(*January 14, 2009*)

[11.1] Let ζ be a primitive n^{th} root of unity in a field of characteristic 0. Let M be the n-by-n matrix with ij^{th} entry ζ^{ij}. Find the multiplicative inverse of M.

Some experimentation (and an exercise from the previous week) might eventually suggest consideration of the matrix A having ij^{th} entry $\frac{1}{n}\,\zeta^{-ij}$. Then the ij^{th} entry of MA is

$$(MA)_{ij} = \frac{1}{n}\sum_k \zeta^{ik-kj} = \frac{1}{n}\sum_k \zeta^{(i-j)k}$$

As an example of a *cancellation principle* we claim that

$$\sum_k \zeta^{(i-j)k} = \begin{cases} 0 & (\text{for } i-j \neq 0) \\ n & (\text{for } i-j = 0) \end{cases}$$

The second assertion is clear, since we'd be summing n 1's in that case. For $i-j \neq 0$, we can change variables in the indexing, replacing k by $k+1 \bmod n$, since ζ^a is well-defined for $a \in \mathbb{Z}/n$. Thus,

$$\sum_k \zeta^{(i-j)k} = \sum_k \zeta^{(i-j)(k+1)} = \zeta^{i-j}\sum_k \zeta^{(i-j)k}$$

Subtracting,

$$(1-\zeta^{i-j})\sum_k \zeta^{(i-j)k} = 0$$

For $i-j \neq 0$, the leading factor is non-zero, so the sum must be zero, as claimed. ///

[11.2] Let $\mu = \alpha\beta^2+\beta\gamma^2+\gamma\alpha^2$ and $\nu = \alpha^2\beta+\beta^2\gamma+\gamma^2\alpha$. Show that these are the two roots of a quadratic equation with coefficients in $\mathbb{Z}[s_1,s_2,s_3]$ where the s_i are the elementary symmetric polynomials in α,β,γ.

Consider the quadratic polynomial

$$(x-\mu)(x-\nu) = x^2-(\mu+\nu)x+\mu\nu$$

We will be done if we can show that $\mu+\nu$ and $\mu\nu$ are symmetric polynomials as indicated. The sum is

$$\mu+\nu = \alpha\beta^2+\beta\gamma^2+\gamma\alpha^2+\alpha^2\beta+\beta^2\gamma+\gamma^2\alpha$$

$$= (\alpha+\beta+\gamma)(\alpha\beta+\beta\gamma+\gamma\alpha)-3\alpha\beta\gamma = s_1s_2-3s_3$$

This expression is plausibly obtainable by a few trial-and-error guesses, and examples nearly identical to this were done earlier. The product, being of higher degree, is more daunting.

$$\mu\nu = (\alpha\beta^2+\beta\gamma^2+\gamma\alpha^2)(\alpha^2\beta+\beta^2\gamma+\gamma^2\alpha)$$

$$= \alpha^3+\alpha\beta^4+\alpha^2\beta^2\gamma^2+\alpha^2\beta^2\gamma^2+\beta^3\gamma^3+\alpha\beta\gamma^4+\alpha^4\beta\gamma+\alpha^2\beta^2\gamma^2+\alpha^3\gamma^3$$

Following the symmetric polynomial algorithm, at $\gamma=0$ this is $\alpha^3\beta^3 = s_2(\alpha,\beta)^3$, so we consider

$$\frac{\mu\nu-s_2^3}{s_3} = \alpha^3+\beta^3+\gamma^3-3s_3-3(\mu+\nu)$$

where we are lucky that the last 6 terms were $\mu+\nu$. We have earlier found the expression for the sum of cubes, and we have expressed $\mu+\nu$, so

$$\frac{\mu\nu-s_2^3}{s_3} = (s_1^3-3s_1s_2+3s_3)-3s_3-3(s_1s_2-3s_3) = s_1^3-6s_1s_2+9s_3$$

and, thus,

$$\mu\nu = s_2^3 + s_1^3 s_3 - 6s_1 s_2 s_3 + 9s_3^2$$

Putting this together, μ and ν are the two roots of

$$x^2 - (s_1 s_2 - 3s_3)x + (s_2^3 + s_1^3 s_3 - 6s_1 s_2 s_3 + 9s_3^2) = 0$$

(One might also speculate on the relationship of μ and ν to solution of the general cubic equation.) ///

[11.3] The 5^{th} cyclotomic polynomial $\Phi_5(x)$ factors into two irreducible quadratic factors over $\mathbb{Q}(\sqrt{5})$. Find the two irreducible factors.

We have shown that $\sqrt{5}$ occurs inside $\mathbb{Q}(\zeta)$, where ζ is a primitive fifth root of unity. Indeed, the discussion of Gauss sums in the proof of quadratic reciprocity gives us the convenient

$$\zeta - \zeta^2 - \zeta^3 + \zeta^4 = \sqrt{5}$$

We also know that $[\mathbb{Q}(\sqrt{5}) : \mathbb{Q}] = 2$, since $x^2 - 5$ is irreducible in $\mathbb{Q}[x]$ (Eisenstein and Gauss). And $[\mathbb{Q}(\zeta) : \mathbb{Q}] = 4$ since $\Phi_5(x)$ is irreducible in $\mathbb{Q}[x]$ of degree $5 - 1 = 4$ (again by Eisenstein and Gauss). Thus, by multiplicativity of degrees in towers of fields, $[\mathbb{Q}(\zeta) : \mathbb{Q}(\sqrt{5})] = 2$.

Thus, since none of the 4 primitive fifth roots of 1 lies in $\mathbb{Q}(\sqrt{5})$, each is necessarily quadratic over $\mathbb{Q}(\sqrt{5})$, so has minimal polynomial over $\mathbb{Q}(\sqrt{5})$ which is quadratic, in contrast to the minimal polynomial $\Phi_5(x)$ over $\mathbb{Q}$. Thus, the 4 primitive fifth roots break up into two (disjoint) bunches of 2, grouped by being the 2 roots of the same quadratic over $\mathbb{Q}(\sqrt{5})$. That is, the fifth cyclotomic polynomial factors as the product of those two minimal polynomials (which are necessarily irreducible over $\mathbb{Q}(\sqrt{5})$).

In fact, we have a trick to determine the two quadratic polynomials. Since

$$\zeta^4 + \zeta^3 + \zeta^2 + \zeta + 1 = 0$$

divide through by ζ^2 to obtain

$$\zeta^2 + \zeta + 1 + \zeta^{-1} + \zeta^{-2} = 0$$

Thus, regrouping,

$$\left(\zeta + \frac{1}{\zeta}\right)^2 + \left(\zeta + \frac{1}{\zeta}\right)^2 - 1 = 0$$

Thus, $\xi = \zeta + \zeta^{-1}$ satisfies the equation

$$x^2 + x - 1 = 0$$

and $\xi = (-1 \pm \sqrt{5})/2$. Then, from

$$\zeta + \frac{1}{\zeta} = (-1 \pm \sqrt{5})/2$$

multiply through by ζ and rearrange to

$$\zeta^2 - \frac{-1 \pm \sqrt{5}}{2}\,\zeta + 1 = 0$$

Thus,

$$x^4 + x^3 + x^2 + x + 1 = \left(x^2 - \frac{-1 + \sqrt{5}}{2}\,x + 1\right)\left(x^2 - \frac{-1 - \sqrt{5}}{2}\,x + 1\right)$$

Alternatively, to see what can be done similarly in more general situations, we recall that $\mathbb{Q}(\sqrt{5})$ is the subfield of $\mathbb{Q}(\zeta)$ fixed pointwise by the automorphism $\zeta \to \zeta^{-1}$. Thus, the 4 primitive fifth roots of unity

should be paired up into the orbits of this automorphism. Thus, the two (irreducible in $\mathbb{Q}(\sqrt{5})[x]$) quadratics are

$$(x-\zeta)(x-\zeta^{-1}) = x^2 - (\zeta+\zeta^{-1})x + 1$$
$$(x-\zeta^2)(x-\zeta^{-2}) = x^2 - (\zeta^2+\zeta^{-2})x + 1$$

Again, without imbedding things into the complex numbers, etc., there is no canonical one of the two square roots of 5, so the $\pm\sqrt{5}$ just means that whichever one we pick first the other one is its negative. Similarly, there is no distinguished one among the 4 primitive fifth roots unless we imbed them into the complex numbers. There is no need to do this. Rather, specify one ζ, and specify a $\sqrt{5}$ by

$$\zeta + \zeta^{-1} = \frac{-1+\sqrt{5}}{2}$$

Then necessarily

$$\zeta^2 + \zeta^{-2} = \frac{-1-\sqrt{5}}{2}$$

And we find the same two quadratic equations again. Since they are necessarily the minimal polynomials of ζ and of ζ^2 over $\mathbb{Q}(\sqrt{5})$ (by the degree considerations) they are irreducible in $\mathbb{Q}(\sqrt{5})[x]$. ///

[11.4] The 7^{th} cyclotomic polynomial $\Phi_7(x)$ factors into two irreducible cubic factors over $\mathbb{Q}(\sqrt{-7}$. Find the two irreducible factors.

Let ζ be a primitive 7^{th} root of unity. Let $H = \langle\tau\rangle$ be the order 3 subgroup of the automorphism group $G \approx (\mathbb{Z}/7)^\times$ of $\mathbb{Q}(\zeta)$ over $\mathbb{Q}$, where $\tau = \sigma_2$ is the automorphism $\tau(\zeta) = \zeta^2$, which has order 3. We have seen that $\mathbb{Q}(\sqrt{-7})$ is the subfield fixed pointwise by H. In particular, $\alpha = \zeta + \zeta^2 + \zeta^4$ should be at most quadratic over $\mathbb{Q}$. Recapitulating the earlier discussion, α is a zero of the quadratic polynomial

$$(x - (\zeta + \zeta^2 + \zeta^4))(x - (\zeta^3 + \zeta^6 + \zeta^5))$$

which will have coefficients in $\mathbb{Q}$, since we have arranged that the coefficients are G-invariant. Multiplying out and simplifying, this is

$$x^2 + x + 2$$

with zeros $(-1 \pm \sqrt{-7})/2$.

The coefficients of the polynomial

$$(x-\zeta)(x-\tau(\zeta))(x-\tau^2(\zeta)) = (x-\zeta)(x-\zeta^2)(x-\zeta^4)$$

will be H-invariant and therefore will lie in $\mathbb{Q}(\sqrt{-7})$. In parallel, taking the primitive 7^{th} root of unity ζ^3 which is not in the H-orbit of ζ, the cubic

$$(x-\zeta^3)(x-\tau(\zeta^3))(x-\tau^2(\zeta^3)) = (x-\zeta^3)(x-\zeta^6)(x-\zeta^5)$$

will also have coefficients in $\mathbb{Q}(\sqrt{-7})$. It is no coincidence that the exponents of ζ occuring in the two cubics are disjoint and exhaust the list $1, 2, 3, 4, 5, 6$.

Multiplying out the first cubic, it is

$$(x-\zeta)(x-\zeta^2)(x-\zeta^4) = x^3 - (\zeta+\zeta^2+\zeta^4)x^2 + (\zeta^3+\zeta^5+\zeta^6)x - 1$$
$$= x^3 - \left(\frac{-1+\sqrt{-7}}{2}\right)x^2 + \left(\frac{-1-\sqrt{-7}}{2}\right)x - 1$$

for a choice of ordering of the square roots. (Necessarily!) the other cubic has the roles of the two square roots reversed, so is

$$(x-\zeta^3)(x-\zeta^6)(x-\zeta^2) = x^3 - (\zeta^3+\zeta^5+\zeta^6)x + (\zeta+\zeta^2+\zeta^4)x - 1$$

$$= x^3 - \left(\frac{-1-\sqrt{-7}}{2}\right)x^2 + \left(\frac{-1+\sqrt{-7}}{2}\right)x - 1$$

Since the minimal polynomials of primitive 7^{th} roots of unity are of degree 3 over $\mathbb{Q}(\sqrt{-7})$ (by multiplicativity of degrees in towers), these cubics are irreducible over $\mathbb{Q}(\sqrt{-7})$. Their product is $\Phi_7(x)$, since the set of all 6 roots is all the primitive 7^{th} roots of unity, and there is no overlap between the two sets of roots. ///

[11.5] Let ζ be a primitive 13^{th} root of unity in an algebraic closure of $\mathbb{Q}$. Find an element α in $\mathbb{Q}(\zeta)$ which satisfies an irreducible cubic with rational coefficients. Find an element β in $\mathbb{Q}(\zeta)$ which satisfies an irreducible quartic with rational coefficients. Determine the cubic and the quartic explicitly.

Again use the fact that the automorphism group G of $\mathbb{Q}(\zeta)$ over $\mathbb{Q}$ is isomorphic to $(\mathbb{Z}/13)^\times$ by $a \to \sigma_a$ where $\sigma_a(\zeta) = \zeta^a$. The unique subgroup A of order 4 is generated by $\mu = \sigma_5$. From above, an element $\alpha \in \mathbb{Q}(\zeta)$ fixed by A is of degree at most $|G|/|A| = 12/4 = 3$ over $\mathbb{Q}$. Thus, try symmetrizing/averaging ζ itself over the subgroup A by

$$\alpha = \zeta + \mu(\zeta) + \mu^2(\zeta) + \mu^3(\zeta) = \zeta + \zeta^5 + \zeta^{12} + \zeta^8$$

The unique subgroup B of order 3 in G is generated by $\nu = \sigma_3$. Thus, necessarily the coefficients of

$$(x-\alpha)(x-\nu(\alpha))(x-\nu^2(\alpha))$$

are in $\mathbb{Q}$. Also, one can see directly (because the ζ^i with $1 \le i \le 12$ are linearly independent over $\mathbb{Q}$) that the images $\alpha, \nu(\alpha), \nu^2(\alpha)$ are distinct, assuring that the cubic is irreducible over $\mathbb{Q}$.

To multiply out the cubic and determine the coefficients as rational numbers it is wise to be as economical as possible in the computation. Since we know *a priori* that the coefficients are rational, we need not drag along all the powers of ζ which appear, since there will necessarily be cancellation. Precisely, we compute in terms of the $\mathbb{Q}$-basis

$$1,\ \zeta,\ \zeta^2,\ \ldots,\ \zeta^{10},\ \zeta^{11}$$

Given ζ^n appearing in a sum, reduce the exponent n modulo 13. If the result is 0, add 1 to the sum. If the result is 12, add -1 to the sum, since

$$\zeta^{12} = -(1 + \zeta + \zeta^2 + \ldots + \zeta^{11})$$

expresses ζ^{12} in terms of our basis. If the reduction mod 13 is anything else, drop that term (since we know it will cancel). And we can go through the monomial summand in lexicographic order. Using this bookkeeping strategy, the cubic is

$$\left(x - (\zeta + \zeta^5 + \zeta^{12} + \zeta^8)\right)\left(x - (\zeta^3 + \zeta^2 + \zeta^{10} + \zeta^{11})\right)\left(x - (\zeta^9 + \zeta^6 + \zeta^4 + \zeta^7)\right)$$

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

Yes, there are $3{\cdot}4^2$ terms to sum for the coefficient of x, and 4^3 for the constant term. Most give a contribution of 0 in our bookkeeping system, so the workload is not completely unreasonable. (A numerical computation offers a different sort of check.) Note that Eisenstein's criterion (and Gauss' lemma) gives another proof of the irreducibility, by replacing x by $x + 4$ to obtain

$$x^3 + 13x^2 + 52x + 65$$

and noting that the prime 13 fits into the Eisenstein criterion here. This is yet another check on the computation.

For the quartic, reverse the roles of μ and ν above, so put

$$\beta = \zeta + \nu(\zeta) + \nu^2(\zeta) = \zeta + \zeta^3 + \zeta^9$$

and compute the coefficients of the quartic polynomial

$$(x-\beta)(x-\mu(\beta))(x-\mu^2(\beta))(x-\mu^3(\beta))$$

$$= \left(x-(\zeta+\zeta^3+\zeta^9)\right)\left(x-(\zeta^5+\zeta^2+\zeta^6)\right)\left(x-(\zeta^{12}+\zeta^{10}+\zeta^4)\right)\left(x-(\zeta^8+\zeta^{11}+\zeta^7)\right)$$

Use the same bookkeeping approach as earlier, to allow a running tally for each coefficient. The sum of the 4 triples is -1. For the other terms some writing-out seems necessary. For example, to compute the constant coefficient, we have the product

$$(\zeta+\zeta^3+\zeta^9)(\zeta^5+\zeta^2+\zeta^6)(\zeta^{12}+\zeta^{10}+\zeta^4)(\zeta^8+\zeta^{11}+\zeta^7)$$

which would seem to involve 81 summands. We can lighten the burden by notating only the exponents which appear, rather than recopying zetas. Further, multiply the first two factors and the third and fourth, leaving a multiplication of two 9-term factors (again, retaining only the exponents)

$$(\,6\quad 3\quad 7\quad 8\quad 5\quad 9\quad 1\quad 11\quad 2\,)(\,7\quad 10\quad 6\quad 5\quad 8\quad 4\quad 12\quad 2\quad 11\,)$$

As remarked above, a combination of an exponent from the first list of nine with an exponent from the second list will give a non-zero contribution only if the sum (reduced modulo 13) is either 0 or 12, contributing 1 or -1 respectively. For each element of the first list, we can keep a running tally of the contributions from each of the 9 elements from the second list. Thus, grouping by the elements of the first list, the contributions are, respectively,

$$(1-1)+(1)+(1-1)+(1-1)+(-1+1)+(1)+(1-1)+(1)(-1+1)=3$$

The third symmetric function is a sum of 4 terms, which we group into two, writing in the same style

$$(\,1\quad 3\quad 9\quad 5\quad 2\quad 6\,)(\,7\quad 10\quad 6\quad 5\quad 8\quad 4\quad 12\quad 2\quad 11\,)$$

$$+(\,6\quad 3\quad 7\quad 8\quad 5\quad 9\quad 1\quad 11\quad 2\,)(\,12\quad 10\quad 4\quad 8\quad 11\quad 7\,)$$

In each of these two products, for each item in the lists of 9, we tally the contributions of the 6 items in the other list, obtaining,

$$(0+0-1+0+1+1+1+0+0)+(1+1+0-1+0+1+0+0+0)=4$$

The computation of the second elementary symmetric function is, similarly, the sum

$$(\,1\quad 3\quad 9\,)(\,5\quad 2\quad 6\quad 12\quad 10\quad 4\quad 8\quad 11\quad 7\,)$$

$$+(\,5\quad 2\quad 6\,)(\,12\quad 10\quad 4\quad 8\quad 11\quad 7\,)+(\,12\quad 10\quad 4\,)(\,8\quad 11\quad 7\,)$$

Grouping the contributions for each element in the lists $1,3,9$ and $5,2,6$ and $12,10,4$, this gives

$$[(1-1)+(1)+(1)]+[(1-1)+(-1+1)+(1)]+[0+0+(-1)]=2$$

Thus, in summary, we have

$$x^4+x^3+2\,x^2-4x+3$$

Again, replacing x by $x+3$ gives

$$x^4+13x^3+65x^2+143x+117$$

All the lower coefficients are divisible by 13, but not by 13^2, so Eisenstein proves irreducibility. This again gives a sort of verification of the correctness of the numerical computation. ///

[11.6] Let $f(x) = x^8 + x^6 + x^4 + x^2 + 1$. Show that f factors into two irreducible quartics in $\mathbb{Q}[x]$. Show that

$$x^8 + 5x^6 + 25x^4 + 125x^2 + 625$$

also factors into two irreducible quartics in $\mathbb{Q}[x]$.

The first assertion can be verified by an elementary trick, namely

$$x^8 + x^6 + x^4 + x^2 + 1 = \frac{x^{10} - 1}{x^2 - 1} = \frac{\Phi_1(x)\Phi_2(x)\Phi_5(x)\Phi_{10}(x)}{\Phi_1(x)\Phi_2(x)}$$

$$= \Phi_5(x)\Phi_{10}(x) = (x^4 + x^3 + x^2 + x + 1)(x^4 - x^3 + x^2 - x + 1)$$

But we do learn something from this, namely that the factorization of the first octic into linear factors naturally has the 8 linear factors occurring in two bunches of 4, namely the primitive 5^{th} roots of unity and the primitive 10^{th} roots of unity. Let ζ be a primitive 5^{th} root of unity. Then $-\zeta$ is a primitive 10^{th}. Thus, the 8 zeros of the *second* polynomial will be $\sqrt{5}$ times primitive 5^{th} and 10^{th} roots of unity. The question is how to group them together in two bunches of four so as to obtain rational coefficients of the resulting two quartics.

The automorphism group G of $\mathbb{Q}(\zeta)$ over $\mathbb{Q}$ is isomorphic to $(\mathbb{Z}/10)^\times$, which is generated by $\tau(\zeta) = \zeta^3$. That is, taking a product of linear factors whose zeros range over an orbit of ζ under the automorphism group G,

$$x^4 + x^3 + x^2 + x + 1 = (x - \zeta)(x - \zeta^3)(x - \zeta^9)(x - \zeta^7)$$

has coefficients in $\mathbb{Q}$ and is the minimal polynomial for ζ over $\mathbb{Q}$. Similarly looking at the orbit of $-\zeta$ under the automorphism group G, we see that

$$x^4 - x^3 + x^2 - x + 1 = (x + \zeta)(x + \zeta^3)(x + \zeta^9)(x + \zeta^7)$$

has coefficients in $\mathbb{Q}$ and is the minimal polynomial for $-\zeta$ over $\mathbb{Q}$.

The discussion of Gauss sums in the proof of quadratic reciprocity gives us the convenient

$$\zeta - \zeta^2 - \zeta^3 + \zeta^4 = \sqrt{5}$$

Note that this expression allows us to see what effect the automorphism $\sigma_a(\zeta) = \zeta^a$ has on $\sqrt{5}$

$$\sigma_a(\sqrt{5}) = \sigma_a(\zeta - \zeta^2 - \zeta^3 + \zeta^4) = \begin{cases} \sqrt{5} & (\text{for } a = 1, 9) \\ -\sqrt{5} & (\text{for } a = 3, 7) \end{cases}$$

Thus, the orbit of $\sqrt{5}\zeta$ under G is

$$\sqrt{5}\zeta,\ \tau(\sqrt{5}\zeta) = -\sqrt{5}\zeta^3,\ \tau^2(\sqrt{5}\zeta) = \sqrt{5}\zeta^4,\ \tau^3(\sqrt{5}\zeta) = -\sqrt{5}\zeta^2$$

giving quartic polynomial

$$(x - \sqrt{5}\zeta)(x + \sqrt{5}\zeta^3)(x - \sqrt{5}\zeta^4)(x + \sqrt{5}\zeta^2)$$

$$= x^4 - \sqrt{5}(\zeta - \zeta^2 - \zeta^3 + \zeta^4)x^3 + 5(-\zeta^4 + 1 - \zeta^3 - \zeta^2 + 1 - \zeta)x^2 - 5\sqrt{5}(\zeta^4 - \zeta^2 + \zeta - \zeta^3)x + 25$$

$$= x^4 - 5x^3 + 15x^2 - 25x + 25$$

We might already be able to anticipate what happens with the other bunch of four zeros, but we can also compute directly (perhaps confirming a suspicion). The orbit of $-\sqrt{5}\zeta$ under G is

$$-\sqrt{5}\zeta,\ \tau(-\sqrt{5}\zeta) = \sqrt{5}\zeta^3,\ \tau^2(-\sqrt{5}\zeta) = -\sqrt{5}\zeta^4,\ \tau^3(-\sqrt{5}\zeta) = \sqrt{5}\zeta^2$$

giving quartic polynomial

$$(x+\sqrt{5}\zeta)(x-\sqrt{5}\zeta^3)(x+\sqrt{5}\zeta^4)(x-\sqrt{5}\zeta^2)$$
$$= x^4 + \sqrt{5}(\zeta - \zeta^2 - \zeta^3 + \zeta^4)x^3 + 5(-\zeta^4 + 1 - \zeta^3 - \zeta^2 + 1 - \zeta)x^2 + 5\sqrt{5}(\zeta^4 - \zeta^2 + \zeta - \zeta^3)x + 25$$
$$= x^4 + 5x^3 + 15x^2 + 25x + 25$$

Thus, we expect that

$$x^8 + 5x^6 + 25x^4 + 125x^2 + 625 = (x^4 - 5x^3 + 15x^2 - 25x + 25) \cdot (x^4 + 5x^3 + 15x^2 + 25x + 25)$$

Note that because of the sign flips in the odd-degree terms in the quartics, the octic can also be written as

$$x^8 + 5x^6 + 25x^4 + 125x^2 + 625 = (x^4 + 15x^2 + 25)^2 - 25(x^3 + 5x)^2$$

(This factorization of an altered product of two cyclotomic polynomials is sometimes called an *Aurifeuille-LeLasseur* factorization after two amateur mathematicians who studied such things, brought to wider attention by E. Lucas in the late 19^{th} century.) ///

[11.7] Let p be a prime not dividing m. Show that in $\mathbb{F}_p[x]$

$$\Phi_{mp}(x) = \Phi_m(x)^{p-1}$$

From the recursive definition,

$$\Phi_{pm}(x) = \frac{x^{pm} - 1}{\prod_{d|m} \Phi_{p^e d}(x) \cdot \prod_{d|m,\ d<m} \Phi_{pd}(x)}$$

In characteristic p, the numerator is $(x^m - 1)^p$. The first product factor in the denominator is $x^m - 1$. Thus, the whole is

$$\Phi_{pm}(x) = \frac{(x^m - 1)^p}{(x^m - 1) \cdot \prod_{d|m,\ d<m} \Phi_{pd}(x)}$$

By induction on $d < m$, in the last product in the denominator has factors

$$\Phi_{pd}(x) = \Phi_d(x)^{p-1}$$

Cancelling,

$$\Phi_{pm}(x) = \frac{(x^m - 1)^p}{(x^m - 1) \cdot \prod_{d|m,\ d<m} \Phi_d(x)^{p-1}} = \frac{(x^m - 1)^{p-1}}{\prod_{d|m,\ d<m} \Phi_d(x)^{p-1}}$$
$$= \left(\frac{x^m - 1}{\prod_{d|m,\ d<m} \Phi_d(x)} \right)^{p-1}$$

which gives $\Phi_m(x)^{p-1}$ as claimed, by the recursive definition. ///