3+2x^2+2x+2$.

(c) $x, x+1, x+2, x+3, x+4, x^2+2, x^2+3, x^2+x+1, x^2+x+2, x^2+2x+3, x^2+2x+4, x^2+3x+3, x^2+3x+4, x^2+4x+1, x^2+4x+2, x^3+x+1, x^3+x+4, x^3+2x+1, x^3+2x+4, x^3+3x+2, x^3+3x+3, x^3+4x+2, x^3+4x+3, x^3+x^2+1, x^3+x^2+2, x^3+x^2+x+3, x^3+x^2+x+4, x^3+x^2+3x+1, x^3+x^2+3x+4, x^3+x^2+4x+1, x^3+x^2+4x+3, x^3+2x^2+1, x^3+2x^2+3, x^3+2x^2+x+3, x^3+2x^2+x+4, x^3+2x^2+2x+2, x^3+2x^2+2x+3, x^3+2x^2+4x+2, x^3+2x^2+4x+4, x^3+3x^2+2, x^3+3x^2+4, x^3+3x^2+x+1, x^3+3x^2+x+2, x^3+3x^2+2x+2, x^3+3x^2+2x+3, x^3+3x^2+4x+1, x^3+3x^2+4x+3, x^3+4x^2+3, x^3+4x^2+4, x^3+4x^2+x+1, x^3+4x^2+x+2, x^3+4x^2+3x+1, x^3+4x^2+3x+4, x^3+4x^2+4x+2, x^3+4x^2+4x+4$.

5. **(a)** We have the following gcd computations in $\mathbb{F}_2[x]$:

$$\begin{aligned}\gcd(x^8 + x + 1, x^2 + x) &= 1,\\ \gcd(x^8 + x + 1, x^4 + x) &= x^2 + x + 1,\end{aligned}$$

that is, $x^8 + x + 1$ is not irreducible (see Algorithm 3.1). We also have:

$$\begin{aligned}\gcd(x^8 + x^3 + 1, x^2 + x) &= 1,\\ \gcd(x^8 + x^3 + 1, x^4 + x) &= 1,\\ \gcd(x^8 + x^3 + 1, x^8 + x) &= x^3 + x + 1,\end{aligned}$$

that is, $x^8 + x^3 + 1$ is not irreducible.

(b) The statement is true. No binomial or quadrinomial (of degree > 1) in $\mathbb{F}_2[x]$ can be irreducible, since such a polynomial has the root 1, that is, the factor $x+1$. An irreducible trinomial in $\mathbb{F}_2[x]$ must be of the form $x^n + x^r + 1$ for $1 \leqslant r \leqslant n-1$. Since $x^n + x^r + 1$ is irreducible if and only if its opposite $x^n + x^{n-r} + 1$ is irreducible, it suffices to restrict our attention to $1 \leqslant r \leqslant n/2$. For $n = 8$, the polynomials corresponding to $r = 1$ and $r = 3$ are reducible by Part (a). Finally, $x^8 + x^2 + 1 = (x^4 + x + 1)^2$ and $x^8 + x^4 + 1 = (x^2 + x + 1)^4$.

6. **(a)** One can see that $f(x)$ has no roots in $\mathbb{F}_5$ and so no linear factors in $\mathbb{F}_5[x]$. Therefore, if $f(x)$ is reducible in $\mathbb{F}_5[x]$, it must be a product of two monic irreducible quadratic factors. Exercise 2.4(c) supplies the list of all monic irreducible quadratic polynomials in $\mathbb{F}_5[x]$. One can check that $f(x)$ is not the product of any two of them (repeated factors should also be considered). A better way is to compute $\gcd(x^4 + x + 4, x^{25} - x) = 1$ (see Algorithm 3.1).

(b) We have $\alpha + \beta = 2\theta^3 + \theta^2 + 2$, and $\alpha - \beta = 2\theta^3 + 4\theta^2 + \theta + 1$. Their product is $\alpha\beta = 2\theta^5 + 4\theta^4 + 4\theta^3 + 2\theta + 2 = 2\theta^4(\theta + 2) + 4\theta^3 + 2\theta + 2 = -2(\theta+4)(\theta+2)+4\theta^3+2\theta+2 = 3(\theta+4)(\theta+2)+4\theta^3+2\theta+2 = 4\theta^3+3\theta^2+1$. In order to compute α/β, we first make an extended gcd calculation to get $(4\theta^2+2\theta+4)\beta+f(\theta) = 1$, that is, $\beta^{-1} = 4\theta^2+2\theta+4$. Therefore, $\alpha/\beta = (2\theta^3+3\theta+4)(4\theta^2+2\theta+4) = 3\theta^5+4\theta^4+2\theta^2+1 = -(3\theta+4)(\theta+4)+2\theta^2+1 = 4\theta^2+4\theta$.

7. (a) $\left(\frac{7}{19}\right) = (-1)^{(7-1)(19-1)/4}\left(\frac{19}{7}\right) = -\left(\frac{19}{7}\right) = -\left(\frac{5}{7}\right) = -(-1)^{(5-1)(7-1)/4}\left(\frac{7}{5}\right) = -\left(\frac{7}{5}\right) = -\left(\frac{2}{5}\right) = -(-1) = +1$, so 7 is a quadratic residue modulo 19. But $19 \equiv 3 \pmod 4$, so -7 is a quadratic non-residue modulo 19. Thus, $x^2 - 7$ is reducible modulo 19, whereas $x^2 + 7$ is irreducible modulo 19.

(b) We take $f(x) = x^2+7$, that is, $\theta^2+7 = 0$, that is, $\theta^2 = -7 = 12$. Since the binary expansion of 11 is $(1011)_2$, the left-to-right exponentiation algorithm proceeds as follows. The product is initialized to 1.

Bit	Operation	Product
1	Sqr	1
	Mul	$2\theta + 3$
0	Sqr	$(2\theta + 3)^2 = 4\theta^2 + 12\theta + 9 = 4 \times 12 + 12\theta + 9 = 12\theta$
1	Sqr	$(12\theta)^2 = 144 \times \theta^2 = 11 \times 12 = 18$
	Mul	$18 \times (2\theta + 3) = 17\theta + 16$
1	Sqr	$(17\theta+16)^2 = 289\theta^2 + 544\theta + 256 = 4 \times 12 + 12\theta + 9 = 12\theta$
	Mul	$(12\theta)(2\theta + 3) = 24\theta^2 + 36\theta = 5 \times 12 + 17\theta = 17\theta + 3$

We conclude that $(2\theta + 3)^{11} = 17\theta + 3$.

8. Let $\alpha = (\alpha_0, \alpha_1, \ldots, \alpha_{N-1})$ and $\beta = (\beta_0, \beta_1, \ldots, \beta_{N-1})$ be the two operands. The sum $\gamma = \alpha + \beta$ is stored in the words $(\gamma_0, \gamma_1, \ldots, \gamma_{N-1})$.

For $i = 0, 1, \ldots, N - 1$, set $\gamma_i = \alpha_i$ XOR β_i.

The schoolbook multiplication $\gamma = \alpha\beta$ can be implemented as follows.

Initialize $\gamma_i = 0$ for $i = 0, 1, 2, \ldots, 2N - 1$.
For $j = 0, 1, 2, \ldots, N - 1$, repeat: {
    For $k = 0, 1, 2, \ldots, w - 1$, repeat: {
        If the k-th bit in the word β_j is 1, then: {
            For $i = 0, 1, 2, \ldots, N - 1$, repeat: {
                XOR γ_{i+j} with LEFT-SHIFT(α_i, k).
                XOR γ_{i+j+1} with RIGHT-SHIFT$(\alpha_i, w - k)$.
            }
        }
    }
}

The left-to-right comb multiplication starts by initializing a $2N$-word product γ to zero. Inside the loop, γ is left-shifted by one bit. Since the final product γ must fit in $2N$ words, this shifting is restricted to $2N$ words only, that is, the *carry* from the most significant word must be zero and is ignored.

Initialize $\gamma_i = 0$ for $i = 0, 1, 2, \ldots, 2N-1$.
For bit position $k = w-1, w-2, \ldots, 1, 0$ (in that order), repeat: {
    For $j = 0, 1, 2, \ldots, N-1$, repeat: {
        If the k-th bit in β_j is 1, then: {
            For $i = 0, 1, 2, \ldots, N-1$, XOR γ_{i+j} with α_i.
        }
    }
    If $k > 0$, LEFT-SHIFT γ by one bit (ignore carry from γ_{2N-1}).
}

Modular reduction and extended Euclidean gcd are based on Euclidean division. Suppose that we want to divide a polynomial $a(x) \in \mathbb{F}_2[x]$ of degree c by a non-zero polynomial $b(x)$ of degree d. Thus, a is stored using $M = \lceil c/w \rceil$ words $a_0, a_1, \ldots, a_{M-1}$, and b using $N = \lceil d/w \rceil$ words $b_0, b_1, \ldots, b_{N-1}$.

Initialize the quotient to the zero polynomial (of degree $m - n$).
While ($c \geqslant d$), repeat: {
    Let $s = c \operatorname{quot} w$ (word index) and $t = c \operatorname{rem} w$ (bit position).
    If the t-th bit in the s-th word of a is 1, then: {
        Set $r = c - d$, $i = r \operatorname{quot} w$, and $k = r \operatorname{rem} w$.
        Set the k-th bit in the i-th word of the quotient polynomial to 1.
        For $j = 0, 1, 2, \ldots, N-1$, repeat: {
            XOR a_{i+j} with LEFT-SHIFT(b_j, k).
            XOR a_{i+j} with RIGHT-SHIFT$(b_j, w-k)$.
        }
    }
    Decrement c by 1.
}
Copy a to the remainder polynomial.

---

9. **(a)** Use the binomial theorem, $2 \equiv 0 \pmod 2$, and $a_i^2 = a_i$ for all i.
(b) Initialize the square to zero. For $i = 0, 1, 2, \ldots, n-1$, set the $2i$-th bit of the square to one if $a_i = 1$. Squaring can be done in linear (in n) time. A general multiplication (schoolbook or comb-based) takes quadratic time.
(c) We use a window of size t. For simplicity, t should divide the bit size w of a word. If $w = 32$ or 64, natural choices for t are $2, 4, 8$. For each t-bit pattern $(a_{t-1}a_{t-2}\ldots a_1 a_0)$, the $2t$-bit pattern $(0a_{t-1}0a_{t-2}\ldots 0a_1 0a_0)$ is precomputed and stored in a table of size 2^t. In the squaring loop, t bits of the operand are processed simultaneously. For a t-bit chunk in the operand, the square is read from the precomputed table and XOR-ed with the output with an appropriate shift. Note that the precomputed table is an absolutely constant table, that is, independent of the operand.

10. We first extract the coefficients of x^{255} through x^{233} from γ_3:

$$\mu = \text{RIGHT-SHIFT}(\gamma_3, 41).$$

We then make these bits in γ_3 zero as follows:

γ_3 is AND-ed with the constant integer 0x1FFFFFFFFFF.

What remains is to add $\mu f_1 = \mu(x^{74}+1) = x^{64}(x^{10}\mu) + \mu$ to γ. Since μ is a 23-bit value, this is done as follows:

γ_1 is XOR-ed with LEFT-SHIFT$(\mu, 10)$,

γ_0 is XOR-ed with μ.

11. **(a)** An element of $\mathbb{F}_{2^{1223}}$ is represented by 1223 bits, that is, by $\lceil 1223/64 \rceil = 20$ words. A product of two elements in $\mathbb{F}_{2^{1223}}$ is a polynomial of degree $\leqslant 2444$ and fits in $\lceil 2445/64 \rceil = 39$ words. Let $\gamma_0, \gamma_1, \ldots, \gamma_{38}$ be such an intermediate product. We need to divide this by the defining polynomial $x^{1223} + x^{255} + 1$. For $r = 38, 37, \ldots, 20$ (in that order), we eliminate the entire γ_r as follows. Let μ be the 64-bit pattern stored in γ_r. After setting $\gamma_r = 0$, we also need to XOR $x^{64r-1223}\mu(x^{255}+1)$ with γ. Since $x^{64r-1223}\mu(x^{255}+1) = x^{64r-968}\mu + x^{64r-1223}\mu = x^{64(r-16)+56}\mu + x^{64(r-20)+57}\mu$, we do the following:

γ_{r-16} is XOR-ed with LEFT-SHIFT$(\mu, 56)$,

γ_{r-15} is XOR-ed with RIGHT-SHIFT$(\mu, 8)$,

γ_{r-20} is XOR-ed with LEFT-SHIFT$(\mu, 57)$,

γ_{r-19} is XOR-ed with RIGHT-SHIFT$(\mu, 7)$.

Then, we have to reduce the coefficients of x^{1279} through x^{1223} in γ_{19} to zero. These bits are extracted as

$\mu =$ RIGHT-SHIFT$(\gamma_{19}, 7)$.

We then set these bits to zero:

AND γ_{19} with the constant word 0x7F.

Finally, we should add $\mu(x^{255}+1) = x^{3\times 64}x^{63}\mu + \mu$ to γ:

γ_3 is XOR-ed with LEFT-SHIFT$(\mu, 63)$,

γ_4 is XOR-ed with RIGHT-SHIFT$(\mu, 1)$,

γ_0 is XOR-ed with μ.

(b) An element of $\mathbb{F}_{2^{571}}$ requires $\lceil 571/64 \rceil = 9$ words. An intermediate product γ is of degree $\leqslant 2 \times 570 = 1140$, and requires $\lceil 1141/64 \rceil = 18$ words. For $r = 17, 16, \ldots, 9$ (in that order), we store $\mu = \gamma_r$, set $\gamma_r = 0$, and add $\mu x^{64r-571}(x^{10} + x^5 + x^2 + 1) = x^{64(r-9)+15}\mu + x^{64(r-9)+10}\mu x^{64(r-9)+7}\mu + x^{64(r-9)+5}\mu$ to γ. This involves the following bit-wise operations:

γ_{r-9} is XOR-ed with LEFT-SHIFT$(\mu, 15)$,

γ_{r-8} is XOR-ed with RIGHT-SHIFT$(\mu, 49)$,

γ_{r-9} is XOR-ed with LEFT-SHIFT$(\mu, 10)$,

γ_{r-8} is XOR-ed with RIGHT-SHIFT$(\mu, 54)$,

γ_{r-9} is XOR-ed with LEFT-SHIFT$(\mu, 7)$,

γ_{r-8} is XOR-ed with RIGHT-SHIFT$(\mu, 57)$,

γ_{r-9} is XOR-ed with LEFT-SHIFT$(\mu, 5)$,

γ_{r-8} is XOR-ed with RIGHT-SHIFT$(\mu, 59)$.

Finally, we need to handle γ_8 (coefficients of x^{575} through x^{571}). This is done by first remembering

$$\mu = \text{RIGHT-SHIFT}(\gamma_8, 59),$$

AND-ing γ_8 with the constant 0x7FFFFFFFFFFFFFF, and adding $(x^{10} + x^5 + x^2 + 1)\mu$ to γ. Since γ is only a 5-bit word, the last task is performed as:

γ_0 is XOR-ed with LEFT-SHIFT$(\mu, 10)$,

γ_0 is XOR-ed with LEFT-SHIFT$(\mu, 5)$,

γ_0 is XOR-ed with LEFT-SHIFT$(\mu, 2)$,

γ_0 is XOR-ed with μ.

12. **(a)** We require 39 32-bit words to store an element of $\mathbb{F}_{2^{1223}}$, and 77 32-bit words to store an intermediate product. The reduction algorithm follows.

For $r = 76, 75, \ldots, 39$ (in that order), repeat: {
  Set $\mu = \gamma_r$ and $\gamma_r = 0$.
  γ_{r-31} is XOR-ed with LEFT-SHIFT$(\mu, 24)$.
  γ_{r-30} is XOR-ed with RIGHT-SHIFT$(\mu, 8)$.
  γ_{r-39} is XOR-ed with LEFT-SHIFT$(\mu, 25)$.
  γ_{r-38} is XOR-ed with RIGHT-SHIFT$(\mu, 7)$.
}
Set $\mu =$ RIGHT-SHIFT$(\gamma_{38}, 7)$, and AND γ_{38} with 0x7F.
γ_7 is XOR-ed with LEFT-SHIFT$(\mu, 31)$.
γ_8 is XOR-ed with RIGHT-SHIFT$(\mu, 1)$.
γ_0 is XOR-ed with μ.

(b) We have $\lceil 571/32 \rceil = 18$ and $\lceil 1141/32 \rceil = 36$.

For $r = 35, 34, \ldots, 18$ (in that order), repeat: {
  Set $\mu = \gamma_r$ and $\gamma_r = 0$.
  γ_{r-18} is XOR-ed with LEFT-SHIFT$(\mu, 15)$.
  γ_{r-17} is XOR-ed with RIGHT-SHIFT$(\mu, 17)$.
  γ_{r-18} is XOR-ed with LEFT-SHIFT$(\mu, 10)$.
  γ_{r-17} is XOR-ed with RIGHT-SHIFT$(\mu, 22)$.
  γ_{r-18} is XOR-ed with LEFT-SHIFT$(\mu, 7)$.
  γ_{r-17} is XOR-ed with RIGHT-SHIFT$(\mu, 25)$.
  γ_{r-18} is XOR-ed with LEFT-SHIFT$(\mu, 5)$.
  γ_{r-17} is XOR-ed with RIGHT-SHIFT$(\mu, 27)$.
}

Set $\mu = \text{RIGHT-SHIFT}(\gamma_{17}, 27)$, and AND γ_{17} with 0x7FFFFFF.
γ_0 is XOR-ed with LEFT-SHIFT$(\mu, 10)$.
γ_0 is XOR-ed with LEFT-SHIFT$(\mu, 5)$.
γ_0 is XOR-ed with LEFT-SHIFT$(\mu, 2)$.
γ_0 is XOR-ed with μ.

---

13. Initialize the u sequence as $u_0 = \beta$ and $u_1 = 0$. The rest of the extended gcd algorithm remains the same. Now, the extended gcd loop maintains the invariance $u_i\beta^{-1}\alpha + v_i f = r_i$ (where f is the defining polynomial). If $r_j = 1$, we have $u_j\beta^{-1}\alpha \equiv 1 \pmod f$, that is, $\beta\alpha^{-1} = u_j$.

14. **(a)** By Fermat's little theorem, $\alpha^{2^n-1} = 1$, so $\alpha^{-1} = \alpha^{2^n-2}$.
(b) The exponentiation algorithm follows.

Initialize *prod* $= 1$.
For $i = 2, 3, 4, \ldots, n-1$, repeat: { Set $\alpha = \alpha^2$, and $prod = prod \times \alpha$.}

---

15. **(a)** We have $\alpha^{2^{2k}-1} = \alpha^{(2^k-1)(2^k+1)} = (\alpha^{2^k-1})^{2^k}\alpha^{2^k-1}$. Moreover, $\alpha^{2^{2k+1}-1} = \alpha^{2^{2k+1}-2+1} = (\alpha^{2^{2k}-1})^2\alpha$.
(b) The following algorithm resembles left-to-right exponentiation.

Let $n-1 = (n_{s-1}n_{s-2}\ldots n_1n_0)_2$ with $n_{s-1} = 1$.
Initialize *prod* $= \alpha$ and $k = 1$.
/* Loop for computing $\alpha^{2^{n-1}-1}$ */
For $i = s-2, s-3, \ldots, 2, 1, 0$, repeat: {
  /* Here, $k = (n_{s-1}n_{s-2}\ldots n_{i+1})_2$, and $prod = \alpha^{2^k-1}$ */
  Set $t = prod$. /* Remember α^{2^k-1} */
  For $j = 1, 2, \ldots, k$, set $prod = prod^2$. /* $prod = (\alpha^{2^k-1})^{2^k}$ */
  Set $prod = prod \times t$. /* $prod = \alpha^{2^{2k}-1} = (\alpha^{2^k-1})^{2^k}\alpha^{2^k-1}$ */
  Set $k = 2k$. /* $k = (n_{s-1}n_{s-2}\ldots n_{i+1}0)_2$ */
  If $(n_i = 1)$ { /* $(n_{s-1}n_{s-2}\ldots n_{i+1}n_i)_2 = (n_{s-1}n_{s-2}\ldots n_{i+1}0)_2 + 1$ */
    Set $prod = prod^2 \times \alpha$ and $k = k+1$.
  }
}
Return $prod^2$.

(c) Let $N_i = (n_{s-1}n_{s-2}\ldots n_i)_2$. The number of squares (in the field) performed by the loop is $\leqslant (N_{s-1} + N_{s-2} + \cdots + N_1) + (s-1) = \lfloor (n-1)/2^{s-1} \rfloor + \lfloor (n-1)/2^{s-2} \rfloor + \cdots + \lfloor n/2 \rfloor + (s-1) \leqslant (n-1)(\frac{1}{2^{s-1}} + \frac{1}{2^{s-2}} + \cdots + \frac{1}{2}) + (s-1) \leqslant (n-1) + (s-1) \leqslant n + s$. The number of field multiplications performed by the loop is $\leqslant 2s$. The algorithm of Exercise 2.14(b), on the other hand, performs about n square and n multiplication operations in the field. Since $s \approx \lg n$, the current algorithm is expected to be faster than the algorithm of Exercise 2.14(b) (unless n is too small).

16. Since $(\alpha^{2^{n-1}})^2 = \alpha^{2^n} = \alpha$ by Fermat's little theorem, $\alpha^{2^{n-1}}$ is a square root of α. Let β_1, β_2 be square roots of α, that is, $\beta_1^2 = \beta_2^2 = \alpha$. Raising to the (2^{n-1})-th power gives $\beta_1^{2^n} = \beta_2^{2^n}$, that is, $\beta_1 = \beta_2$.

17. **(a)** See Exercise 2.16.

(b) Let $\alpha = a_0 + a_1\theta + a_2\theta^2 + \cdots + a_{n-1}\theta^{n-1}$. Take $A_0(\theta) = \sum_{i=0}^{k} a_{2i}\theta^i$, where $k = (n-1)/2$ if n is odd, or $(n-2)/2$ if n is even. Also take $A_1(\theta) = \sum_{i=0}^{l} a_{2i+1}\theta^i$, where $l = (n-3)/2$ if n is odd, or $(n-2)/2$ if n is even.

(c) We have $\sqrt{\alpha} = A_0(\theta) + \sqrt{\theta}A_1(\theta)$. We precompute $\sqrt{\theta}$ (for example, using Part (a)). The polynomials A_0, A_1 can be easily extracted from the bit pattern of α using bit-wise operations. A precomputation table (the inverse of the table in Exercise 2.9(c)) can speed up this construction. After this, we have one multiplication (by the precomputed $\sqrt{\theta}$) and one addition in the field.

18. We have $x \equiv x \times 1 \equiv x(x^{1223} + x^{255}) \equiv (x^{612} + x^{128})^2 \pmod{f(x)}$.

19. **(a)** If both n, k are even, then $x^n + x^k + 1 = (x^{n/2} + x^{k/2} + 1)^2$ is not irreducible.

(b) We have $\theta = \theta \times 1 = \theta(\theta^n + \theta^k) = (\theta^{(n+1)/2} + \theta^{(k+1)/2})^2$.

(c) We have:

$$
\begin{aligned}
& \theta = \theta^{n+1} + \theta \times \theta^k \\
\Rightarrow\quad & \sqrt{\theta} = \theta^{(n+1)/2} + \sqrt{\theta} \times \theta^{k/2} \\
\Rightarrow\quad & \sqrt{\theta}(\theta^{k/2} + 1) = \theta^{(n+1)/2} \\
\Rightarrow\quad & \sqrt{\theta}(\theta^{k/2} + 1)^2 = \sqrt{\theta}(\theta^k + 1) = \sqrt{\theta} \times \theta^n = \theta^{(n+1)/2}(\theta^{k/2} + 1) \\
\Rightarrow\quad & \sqrt{\theta} = \theta^{-(n-1)/2}(\theta^{k/2} + 1).
\end{aligned}
$$

(d) We can similarly derive that $\sqrt{\theta} = \theta^{-(k-1)/2}(\theta^{n/2} + 1)$ in this case.

20. Under Kawahara et al.'s encoding, an element $a = a_0 + a_1\theta + a_2\theta^2 + \cdots + a_{n-1}\theta^{n-1}$ is represented by two bit arrays. With a packing of w bits per word, the high-order bit array is represented as $(a_0^{(hi)}, a_1^{(hi)}, \ldots, a_{N-1}^{(hi)})$, where $N = \lceil n/w \rceil$. Likewise, the low-order bit array for a is represented by N words $(a_0^{(lo)}, a_1^{(lo)}, \ldots, a_{N-1}^{(lo)})$. Let us call these word arrays as $a^{(hi)}$ and $a^{(lo)}$. An arithmetic operation accepts as input two word arrays representing each input, and outputs two word arrays representing the output.

The code for addition uses two temporary words h and l:

For $i = 0, 1, 2, \ldots, N-1$, repeat: {
  Set $h = a_i^{(hi)}$ XOR $b_i^{(hi)}$, and $l = a_i^{(lo)}$ XOR $b_i^{(lo)}$.
  Set $c_i^{(hi)} = l$ OR (h XOR $a_i^{(lo)}$).
  Set $c_i^{(lo)} = h$ OR (l XOR $a_i^{(hi)}$).
}

The subtraction $a - b$ can be similarly handled:

For $i = 0, 1, 2, \ldots, N-1$, repeat: {
  Set $h = a_i^{(hi)}$ XOR $b_i^{(lo)}$, and $l = a_i^{(lo)}$ XOR $b_i^{(hi)}$.
  Set $c_i^{(hi)} = l$ OR (h XOR $a_i^{(lo)}$).
  Set $c_i^{(lo)} = h$ OR (l XOR $a_i^{(hi)}$).
}

Schoolbook multiplication handles three cases based on the multiplier coefficient b_j. If $b_j = 0$, nothing needs to be done. If $b_j = 1$, then $x^j b$ is added to a. Finally, if $b_j = 2$, then $x^j b$ is subtracted from a. We use the above addition and subtraction codes. Let us denote the k-th bit of a word u as $(u)_k$. Also, let LEFT-SHIFT$_3(b, k)$ denote the word-by-word left shift by k bits in both the high- and low-order arrays of b. Since the representation of 0 is $(1, 1)$, we assume that LEFT-SHIFT$_3$ packs the vacant positions with 1 bits. Right shifts are analogously defined.

Initialize $c_i^{(hi)} = c_i^{(lo)} = 111\ldots1 = 2^w - 1$ for $i = 0, 1, 2, \ldots 2N - 1$.
For $j = 0, 1, 2, \ldots, N - 1$, repeat: {
  For $k = 0, 1, 2, \ldots, w - 1$, repeat: {
    If $(b_j^{(hi)})_k = 0$ and $(b_j^{(lo)})_k = 1$, then: {
      Add LEFT-SHIFT$_3(b, k)$ to $(c_j^{(hi)}, \ldots, c_{j+N-1}^{(hi)}), (c_j^{(lo)}, \ldots, c_{j+N-1}^{(lo)})$.
      Add RIGHT-SHIFT$_3(b, w - k)$ to $(c_{j+1}^{(hi)}, \ldots, c_{j+N}^{(hi)}), (c_{j+1}^{(lo)}, \ldots, c_{j+N}^{(lo)})$.
    } else if $(b_j^{(hi)})_k = 1$ and $(b_j^{(lo)})_k = 0$, then: {
      Subtract LEFT-SHIFT$_3(b, k)$ from $(c_j^{(hi)}, \ldots, c_{j+N-1}^{(hi)}),(c_j^{(lo)}, \ldots, c_{j+N-1}^{(lo)})$.
      Subtract RIGHT-SHIFT$_3(b,w-k)$ from $(c_{j+1}^{(hi)}, \ldots, c_{j+N}^{(hi)}),(c_{j+1}^{(lo)}, \ldots, c_{j+N}^{(lo)})$.
    }
  }
}

---

21. Each bit array of an element of $\mathbb{F}_{3^{509}}$ requires $\lceil 509/64 \rceil = 8$ words. An intermediate product requires two bit arrays each with $\lceil 1017/64 \rceil = 16$ words. First, note that $-x^{64r-509}(-x^{318} - x^{191} + x^{127} + 1) = x^{64(r-3)+1} + x^{64(r-5)+2} - x^{64(r-6)+2} - x^{64(r-8)+3}$. Moreover, $-(-x^{318} - x^{191} + x^{127} + 1) = x^{4\times64+62} + x^{2\times64+63} - x^{1\times64+63} - 1$. In the following algorithm, we reduce an intermediate product c by the defining polynomial. We use Kawahara et al.'s formulas for addition and subtraction of word pairs. Here, LEFT-SHIFT$_3$ and RIGHT-SHIFT$_3$ are defined as in the solution of Exercise 2.20.

For $r = 15, 14, \ldots, 8$ (in that order), repeat: {
  Set $h = c_r^{(hi)}$, $l = c_r^{(lo)}$, and $c_r^{(hi)} = c_r^{(lo)} =$0xFFFFFFFFFFFFFFFF.
  Add (LEFT-SHIFT$_3(h, 1)$,LEFT-SHIFT$_3(l, 1)$) to $(c_{r-3}^{(hi)}, c_{r-3}^{(lo)})$.
  Add (RIGHT-SHIFT$_3(h, 63)$,RIGHT-SHIFT$_3(l, 63)$) to $(c_{r-2}^{(hi)}, c_{r-2}^{(lo)})$.
  Add (LEFT-SHIFT$_3(h, 2)$,LEFT-SHIFT$_3(l, 2)$) to $(c_{r-5}^{(hi)}, c_{r-5}^{(lo)})$.
  Add (RIGHT-SHIFT$_3(h, 62)$,RIGHT-SHIFT$_3(l, 62)$) to $(c_{r-4}^{(hi)}, c_{r-4}^{(lo)})$.
  Subtract (LEFT-SHIFT$_3(h, 2)$,LEFT-SHIFT$_3(l, 2)$) from $(c_{r-6}^{(hi)}, c_{r-6}^{(lo)})$.
  Subtract (RIGHT-SHIFT$_3(h, 62)$,RIGHT-SHIFT$_3(l, 62)$) from $(c_{r-5}^{(hi)}, c_{r-5}^{(lo)})$.
  Subtract (LEFT-SHIFT$_3(h, 3)$,LEFT-SHIFT$_3(l, 3)$) from $(c_{r-8}^{(hi)}, c_{r-8}^{(lo)})$.
  Subtract (RIGHT-SHIFT$_3(h, 61)$,RIGHT-SHIFT$_3(l, 61)$) from $(c_{r-7}^{(hi)}, c_{r-7}^{(lo)})$.
}
Set $h =$ RIGHT-SHIFT$_3(c_7^{(hi)}, 61)$, and $l =$ RIGHT-SHIFT$_3(c_7^{(lo)}, 61)$.

OR $c_7^{(hi)}$ and $c_7^{(lo)}$ with 0xE000000000000000.
Add (LEFT-SHIFT$_3(h, 62)$,LEFT-SHIFT$_3(l, 62)$) to $(c_4^{(hi)}, c_4^{(lo)})$.
Add (RIGHT-SHIFT$_3(h, 2)$,RIGHT-SHIFT$_3(l, 2)$) to $(c_5^{(hi)}, c_5^{(lo)})$.
Add (LEFT-SHIFT$_3(h, 63)$,LEFT-SHIFT$_3(l, 63)$) to $(c_2^{(hi)}, c_2^{(lo)})$.
Add (RIGHT-SHIFT$_3(h, 1)$,RIGHT-SHIFT$_3(l, 1)$) to $(c_3^{(hi)}, c_3^{(lo)})$.
Subtract (LEFT-SHIFT$_3(h, 63)$,LEFT-SHIFT$_3(l, 63)$) from $(c_1^{(hi)}, c_1^{(lo)})$.
Subtract (RIGHT-SHIFT$_3(h, 1)$,RIGHT-SHIFT$_3(l, 1)$) from $(c_2^{(hi)}, c_2^{(lo)})$.
Subtract (h, l) from $(c_0^{(hi)}, c_0^{(lo)})$.

---

22. The integers in the range 0 through $p^n - 1$ have unique n-digit p-ary representations. In order to do arithmetic on integers of these forms, we first need to unpack the operands and extract their p-ary digits. After the operation, we need to pack the p-ary digits back to an integer. I shortly illustrate the notion of packing and unpacking for the special cases $p = 2$ and $p = 3$.

The packing and unpacking overheads, if incurred frequently, adds non-negligible overhead to the arithmetic routines, and should be avoided. In short, this packed representation is not a very efficient way of storing field elements. There is, however, a small benefit of this packed representation. Suppose that we represent $\mathbb{F}_{p^n}$ as $\mathbb{F}_{p^{uv}} = \mathbb{F}_p(\theta, \psi)$, where θ is of degree u over $\mathbb{F}_p$, and ψ is of degree v over $\mathbb{F}_{p^u}$. Expanding an element $\alpha \in \mathbb{F}_{p^n}$ to the base p^u (identified with ψ) expresses α as an $\mathbb{F}_{p^u}$-linear combination of $1, \psi, \psi^2, \ldots, \psi^{v-1}$. Each coefficient in this expansion is an integer between 0 through $p^u - 1$, and stands for an element of $\mathbb{F}_{p^u}$ represented in base p. This construction works for an arbitrarily long tower of field extensions, and we do not require specialized complicated data structures for storing elements of any field in the tower.

If $p = 2$, the integer representing a field element stores the bits (coefficients of θ^i) in itself. There is no need for explicit packing and unpacking. Word-wise operations apply directly to the words of the operand integers.

For $p = 3$, the situation is different. Let an integer $\alpha \in \{0, 1, 2, \ldots, 3^n - 1\}$ stand for an element of $\mathbb{F}_{3^n} = \mathbb{F}_3(\theta)$ (for a suitable θ). The ternary digits of α are conceptually the coefficients of θ^i for $i = 0, 1, 2, \ldots, n - 1$. However, we have been using Kawahara et al.'s representation of elements of $\mathbb{F}_{3^n}$. Therefore, extracting the ternary digits of α needs to be followed by a conversion of the digit streams to two word arrays $\alpha^{(hi)}$ and $\alpha^{(lo)}$ of size $N = \lceil n/w \rceil$, where w is the number of bits per word. The unpacking procedure is described now.

Initialize $\alpha^{(hi)}$ and $\alpha^{(lo)}$ to strings of Nw one bits.
For $i = 0, 1, 2, \ldots, n - 1$, repeat: {
    Set $j = \lfloor i/w \rfloor$ (word index), and $k = i \text{ rem } w$ (bit index).
    Retrieve the next ternary coefficient as $c = \alpha \text{ rem } 3$.
    Delete c from α by setting $\alpha = \lfloor \alpha/3 \rfloor$.
    If $c = 1$, change the k-th bit of $\alpha_j^{(hi)}$ to 0,
    else if $c = 2$, change the k-th bit of $\alpha_j^{(lo)}$ to 0.
}

The packing procedure accepts $\alpha^{(hi)}$ and $\alpha^{(lo)}$ as input, and produces an integer $\alpha \in \{0, 1, 2, \ldots, 3^n - 1\}$ as output.

Initialize $\alpha = 0$.
For $j = N-1, N-2, \ldots, 1, 0$, repeat: {
  For $k = w-1, w-2, \ldots, 1, 0$, repeat: {
    Set $\alpha = 3\alpha$.
    If $(c_j^{(hi)})_k = 0$ and $(c_j^{(lo)})_k = 1$, set $\alpha = \alpha + 1$.
    else if $(c_j^{(hi)})_k = 1$ and $(c_j^{(lo)})_k = 0$, set $\alpha = \alpha + 2$.
  }
}

---

23. Addition: $O(n \log p)$.
Subtraction: $O(n \log p)$.
Raw multiplication (without reduction): $O(n^2 \log^2 p)$.
Reduction: $O(n^2 \log^2 p)$.
Euclidean gcd: $O(n^2 \log^2 p)$.

24. Let us represent elements of $\mathbb{F}_{p^n}$ in a basis $\beta_0, \beta_1, \ldots, \beta_{n-1}$. Take an element $\alpha = a_0\beta_0 + a_1\beta_1 + a_2\beta_2 + \cdots + a_{n-1}\beta_{n-1}$ with each $a_i \in \mathbb{F}_p$. We then have $a_i^p = a_i$ for all i. Therefore, $\alpha^p = a_0\beta_0^p + a_1\beta_1^p + a_2\beta_2^p + \cdots + a_{n-1}\beta_{n-1}^p$. If we precompute and store each β_i^p as an $\mathbb{F}_p$-linear combination of $\beta_0, \beta_1, \ldots, \beta_{n-1}$, computing α^p can be finished in $O(n^2)$ time.

If $\beta_0, \beta_1, \beta_2, \ldots, \beta_{n-1}$ constitute a normal basis of $\mathbb{F}_{p^n}$ over $\mathbb{F}_p$ with $\beta_i = \beta^{p^i}$, then we have $\beta_i^p = \beta_{(i+1) \operatorname{rem} n}$. Therefore, the p-th power exponentiation of $(a_0, a_1, \ldots, a_{n-1})$ is the cyclic shift $(a_{n-1}, a_0, a_1, \ldots, a_{n-2})$. That is, p-th power exponentiation with respect to a normal basis is very efficient.

25. **(a)** By Fermat's little theorem, $(\alpha^r)^{p-1} = 1$. Now, use Proposition 2.28.
(b) Since $\alpha^r \in \mathbb{F}_p$, its inverse $(\alpha^r)^{-1}$ is computed in the field $\mathbb{F}_p$. This involves integer arithmetic only, and can be efficiently done, particularly if p is small. Moreover, $\alpha^{r-1} = \alpha^{p+p^2+\cdots+p^{n-1}} = \alpha^p\alpha^{p^2}\cdots\alpha^{p^{n-1}}$. Since p-th power exponentiation is efficiently computable, one easily gets $\alpha^p, \alpha^{p^2} = (\alpha^p)^p, \alpha^{p^3} = (\alpha^{p^2})^p$, and so on. We finally need to multiply $(\alpha^r)^{-1}$ with α^{r-1}.

26. **(a)** Computing $(a_0 + a_1\theta)(b_0 + b_1\theta)$ involves the three $\mathbb{F}_q$-multiplications a_0b_0, a_1b_1 and $(a_0 + a_1)(b_0 + b_1)$. We have $(a_0 + a_1\theta)(b_0 + b_1\theta) = (a_0b_0) + ((a_0 + a_1)(b_0 + b_1) - a_0b_0 - a_1b_1)\theta + (a_1b_1)\theta^2$.
(b) We first write the input operands as $(a_0 + a_1\theta) + (a_2)\theta^2$ and $(b_0 + b_1\theta) + (b_2)\theta^2$. The first level of Karatsuba–Ofman multiplication involves computing the three products $(a_0 + a_1\theta)(b_0 + b_1\theta)$, a_2b_2 and $(a_0 + a_2 + a_1\theta)(b_0 + b_2 + b_1\theta)$, of which only one (a_2b_2) is an $\mathbb{F}_q$-multiplication. Applying a second level of Karatsuba–Ofman multiplication on $(a_0 + a_1\theta)(b_0 + b_1\theta)$ requires three $\mathbb{F}_q$-multiplications: a_0b_0, a_1b_1, and $(a_0 + a_1)(b_0 + b_1)$. Likewise, computing $(a_0 + a_2 + a_1\theta)(b_0 + b_2 + b_1\theta)$ involves three $\mathbb{F}_q$-multiplications: $(a_0 + a_2)(b_0 + b_2)$, a_1b_1, and $(a_0 + a_1 + a_2)(b_0 + b_1 + b_2)$. Finally, note that the product a_1b_1 appears

in both the second-level Karatsuba–Ofman multiplications, and needs to be computed only once.

(c) The first level of Karatsuba–Ofman multiplication involves three products of degree-one polynomials, each requiring three $\mathbb{F}_q$-multiplications in the second level.

(d) Let us write the input operands as $(a_0+a_1\theta+a_2\theta^2)+(a_3+a_4\theta)\theta^3$ and $(b_0+b_1\theta+b_2\theta^2)+(b_3+b_4\theta)\theta^3$. In the first level of Karatsuba–Ofman multiplication, we need the three products $(a_0+a_1\theta+a_2\theta^2)(b_0+b_1\theta+b_2\theta^2)$ (requiring six $\mathbb{F}_q$-multiplications by Part (b)), $(a_3+a_4\theta)(b_3+b_4\theta)$ (requiring three $\mathbb{F}_q$-multiplications by Part (a)), and $((a_0+a_3)+(a_1+a_4)\theta+a_2\theta^2)((b_0+b_3)+(b_1+b_4)\theta+b_2\theta^2)$ (requiring six $\mathbb{F}_q$-multiplications again by Part (b)). However, the $\mathbb{F}_q$-product a_2b_2 is commonly required in the first and the third of these three first-level products, and needs to be computed only once.

(e) The first level of Karatsuba–Ofman multiplication involves three products of degree-two polynomials, each requiring six $\mathbb{F}_q$-multiplications by Part (b).

27. By Fermat's little theorem, $\left(\alpha^{p^{n-1}}\right)^p = \alpha^{p^n} = \alpha$. If β is a p-th root of α, we have $\beta^p = \alpha$, that is, $\beta = \beta^{p^n} = (\beta^p)^{p^{n-1}} = \alpha^{p^{n-1}}$.

28. Write $\alpha = a_0 + a_1\theta + a_2\theta^2 + \cdots + a_{n-1}\theta^{n-1} = A_0(\theta^p) + \theta A_1(\theta^p) + \theta^2 A_2(\theta^p) + \cdots + \theta^{p-1}A_{p-1}(\theta^p)$, where $A_i(x) = a_i + a_{i+p}x + a_{i+2p}x^2 + \cdots$. But then, $\sqrt[p]{\alpha} = A_0(\theta) + \sqrt[p]{\theta}A_1(\theta) + \sqrt[p]{\theta^2}A_2(\theta) + \cdots + \sqrt[p]{\theta^{p-1}}A_{p-1}(\theta)$. We precompute $\sqrt[p]{\theta^i}$ for $i = 0, 1, 2, \ldots, p-1$. Extraction of the polynomials $A_i(\theta)$ is easy from the sequence $a_0, a_1, a_2, \ldots, a_{n-1}$.

29. Verify that $(x^{467} + x^{361} - x^{276} + x^{255} + x^{170} + x^{85})^3 \equiv x \pmod{f(x)}$, and $(-x^{234} + x^{128} - x^{43})^3 \equiv x^2 \pmod{f(x)}$.

30. Let us represent $\mathbb{F}_8 = \mathbb{F}_2(\theta)$, where $\theta^3 + \theta + 1 = 0$. The minimal polynomial is 0 is x, and that of 1 is $x+1$. The conjugates of θ are θ, θ^2 and $\theta^4 = \theta(\theta+1) = \theta^2 + \theta$. For all these three elements, the minimal polynomial is $x^3 + x + 1$. For the three remaining elements of $\mathbb{F}_8$ (that is, $\theta + 1, \theta^2 + 1, \theta^2 + \theta + 1$), the minimal polynomial is $x^3 + x^2 + 1$ (this is the only other cubic monic irreducible polynomial in $\mathbb{F}_2[x]$).

31. Computing modulo the polynomial $\theta^4 + \theta + 4$ gives:

$$
\begin{aligned}
\alpha &= 2\theta^3 + 3\theta + 4, \\
\alpha^5 &= 4\theta^3 + 4\theta^2 + 3, \\
\alpha^{25} &= 3\theta^2, \\
\alpha^{125} &= 4\theta^3 + 3\theta^2 + 2\theta + 3.
\end{aligned}
$$

Therefore, the minimal polynomial of α over $\mathbb{F}_5$ is

$$(x-\alpha)(x-\alpha^5)(x-\alpha^{25})(x-\alpha^{125}) = x^4 + 2x^2 + 3x + 1.$$

For β, we have the following calculations:

$$\beta = \theta^2 + 2\theta + 3,$$

$$\begin{aligned}
\beta^5 &= 3\theta^3 + 4\theta^2 + \theta + 4, \\
\beta^{25} &= 3\theta^3 + \theta^2 + 4, \\
\beta^{125} &= 4\theta^3 + 4\theta^2 + 2\theta + 1,
\end{aligned}$$

that is, the minimal polynomial of β over $\mathbb{F}_5$ is

$$(x - \beta)(x - \beta^5)(x - \beta^{25})(x - \beta^{125}) = x^4 + 3x^3 + 3x^2 + 4x + 1.$$

32. We represent $\mathbb{F}_{16}$ as $\mathbb{F}_2(\theta)$, where $\theta^4 + \theta + 1 = 0$. The order of the group $\mathbb{F}_{16}^*$ is 15, that is, every element $\alpha \in \mathbb{F}_{16}^*$ has order $1, 3, 5$, or 15. We have $\theta \neq 1$, $\theta^3 \neq 1$, and $\theta^5 = \theta(\theta + 1) = \theta^2 + \theta \neq 1$. Thus, θ is a primitive element of $\mathbb{F}_{16}$.

We claim that $\gamma = \theta^3$ is a normal element of $\mathbb{F}_{16}$. For the proof, note that

$$\begin{aligned}
\gamma &= \theta^3, \\
\gamma^2 &= \theta^6 = \theta^2(\theta + 1) = \theta^3 + \theta^2, \\
\gamma^4 &= \theta^6 + \theta^4 = \theta^4(\theta^2 + 1) = (\theta + 1)(\theta^2 + 1) = \theta^3 + \theta^2 + \theta + 1, \\
\gamma^8 &= \theta^6 + \theta^4 + \theta^2 + 1 = (\theta^2 + 1)(\theta + 1) + \theta^2 + 1 = \theta(\theta^2 + 1) = \theta^3 + \theta.
\end{aligned}$$

This means that

$$\begin{pmatrix} \gamma \\ \gamma^2 \\ \gamma^4 \\ \gamma^8 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 \\ \theta \\ \theta^2 \\ \theta^3 \end{pmatrix}.$$

The change-of-basis matrix has determinant one modulo 2, that is, the conjugates of γ are linearly independent over $\mathbb{F}_2$.

Since $\operatorname{ord}\theta = 15$, we have $\operatorname{ord}(\theta^3) = 15/\gcd(3, 15) = 5$, that is, θ^3 is not a primitive element of $\mathbb{F}_{16}$.

33. Represent $\mathbb{F}_{27} = \mathbb{F}_{3^3}$ as $\mathbb{F}_3(\theta)$, where $\theta^3 + 2\theta + 1 = 0$. The order of $\mathbb{F}_{27}^*$ is $27 - 1 = 2 \times 13$, that is, it suffices to compute α^2 and $\alpha^{13} = \alpha \times \alpha^4 \times \alpha^8$ in order to determine whether $\alpha \in \mathbb{F}_{27}^*$ is primitive. Let us take $\alpha = \theta$. We have

$$\begin{aligned}
\alpha^2 &= \theta^2, \\
\alpha^4 &= \theta^4 = \theta(\theta + 2) = \theta^2 + 2\theta, \\
\alpha^8 &= \theta^4 + 4\theta^3 + 4\theta^2 = (\theta + 1)(\theta + 2) + \theta^2 = 2\theta^2 + 2.
\end{aligned}$$

Therefore, $\theta^{13} = \theta^8 \times \theta^4 \times \theta = (2\theta^2 + 2)(\theta^2 + 2\theta)\theta$. Simplification using $\theta^3 = \theta + 2$ gives $\theta^{13} = 2$. Since $\theta^2 \neq 1$ and $\theta^{13} \neq 1$, we conclude that θ is a primitive element of $\mathbb{F}_{27}$.

We then claim that $\beta = \theta^2 + 2$ is a normal element of $\mathbb{F}_{27}$. To this effect, we compute:

$$\begin{aligned}
\beta &= \theta^2 + 2 \\
\beta^3 &= \theta^6 + 2 = (\theta + 2)^2 + 2 = \theta^2 + \theta, \\
\beta^9 &= \theta^6 + \theta^3 = \theta^3(\theta^3 + 1) = (\theta + 2)\theta = \theta^2 + 2\theta.
\end{aligned}$$

Therefore,

$$\begin{pmatrix} \beta \\ \beta^3 \\ \beta^9 \end{pmatrix} = \begin{pmatrix} 2 & 0 & 1 \\ 0 & 1 & 1 \\ 0 & 2 & 1 \end{pmatrix} \begin{pmatrix} 1 \\ \theta \\ \theta^2 \end{pmatrix}$$

The determinant of the transformation matrix is $2 \times (1-2) \equiv 1 \not\equiv 0 \pmod 3$.

But β is not a primitive element of $\mathbb{F}_{27}$, since we can show that $\beta^{13} = 1$.

34. Represent $\mathbb{F}_{25} = \mathbb{F}_5(\theta)$, where $\theta^2 + 2 = 0$. We now show that $\alpha = \theta + 1$ is a primitive normal element of $\mathbb{F}_{25}$.

The order of $\mathbb{F}_{25}^*$ is $24 = 2^3 \times 3$. It therefore suffices to show that $\alpha^{24/2} = \alpha^{12} \neq 1$ and $\alpha^{24/3} = \alpha^8 \neq 1$. We have

$$\begin{aligned} \alpha^2 &= \theta^2 + 2\theta + 1 = 2\theta + 4, \\ \alpha^4 &= 4\theta^2 + \theta + 1 = \theta + 3, \\ \alpha^8 &= \theta^2 + \theta + 4 = \theta + 2. \end{aligned}$$

Therefore, $\alpha^8 \neq 1$. Moreover, $\alpha^{12} = \alpha^8 \times \alpha^4 = (\theta+2)(\theta+3) = \theta^2+1 = 4 \neq 1$.

We now compute

$$\alpha^5 = \alpha \times \alpha^4 = (\theta+1)(\theta+3) = \theta^2 + 4\theta + 3 = 4\theta + 1.$$

It then follows that

$$\begin{pmatrix} \alpha \\ \alpha^5 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 4 \end{pmatrix} \begin{pmatrix} 1 \\ \theta \end{pmatrix}.$$

The determinant of the transformation matrix is $4 - 1 \not\equiv 0 \pmod 5$, that is, α is a normal element of $\mathbb{F}_{25}^*$.

35. We claim that 2 is a primitive element in $\mathbb{F}_{29}$. The size of $\mathbb{F}_{29}^*$ is $28 = 2^2 \times 7$, so it suffices to show that $2^{14} \not\equiv 1 \pmod{29}$ and $2^4 \not\equiv 1 \pmod{29}$. Since $29 \equiv 5 \pmod 8$, we have $\left(\frac{2}{29}\right) = -1$, and so by Euler's criterion, $2^{(29-1)/2} \equiv 2^{14} \equiv -1 \pmod{29}$. On the other hand, $2^4 \equiv 16 \not\equiv 1 \pmod{29}$.

36. **(a)** The monic linear irreducible polynomials over $\mathbb{F}_4$ are $x, x+1, x+\theta, x+\theta+1$. The products of any two (including repetition) of these polynomials are the reducible monic quadratic polynomials—there are ten of them: x^2, x^2+1, $x^2+\theta+1$, $x^2+\theta$, x^2+x, $x^2+\theta x$, $x^2+(\theta+1)x$, $x^2+(\theta+1)x+\theta$, $x^2+\theta x+(\theta+1)$, and x^2+x+1. The remaining six monic quadratic polynomials are irreducible: $x^2+x+\theta$, $x^2+x+(\theta+1)$, $x^2+\theta x+1$, $x^2+\theta x+\theta$, $x^2+(\theta+1)x+1$, and $x^2+(\theta+1)x+(\theta+1)$.

(b) Let us use the polynomial $x^2+x+\theta$ to represent $\mathbb{F}_{16}$. That is, $\mathbb{F}_{16} = \mathbb{F}_4(\psi)$, where $\psi^2 + \psi + \theta = 0$. Let us take two elements

$$\begin{aligned} \alpha &= (a_3\theta + a_2)\psi + (a_1\theta + a_0), \\ \beta &= (b_3\theta + b_2)\psi + (b_1\theta + b_0) \end{aligned}$$

in $\mathbb{F}_{16}$. The formula for their sum is simple:

$$\alpha + \beta = [(a_3+b_3)\theta + (a_2+b_2)]\psi + [(a_1+b_1)\theta + (a_0+b_0)].$$

The product involves reduction with respect to both θ and ψ.

$$\begin{aligned}
\alpha\beta &= [(a_3\theta+a_2)(b_3\theta+b_2)]\psi^2+[(a_3\theta+a_2)(b_1\theta+b_0)+(a_1\theta+a_0)(b_3\theta+b_2)]\psi+\\
&\quad [(a_1\theta+a_0)(b_1\theta+b_0)]\\
&= [(a_3b_3+a_3b_2+a_2b_3)\theta+(a_3b_3+a_2b_2)]\psi^2+\\
&\quad [(a_3b_1+a_3b_0+a_2b_1+a_1b_3+a_1b_2+a_0b_3)\theta+(a_3b_1+a_2b_0+a_1b_3+a_0b_2)]\psi+\\
&\quad [(a_1b_1+a_1b_0+a_0b_1)\theta+(a_1b_1+a_0b_0)]\\
&= [(a_3b_3+a_3b_2+a_2b_3)\theta+(a_3b_3+a_2b_2)](\psi+\theta)+\\
&\quad [(a_3b_1+a_3b_0+a_2b_1+a_1b_3+a_1b_2+a_0b_3)\theta+(a_3b_1+a_2b_0+a_1b_3+a_0b_2)]\psi+\\
&\quad [(a_1b_1+a_1b_0+a_0b_1)\theta+(a_1b_1+a_0b_0)]\\
&= \Big[(a_3b_3+a_3b_2+a_3b_1+a_3b_0+a_2b_3+a_2b_1+a_1b_3+a_1b_2+a_0b_3)\theta+\\
&\quad (a_3b_3+a_3b_1+a_2b_2+a_2b_0+a_1b_3+a_0b_2)\Big]\psi+\\
&\quad \Big[(a_3b_3+a_3b_2+a_2b_3)\theta^2+(a_3b_3+a_2b_2+a_1b_1+a_1b_0+a_0b_1)\theta+(a_1b_1+a_0b_0)\Big]\\
&= \Big[(a_3b_3+a_3b_2+a_3b_1+a_3b_0+a_2b_3+a_2b_1+a_1b_3+a_1b_2+a_0b_3)\theta+\\
&\quad (a_3b_3+a_3b_1+a_2b_2+a_2b_0+a_1b_3+a_0b_2)\Big]\psi+\\
&\quad \Big[(a_3b_2+a_2b_3+a_2b_2+a_1b_1+a_2b_0+a_0b_1)\theta+(a_3b_3+a_3b_2+a_2b_3+a_1b_1+a_0b_0)\Big]
\end{aligned}$$

(c) We have $|\mathbb{F}_{16}^*| = 15 = 3\times 5$, $\psi^3 = (\theta+1)\psi+\theta \neq 1$ and $\psi^5 = \theta \neq 1$, so ψ is a primitive element of $\mathbb{F}_{16}$.
(d) We have the following powers of $\gamma = (\theta+1)\psi+1$:

$$\begin{aligned}
\gamma &= (\theta+1)\psi+1,\\
\gamma^2 &= (\theta)\psi+(\theta),\\
\gamma^4 &= (\theta+1)\psi+(\theta),\\
\gamma^8 &= (\theta)\psi.
\end{aligned}$$

Thus, the minimal polynomial of γ over $\mathbb{F}_2$ is $(x+\gamma)(x+\gamma^2)(x+\gamma^4)(x+\gamma^8) = x^4+x^3+x^2+x+1$.
(e) The minimal polynomial of γ over $\mathbb{F}_4$ is $(x+\gamma)(x+\gamma^4) = (x+(\theta+1)\psi+1)(x+(\theta+1)\psi+\theta) = x^2+(\theta+1)x+1$.

37. (a) The conjugates of θ are

$$\begin{aligned}
&\theta,\\
&\theta^2,\\
&\theta^4,\\
&\theta^8 = \theta^2(\theta^3+1) = \theta^5+\theta^2,\\
&\theta^{16} = \theta^{10}+\theta^4 = \theta^4(\theta^3+1)+\theta^4 = \theta^7 = \theta^4+\theta, \text{ and}\\
&\theta^{32} = \theta^8+\theta^2 = \theta^2(\theta^3+1)+\theta^2 = \theta^5.
\end{aligned}$$

(b) It suffices to compute θ^h only for $h|63$. Now, $\theta \neq 1$, $\theta^3 \neq 1$, $\theta^7 = \theta(\theta^3+1) = \theta^4 + \theta \neq 1$, and $\theta^9 = \theta^3(\theta^3+1) = \theta^6 + \theta^3 = 1$. Therefore, the order of θ is 9, that is, θ is not a primitive element of $\mathbb{F}_{64}^*$.

Alternatively, by Part (a), $\theta^{32} = \theta^5$, that is, $\theta^{27} = 1$, that is, $\operatorname{ord}\theta$ divides 27 and so is smaller than $64 - 1 = 63$.

(c) We have $\theta^6 + \theta^3 + 1 = 0$, that is, $(\theta^3)^2 + (\theta^3) + 1 = 0$, that is, $f_{\theta^3,2}(x) = x^2 + x + 1$.

If you choose, you may go as computers would do, that is, write $\alpha = \theta^3$, and then show that $\alpha^2 = \theta^3 + 1$ and $\alpha^4 = \theta^6 + 1 = \theta^3 = \alpha$, so that $f_{\theta^3,2}(x) = (x-\alpha)(x-\alpha^2) = (x+\theta^3)(x+\theta^3+1) = x^2 + x + 1$.

38. **(a)** By construction, θ itself is a root of $x^2 + x + 2$. Its other root is $\theta^3 = -\theta(\theta+2) = -\theta^2 - 2\theta = \theta + 2 - 2\theta = -\theta + 2 = 2\theta + 2$.

(b) Since $x^2 + x + 2$ is irreducible over $\mathbb{Z}_3$, it has no roots modulo 3 and so no roots modulo $3^2 = 9$ too.

(c) The order of $\mathbb{F}_9^*$ is $9 - 1 = 8 = 2^3$. We have $\theta^4 = (\theta+2)^2 = \theta^2 + \theta + 1 = -\theta - 2 + \theta + 1 = -1 = 2 \neq 1$, that is, θ is a primitive element of $\mathbb{F}_9$.

(d) Suppose not. Then, it has one root α (in fact, both the roots) in $\mathbb{F}_9$, that is, $\theta = \alpha^2$. But then $\theta^4 = \alpha^8 = 1$ (since $\alpha \in \mathbb{F}_9^*$), that is, θ is not a primitive element of $\mathbb{F}_9$, a contradiction.

(e) We have $\psi^{16} = (\psi^2)^8 = \theta^8 = 1$, that is, ψ is not primitive in $\mathbb{F}_{81}$.

(f) The conjugates of ψ over $\mathbb{F}_3$ are ψ, $\psi^3 = \theta\psi$, $\psi^9 = \theta^3\psi^3 = \theta^4\psi = 2\psi$ and $\psi^{27} = 8\psi^3 = 2\theta\psi$. Therefore, the minimal polynomial of ψ over $\mathbb{F}_3$ is

$$\begin{aligned}
& (x-\psi)(x-\theta\psi)(x-2\psi)(x-2\theta\psi) \\
= \;& (x-\psi)(x+\psi)(x-\theta\psi)(x+\theta\psi) \\
= \;& (x^2-\psi^2)(x^2-\theta^2\psi^2) \\
= \;& (x^2-\theta)(x^2-\theta^3) \\
= \;& x^4 - (\theta+\theta^3)x^2 + \theta^4 \\
= \;& x^4 - (\theta+2\theta+2)x^2 + 2 = x^4 - 2x^2 + 2 = x^4 + x^2 + 2.
\end{aligned}$$

There are other ways of arriving at this polynomial. First, note that $\theta^2+\theta+2 = 0$ and $\psi^2 = \theta$. Combining these two equations gives $\psi^4 + \psi^2 + 2 = 0$, that is, ψ is a root of the polynomial $x^4 + x^2 + 2 \in \mathbb{F}_3[x]$. The degree of ψ (over $\mathbb{F}_3$) is four, so $x^4 + x^2 + 2$ has to be irreducible modulo 3. Finally, since ψ cannot satisfy two different monic irreducible polynomials in $\mathbb{F}_3[x]$ of degree four, the minimal polynomial of ψ over $\mathbb{F}_3$ has to be $x^4 + x^2 + 2$.

39. We have

$$\begin{aligned}
\gamma &= \theta + 1, \\
\gamma^2 &= \theta^2 + 1, \\
\gamma^4 &= \theta^4 + 1, \\
\gamma^8 &= \theta^8 + 1 = \theta^3(\theta^2+1) + 1 = \theta^5 + \theta^3 + 1 = \theta^3 + \theta^2, \\
\gamma^{16} &= \theta^6 + \theta^4 = \theta(\theta^2+1) + \theta^4 = \theta^4 + \theta^3 + \theta.
\end{aligned}$$

Therefore, $(\gamma \quad \gamma^2 \quad \gamma^4 \quad \gamma^8 \quad \gamma^{16})^{\mathrm{t}} = T\,(1 \quad \theta \quad \theta^2 \quad \theta^3 \quad \theta^4)^{\mathrm{t}}$, where T is the 5×5 transformation matrix whose determinant is

$$\begin{aligned}
&\begin{vmatrix} 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 \end{vmatrix} \\
\equiv &\begin{vmatrix} 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 \end{vmatrix} \ \text{(adding to the topmost row all of the remaining rows)} \\
\equiv &\begin{vmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 \end{vmatrix} \quad \text{(expanding about the topmost row)} \\
\equiv &\begin{vmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \end{vmatrix} \quad \text{(expanding about the leftmost column)} \\
\equiv &\begin{vmatrix} 0 & 1 \\ 1 & 0 \end{vmatrix} \quad \text{(expanding about the topmost row)} \\
\equiv &\ 1 \pmod 2.
\end{aligned}$$

Therefore, γ is a normal element of $\mathbb{F}_{32}$.

40. (a) As in Exercise 2.34, we represent $\mathbb{F}_{25} = \mathbb{F}_5(\theta)$ with $\theta^2+2 = 0$. We compute Zech logarithms to the primitive base $\alpha = \theta + 1$. First, we list powers of α.

i	0	1	2	3	4	5	6	7
α^i	1	$\theta+1$	$2\theta+4$	θ	$\theta+3$	$4\theta+1$	3	$3\theta+3$

i	8	9	10	11	12	13	14	15
α^i	$\theta+2$	3θ	$3\theta+4$	$2\theta+3$	4	$4\theta+4$	$3\theta+1$	4θ

i	16	17	18	19	20	21	22	23
α^i	$4\theta+2$	$\theta+4$	2	$2\theta+2$	$4\theta+3$	2θ	$2\theta+1$	$3\theta+2$

The Zech logarithm table for $\mathbb{F}_{25}$ follows.

i	0	1	2	3	4	5	6	7	8	9	10	11
z_i	18	8	21	1	17	16	12	10	4	14	9	2

i	12	13	14	15	16	17	18	19	20	21	22	23
z_i	–	15	23	5	20	3	6	11	13	22	19	7

(b) Represent $\mathbb{F}_{27} = \mathbb{F}_3(\theta)$ with $\theta^3 + 2\theta + 1 = 0$ as in Exercise 2.33, and compute Zech logarithms to the base θ.

i	0	1	2	3	4	5	6	7	8	9	10	11	12
z_i	13	9	21	1	18	17	11	4	15	3	6	10	2

i	13	14	15	16	17	18	19	20	21	22	23	24	25
z_i	–	16	25	22	20	7	23	5	12	14	24	19	8

(c) The Zech logarithms in $\mathbb{F}_{29}$ to the primitive base 2 are:

i	0	1	2	3	4	5	6	7	8	9	10	11	12	13
z_i	1	5	22	10	21	2	12	18	16	24	23	9	3	27

i	14	15	16	17	18	19	20	21	22	23	24	25	26	27
z_i	–	14	19	26	13	15	8	11	6	25	17	7	20	4

41. As in Exercise 2.32, we represent $\mathbb{F}_{16} = \mathbb{F}_2(\phi)$ with $\phi^4 + \phi + 1 = 0$. The representation of $\mathbb{F}_{16}$ in Exercise 2.36 is $\mathbb{F}_{16} = \mathbb{F}_2(\theta)(\psi)$, where $\theta^2 + \theta + 1 = 0$ and $\psi^2 + \psi + \theta = 0$. We need to compute the change-of-basis matrix from the polynomial basis $(1, \phi, \phi^2, \phi^3)$ to the composite basis $(1, \theta, \psi, \theta\psi)$. To that effect, we note that ϕ satisfies $x^4 + x + 1 = 0$, and obtain a root of this polynomial in the second representation. Squaring $\psi^2 + \psi + \theta = 0$ gives $\psi^4 + \psi^2 + \theta^2 = 0$, that is, $\psi^4 + (\psi^2 + \psi + \theta) + \psi + (\theta^2 + \theta) = 0$, that is, $\psi^4 + \psi + 1 = 0$. We consider the linear map μ taking ϕ to ψ, and obtain:

$$\begin{aligned}
\mu(1) &= 1, \\
\mu(\phi) &= \psi, \\
\mu(\phi^2) &= \psi^2 = \psi + \theta, \\
\mu(\phi^3) &= \psi(\psi + \theta) = \psi^2 + \psi\theta = \theta + \psi + \psi\theta.
\end{aligned}$$

Therefore, the change-of-basis matrix is

$$T = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 \end{pmatrix}$$

42. We iteratively find elements $\beta_0, \beta_1, \ldots, \beta_{n-1}$ to form an $\mathbb{F}_p$-basis of $\mathbb{F}_{p^n}$. Initially, any non-zero element of $\mathbb{F}_{p^n}$ can be taken as β_0, so the number of choices is $p^n - 1$. Now, suppose that i linearly independent elements $\beta_0, \beta_1, \ldots, \beta_{i-1}$ are chosen. The number of all possible $\mathbb{F}_p$-linear combinations of these i elements is exactly p^i. We choose any β_i which is not a linear combination of $\beta_0, \beta_1, \ldots, \beta_{i-1}$, that is, the number of choices for β_i is exactly $p^n - p^i$.

43. Consider the tower of extensions $\mathbb{F}_p \subseteq \mathbb{F}_p(\alpha) \subseteq \mathbb{F}_{p^n}$. Then, $d = \deg f_\alpha(x)$ is the $\mathbb{F}_p$-dimension of $\mathbb{F}_p(\alpha)$, whereas n is the $\mathbb{F}_p$-dimension of $\mathbb{F}_{p^n}$. Thus, $d|n$.

44. Both the parts follow from the following result.

Claim: Let $d = \gcd(m, n)$. Then, g decomposes in $\mathbb{F}_{2^m}[x]$ into a product of d irreducible polynomials each of degree n/d.

Proof Take any root $\alpha \in \overline{\mathbb{F}}_p$ of g. The conjugates of α over $\mathbb{F}_{p^m}$ are α, α^{p^m}, $\alpha^{(p^m)^2}, \ldots, \alpha^{(p^m)^{t-1}}$, where t is the smallest integer for which $\alpha^{(p^m)^t} = \alpha$. On the other hand, $\deg g = n$, and g is irreducible over $\mathbb{F}_p$, implying that $\alpha^{p^k} = \alpha$ if and only if k is a multiple of n. Therefore, $mt \equiv 0 \pmod{n}$. The smallest positive integral solution for t is n/d. That is, the degree of α over $\mathbb{F}_{p^m}$ is exactly n/d. Since this is true for any root of g, the claim is established. •

45. Let $f(x) = a_1x^{e_1} + a_2x^{e_2} + \cdots + a_tx^{e_t}$ with $e_1, e_2, \ldots, e_t \in \mathbb{N}_0$ distinct from one another, and with each $a_i \in \mathbb{F}_{p^n}^*$. Then, $f'(x) = a_1e_1x^{e_1-1} + a_2e_2x^{e_2-1} + \cdots + a_te_tx^{e_t-1}$, that is, $f'(x) = 0$ if and only if each e_i is divisible by p. Let us write $e_i = p\epsilon_i$ for $i = 1, 2, \ldots, t$. Moreover, by Fermat's little theorem, $a_i^{p^n} = a_i$ for all i. It then follows that $f(x) = g(x)^p$, where $g(x) = a_1^{p^{n-1}}x^{\epsilon_1} + a_2^{p^{n-1}}x^{\epsilon_2} + \cdots + a_t^{p^{n-1}}x^{\epsilon_t} \in \mathbb{F}_{p^n}[x]$.

46. We have $(x+\alpha)^q - (x+\alpha) = x^q + \alpha^q - x - \alpha = x^q - x$, since $\alpha^q = \alpha$ for all $\alpha \in \mathbb{F}_q$. But q is odd, so $(x+\alpha)^q - (x+\alpha) = (x+\alpha)((x+\alpha)^{(q-1)/2} - 1)$ $((x+\alpha)^{(q-1)/2} + 1)$.

47. For any $\alpha \in \mathbb{F}_q$, we have $\alpha^q = \alpha$, and so $(x+\alpha)^q + (x+\alpha) = x^q + \alpha^q + x + \alpha = x^q + x$. Let $g(x) = (x+\alpha) + (x+\alpha)^2 + (x+\alpha)^4 + \cdots + (x+\alpha)^{2^{n-1}}$. Then, $g(x)^2 = (x+\alpha)^2 + (x+\alpha)^4 + \cdots + (x+\alpha)^{2^{n-1}} + (x+\alpha)^{2^n}$, so $g(x)(g(x)+1) = g(x)^2 + g(x) = (x+\alpha)^{2^n} + (x+\alpha) = (x+\alpha)^q + (x+\alpha) = x^q + x$.

48. Let $q - 1 = p_1^{e_1}p_2^{e_2}\cdots p_t^{e_t}$ be the complete prime factorization of $q-1$. We then proceed as follows to compute the order h of $\alpha \in \mathbb{F}_q^*$.

Initialize $h = 1$.
For $i = 1, 2, \ldots, t$, repeat: {
    Let $r = (q-1)/p_i^{e_i}$, and compute $\beta = \alpha^r$.
    While $(\beta \neq 1)$, repeat: { Multiply h by p_i, and set $\beta = \beta^{p_i}$. }
}
Return h.

---

49. For any $\gamma \in \mathbb{F}_{p^n}^*$, the order $h = \operatorname{ord}\gamma$ divides $p^n - 1$. In particular, $p \nmid h$. Therefore, the order of γ^p is $h/\gcd(h,p) = h/1 = h$.

50. Take any primitive element γ of $\mathbb{F}_{p^n}$. By Exercise 2.49, all its n conjugates $\gamma, \gamma^p, \gamma^{p^2}, \ldots, \gamma^{p^{n-1}}$ have the same order, and are again primitive. Finally, there are $\phi(p^n - 1)$ primitive elements in $\mathbb{F}_{p^n}^*$.

51. By Fermat's little theorem, there exists exactly d solutions of $x^d = 1$ in $\mathbb{F}_q$ for any $d|(q-1)$ (use a proof as in Theorem 1.57). Therefore, for $i \in \{1, 2, \ldots, r\}$ and for $1 \leqslant u_i \leqslant e_i$, there are exactly $p_i^{u_i} - p_i^{u_i-1}$ elements of order exactly equal to $p_i^{u_i}$. On the other hand, there is a unique element of order p_i^0. Any element $\alpha \in \mathbb{F}_q^*$ can be decomposed uniquely as $\alpha = \alpha_1\alpha_2\cdots\alpha_r$ with order of α_i equal to $p_i^{u_i}$ for all i. But then, the order of α is $\prod_{i=1}^r p_i^{u_i}$, and there exist exactly $\prod_{i=1}^{r} \delta_i$ elements of $\mathbb{F}_q^*$ of this order, where $\delta_i = p_i^{u_i} - p_i^{u_i-1}$ if $u_i > 0$, or 1 if $u_i = 0$. It therefore follows that

$$\begin{aligned} \sum_{\alpha \in \mathbb{F}_q^*} \operatorname{ord} \alpha &= \sum_{u_1, u_2, \ldots, u_r} p_1^{u_1} p_2^{u_2} \cdots p_r^{u_r} \delta_1 \delta_2 \cdots \delta_r \\ &= \prod_{i=1}^{r} \left[1 + \sum_{u_i=1}^{e_i} (p_i^{2u_i} - p_i^{2u_i-1}) \right] = \prod_{i=1}^{r} \frac{p_i^{2e_i+1} + 1}{p_i + 1}. \end{aligned}$$

52. $\mathbb{F}_q^*$ contains exactly $(q-1)/2$ quadratic residues and exactly $(q-1)/2$ quadratic non-residues. If $\alpha = \beta^2$ (with $\beta \in \mathbb{F}_q^*$) is a quadratic residue, then $\alpha^{(q-1)/2} = \beta^{q-1} = 1$. Every element of $\mathbb{F}_q^*$ satisfies $x^{q-1} - 1 = (x^{(q-1)/2} - 1)(x^{(q-1)/2} + 1) = 0$, and the quadratic residues are roots of the first factor. Therefore, the quadratic non-residues α must satisfy $\alpha^{(q-1)/2} + 1 = 0$, that is, $\alpha^{(q-1)/2} = -1$.

53. If α is a t-th power residue, then $\beta^t = \alpha$ for some $\beta \in \mathbb{F}_q^*$. But then, $\alpha^{(q-1)/d} = (\beta^t)^{(q-1)/d} = (\beta^{q-1})^{t/d} = 1$ by Fermat's little theorem.

Proving the converse requires more effort. Let γ be a primitive element in $\mathbb{F}_q^*$. Then, an element γ^i is a t-th power residue if and only if $\gamma^i = (\gamma^y)^t$ for some y, that is, the congruence $ty \equiv i \pmod{q-1}$ is solvable for y, that is, $\gcd(t, q-1) | i$. Thus, the values of $i \in \{0, 1, 2, \ldots, q-2\}$ for which γ^i is a t-th power residue are precisely $0, d, 2d, \ldots, (\frac{q-1}{d} - 1)d$, that is, there are exactly $(q-1)/d$ t-th power residues in $\mathbb{F}_q^*$. All these t-th power residues satisfy $x^{(q-1)/d} = 1$. But then, since $x^{(q-1)/d} - 1$ cannot have more than $(q-1)/d$ roots, no t-th power non-residue can satisfy $x^{(q-1)/d} = 1$.

54. If $q = 2^n$, take $x = 0$ and $y = a^{2^{n-1}}$. So assume that q is odd, and write the given equation as $x^2 = \alpha - y^2$. As y ranges over all values in $\mathbb{F}_q$, the quantity y^2 ranges over a total of $(q+1)/2$ values (zero, and all the quadratic residues), that is, $\alpha - y^2$ too assumes $(q+1)/2$ distinct values. Not all these values can be quadratic non-residues, since there are only $(q-1)/2$ non-residues in $\mathbb{F}_q$.

55. If $\gcd(r, q-1) = 1$, then $ur + v(q-1) = 1$ for some $u, v \in \mathbb{Z}$, that is, $(\gamma^u)^r = \gamma$, that is, γ^u is a root of $x^r - \gamma$. Conversely, let $\delta \in \mathbb{F}_q^*$ satisfy $\delta^r = \gamma$. Let $e = \operatorname{ord} \delta$. But then, $q - 1 = \operatorname{ord} \gamma = e / \gcd(e, r)$. Moreover, $e | (q-1)$. So we must have $e = q - 1$ and $\gcd(e, r) = 1$, that is, $\gcd(r, q-1) = 1$.

56. Suppose that there is an isomorphism $\mu : \mathbb{Q}(\sqrt{2}) \to \mathbb{Q}(\sqrt{3})$. Let $\mu(\sqrt{2}) = a + b\sqrt{3}$ with $a, b \in \mathbb{Q}$. If $b = 0$, then $\mu(a) = \mu(\sqrt{2}) = a$, violating that μ is injective, so $b \neq 0$. But then, $2 = \mu(2) = \mu(\sqrt{2})^2 = (a + b\sqrt{3})^2 = (a^2 + 3b^2) + 2ab\sqrt{3}$. Since $b \neq 0$, we must have $a = 0$, that is, $3b^2 = 2$, that is, $b = \sqrt{2/3}$, a contradiction to the fact that b is rational.

57. Take $F = \mathbb{Q}$, and $f(x) = x^2 + 1$. The two roots of f are $\theta = \mathrm{i}$ and $\psi = -\mathrm{i}$. Since $-\mathrm{i} \in \mathbb{Q}(\mathrm{i})$ and $\mathrm{i} \in \mathbb{Q}(-\mathrm{i})$, we have $\mathbb{Q}(\theta) = \mathbb{Q}(\psi)$ in this case.

Now, take $F = \mathbb{Q}$ and $f(x) = x^3 - 2$. The three roots of f are $\theta = \sqrt[3]{2}, \psi = \sqrt[3]{2}\omega$, and $\phi = \sqrt[3]{2}\omega^2$, where $\sqrt[3]{2}$ is the real cube root of 2, and $\omega = \frac{1+\mathrm{i}\sqrt{3}}{2}$ is a primitive third root of unity. We have $\mathbb{Q}(\theta) \subseteq \mathbb{R}$ and $\mathbb{Q}(\psi) \not\subseteq \mathbb{R}$, that is, these two extensions, although isomorphic, are distinct as sets.

58. **(a)** Let t be the smallest positive integer for which $\alpha^{p^t} = \alpha$. The minimal polynomial $f_\alpha(x) \in \mathbb{F}_p[x]$ of α is of degree t, and t divides n. Therefore,

$$(x-\alpha)(x-\alpha^p)(x-\alpha^{p^2})\cdots(x-\alpha^{p^{n-1}}) = f_\alpha(x)^{n/t} \in \mathbb{F}_p[x].$$

Now, observe that $\mathrm{Tr}(\alpha)$ is the negative of the coefficient of x^{n-1}, and $\mathrm{N}(\alpha)$ is $(-1)^n$ times the constant term in $f_\alpha(x)^{n/t}$.

(b) If $\alpha \in \mathbb{F}_p$, then $\alpha^{p^i} = \alpha$ for all $i \in \mathbb{N}_0$.

(c) For any $\alpha, \beta \in \mathbb{F}_{p^n}$ and for any $i \in \mathbb{N}_0$, we have $(\alpha+\beta)^{p^i} = \alpha^{p^i} + \beta^{p^i}$, and $(\alpha\beta)^{p^i} = \alpha^{p^i}\beta^{p^i}$.

(d) If $\alpha = \gamma^p - \gamma$, then by additivity of the trace function, we have $\mathrm{Tr}(\alpha) = \mathrm{Tr}(\gamma^p) - \mathrm{Tr}(\gamma) = (\gamma^p + \gamma^{p^2} + \gamma^{p^3} + \cdots + \gamma^{p^n}) - (\gamma + \gamma^p + \gamma^{p^2} + \cdots + \gamma^{p^{n-1}}) = 0$, since $\gamma^{p^n} = \gamma$ by Fermat's little theorem.

Conversely, suppose that $\mathrm{Tr}(\alpha) = 0$. It suffices to show that the polynomial $x^p - x - \alpha$ has at least one root in $\mathbb{F}_{p^n}$. Since $x^{p^n} - x$ is the product of all monic linear polynomials in $\mathbb{F}_{p^n}[x]$, the number of roots of $x^p - x - \alpha$ is the degree of the gcd of $x^p - x - \alpha$ with $x^{p^n} - x$. In order to compute this gcd, we compute $x^{p^n} - x$ modulo $x^p - x - \alpha$. But $x^p \equiv x + \alpha \pmod{x^p - x - \alpha}$, so

$$\begin{aligned}
x^{p^n} - x &\equiv (x+\alpha)^{p^{n-1}} - x \\
&\equiv x^{p^{n-1}} + \alpha^{p^{n-1}} - x \\
&\equiv (x+\alpha)^{p^{n-2}} + \alpha^{p^{n-1}} - x \\
&\equiv x^{p^{n-2}} + \alpha^{p^{n-2}} + \alpha^{p^{n-1}} - x \\
&\equiv \cdots \\
&\equiv x + \alpha + \alpha^p + \alpha^{p^2} + \cdots + \alpha^{p^{n-2}} + \alpha^{p^{n-1}} - x \\
&\equiv \mathrm{Tr}(\alpha) \\
&\equiv 0 \pmod{x^p - x - \alpha}.
\end{aligned}$$

Therefore, $\gcd(x^p - x - \alpha, x^{p^n} - x) = x^p - x - \alpha$, that is, $\alpha = \gamma^p - \gamma$ for p distinct elements of $\mathbb{F}_{p^n}$.

59. **(a)** This is the same as Exercise 2.58(d) for $p = 2$.

(b) Let $\gamma = \alpha^{2^1} + \alpha^{2^3} + \alpha^{2^5} + \cdots + \alpha^{2^{n-2}}$. Then, $\gamma^2 = \alpha^{2^2} + \alpha^{2^4} + \alpha^{2^6} + \cdots + \alpha^{2^{n-1}}$, so $\gamma^2 + \gamma = \alpha^2 + \alpha^{2^2} + \alpha^{2^3} + \cdots + \alpha^{p^{n-1}} = \mathrm{Tr}(\alpha) + \alpha = \alpha$. The sum of the two roots of $x^2 + x + \alpha$ is 1, so the other solution of $x^2 + x = \alpha$ is $\gamma + 1$.

(c) Rewrite the equation as $x^2 + \frac{b}{a}x + \frac{c}{a} = 0$. Substitute $x = \frac{b}{a}y$ to get $(\frac{b}{a})^2y^2 + (\frac{b}{a})^2y + \frac{c}{a} = 0$, that is, $y^2 + y = \alpha$, where $\alpha = \frac{ca}{b^2}$. By Part (a), this equation is solvable if and only if $\mathrm{Tr}(\alpha) = 0$. If so, the solutions for y are γ and $\gamma + 1$ (see Part (b)). Thus, the solutions for x are $x = \frac{b}{a}\gamma$ and $\frac{b}{a}(\gamma + 1)$.

60. **(a)** If $\alpha = \gamma^{2k}$, then $x^2 = \alpha$ has a solution $x = \gamma^k$. Conversely, if $x^2 = \alpha$ has a solution $\beta = \gamma^k$, then $\alpha = \beta^2 = \gamma^{2k} = \gamma^{(2k) \operatorname{rem} (q-1)}$. Since q is odd, $(2k) \operatorname{rem} (q-1)$ is even.

(b) If k is even, then $l = k/2$. If k is odd, then $l = [k + (q-1)]/2$. Another (less efficient) formula is $l \equiv kq/2 \pmod{q-1}$.

61. **(a)** Let $\theta_0, \theta_1, \ldots, \theta_{n-1}$ constitute an $\mathbb{F}_p$-basis of $\mathbb{F}_{p^n}$. Let A_i denote the i-th column of A (for $i = 0, 1, 2, \ldots, n-1$). Suppose that $a_0 A_0 + a_1 A_1 + \cdots + a_{n-1} A_{n-1} = 0$. Let $\alpha = a_0\theta_0 + a_1\theta_1 + \cdots + a_{n-1}\theta_{n-1}$. Since $a_i^p = a_i$ for all i, we then have $a_0 \operatorname{Tr}(\theta_i\theta_0) + a_1 \operatorname{Tr}(\theta_i\theta_1) + \cdots + a_{n-1} \operatorname{Tr}(\theta_i\theta_{n-1}) = \operatorname{Tr}(\theta_i(a_0\theta_0 + a_1\theta_1 + \cdots + a_{n-1}\theta_{n-1})) = \operatorname{Tr}(\theta_i\alpha) = 0$ for all i. Since $\theta_0, \theta_1, \ldots, \theta_{n-1}$ constitute a basis of $\mathbb{F}_{p^n}$ over $\mathbb{F}_p$, it follows that $\operatorname{Tr}(\beta\alpha) = 0$ for all $\beta \in \mathbb{F}_{p^n}$. If $\alpha \neq 0$, this in turn implies that $\operatorname{Tr}(\gamma) = 0$ for all $\gamma \in \mathbb{F}_{p^n}$. But the polynomial $x + x^p + x^{p^2} + \cdots + x^{p^{n-1}}$ can have at most p^{n-1} roots. Therefore, we must have $\alpha = 0$. But then, by the linear independence of $\theta_0, \theta_1, \ldots, \theta_{n-1}$, we conclude that $a_0 = a_1 = \cdots = a_{n-1} = 0$, that is, the columns of A are linearly independent, that is, $\Delta(\theta_0, \theta_1, \ldots, \theta_{n-1}) \neq 0$.

Conversely, if $\theta_0, \theta_1, \ldots, \theta_{n-1}$ are linearly dependent, then $a_0\theta_0 + a_1\theta_1 + \cdots + a_{n-1}\theta_{n-1} = 0$ for some $a_0, a_1, \ldots, a_{n-1} \in \mathbb{F}_p$, not all zero. But then, for all $i \in \{0, 1, 2, \ldots, n-1\}$, we have $a_0\theta_i\theta_0 + a_1\theta_i\theta_1 + \cdots + a_{n-1}\theta_i\theta_{n-1} = 0$, that is, $a_0 \operatorname{Tr}(\theta_i\theta_0) + a_1 \operatorname{Tr}(\theta_i\theta_1) + \cdots + a_{n-1} \operatorname{Tr}(\theta_i\theta_{n-1}) = 0$, that is, the columns of A are linearly dependent, that is, $\Delta(\theta_0, \theta_1, \ldots, \theta_{n-1}) = 0$.

(b) The (i,j)-th entry of $B^{\mathrm{t}}B$ is $\theta_i\theta_j + \theta_i^p\theta_j^p + \cdots + \theta_i^{p^{n-1}}\theta_j^{p^{n-1}} = \operatorname{Tr}(\theta_i\theta_j)$. Finally, note that $\det A = (\det B)^2$.

(c) Consider the van der Monde matrix

$$V(\lambda_0, \lambda_1, \ldots, \lambda_{n-1}) = \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ \lambda_0 & \lambda_1 & \lambda_2 & \cdots & \lambda_{n-1} \\ \lambda_0^2 & \lambda_1^2 & \lambda_2^2 & \cdots & \lambda_{n-1}^2 \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ \lambda_0^{n-1} & \lambda_1^{n-1} & \lambda_2^{n-1} & \cdots & \lambda_{n-1}^{n-1} \end{pmatrix}.$$

If $\lambda_i = \lambda_j$, the determinant of this matrix is 0. It therefore follows that

$$\det V(\lambda_0, \lambda_1, \ldots, \lambda_{n-1}) = \pm \prod_{0 \leqslant i < j \leqslant n-1} (\lambda_i - \lambda_j).$$

If we take $\theta_i = \theta^i$ in Part (b), we see that $B^{\mathrm{t}} = V(\theta, \theta^p, \theta^{p^2}, \ldots, \theta^{p^{n-1}})$. Finally, $\det B = \det B^{\mathrm{t}}$, and $\det A = (\det B)^2$.

62. The following function inverts $a(x) \in \mathbb{F}_2[x]$ modulo $f(x) \in \mathbb{F}_2[x]$.

```
EucInv2(a,f) = \
   r2 = Mod(1,2) * f; r1 = Mod(1,2) * a; \
   v2 = Mod(0,2); v1 = Mod(1,2); \
   while (poldegree(r1) > 0, \
      r = r2 % r1; q = (r2 - r) / r1; v = v2 - q * v1;
      r2 = r1; r1 = r; v2 = v1; v1 = v; \
   ); \
   return(lift(v1))

EucInv2(x^6+x^3+x^2+x, x^7+x^3+1)
```

63. The binary inverse algorithm for inverting a modulo f follows.

```
BinInv2(a,f) = \
   r1 = Mod(1,2) * a; r2 = Mod(1,2) * f; u1 = Mod(1,2); u2 = Mod(0,2); \
   while (1, \
      while(polcoeff(r1,0)==Mod(0,2), \
         r1 = r1 / (Mod(1,2) * x); \
         if (polcoeff(u1,0) == Mod(1,2), u1 = u1 + f); \
         u1 = u1 / (Mod(1,2) * x); \
         if (poldegree(r1) == 0, return(lift(u1))); \
      ); \
      while(polcoeff(r2,0)==Mod(0,2), \
         r2 = r2 / (Mod(1,2) * x); \
         if (polcoeff(u2,0) == Mod(1,2), u2 = u2 + f); \
         u2 = u2 / (Mod(1,2) * x); \
         if (poldegree(r2) == 0, return(lift(u2))); \
      ); \
      if (poldegree(r1) >= poldegree(r2), \
         r1 = r1 + r2; u1 = u1 + u2, \
         r2 = r2 + r1; u2 = u2 + u1 \
      ) \
   )

BinInv2(x^6+x^3+x^2+x, x^7+x^3+1)
```

64. In the following code, we first write a function to remove k factors of x from u modulo f. This does not take into account any special form of the defining polynomial f. The function for inverting a modulo f follows this function.

```
rmx2(u,k,f) = \
  while (k > 0, \
     if (polcoeff(u,0) == Mod(1,2), u = u + f); \
     u = u / (Mod(1,2) * x); k--; \
  ); \
  return(lift(u))

AlmInv2(a,f) = \
   k = 0; \
   r1 = Mod(1,2) * a; r2 = Mod(1,2) * f; \
   u1 = Mod(1,2); u2 = Mod(0,2); \
   while (1, \
      while(polcoeff(r1,0)==Mod(0,2), \
         k++; r1 = r1 / (Mod(1,2) * x); u2 = u2 * (Mod(1,2) * x); \
         if (poldegree(r1) == 0, return(rmx2(u1,k,f))); \
      ); \
      while(polcoeff(r2,0)==Mod(0,2), \
         k++; r2 = r2 / (Mod(1,2) * x); u1 = u1 * (Mod(1,2) * x); \
         if (poldegree(r2) == 0, return(rmx2(u2,k,f))); \
      ); \
      if (poldegree(r1) >= poldegree(r2), \
         r1 = r1 + r2; u1 = u1 + u2, \
         r2 = r2 + r1; u2 = u2 + u1 \
      ) \
   )
```

```
AlmInv2(x^6+x^3+x^2+x, x^7+x^3+1)
```

65. The following GP/PARI function accepts as input the element $a(x)$ that we want to invert, the characteristic p, and the defining polynomial $f(x)$. The extension degree is obtained from f.

```
EucInv(a,p,f) = \
   r2 = Mod(1,p) * f; r1 = Mod(1,p) * a; \
   v2 = Mod(0,p); v1 = Mod(1,p); \
   while (poldegree(r1) > 0, \
      r = r2 % r1; q = (r2 - r) / r1; \
      v = v2 - q * v1; \
      r2 = r1; r1 = r; v2 = v1; v1 = v; \
   ); \
   return(lift(v1/polcoeff(r1,0)))

EucInv(x^6+x^3+x^2+x, 2, x^7+x^3+1)
EucInv(9*x^4+7*x^3+5*x^2+3*x+2, 17, x^5+3*x^2+5)
```

66. The following GP/PARI function accepts as input the element $a(x)$ that we want to invert, the characteristic p, and the defining polynomial $f(x)$.

```
BinInv(a,p,f) = \
   local(r1,r2,u1,u2); \
   r1 = Mod(1,p) * a; r2 = Mod(1,p) * f; \
   u1 = Mod(1,p); u2 = Mod(0,p); \
   while (1, \
      while(polcoeff(r1,0)==Mod(0,p), \
         r1 = r1 / (Mod(1,p) * x); \
         if (polcoeff(u1,0) != Mod(0,p), \
            u1 = u1 - (polcoeff(u1,0) / polcoeff(f,0)) * f \
         ); \
         u1 = u1 / (Mod(1,p) * x); \
         if (poldegree(r1) == 0, return(lift(u1/polcoeff(r1,0)))); \
      ); \
      while(polcoeff(r2,0)==Mod(0,p), \
         r2 = r2 / (Mod(1,p) * x); \
         if (polcoeff(u2,0) != Mod(0,p), \
            u2 = u2 - (polcoeff(u2,0) / polcoeff(f,0)) * f
         ); \
         u2 = u2 / (Mod(1,p) * x); \
         if (poldegree(r2) == 0, return(lift(u2/polcoeff(r2,0)))); \
      ); \
      if (poldegree(r1) >= poldegree(r2), \
         c = polcoeff(r1,0)/polcoeff(r2,0); r1 = r1 - c*r2; u1 = u1 - c*u2, \
         c = polcoeff(r2,0)/polcoeff(r1,0); r2 = r2 - c*r1; u2 = u2 - c*u1 \
      ) \
   )
```

A couple of calls of this function follow.

```
BinInv(x^6+x^3+x^2+x, 2, x^7+x^3+1)
BinInv(9*x^4+7*x^3+5*x^2+3*x+2, 17, x^5+3*x^2+5)
```

67. First, we need a function to remove the desired (k) factors of x from a polynomial u modulo the defining polynomial f. Let p be the characteristic of the field, and a the element to be inverted.

```
rmx(u,k,p,f) = \
   while (k > 0, \
      if (polcoeff(u,0) != Mod(0,p), \
         c = polcoeff(u,0) / polcoeff(f,0); \
         u = u - c * f; \
      ); \
      u = u / (Mod(1,p) * x); k--; \
   ); \
   return(lift(u))

AlmInv(a,p,f) = \
   k = 0; \
   r1 = Mod(1,p) * a; r2 = Mod(1,p) * f; u1 = Mod(1,p); u2 = Mod(0,p); \
   while (1, \
      while(polcoeff(r1,0)==Mod(0,p), \
         k++; \
         r1 = r1 / (Mod(1,p) * x); u2 = u2 * (Mod(1,p) * x); \
         if (poldegree(r1) == 0, return(rmx(u1/polcoeff(r1,0),k,p,f))); \
      ); \
      while(polcoeff(r2,0)==Mod(0,p), \
         k++; \
         r2 = r2 / (Mod(1,p) * x); u1 = u1 * (Mod(1,p) * x); \
         if (poldegree(r1) == 0, return(rmx(u2/polcoeff(r2,0),k,p,f))); \
      ); \
      if (poldegree(r1) >= poldegree(r2), \
         c = polcoeff(r1,0) / polcoeff(r2,0); r1 = r1 - c*r2; u1 = u1 - c*u2, \
         c = polcoeff(r2,0) / polcoeff(r1,0); r2 = r2 - c*r1; u2 = u2 - c*u1 \
      ) \
   )

AlmInv(x^6+x^3+x^2+x, 2, x^7+x^3+1)
AlmInv(9*x^4+7*x^3+5*x^2+3*x+2, 17, x^5+3*x^2+5)
```

68. We now rewrite the function `isnormal` so that it takes two arguments: the element a in the field, and the defining polynomial f.

```
isnormal(a,f) = \
   n = poldegree(f); \
   M = matrix(n,n); \
   for (i=1,n, \
      for (j=0,n-1, M[i,j+1] = polcoeff(a,j)); \
      a = (a^2) % f; \
   ); \
   if(matdet(M)==Mod(1,2), print("normal");1, print("not normal");0)
```

69. First, we write two functions for computing the trace and the norm of $a \in \mathbb{F}_{p^n}$. The characteristic p and the defining polynomial f are also passed to these functions. The extension degree n is determined from f.

```
abstrace(p,f,a) = \
   local(n,s,u); \
   f = Mod(1,p) * f; \
   a = Mod(1,p) * a; \
   n = poldegree(f); \
   s = u = a; \
   for (i=1,n-1, \
      u = lift(Mod(u,f)^p); \
      s = s + u; \
   ); \
   return(lift(s));

absnorm(p,f,a) = \
   local(n,t,u); \
   f = Mod(1,p) * f; \
   a = Mod(1,p) * a; \
   n = poldegree(f); \
   t = u = a; \
   for (i=1,n-1, \
      u = lift(Mod(u,f)^p); \
      t = (t * u) % f; \
   ); \
   return(lift(t));
```

The following statements print the traces and norms of all elements of $\mathbb{F}_{64} = \mathbb{F}_2(\theta)$, where $\theta^6 + \theta + 1 = 0$.

```
f = x^6 + x + 1;
p = 2;
for (i=0,63, \
   a = 0; t = i; \
   for (j=0, 5, c = t % 2; a = a + c * x^j; t = floor(t/2)); \
   print("a = ", a, ", Tr(a) = ", abstrace(p,f,a), ", N(a) = ", absnorm(p,f,a)) \
)
```