Review/Outline

Frobenius automorphisms

Other roots of equations

Counting irreducibles

Counting primitive polynomials

Finding equation with given root

Irreducible binary quintics

Counting irreducibles

Theorem: Let p be prime. Fix a degree d. The number of irreducible **monic** (=leading coefficient 1) polynomials of degree d in $\mathbf{F}_p[x]$ is

$$\frac{p^d - \sum_{q|d} p^{d/q} + \sum_{q_1,q_2|d} p^{d/q_1 q_2} - \dots}{d}$$

where $q_1, q_2, \dots$ are *distinct* primes dividing d.

That is, let Q be the set of *distinct* prime factors of d, and $|Q|$ the number of elements in Q. Then the number of irreducibles of degree d is

$$\frac{1}{d} \cdot \sum_{i=0}^{|Q|} (-1)^i \sum_{q_1 < \dots < q_i} p^{d/q_1 \dots q_i}$$

where $\{q_1, \dots, q_i\}$ is summed over i-element subsets of Q.

For example, in some simple cases:
degree d prime:

$$\frac{p^d - p}{d}$$

$d = qr$ with q, r distinct primes:

$$\frac{p^{qr} - p^q - p^r + p}{qr}$$

$d = abc$ with a, b, c distinct primes:

$$\frac{p^{abc} - p^{ab} - p^{ac} - p^{bc} + p^a + p^b + p^c - p}{abc}$$

For $d = q^2$ with q prime:

$$\frac{p^{q^2} - p^q}{q^2}$$

for $d = q^3$ with q prime:

$$\frac{p^{q^3} - p^{q^2}}{q^3}$$

for $d = q^4$ with q prime:

$$\frac{p^{q^4} - p^{q^3}}{q^3}$$

Example: Find the number of irreducibles of degree 60 in $\mathbf{F}_2[x]$. By trial division, $60 = 2^2 \cdot 3 \cdot 5$, so the list of primes dividing 60 is $2, 3, 5$. Thus, by the theorem, with $p = 2$, $d = 60$, and $Q = \{2, 3, 5\}$, the number of irreducibles of degree 60 is

$$\frac{1}{60} \cdot \Big(2^{60} - 2^{60/2} - 2^{60/3} - 2^{60/5}$$

$$+2^{60/6} + 2^{60/10} + 2^{60/15} - 2^{60/30}\Big)$$

$$= 19,215,358,392,200,893$$

Euler's φ-function

Euler's φ-function, or **totient** function is

$$\varphi(n) = \text{no. } t \text{ with } 1 \leq t \leq n \text{ and } \gcd(t, n) = 1$$

Do *not* evaluate $\varphi(n)$ by enumeration, but, instead, use

Theorem: Let

$$n = p_1^{e_1} \dots p_t^{e_t}$$

be the factorization of n into primes, with $p_1 < \dots < p_t$ and all $e_i \geq 1$. Then

$$\varphi(n) = (p_1 - 1)p_1^{e_1 - 1} \dots (p_t - 1)p_t^{e_t - 1}$$

Examples:

$$\varphi(10) = \varphi(2 \cdot 5) = (2 - 1) \cdot (5 - 1) = 4$$

$$\varphi(12) = \varphi(2^2 \cdot 3) = (2 - 1)2 \cdot (3 - 1) = 4$$

$$\varphi(15) = \varphi(3 \cdot 5) = (3 - 1) \cdot (5 - 1) = 8$$

$$\varphi(30) = \varphi(2 \cdot 3 \cdot 5) = (2 - 1) \cdot (3 - 1) \cdot (5 - 1) = 8$$

$$\varphi(100) = \varphi(2^2 \cdot 5^2) = (2 - 1)2 \cdot (5 - 1)5 = 40$$

Counting primitives

Theorem: Let q be a prime power. Fix a degree d. The number of *primitive monic* degree d polynomials in $\mathbf{F}_q[x]$ is

$$\frac{\varphi(q^d - 1)}{d}$$

Example: To count primitive monic degree 10 polynomials in $\mathbf{F}_2[x]$, in the theorem $d = 10$ and $q = 2$, factor $2^{10} - 1$ by trial division

$$2^{10} - 1 = 1023 = 3 \cdot 11 \cdot 31$$

$$\text{no. prim. } 10^{\text{th}} \text{ deg} = \frac{\varphi(2^{10} - 1)}{10}$$

$$= \frac{(3-1)(11-1)(31-1)}{10} = 60$$

using also the formula for Euler's φ-function.

Remark: Note that (from the theorem) there are $(2^{10} - 2^5 - 2^2 + 2)/10 = 99$ irreducibles of degree 10.

Finding equations with specified root(s)

Another application of the *Frobenius automorphism* of finite fields.

Fix a prime p, an irreducible cubic $P(x)$ in $\mathbf{F}_p[x]$, and let

$$\alpha = x\text{-mod-}P(x)$$

Recall that $P(\alpha) = 0$.

Every element β of the field

$$\mathbf{F}_{p^3} = GF(p^3) \approx \mathbf{F}_p[x]/P(x)$$

is uniquely representable in the reduced form

$$\beta = a \cdot \alpha^2 + b \cdot \alpha + c$$

with $a, b, c \in \mathbf{F}_p$. If $a = b = 0$, then $\beta = c \in \mathbf{F}_p$.

Let $\beta = a \cdot \alpha^2 + b \cdot \alpha + c$ with not both a and b zero.

Problem: Find the (cubic) equation $Y^3 + AY^2 + BY + C = 0$ of which β is a root, with $A, B, C \in \mathbf{F}_p$.

That is, find $A, B, C \in \mathbf{F}_p$ such that β is a root of that equation.

We know, or at least believe, that the complete list of roots of the equation of which β is a root is

$$\beta,\ \beta^p,\ \beta^{p^2}$$

These are not reduced expressions, however, so it is moderately inconvenient to manipulate them as they stand.

And if distinct elements r, s, t are roots of a monic equation, then the equation is

$$(Y - r)(Y - s)(Y - t) = 0$$

Multiplying out, the polynomial is

$$Y^3 - (r + s + t)Y^2 + (rs + st + tr)Y - rst$$

So the coefficients above are

$$A = r + s + t$$

$$B = rs + st + tr$$

$$C = rst$$

Example: Let $P(x)$ be the (by trial division) irreducible $x^3 + x + 1$ in $\mathbf{F}_2[x]$, and

$$\alpha = x\text{-mod-}P(x)$$

Let $\beta = \alpha^2 + \alpha + 1$. Find the (cubic) equation $Y^3 + AY^2 + BY + C = 0$ of which β is a root, with $A, B, C \in \mathbf{F}_2$.

The complete list of roots of the equation of which β is a root are its images by the Frobenius automorphism, namely

$$\beta,\ \beta_2 = \beta^2,\ \beta_3 = \beta^{2^2}$$

In terms of α, these are

$$\beta = \alpha^2+\alpha+1,\ \beta_2 = (\alpha^2+\alpha+1)^2,\ \beta_3 = (\alpha^2+\alpha+1)^4$$

or, since the ground field is $\mathbf{F}_2$, more simply

$$\beta = \alpha^2+\alpha+1,\ \beta_2 = \alpha^4+\alpha^2+1,\ \beta_3 = \alpha^8+\alpha^4+1$$

What cubic equation $Y^3 - AY^2 + BY - C = 0$ is satisfied by these three?

We should *reduce* these expressions first:

$$\beta = \alpha^2 + \alpha + 1 \text{ is reduced}$$

And

$$(x^4 + x^2 + 1) \,\%\, (x^3 + x + 1) = x + 1$$

so

$$\beta_2 = \alpha^4 + \alpha^2 + 1 = \alpha + 1$$

And it is more convenient to apply the Frobenius to this, rather than to put $\beta_3 = \alpha^8 + \alpha^4 + 1$ into reduced form. Namely

$$\beta_3 = \beta_2^2 = (\alpha + 1)^2 = \alpha^2 + 1$$

Then the coefficient A is

$$\beta + \beta_2 + \beta_3 = (\alpha^2 + \alpha + 1) + (\alpha + 1) + (\alpha^2 + 1) = 1$$

The most expensive-to-compute coefficient B is

$$\beta\beta_2 + \beta_2\beta_3 + \beta_3\beta$$

$$= (\alpha^2+\alpha+1)(\alpha+1)+(\alpha+1)(\alpha^2+1)+(\alpha^2+1)(\alpha^2+\alpha+1)$$

$$= (\alpha^3 + 1) + (\alpha^3 + \alpha^2 + \alpha + 1) + (\alpha^4 + \alpha^3 + \alpha + 1)$$

$$= \alpha^4 + \alpha^3 + \alpha^2 + 1$$

Reduce

$$(x^4 + x^3 + x^2 + 1) \,\%\, (x^3 + x + 1) = 0$$

so the coefficient B is 0.

The last coefficient C, is non-zero, so must be 1, since our ground field $\mathbf{F}_2$ is so little. But let's see how to do the computation systematically. That last coefficient is

$$C = \beta\beta_2\beta_3$$

$$= (\alpha^2 + \alpha + 1)(\alpha + 1)(\alpha^2 + 1)$$

$$= (\alpha^3 + 1)(\alpha^2 + 1) = \alpha^5 + \alpha^3 + \alpha^2 + 1$$

Reduce

$$(x^5 + x^3 + x^2 + 1) \,\%\, (x^3 + x + 1) = 1$$

So $C = 1$, and the cubic equation $\beta = \alpha^2 + \alpha + 1$ satisfies is

$$Y^3 - Y^2 - 1 = 0$$

or, since $-1 = +1$ in $\mathbf{F}_2$,

$$Y^3 + Y^2 + 1 = 0$$

Remark: After all, this *is* the only other irreducible cubic in $\mathbf{F}_2[x]$.

Example: Let $P(x)$ be the (by trial division) irreducible $x^3 + 2x + 1$ in $\mathbf{F}_3[x]$, and

$$\alpha = x\text{-mod-}P(x)$$

Let $\beta = \alpha^2 + 1$. Find the (cubic) equation $Y^3 - AY^2 + BY - C = 0$ of which β is a root, with $A, B, C \in \mathbf{F}_3$.

The complete list of roots of the equation of which β is a root are its images by the Frobenius automorphism, namely

$$\beta,\ \beta_2 = \beta^3,\ \beta_3 = \beta^{3^2}$$

In terms of α, these are

$$\beta = \alpha^2 + 1,\ \beta_2 = (\alpha^2 + 1)^3,\ \beta_3 = (\alpha^2 + 1)^9$$

or, since the ground field is $\mathbf{F}_3$,

$$\beta = \alpha^2 + 1,\ \beta_2 = \alpha^6 + 1,\ \beta_3 = \alpha^{18} + 1$$

What cubic equation $Y^3 - AY^2 + BY - C = 0$ is satisfied by these three?

We should *reduce* these expressions first:

$$\beta = \alpha^2 + 1 \text{ is reduced}$$

$$(x^6 + 1) \,\%\, (x^3 + 2x + 1) = x^2 + x + 2$$

so

$$\beta_2 = \alpha^2 + \alpha + 2$$

And it is probably more convenient to apply the Frobenius to this, rather than to put $\beta_3 = \alpha^{18} + 1$ into reduced form. Namely

$$\beta_3 = \beta_2^3 = (\alpha^2 + \alpha + 2)^3 = \alpha^6 + \alpha^3 + 2$$

Reducing,

$$(x^6 + x^3 + 2) \,\%\, (x^3 + x + 2) = x^2 + 2x + 2$$

so

$$\beta_3 = \alpha^2 + 2\alpha + 2$$

Then the coefficient A is

$$A = \beta + \beta_2 + \beta_3 =$$

$$(\alpha^2 + 1) + (\alpha^2 + \alpha + 2) + (\alpha^2 + 2\alpha + 2) = \boxed{2}$$

The most expensive-to-compute coefficient B is

$$\beta\beta_2 + \beta_2\beta_3 + \beta_3\beta$$
$$= (\alpha^2+1)(\alpha^2+\alpha+2) + (\alpha^2+\alpha+2)(\alpha^2+2\alpha+2)$$
$$+(\alpha^2+2\alpha+2)(\alpha^2+1)$$
$$= (\alpha^4+\alpha^3+\alpha+2) + (\alpha^4+1) + (\alpha^4+2\alpha^3+2\alpha+2)$$
$$= 3\alpha^4 + 3\alpha^3 + 3\alpha + 5 = 2$$

(since $3 = 0$ here) so the coefficient $B = \boxed{2}$.

The last coefficient is

$$C = \beta\beta_2\beta_3$$
$$= (\alpha^2+1)(\alpha^2+\alpha+2)(\alpha^2+2\alpha+2)$$
$$= \alpha^6 + \alpha^4 + \alpha^2 + 1$$

Reduce

$$(x^6 + x^4 + x^2 + 1) \,\%\, (x^3 + 2x + 1) = 2$$

so $C = \boxed{2}$.

So the equation satisfied by $\alpha^2 + 1$ is

$$Y^3 - 2Y^2 + 2Y - 2 = 0$$

or

$$Y^3 + Y^2 + 2Y + 1 = 0$$

since $3 = 0$ here.

Roots of distinct irreducibles

Theorem: Let $P(x)$ and $Q(x)$ be distinct monic *irreducible* polynomials in some $\mathbf{F}_q[x]$. Then no root of $P(x) = 0$ is a root of $Q(x) = 0$.

Proof: Since P and Q are distinct (monic) irreducibles, there are polynomials r, s such that

$$1 = rP + sQ$$

Let α be a root of $P(x) = 0$ in some bigger field $\mathbf{F}_{q^m}$. Then $x - \alpha$ divides $P(x)$ in the larger polynomial ring $\mathbf{F}_{p^m}[x]$. If α were a root of $Q(x) = 0$ then $x - \alpha$ would also divide $Q(x)$. But then the relation $1 = rP + sQ$ would imply that $x - \alpha$ would divide 1, which is false. Thus, $x - \alpha$ does not divide $Q(x)$. ///

Solving equations

Model the finite field $\mathbf{F}_{32}$ as $\mathbf{F}_2[x]/P(x)$ where

$$P(x) = x^5 + x^2 + 1$$

Let

$$\alpha = x\text{-mod-}P(x)$$

We know that α satisfies

$$P(\alpha) = 0$$

and every β in this $\mathbf{F}_{32}$ has a unique expression of the form (with $a, b, c, d, e \in \mathbf{F}_2$)

$$\beta = a + b\alpha + c\alpha^2 + d\alpha^3 + e\alpha^4$$

As a (possibly surprising) consequence of the *essential uniqueness of* $\mathbf{F}_{32}$, for *every* irreducible quintic $Q(x)$ in $\mathbf{F}_2[x]$ the equation

$$Q(x) = 0$$

has a root (in fact, 5) in $\mathbf{F}_{32} = \mathbf{F}_2[x]/P(x)$. That is, there is some expression β such that

$$Q(\beta) = 0$$

Problem: How to find the root β?

Remark: Conveniently, since $2^5 - 1 = 31$ is *prime* (by trial division), these irreducible quintics are also *primitive*. In other words, α is a **primitive root** in $\mathbf{F}_{32}$. And any (non-zero) element of $\mathbf{F}_{32}$ is of the form α^t for some t in the range $1 \leq t \leq 31$.

Thus, we might try plugging α, α^2, α^3, etc into $Q(x)$ to see whether we get 0.

That is, replace x by x^2, x^3, x^4, etc and reduce modulo $P(x)$ to see if we get 0. If

$$Q(x^t) \,\%\, P(x) = 0$$

then $\beta = \alpha^t$ is the desired root.

And then *reduce* $x^t \,\%\, P(x)$ to get a reduced expression for β in terms of α.

How to do the testing efficiently?

We will systematically but fairly efficiently investigate irreducible binary quintics. From the counting formula above, there are exactly

$$\frac{2^5 - 2}{5} = 6$$

Proposition: The six irreducible binary quintics are

$$Q_1(x) = x^5 + x^2 + 1$$

$$Q_2(x) = x^5 + x^3 + 1$$

$$Q_3(x) = x^5 + x^3 + x^2 + x + 1$$

$$Q_4(x) = x^5 + x^4 + x^2 + x + 1$$

$$Q_5(x) = x^5 + x^4 + x^3 + x + 1$$

$$Q_6(x) = x^5 + x^4 + x^3 + x^2 + 1$$

Proof: For trial division we must verify non-divisibility by the irreducibles of degree $\leq 5/2$, namely x, $x + 1$, and $x^2 + x + 1$. For non-divisibility by x, the constant term must be 1. For non-divisibility by $x + 1$, the value of the polynomial at 1 must be non-zero, so there must be an *odd* number of non-zero coefficients. Thus, among the middle 4 coefficients, either 1 or 3 are non-zero. This gives

$$\binom{4}{1} + \binom{4}{3} = 8$$

among which lie the 6 irreducibles.

Assuming non-divisibility by x and $x+1$, a quintic divisible by x^2+x+1 must be

$$\text{quintic} = (x^2+x+1)\cdot(\text{irred cubic})$$

From trial division, there are only two irreducible cubics, x^3+x+1 and x^3+x^2+1, giving **reducible quintics**

$$(x^2+x+1)(x^3+x+1) = x^5+x^4+1$$

$$(x^2+x+1)(x^3+x^2+1) = x^5+x+1$$

Thus, the other 6 quintics with constant term 1 and an odd number of middle/inner coefficients are all irreducible. ///

Remark: It is not obvious, but is true, that

$$\frac{x^{31}-1}{x-1} = Q_1(x)Q_2(x)Q_3(x)Q_4(x)Q_5(x)Q_6(x)$$

Remark: The first structure is that these irreducible quintics occur in pairs, each obtained from the other by reversing the coefficients front-to-back. There are 3 pairs

$$Q_1 = x^5 + x^2 + 1 \longleftrightarrow x^5 + x^3 + 1 = Q_2$$

$$Q_3 = x^5 + x^3 + x^2 + x + 1 \leftrightarrow x^5 + x^4 + x^3 + x^2 + 1 = Q_6$$

$$Q_4 = x^5 + x^4 + x^2 + x + 1 \leftrightarrow x^5 + x^4 + x^3 + x + 1 = Q_5$$

In each case, the effect is due to

$$x^5 \cdot Q_1(x^{-1}) = Q_2(x)$$

$$x^5 \cdot Q_3(x^{-1}) = Q_6(x)$$

$$x^5 \cdot Q_4(x^{-1}) = Q_5(x)$$

That is, the **inverses** of the roots of $Q_1(x) = 0$ are the roots of $Q_2(x) = 0$, and so on.

Remark: Further, since $2^5 - 1 = 31$ is prime (by trial division), each irreducible quintic is *primitive*. Thus, given a root α of a given irreducible quintic $P(x) = 0$, the roots of any other irreducible quintic $Q(x) = 0$ are of the form α^t for $1 \leq t < 31$. Keep in mind that $\alpha^{31} = 1$.

From the theorem above, the quintuples of roots of the 6 different irreducible quintics are **disjoint**. That is, the 30 elements in

$$\mathbf{F}_{32} - \mathbf{F}_2 = (\mathbf{F}_{32} \text{ take away } \mathbf{F}_2)$$

form 6 disjoint sets of 5 elements, each set of 5 being the set of roots of an irreducible quintic.

For *one* root β of $Q(x) = 0$, the images of β under the Frobenius automorphism

$$\beta, \beta^2, \beta^{2^2}, \beta^{2^3}, \beta^{2^4}$$

make up the complete list of roots of $Q(x) = 0$. For $\beta = \alpha^t$, the list can be rewritten

$$\alpha^t, \alpha^{2t}, \alpha^{2^2 t}, \alpha^{2^3 t}, \alpha^{2^4 t}$$

and *exponents are mod* 31 since $\alpha^{31} = 1$.

Thus, the 6 batches of quintuples of roots consist of collections $R_1, \ldots, R_6$ of 5 integers (exponents t with $\beta = \alpha^t$) mod 31 which differ from each other by powers of 2 (mod 31).

Since the collection $\mathbf{Z}/31^\times$ of exponents of α ($\neq \alpha^0$) has **primitive root** 3, index the quintuples in a **structured** way

$$R_1 = \{1, 2, 4, 8, 16\}$$

$$R_2 = 3 \cdot R_1 = \{3, 6, 12, 24, 17\}$$

$$R_3 = 3^2 \cdot R_1 = 3 \cdot R_2 = \{9, 18, 5, 10, 20\}$$

$$R_4 = 3^3 \cdot R_1 = 3 \cdot R_3 = \{27, 23, 15, 30, 29\}$$

$$R_5 = 3^4 \cdot R_1 = 3 \cdot R_4 = \{19, 7, 14, 28, 25\}$$

$$R_6 = 3^5 \cdot R_1 = 3 \cdot R_5 = \{26, 21, 11, 22, 13\}$$

The sets of roots occur in **pairs**, related by inverse (exponent multiplied by -1 mod 31):

$$(-1) \cdot R_1 = R_4$$

$$(-1) \cdot R_2 = R_5$$

$$(-1) \cdot R_3 = R_6$$

Remark: For α satisfying an irreducible (quintic or any other degree) $Q(x) = 0$, there is an easy way to obtain a reduced expression for α^{-1} in terms of α.

Treat just the binary case, for simplicity.

For example, suppose that

$$\alpha^5 + \alpha^2 + 1 = 0$$

Move the 1 to the other side

$$\alpha^5 + \alpha^2 = 1$$

Divide by α (multiply by α^{-1})

$$\alpha^4 + \alpha = \alpha^{-1}$$

If two exponents s and t differ by some power of 2 modulo 31, that is, if there is ℓ such that

$$s = 2^\ell \cdot t \bmod 31$$

then write

$$s = t \bmod \langle 2 \rangle$$

Then α^s and α^t will be roots of the *same* ireducible quintic.

Thus, given a root α of $Q_1(x) = 0$, α^3 is a root of some $Q_j(x) = 0$, $j \neq 1$. Since the roots of $Q_2(x) = 0$ are the *inverses* of the roots of $Q_1(x) = 0$, and since

$$-1 \neq 3 \bmod \langle 2 \rangle$$

α^3 is definitely not a root of Q_2, either.

So α^3 is a root of one of Q_3, Q_4, Q_5, Q_6. Hard to guess which. With $j = 3, 4, 5, 6$, compute

$$Q_j(x^3) \,\%\, Q_1(x)$$

and see which one is 0.

After at worst 3 divisions of degree-15 polynomial by the quintic $Q_1(x) = x^5 + x^2 + 1$, since after 3 failures we *know* the last one succeeds:

For root α of

$$Q_1(x) = x^5 + x^2 + 1 = 0$$

the cube α^3 is a root of

$$Q_6(x) = x^5 + x^4 + x^3 + x^2 + 1 = 0$$

Next, because $-1 \neq 3 \bmod \langle 2 \rangle$, $(\alpha^3)^3$ cannot be a root of the quintic $Q_3(x) = 0$ whose roots are the inverses of those of Q_6.

And $-1 \neq 3^2 \bmod \langle 2 \rangle$, so also $(\alpha^3)^3$ cannot be a root of $Q_2(x) = 0$, whose roots are inverses of those of $Q_1(x) = 0$.

Thus, $(\alpha^3)^3$ is a root of either $Q_3(x) = 0$ or of $Q_4(x) = 0$.

Since we already know that $\beta = \alpha^3$ is a root of $Q_6(x) = 0$, we do *not* compute $Q_j(x^9) \,\%\, Q_1(x)$ with $j = 3, 4$, but, instead, more simply

$$Q_3(x^3) \,\%\, Q_6(x)$$

If this *is* 0, then α^9 is a root of $Q_3(x) = 0$. If it is *not* 0 then α^9 is a root of $Q_4(x) = 0$, *because there is no other choice!*

Thus, after one division of degree-15 polynomial by a quintic, whichever way things turn out:

For root α of

$$Q_1(x) = x^5 + x^2 + 1 = 0$$

the cubed cube α^9 is a root of

$$Q_4(x) = x^5 + x^4 + x^2 + x + 1 = 0$$

We have no serious computations left to do:

To see which quintic α^{3^3} is a root of, observe that

$$3^3 = 27 = 2^2 \cdot (-1) \bmod 31$$

so

$$3^3 = -1 \bmod \langle 2 \rangle$$

Thus, α^{3^3} is a root of the same quintic of which α^{-1} is a root, namely $Q_2(x) = 0$.

Likewise, $\alpha^{3^4} = (\alpha^3)^{3^3}$ is a root of the same quintic of which $(\alpha^3)^{-1}$ is a root, namely $Q_3(x)$.

Likewise, $\alpha^{3^5} = (\alpha^{3^2})^{3^3}$ is a root of the same quintic of which $(\alpha^{3^2})^{-1}$ is a root, namely $Q_5(x)$.

In summary:

Theorem:

$$\alpha \text{ a root of } Q_1(x) = x^5 + x^2 + 1 = 0$$

$$\alpha^3 \text{ is root of } Q_6(x) = x^5 + x^4 + x^3 + x^2 + 1 = 0$$

$$\alpha^{3^2} \text{ is root of } Q_4(x) = x^5 + x^4 + x^2 + x + 1 = 0$$

$$\alpha^{3^3} \text{ is root of } Q_2(x) = x^5 + x^3 + 1 = 0$$

$$\alpha^{3^4} \text{ is root of } Q_3(x) = x^5 + x^3 + x^2 + x + 1 = 0$$

$$\alpha^{3^5} \text{ is root of } Q_5(x) = x^5 + x^4 + x^3 + x + 1 = 0$$

This can be rewritten in a more suggestive fashion:

Corollary:

For root β of $Q_1 = 0$, β^3 is root of $Q_6 = 0$
For root β of $Q_6 = 0$, β^3 is root of $Q_4 = 0$
For root β of $Q_4 = 0$, β^3 is root of $Q_2 = 0$
For root β of $Q_2 = 0$, β^3 is root of $Q_3 = 0$
For root β of $Q_3 = 0$, β^3 is root of $Q_5 = 0$
For root β of $Q_5 = 0$, β^3 is root of $Q_1 = 0$

Example: Let α be a root of $x^5 + x^4 + x^3 + x^2 + 1 = 0$, and express *some* root of $x^5 + x^4 + x^3 + x + 1 = 0$ in the reduced form

$$a + b\alpha + c\alpha^2 + d\alpha^3 + e\alpha^4 (a, b, c, d, e \in \mathbf{F}_2)$$

α is a root of the quintic labelled Q_6 above, and the desired quintic is Q_5. The corollary above says that α^3 is a root of Q_4, α^{3^2} is a root of Q_2, α^{3^3} is a root of Q_3, and α^{3^4} is a root of Q_5.

Thus, the issue seems to be to rewrite α^{3^4} in reduced form.

But the exponent 3^4 is mod 31, and we can change it by powers of 2 (mod 31), as well (merely giving a *different* root of the same polynomial). $3^4 \,\%\, 31 = 19$, and $2 \cdot 19 \,\%\, 31 = 7$, so we really only need to compute

$$x^7 \,\%\, (x^5 + x^4 + x^3 + x^2 + 1) = x^3 + x^2 + x$$

Thus,

$$\beta = \alpha^3 + \alpha^2 + \alpha$$

is a root of the other quintic

$$x^5 + x^4 + x^3 + x + 1 = 0$$