January 2018, Q3

Fact: the unique monic irreducible polynomial (AKA minimal polynomial) of the nth primitive root of unity is the nth cyclotomic polynomial

$$x^n - 1 = \prod_{d \mid n} \Phi_d(x).$$

Fact: if p is a prime number, then the pth cyclotomic polynomial is given by

$$\Phi_p(x) = \sum_{i=0}^{p-1} x^i = \frac{X^{p-1}}{x-1}.$$

Fact: the pth cyclotomic polynomial satisfies

$\Phi_p(x+1)$ is p-Eisenstein (and hence irreducible).

Fact: if p(x) is the unique irreducible monic polynomial with root C, then the dimension of the k-vector space k(C) is the degree p(x). Put another way, we have that [k(C) : k] = deg(p).

Fact: the Galois group of the nth cyclotomic polynomial is the group of units of Z/nZ.

$$\mathrm{Gal}_{\mathbb{Q}}(\mathbb{Q}(\omega), \mathbb{Q}) \cong (\mathbb{Z}/_n\mathbb{Z})^{\times} \cong \frac{\mathbb{Z}}{\phi(n)\mathbb{Z}}$$

$\phi(n) =$ #{k | k is a positive integer and gcd(k, n) = 1} = Euler totient function of n

$\omega =$ primitive nth root of unity

If m is a unit modulo n, then there exists an x such mx = 1 (mod n). Put another way, there exists a y such that mx + ny = 1. By Bézout's Theorem, we must have that gcd(m, n) = 1.

$$x^4 - 1 = \Phi_1(x)\,\Phi_2(x)\,\Phi_4(x) \qquad \Phi_1(x) = x - 1$$

$$\frac{x^4 - 1}{(x-1)(x+1)} = x^2 + 1 = \Phi_4(x)$$

---

August 2014, Q6

Hint: the characteristic of F = Z/31Z is 31. In particular, it's finite, so we have access to things like Fermat's Little Theorem.

Fermat's Little Theorem: $a^{p-1} \equiv 1 \pmod{p}$ for all nonzero a in a field of characteristic p.

$$\alpha^5 \equiv 2 \Rightarrow \alpha^{30} \equiv 2^6 \equiv 2 \quad >!< \quad \longleftarrow \left\{ \begin{array}{l} \alpha^5 \equiv 2 \\ \alpha^{?} \equiv 1 \end{array} \right. \pmod{31}$$

Hint: if alpha is a root of some irreducible quadratic factor, then there is a field extension F(alpha) of F of degree 2, so the order of F(alpha) is 31^2 = 961.

August 2018, Q3

Observation: there is no elegant way to do this (i.e., no Eisentein, no Gauss's Lemma), so we need to proceed by brute-force check.

Silver Lining: this is degree five, so it suffices to show there are no irreducible linear or quadratic factors (because $5 = 4 + 1 = 3 + 2 = 3 + 1 + 1 = 2 + 1 + 1 + 1 = 1 + 1 + 1 + 1 + 1$).

Factor Theorem: $f(x)$ has a linear factor $x - a$ if and only if $f(a) = 0$.

$x^2$, $x^2 + 1$, $x^2 + x$, $\boxed{x^2 + x + 1}$ are the only quadratic polynomials.

reducible factors    irreducible factor

Show that $x^2 + x + 1$ does not divide $f(x)$. (Use the Division Algorithm.)

---

January 2010, Q4, involves some trickery (explicitly, you need to use some trig identities), so don't worry about that one too much. January 2015, Q4, gets the idea across.

January 2017, Q4b, is a painful computation. August 2018, Q3b, gets the idea across.