# 7210 HW 12

Duncan Wilkie

29 November 2022

**Problem 1** (D&F 13.1.1)**.** *Show that $p(x) = x^3 + 9x + 6$ is irreducible in $\mathbb{Q}[x]$. Let $\theta$ be a root of $p(x)$. Find the inverse of $1 + \theta$ in $\mathbb{Q}(\theta)$.*

*Proof.* The first part is immediate from Eisenstein's criterion over $\mathbb{Z}[x]$: $p$ is a monic polynomial with 3 dividing all non-leading coefficients and $3^2 = 9$ not dividing its constant coefficient, so it is irreducible in $\mathbb{Q}[x]$. In the field $\mathbb{Q}[x]$, which is of course a PID, we can find multipliers satisfying the Bézout relation

$$a(x)(1 + x) + b(x)(x^3 + 9x + 6) = 1$$

since the gcd of the two fixed factors is 1 because $p$ is irreducible. Equivalently,

$$a(x)(1 + x) = 1 - b(x)(x^3 + 9x + 6),$$

implying in $\mathbb{Q}(\theta) \cong \mathbb{Q}[x]/(x^3 + 9x + 6)$ that $a(\theta)(1 + \theta) = 1$. We apply the Euclidean algorithm to find $a$:

$$x^3 + 9x + 6 = (x^2 - x + 10)(1 + x) - 4$$

$$1 + x = \left(\frac{1}{4} + \frac{x}{4}\right)4 + 0$$

so $4 \sim 1$ is indeed the gcd. We equivalently have

$$1 = \left(-\frac{1}{4}\right)(x^3 + 9x + 6) + \left(-\frac{x^2}{4} + \frac{x}{4} + \frac{5}{2}\right)(1 + x)$$

so $(1 + \theta)^{-1} = -\frac{1}{4}\left(\theta^2 - \theta + 10\right)$. □

**Problem 2** (D&F 13.5.6)**.** *Prove that $x^{p^n-1} - 1 = \prod_{\alpha \in \mathbb{F}_{p^n}^\times}(x - \alpha)$. Conclude that $\prod_{\alpha \in \mathbb{F}_{p^n}^\times} \alpha = (-1)^{p^n}$ so the product of the nonzero elements of a finite field is $+1$ if $p = 2$ and $-1$ if $p$ is odd. For $p$ odd and $n = 1$ derive **Wilson's Theorem**: $(p - 1)! \equiv -1 \pmod{p}$*

*Proof.* Since $\mathbb{F}_{p^n}$'s multiplicative group is of order $p^n - 1$, then certainly $\alpha^{p^n-1} = 1 \Leftrightarrow \alpha^{p^n-1} - 1 = 0$ for all $\alpha \in \mathbb{F}_{p^n}^\times$. Accordingly, $x^{p^n-1} - 1$ has a root at every unit in $\mathbb{F}_{p^n}$, meaning it has a linear factor for every such unit; since the product of such factors is a polynomial of degree $p^n - 1$, there can be no additional factors.

Evaluating this at $x = 0$,

$$\prod_{\alpha \in \mathbb{F}_{p^n}^\times} -\alpha = -1 \Leftrightarrow (-1)^{p^n-1} \prod_{\alpha \in \mathbb{F}_{p^n}^\times} \alpha = -1 \Leftrightarrow \prod_{\alpha \in \mathbb{F}_{p^n}^\times} \alpha = (-1)^{-p^n} = (-1)^{p^n}$$

since integer parity is preserved under negation.

For $n = 1$, the fields are of the form $\mathbb{Z}/p\mathbb{Z}$, and the elements are equivalence classes $\bar{0}, \bar{1}, \ldots, \overline{p-1}$. Accordingly, applying this result yields the product of all field elements $\overline{p-1} \cdot \overline{p-2} \cdots \bar{1}$ being equal to $(\overline{-1})^p$, which for odd primes, is $-1 \pmod{p}$, proving Wilson's theorem. □

**Problem 3** (D&F 13.5.8)**.** *Prove that $f(x)^p = f(x^p)$ for any polynomial $f(x) \in \mathbb{F}_p[x]$.*

*Proof.* For finite fields, the Frobenius endomorphism is in fact a homomorphism, meaning it distributes over products and sums, so

$$(a_0 + a_1 x + \cdots + a_n x^n)^p = a_0^p + a_1^p x^p + \cdots + a_n^p \underbrace{x^p \cdot x^p \cdots x^p}_{n \text{ times}}.$$

A coefficient is either zero, in which case the equality of the two forms is immediate, or an element of $\mathbb{F}_p^\times$, which has order $p-1$, meaning $a_i^p = a_i a_i^{p-1} = a_i$, so the polynomial is

$$a_0 + a_1 x + \cdots + a_n (x^p)^n = f(x^p).$$

□

**Problem 4** (D&F 13.5.9)**.** *Show that the binomial coefficient $\binom{pn}{pi}$ is the coefficient of $x^{pi}$ in the expansion of $(1+x)^{pn}$. Working over $\mathbb{F}_p$ show that this is the coefficient of $(x^p)^i$ in $(1+x^p)^n$ and hence prove that $\binom{pn}{pi} \equiv \binom{n}{i} \pmod{p}$.*

*Proof.* By the binomial theorem (which was proven in a general context on a previous homework),

$$(1+x)^{pn} = \sum_{i=0}^{pn} \binom{pn}{i} x^i$$

so the coefficient of $x^{pi}$ is $\binom{pn}{pi}$. Using the Frobenius endomorphism on $\mathbb{F}_p$,

$$(1+x)^{pn} = (1^p + x^p)^n = (1+x^p)^n,$$

which, together with the fact that $x^{pi} = (x^p)^i$, demonstrates that $\binom{pn}{pi}$ is the coefficient of $(x^p)^i$ in $(1+x^p)^n$. This latter term is, by the binomial theorem again,

$$(1+x^p)^n = \sum_{i=0}^{n} \binom{n}{i} x^{pi}.$$

Comparing the coefficients of $x^{pi}$,

$$\binom{pn}{pi} = \binom{n}{i}$$

in $\mathbb{F}_p$, i.e.

$$\binom{pn}{pi} = \binom{n}{i} \pmod{p}.$$

□