(*January 14, 2009*)

[05.1] Gracefully verify that the octic $x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$ factors properly in $\mathbb{Q}[x]$.

This octic is

$$\frac{x^9 - 1}{x - 1} = \frac{x^3 - 1)(x^6 + x^3 + 1)}{x - 1} = (x^2 + x + 1)\,(x^6 + x^3 + 1)$$

for example. We might anticipate this reducibility by realizing that

$$x^9 - 1 = \Phi_1(x)\,\Phi_3(x)\,\Phi_9(x)$$

where Φ_n is the n^{th} cyclotomic polynomial, and the given octic is just $(x^9 - 1)/\Phi_1(x)$, so what is left *at least* factors as $\Phi_3(x)\,\Phi_9(x)$.

[05.2] Gracefully verify that the quartic $x^4 + x^3 + x^2 + x + 1$ is irreducible in $\mathbb{F}_2[x]$.

Use the recursive definition of cyclotomic polynomials

$$\Phi_n(x) = \frac{x^n - 1}{\prod_{d|n,\ d<n}\ \Phi_d(x)}$$

Thus, the given quartic is $\Phi_5(x)$. And use the fact that for the characteristic of the field k not dividing n, $\Phi_n(\alpha) = 0$ if and only if α is of order n in $k^\times$. If it had a linear factor $x - \alpha$ with $\alpha \in \mathbb{F}_2$, then $\Phi_4(\alpha) = 0$, and α would be of order 5 in $\mathbb{F}_2^\times$. But $\mathbb{F}_2^\times$ is of order 1, so has no elements of order 5 (by Lagrange). (We saw earlier that) existence of an irreducible quadratic factor of $\Phi_4(x)$ in $\mathbb{F}_2[x]$ is equivalent to existence of an element α of order 5 in $\mathbb{F}_{2^2}^\times$, but $|\mathbb{F}_{2^2}^\times| = 2^2 - 1 = 3$, which is not divisible by 5, so (Lagrange) has no element of order 5. The same sort of argument would show that there is no irreducible cubic factor, but we already know this since if there were any proper factorization then there would be a proper factor of at most half the degree of the quartic. But there is no linear or quadratic factor, so the quartic is irreducible.

[05.3] Gracefully verify that the sextic $x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$ is irreducible in $\mathbb{F}_3[x]$.

Use the recursive definition of cyclotomic polynomials

$$\Phi_n(x) = \frac{x^n - 1}{\prod_{d|n,\ d<n}\ \Phi_d(x)}$$

Thus, the given sextic is $\Phi_7(x)$. And use the fact that for the characteristic of the field k not dividing n, $\Phi_n(\alpha) = 0$ if and only if α is of order n in $k^\times$. If it had a linear factor $x - \alpha$ with $\alpha \in \mathbb{F}_3$, then $\Phi_7(\alpha) = 0$, and α would be of order 7 in $\mathbb{F}_2^\times$. But $\mathbb{F}_3^\times$ is of order 2, so has no elements of order 7 (Lagrange). Existence of an (irreducible) quadratic factor of $\Phi_7(x)$ in $\mathbb{F}_3[x]$ is equivalent to existence of an element α of order 7 in $\mathbb{F}_{3^2}^\times$, but $|\mathbb{F}_{3^2}^\times| = 3^2 - 1 = 8$, which is not divisible by 7, so (Lagrange) has no element of order 5. Similarly, if there were an (irreducible) cubic factor, then there would be a root in a cubic extension $\mathbb{F}_{3^3}$ of $\mathbb{F}_3$, but $\mathbb{F}_{3^3}^\times$ has order $3^3 - 1 = 26$ which is not divisible by 7, so there is no such element. If there were any proper factorization then there would be a proper factor of at most half the degree of the sextic. But there is no linear, quadratic, or cubic factor, so the sextic is irreducible.

[05.4] Gracefully verify that the quartic $x^4 + x^3 + x^2 + x + 1$ in factors into two irreducible quadratics in $\mathbb{F}_{19}[x]$.

As above, we see that the quartic is the 5^{th} cyclotomic polynomial. If it had a linear factor in $\mathbb{F}_{19}[x]$ then (since the characteristic 19 does not divide the index 5) there would be an element of order 5 in $\mathbb{F}_{19}^\times$, but the latter group has order $19 - 1$ not divisible by 5, so (Lagrange) there is no such element. But the quadratic extension $\mathbb{F}_{19^2}$ of $\mathbb{F}_{19}$ has multiplicative group with order $19^2 - 1 = 360$ which is divisible by 5, so there is an element α of order 5 there.

Since $\alpha \in \mathbb{F}_{19^2} - \mathbb{F}_{19}$, the minimal polynomial $M(x)$ of α over $\mathbb{F}_{19}$ is quadratic. We have shown that in this circumstance the polynomial M divides the quartic. (Again, the proof is as follows: Let

$$x^4 + x^3 + x^2 + x + 1 = Q(x) \cdot M(x) + R(x)$$

with $Q, R \in \mathbb{F}_{19}[x]$ and $\deg R < \deg M$. Evaluating at α gives $R(\alpha) = 0$, which (by minimality of M) implies R is the 0 polynomial. Thus, M divides the quartic.) The quotient of the quartic by M is quadratic, and (as we've already seen) has no linear factor in $\mathbb{F}_{19}[x]$, so is irreducible.

[05.5] Let $f(x) = x^6 - x^3 + 1$. Find primes p with each of the following behaviors: f is irreducible in $\mathbb{F}_p[x]$, f factors into irreducible quadratic factors in $\mathbb{F}_p[x]$, f factors into irreducible cubic factors in $\mathbb{F}_p[x]$, f factors into linear factors in $\mathbb{F}_p[x]$.

By the recursive definition and properties of cyclotomic polynomials, we recognize $f(x)$ as the 18^{th} cyclotomic polynomial $\Phi_{18}(x)$. For a prime p not dividing 18, zeros of Φ_{18} are exactly elements of order 18. Thus, if $p^d - 1 = 0 \bmod 18$ but no smaller exponent than d achieves this effect, then $\mathbb{F}_{p^d}^\times$ (proven *cyclic* by now) has an element of order 18, whose minimal polynomial divides $\Phi_{18}(x)$.

We might observe that $(\mathbb{Z}/18)^\times$ is itself *cyclic*, of order $\varphi(18) = \varphi(2)\varphi(3^2) = (3-1)3 = 6$, so has elements of all possible orders, namely $1, 2, 3, 6$.

For $p = 1 \bmod 18$, for example $p = 19$, already $p - 1 = 0 \bmod 18$, so $f(x)$ has a *linear* factor in $\mathbb{F}_{19}[x]$. This is the case of order 1 element in $(\mathbb{Z}/18)^\times$.

A moment's thought might allow a person to realize that $17 = -1$ is an element (and the only element) of order 2 in $(\mathbb{Z}/18)^\times$. So any prime $p = 17 \bmod 18$ (for example $p = 17$ itself, by coincidence prime) will have the property that $\mathbb{F}_{p^2}^\times$ has elements of order 18. Indeed, by properties of cyclic groups, it will have $\varphi(18) = 6$ elements of order 18 there, each of whose minimal polynomial is quadratic. Thus (since a quadratic has at most two zeros) there are at least 3 irreducible quadratics dividing the sextic $\Phi_{18}(x)$ in $\mathbb{F}_p[x]$. Thus, since degrees add in products, these three quadratics are *all* the factors of the sextic.

After a bit of trial and error, one will find an element of order 3 in $(\mathbb{Z}/18)^\times$, such as 7. Thus, for $p = 7 \bmod 18$ (such as 7 itself, which by coincidence is prime), there is no element of order 18 in $\mathbb{F}_p$ or in $\mathbb{F}_{p^2}$, but there *is* one in $\mathbb{F}_{p^3}$, whose minimal polynomial over $\mathbb{F}_p$ is therefore cubic and divides Φ_{18}. Again, by properties of cyclic groups, there are exactly $\varphi(18) = 6$ such elements in $\mathbb{F}_{p^3}$, with cubic minimal polynomials, so there are at least (and, thus, exactly) two different irreducible cubics in $\mathbb{F}_p[x]$ dividing $\Phi_{18}(x)$ for such p.

After a bit more trial and error, one finds an element of order 6 in $(\mathbb{Z}/18)^\times$, such as 5. (The other is 11.) Thus, for $p = 5 \bmod 18$ (such as 5 itself, which by coincidence is prime), there is no element of order 18 in $\mathbb{F}_p$ or in $\mathbb{F}_{p^2}$, or $\mathbb{F}_{p^3}$, but there is one in $\mathbb{F}_{p^6}$. (By Lagrange, the only possible orders of p in $(\mathbb{Z}/18)^\times$ are $1, 2, 3, 6$, so we need not worry about p^4 or p^5). The minimal polynomial of such an element is $\Phi_{18}(x)$, which is (thus, necessarily) irreducible in $\mathbb{F}_p[x]$.

[05.6] Explain why $x^4 + 1$ properly factors in $\mathbb{F}_p[x]$ for any prime p.

As in the previous problems, we observe that $x^4 + 1$ is the 8^{th} cyclotomic polynomial. If $p|8$, namely $p = 2$, then this factors as $(x-1)^4$. For odd p, if $p = 1 \bmod 8$ then $\mathbb{F}_p^\times$, which we now know to be *cyclic*, has an element of order 8, so $x^4 + 1$ has a linear factor. If $p \neq 1 \bmod 8$, write $p = 2m + 1$, and note that

$$p^2 - 1 = (2m+1)^2 - 1 = 4m^2 + 4m = m(m+1) \cdot 4$$

so, if m is odd, $m + 1$ is even and $p^2 - 1 = 0 \bmod 8$, and if m is even, the same conclusion holds. That is, for odd p, $p^2 - 1$ is invariably divisible by 8. That is, (using the cyclic-ness of any finite field) there is an element of order 8 in $\mathbb{F}_{p^2}$. The minimal polynomial of this element, which is quadratic, divides $x^4 + 1$ (as proven in class, with argument recalled above in another example).

[05.7] Explain why $x^8 - x^7 + x^5 - x^4 + x^3 - x + 1$ properly factors in $\mathbb{F}_p[x]$ for any prime p. (*Hint:* It factors either into linear factors, irreducible quadratics, or irreducible quartics.)

The well-read person will recognize this octic as $\Phi_{15}(x)$, the fifteenth cyclotomic polynomial. For a prime p not dividing 15, zeros of Φ_15 in a field $\mathbb{F}_{p^d}$ are elements of order 15, which happens if and only if

$p^d - 1 = 0 \bmod 15$, since we have shown that $\mathbb{F}_{p^d}^\times$ is cyclic. The smallest d such that $p^d = 1 \bmod 15$ is the order of p in $(\mathbb{Z}/15)^\times$. After some experimentation, one may realize that $(\mathbb{Z}/15)^\times$ is *not* cyclic. In particular, every element is of order 1, 2, or 4. (How to see this?) Granting this, for any p other than 3 or 5, the minimal polynomial of an order 15 element is linear, quadratic, or quartic, and divides Φ_{15}.

For $p = 3$, there is some degeneration, namely $x^3 - 1 = (x-1)^3$. Thus, in the (universal) expression

$$\Phi_{15}(x) = \frac{x^{15}-1}{\Phi_1(x)\,\Phi_3(x)\,\Phi_5(x)}$$

we actually have

$$\Phi_{15}(x) = \frac{(x^5-1)^3}{(x-1)^2\,(x^5-1)} = \frac{(x^5-1)^2}{(x-1)^2} = (x^4+x^3+x^2+1)^2$$

For $p = 5$, similarly, $x^5 - 1 = (x-1)^5$, and

$$\Phi_{15}(x) = \frac{x^{15}-1}{\Phi_1(x)\,\Phi_3(x)\,\Phi_5(x)} = \frac{(x^3-1)^5}{(x^3-1)\,(x-1)^4} = \frac{(x^3-1)^4}{(x-1)^4} = (x^2+x+1)^4$$

[05.8] Why is $x^4 - 2$ irreducible in $\mathbb{F}_5[x]$?

A zero of this polynomial would be a fourth root of 2. In $\mathbb{F}_5^\times$, one verifies by brute force that 2 is of order 4, so is a generator for that (cyclic) group, so is not a square in $\mathbb{F}_5^\times$, much less a fourth power. Thus, there is no linear factor of $x^4 - 2$ in $\mathbb{F}_5[x]$.

The group $\mathbb{F}_{5^2}^\times$ is cyclic of order 24. If 2 were a fourth power in $\mathbb{F}_{5^2}$, then $2 = \alpha^4$, and $2^4 = 1$ gives $\alpha^{16} = 1$. Also, $\alpha^{24} = 1$ (Lagrange). Claim that $\alpha^8 = 1$: let $r, s \in \mathbb{Z}$ be such that $r \cdot 16 + s \cdot 24 = 8$, since 8 is the greatest common divisor. Then

$$\alpha^8 = \alpha^{16r+24s} = (\alpha^{16})^r \cdot (\alpha^{24})^s = 1$$

This would imply

$$2^2 = (\alpha^4)^2 = \alpha^8 = 1$$

which is false. Thus, 2 is not a fourth power in $\mathbb{F}_{5^2}$, so the polynomial $x^4 - 2$ has no quadratic factors.

A quartic with no linear or quadratic factors is irreducible (since any proper factorization of a polynomial P must involve a factor of degree at most half the degree of P). Thus, $x^4 - 2$ is irreducible in $\mathbb{F}_5[x]$.

[05.9] Why is $x^5 - 2$ irreducible in $\mathbb{F}_{11}[x]$?

As usual, to prove irreducibility of a quintic it suffices to show that there are no linear or quadratic factors. To show the latter it suffices to show that there is no zero in the underlying field (for linear factors) or in a quadratic extension (for irreducible quadratic factors).

First determine the order of 2 in $\mathbb{F}_{11}$: since $|\mathbb{F}_{11}^\times| = 10$, it is either $1, 2, 5$, or 10. Since $2 \neq 1 \bmod 11$, and $2^2 - 1 = 3 \neq 0 \bmod 11$, and $2^5 - 1 = 31 \neq 0 \bmod 11$, the order is 10. Thus, in $\mathbb{F}_{11}$ it cannot be that 2 is a fifth power.

The order of $\mathbb{F}_{11^2}^\times$ is $11^2 - 1 = 120$. If there were a fifth root α of 2 there, then $\alpha^5 = 2$ and $2^{10} = 1$ imply $\alpha^{50} = 1$. Also, (Lagrange) $\alpha^{120} = 1$. Thus, (as in the previous problem) α has order dividing the *gcd* of 50 and 120, namely 10. Thus, if there were such α, then

$$2^2 = (\alpha^5)^2 = \alpha^{10} = 1$$

But $2^2 \neq 1$, so there is no such α.