So $\mathbf{Q}-\mathbf{I}=\mathbf{E}$ has rank 2, the null space of $\mathbf{E}$ has dimension 3, $f(x)$ has three distinct irreducible factors, and the vectors $\mathbf{b}$ satisfying $\mathbf{bE}=0$ have the form

$$\mathbf{b}=(b_0,b_1,b_2,b_3,b_4)=(b_0,b_3,0,b_3,b_4),$$

where b_0,b_3 and b_4 are arbitrary. Thus $f(x)$ divides $h(x)^3-h(x)$ where we can choose $h(x)=x^4$, or $h(x)=x+x^3$, or $h(x)=1$, or any $\mathbb{F}_3$-linear combination of those three choices.

Exercises.

7. Find the three irreducible factors of $f(x)$ in Example 11.

8. Factor $x^{10}+x^9+x^7+x^3+x^2+1$ in $\mathbb{F}_2[x]$.

9. Factor $x^8+x^7+x^6+x^4+1$ in $\mathbb{F}_2[x]$.

10. Show that x^5+x^2+1 is irreducible in $\mathbb{F}_2[x]$.

11. Show that x^7+x^3+1 is irreducible in $\mathbb{F}_2[x]$.

12. Show that $7x^7+6x^6+4x^4+3x^3+2x^2+2x+1$ is irreducible in $\mathbb{Q}[x]$ (use the last exercise).

13. Use Berlekamp's algorithm to factor x^2-q in $\mathbb{F}_p[x]$, where q and p are coprime, and prove Euler's Lemma (Section 21B) that q is a quadratic residue mod p, that is, $x^2-q\equiv 0 \pmod{p}$ has a root, iff $q^{(p-1)/2}\equiv 1 \pmod{p}$.

D. The Hensel Factorization Method

Given a bound B on the coefficients of factors of a polynomial $f(x)$ in $\mathbb{Z}[x]$, we can look for factorizations of $f(x)$ modulo M for $M\geq 2B$. Any factor of f modulo M corresponds to at most one possible factor of f in $\mathbb{Z}[x]$, because there will be only one polynomial in $\mathbb{Z}[x]$ that will satisfy the bound on coefficients and reduce to the given factor of f modulo M.

Thus we wish to find factorizations of f modulo M, where M may be large.

There are two choices on how to proceed.

One is to find primes $p>2B$ and use Berlekamp's algorithm to factor f modulo p. If we're lucky, f will have few irreducible factors modulo p, so there will be few choices for factorizations of f in $\mathbb{Z}[x]$.

An alternative is to find a small prime p so that f factors modulo p into few distinct irreducible factors, and then lift the factorization modulo p to a unique factorization modulo p^{2^e} for e so large so that $p^{2^e}>2B$.

This method, called the Hensel factorization method [Zassenhaus (1978)], uses an extension of coprimeness to polynomials with coefficients not in a field.

Defini ion. Let R be a commutative ring, and f,g be polynomials of degrees ≥ 1 with coefficients in R. Then f and g are *coprime* if there exist polynomials r,s with coefficients in R so that

$$rf + sg = 1.$$

If $R = \mathbb{Z}/m\mathbb{Z}$ and f, g are polynomials with integer coefficients, we'll say that f and g are *coprime modulo m*, if the images of f and g in $\mathbb{Z}/m\mathbb{Z}[x]$ are coprime, that is, if there exist polynomials r, s in $\mathbb{Z}[x]$ so that $fr + gs \equiv 1 \pmod{m}$.

In short, we extend the definition of coprime by using the Bezout Identity criterion.

Before presenting the main result, we need an auxiliary result about coprime polynomials.

Proposition 10. *Let g,h be monic and coprime in $R[x]$. Then for all k in $R[x]$ there exist polynomials a,b in $R[x]$ with $ag + bh = k$. If* $\deg k < \deg(fg)$*, then we can choose a, b with* $\deg(a) < \deg(h), \deg(b) < deg(g)$.

Proof. Since g and h are coprime, there exist polynomials r,s so that $gr + hs = 1$. It follows that $grk + hsk = k$.

Suppose $\deg(k) < \deg(fg)$ and there exist a,b in $R[x]$ so that $ag + bh = k$ with $\deg(b) \geq \deg(g)$. Then $b = gq + s$ with $\deg(s) < \deg(g)$, and

$$ag + (gq + s)h = k.$$

Hence $(a + qh)g + sh = k$, or, letting $r = a + qh$, then

$$rg + sh = k.$$

Since $\deg(s) < \deg(g)$, we have $\deg(sh) < \deg(gh)$, and also $\deg(k) < \deg(gh)$. So $\deg(rg) < \deg(gh)$. Since g is monic, it follows that $\deg(r) < \deg(h)$. □

Here is the main result.

Theorem 11. *Let f be a monic polynomial in $\mathbb{Z}[x]$. Suppose there are monic polynomials g_1, h_1 in $\mathbb{Z}[x]$ so that g_1 and h_1 are coprime modulo m and* $f = g_1 h_1 \pmod{m}$. *Then there exist unique monic polynomials g_2 and f_2 so that*

$$g_2 \equiv g_1 \pmod{m}$$
$$h_2 \equiv h_1 \pmod{m},$$

g_2 and h_2 are coprime modulo m^2, and

$$f \equiv g_2 h_2 \pmod{m^2}.$$

Proof. The proof shows how to construct g_2 and h_2.

We write

$$g_2 = g_1 + mb$$
$$h_2 = h_1 + mc$$

for polynomials b, c in $\mathbb{Z}[x]$ with $\deg(b) < \deg(g_1), \deg(c) < \deg(h_1)$ that we need to find. To find them, we note that since $f \equiv g_1 h_1 \pmod{m}$, we have

$$f = g_1 h_1 + mk$$

for some polynomial k in $\mathbb{Z}[x]$. Since f, g_1 and h_1 are monic, $\deg(k) < \deg(g_1 h_1)$. Then

$$\begin{aligned} g_2 h_2 - f &= (g_1 + mb)(h_1 + mc) - (g_1 h_1 + mk) \\ &= g_1 h_1 + mg_1 c + mh_1 b + m^2 bc - g_1 h_1 - mk. \end{aligned}$$

For the left side to be congruent to 0 modulo m^2, we need

$$m(g_1 c + h_1 b - k) \equiv 0 \pmod{m^2},$$

or

$$g_1 c + h_1 b - k \equiv 0 \pmod{m}.$$

But since g_1 and h_1 are coprime modulo m, there exist polynomials c and b so that

$$g_1 c + h_1 b \equiv k \pmod{m},$$

and since $\deg(k) < \deg(g_1 h_1)$, we may choose the polynomials c and b so that $\deg c < \deg h_1$ and $\deg b < \deg g_1$. Then by the way we chose c and b, the polynomials $g_2 = g_1 + mb$ and $h_2 = h_1 + mc$ are monic and satisfy

$$f \equiv g_2 h_2 \pmod{m^2}.$$

To finish the proof we need to show that g_2 and h_2 are coprime modulo m^2. So we seek polynomials r_2 and s_2 so that

$$r_2 g_2 + s_2 h_2 \equiv 1 \pmod{m^2}.$$

Since g_1 and h_1 are coprime, there exist polynomials r_1 and s_1 so that $r_1 g_1 + s_1 h_1 = 1 + mz$ for some polynomial z. We write

$$r_2 = r_1 + mw, \quad s_2 = s_1 + my$$

for unknown polynomials w, y in $\mathbb{Z}[x]$, and substitute for r_2, g_2, s_2 and h_2 in the desired congruence

$$r_2 g_2 + s_2 h_2 \equiv 1 \pmod{m^2}.$$

to obtain

$$\begin{aligned} &(r_1 + mw)(g_1 + mb) + (s_1 + my)(h_1 + mc) \\ &\qquad \equiv r_1 g_1 + mwg_1 + mr_1 b + s_1 h_1 + ms_1 c + myh_1 \pmod{m^2} \\ &\qquad \equiv 1 + mz + m(wg_1 + r_1 b + s_1 c + yh_1) \pmod{m^2}. \end{aligned}$$

For this last expression to be congruent to 1 modulo m^2, we need to find polynomials w, y so that

$$wg_1 + yh_1 \equiv -z - r_1 b - s_1 c \pmod{m}.$$

But since g_1 and h_1 are coprime modulo m, it follows that we can find w, y satisfying this last congruence. That means there exist $r_2 = r_1 + mw, s_2 = s_1 + my$ so that

$$r_2 g_2 + s_2 h_2 \equiv 1 \pmod{m^2}.$$

Thus g_2 and h_2 are coprime modulo m^2, and that completes the proof. □

Example 12. Let $f(x) = x^4 + 23x^3 - 15x^2 + 17x - 7$. We find that

$$f(x) \equiv x^4 + 2x^3 + 3x^2 + 2x + 2 = (x^2+1)(x^2+2x+2) \pmod{3},$$

so $f(x)$ factors modulo 3 into the product of two distinct polynomials that are irreducible modulo 3, and hence coprime modulo 3.

Now we want to factor $f(x)$ modulo 9. So let $g_1 = x^2+1, h_1 = x^2+2x+2$, and let

$$g_2 = g_1 + 3b = (x^2+1) + 3b$$
$$h_2 = h_1 + 3c = (x^2+2x+2) + 3c$$

for some polynomials b, c with $\deg c < \deg h_1, \deg b < \deg g_1$. Then

$$g_2 h_2 \equiv (x^2+1)(x^2+2x+2) + 3c(x^2+1) + 3b(x^2+2x+2) \pmod{9}.$$

To find b, c we set up the congruence

$$f \equiv g_2 h_2 \pmod{9}$$

and substitute:

$$x^4 + 23x^3 - 15x^2 + 17x - 7 \equiv (x^4 + 2x^3 + 3x^2 + 2x + 2) + 3c(x^2+1) + 3b(x^2+2x+2) \pmod{9};$$

or

$$21x^3 - 18x^2 + 15x - 9 \equiv 3c(x^2+1) + 3b(x^2+2x+2) \pmod{9}.$$

Factoring 3 out of everything yields

$$7x^3 - 6x^2 + 5x - 3 \equiv c(x^2+1) + b(x^2+2x+2) \pmod{3},$$

which we know we can solve for polynomials b, c of degree ≤ 2 since x^2+1 and x^2+2x+2 are coprime modulo 3.

To solve the congruence for b and c, we set up some linear equations: write $b = rx + s, c = tx + v$, then

$$7x^3 - 6x^2 + 5x - 3 \equiv (tx+v)(x^2+1) + (rx+s)(x^2+2x+2) \pmod{3}.$$

Equating the coefficients of $1, x, x^2, x^3$ on both sides yields

$$\begin{aligned}
-3 &\equiv v + 2s \\
5 &\equiv t + 2r + 2s \\
-6 &\equiv v + 2r + s \\
7 &\equiv t + r \pmod 3.
\end{aligned}$$

One sees easily that $r = t = 2, s = v = 1$ is the unique solution, so

$$b = 2x + 1, c = 2x + 1.$$

Thus

$$\begin{aligned}
g_2 = g_1 + 3b &\equiv (x^2 + 1) + 3(2x + 1) \equiv x^2 + 6x + 4, \\
h_2 = h_1 + 3c = (x^2 + 2x + 2) &+ 3(2x + 1) \equiv x^2 + 8x + 5,
\end{aligned}$$

and it is easily checked that

$$\begin{aligned}
(x^2 + 6x + 4)(x^2 + 8x + 5) &= x^4 + 14x^3 + 57x^2 + 62x + 20 \\
&\equiv x^4 + 23x^3 - 15x^2 + 17x - 7 = f(x) \pmod 9.
\end{aligned}$$

In a similar way we can lift the factorization modulo 9 to one modulo $9^2 = 81$, then to $81^2 = 6561$ and beyond, until we get past the bound on the coefficients of any degree 2 factor of $f(x)$, at which point we either find a factorization of f in $\mathbb{Z}[x]$ or show that none exists that reduces to $f = g_1 h_1$ modulo 3. In the latter case, f must be irreducible in $\mathbb{Q}[x]$.

Note that $\|f\| = (1^2 + 23^2 + 15^2 + 17^2 + 7^2)^{1/2} = \sqrt{1093} = 33.06$, so using the Mignotte bound we would need only to look at a factorization of f modulo 81 to either find a factorization of f or show that f is irreducible.

It turns out that $f(x)$ is irreducible modulo 5, so must be irreducible in $\mathbb{Q}[x]$.

Exercises.

14. Factor $x^4 - x^3 - 84x^2 + 125x - 13$ modulo 5, then modulo 25, then in $\mathbb{Z}$.

15. Factor $x^4 + 2x^3 - 38x^2 - 69x - 28$ modulo 3, then modulo 9, then in $\mathbb{Z}$.

16. Factor $x^4 + x^2 + 2$ modulo 2, then modulo 4, then modulo 16, then in $\mathbb{Z}$.