Math 566 - Homework 8
SOLUTIONS
Prof Arturo Magidin

1. Let $f = a_0 + a_1x + \cdots + a_nx^n \in \mathbb{Z}[x]$ be primitive, $a_n \neq 0$, and let p be a prime number. Let
$$\overline{f} = \overline{a_0} + \overline{a_1}x + \cdots + \overline{a_n}x^n \in \mathbb{Z}_p[x],$$
where $\overline{a}$ is the image of a in $\mathbb{Z}_p$ under the canonical map $\mathbb{Z} \to \mathbb{Z}_p$ from the integers to the integers modulo p.

   (i) Show that if f is monic and $\overline{f}$ is irreducible in $\mathbb{Z}_p[x]$ for some prime p, then f is irreducible in $\mathbb{Z}[x]$.

   Proof. Suppose that $f = gh$ with $g, h \in \mathbb{Z}[x]$. Since f is monic, the leading coefficients of g and h are both units and multiply to 1, so they are both equal to 1 or both equal to -1. Multiplying each by -1 if necessary, we may assume that both g and h are monic.

   Reducing modulo p, we obtain that $\overline{f} = \overline{g}\overline{h}$; since g and h are monic, $\deg(\overline{g}) = \deg(g)$ and $\deg(\overline{h}) = \deg(h)$. Since $\overline{f}$ is irreducible, then one of $\overline{h}$ or $\overline{g}$ is a unit, hence of degree 0, and so either g is constant (and being monic, equal to 1) or h is constant (and being monic, equal to 1). This shows that any factorization of f into a product of two polynomials always has one factor be a unit, so f is irreducible in $\mathbb{Z}[x]$, as claimed. $\Box$

   (ii) Show the result still holds if we replace "f is monic" with "a_n is not a multiple of p".

   Proof. In the argument above, instead of concluding that we may take g and h both monic, we have that g and h both have leading coefficient which is not a multiple of p; that suffices to show that $\deg(\overline{g}) = \deg(g)$ and $\deg(\overline{h}) = \deg(h)$; so we can still conclude that either g or h are constant. Now we use the assumption that f is primitive to conclude that both g and h are primitive, and a constant primitive polynomial in $\mathbb{Z}[x]$ must be either 1 or -1, that is a unit. So again we get that f is irreducible.

   (iii) Give an example to show that the conclusion may fail to hold if a_n is divisible by p.

   Answer. Consider $f(x) = 3x^2 + 4x + 1 = (x + 1)(3x + 1)$. This is a primitive reducible polynomial in $\mathbb{Z}[x]$. If we take $p = 3$ and reduce, we get $\overline{f}(x) = \overline{1}x + \overline{1}$, which is degree 1 and hence irreducible. So even though the polynomial is primitive and the reduction modulo p is irreducible, the original polynomial is not irreducible. $\Box$

2. Prove that if F is a field, and $n \geq 2$, then $F[x_1, \ldots, x_n]$ is not a PID.

   Proof. We proved in the last homework that if D is a domain and $c \in D$ is irreducible, then (x, c) is not principal in $D[x]$.

   Since x_1 is an irreducible element in the domain $F[x_1, \ldots, x_{n-1}]$, then (x_1, x_n) is an ideal in $F[x_1, \ldots, x_{n-1}][x_n] = F[x_1, \ldots, x_n]$ that is not principal. So $F[x_1, \ldots, x_n]$ is not a PID. $\Box$

3. In $\mathbb{Z}$, given any $n > 1$, for every $a > 0$ there exist unique $r \geq 0$, and integers $a_0, \ldots, a_r$, $0 \leq a_i < n$, $a_r \neq 0$, such that
$$a = a_0 + a_1n + a_2n^2 + \cdots + a_rn^r;$$
that is, we can write every number in "base n", and the digits are uniquely determined. Prove the following analog for polynomials:

   Let F be a field, and let $g \in F[x]$, $\deg(g) \geq 1$. Prove that for every nonzero $f \in F[x]$ there exist unique $r \geq 0$ and polynomials $f_0, \ldots, f_r \in F[x]$, each f_i either equal to 0 or with $\deg(f_i) < \deg(g)$, and $f_r \neq 0$, such that
$$f = f_0 + f_1g + \cdots + f_rg^r;$$
that is, we can express every polynomial uniquely in "base g."

Proof. The idea is the same as for numbers: divide by g and take the remainder to get f_0; then take the quotient and divide by g, and the remainder is f_1; etc.

Existence. We proceed by induction on $\deg(f)$. Assume the result holds for all polynomials of degree smaller than $\deg(f)$.

If $\deg(f) < \deg(g)$, then take $r = 0$ and $f_0 = f$. Then $f = f_0$ and we are done.

If $\deg(f) \geq \deg(g)$, then we can write $f = qg + h$, with $h = 0$ or $\deg(h) < \deg(g)$; set $f_0 = h$. Now note that $q \neq 0$, since $\deg(f) \geq \deg(g)$, and that $\deg(qg) = \deg(f - h) = \deg(f)$ (since either $h = 0$ or else $\deg(h) < \deg(f)$); therefore, $\deg(q) = \deg(f) - \deg(g) < \deg(f)$. Thus, by the induction hypothesis, we can write

$$q = q_0 + q_1 g + \cdots + q_s g^s$$

where q_i are polynomials, each either equal to 0 or with $\deg(q_i) < \deg(g)$, and $q_s \neq 0$. Therefore,

$$f = f_0 + qg = f_0 + (q_0 + q_1 g + \cdots + q_s g^s)g = f_0 + q_0 g + q_1 g^2 + \cdots + q_s g^{s+1}.$$

Set $r = s + 1$, and $f_i = q_{i-1}$ for $i = 1, \ldots, r$. This gives an expression for f in the desired form, completing the induction.

Uniqueness. We proceed by induction on $\deg(f)$. Assume the result holds for all polynomials of degree strictly smaller than $\deg(f)$.

Let

$$f = f_0 + f_1 g + \cdots + f_r g^r = h_0 + h_1 g + \cdots + h_s g^s.$$

Setting $q_1 = (f_1 + f_2 g + \cdots + f_r g^{r-1})$ and $q_2 = h_1 + h_2 g + \cdots + h_s g^{s-1}$, we note that

$$f = f_0 + q_1 g = h_0 + q_2 g,$$

and each of f_0, h_0 is either 0 or of degree strictly smaller than g. By the uniqueness clause of the Division Algorithm for polynomials, we conclude that $f_0 = h_0$ and $q_1 = q_2$. Now notice that q_1 and q_2 have degree strictly smaller than f, so applying the induction hypothesis to the two expressions

$$q_1 = q_2 = f_1 + f_2 g + \cdots + f_r g^{r-1} = h_1 + h_2 g + \cdots + h_s g^{s-1}$$

we conclude that $r - 1 = s - 1$ and that $f_1 = h_1$, $f_2 = h_2, \ldots, f_r = h_r$. Thus, $r = s$ and $f_i = h_i$ for $i = 0, \ldots, r$, proving uniqueness. □

4. We prove **Schönemann's Irreducibility Criterion.** Let $f(x) \in \mathbb{Z}[x]$ be a polynomial with integer coefficients, $\deg(f) = n > 0$, and assume that there exists a prime p, and integer a, and a polynomial $\mathcal{F}(x) \in \mathbb{Z}[x]$ such that

$$f(x) = (x - a)^n + p\mathcal{F}(x) \quad \text{and } \mathcal{F}(a) \not\equiv 0 \pmod{p}.$$

We will prove that if this occurs, then $f(x)$ is irreducible in $\mathbb{Q}[x]$.

(i) Show that the leading coefficient of f is not divisible by p.

Proof. Note that $\deg(\mathcal{F}(x)) \leq n$ (since $\deg(g + h) \leq \max(\deg g, \deg h)$, with equality if $\deg(g) \neq \deg(h)$). Write

$$f(x) = a_0 + a_1 x + \cdots + a_n x^n,$$
$$\mathcal{F}(x) = b_0 + b_1 x + \cdots + b_n x^n,$$

where $a_n \neq 0$, but we allow $b_n = 0$. Since $(x - a)^n = x^n +$ terms of lower degree, we have $a_n = 1 + pb_n$. Therefore, $a_n \equiv 1 \pmod{p}$, so a_n is not divisible by p. □

(ii) Assume that $f(x) = G(x)H(x)$ with $G(x)$, $H(x)$ polynomials with integer coefficients. Let $\overline{f(x)}$, $\overline{G(x)}$ and $\overline{H(x)}$ denote the images of $f(x)$, $G(x)$, and $H(x)$ in $(\mathbb{Z}/p\mathbb{Z})[x]$ obtained by reducing the coefficients modulo p. Prove that we have $\deg(\overline{G(x)}) = \deg(G(x))$ and $\deg(\overline{H(x)}) = \deg(H(x))$.

Proof. The leading coefficient of $f(x)$, a_n, is the product of the leading coefficient of G and the leading coefficient of H. Since p does not divide a_n, p cannot divide the leading coefficient of G nor the leading coefficient of H, so when we reduce modulo p, the leading coefficient of $\overline{G(x)}$ is the reduction modulo p of the leading coefficient of $G(x)$ (which is not zero). So $\deg(\overline{G(x)}) = \deg(G(x))$, as claimed. Same argument holds for $\overline{H(x)}$. □

(iii) Show that $\overline{G(x)} = (x - \overline{a})^i$ and $\overline{H(x)} = (x - \overline{a})^j$ for some nonnegative integers i, j with $i + j = n$.

Proof. Note that $\mathbb{Z}/p\mathbb{Z}$ is a field, so the ring of polynomials with coefficients in $\mathbb{Z}/p\mathbb{Z}$ is a Euclidean domain, hence a Unique Factorization Domain. Since $f(x) = (x - a)^n + p\mathcal{F}(x)$, it follows that

$$\overline{f(x)} = \overline{(x-a)^n + p\mathcal{F}(x)} = \overline{(x-a)}^n + \overline{p}\,\overline{\mathcal{F}(x)} = \overline{(x-a)}^n = (x - \overline{a})^n.$$

Since $\overline{f(x)} = \overline{G(x)}\,\overline{H(x)}$, by unique factorization we must have $\overline{G(x)} = (x - \overline{a})^i$, $\overline{H(x)} = (x - \overline{a})^j$ for some nonnegative integers i and j with $i + j = n$, as claimed. □

(iv) Show that if $i, j > 0$, then $G(a) \equiv H(a) \equiv 0 \pmod{p}$.

Proof. Since $\overline{G(x)} = (x - \overline{a})^i$, it follows that if $i > 0$, then

$$\overline{G(a)} = (\overline{a} - \overline{a})^i = \overline{0},$$

so $G(a) \equiv 0 \pmod{p}$; similarly, if $j > 0$, then $\overline{H(a)} = (\overline{a} - \overline{a})^j = \overline{0}$, so $H(a) \equiv 0 \pmod{p}$. □

(v) Show that if $i, j > 0$, then $p\mathcal{F}(a) \equiv 0 \pmod{p^2}$, and reach a contradiction.

Proof. Since each of $G(a)$ and $H(a)$ are divisible by p, then $G(a)H(a)$ is divisible by p^2. Therefore,

$$\begin{aligned} 0 &\equiv G(a)H(a) \pmod{p^2} \\ &\equiv f(a) \pmod{p^2} \\ &\equiv (a-a)^n + p\mathcal{F}(a) \pmod{p^2} \\ &\equiv p\mathcal{F}(a) \pmod{p^2}. \end{aligned}$$

But if $p\mathcal{F}(a) \equiv 0 \pmod{p^2}$, then $\mathcal{F}(a) \equiv 0 \pmod{p}$, which contradicts our assumption that $\mathcal{F}(a) \not\equiv 0 \pmod{p}$. □

(vi) Conclude that $f(x)$ is irreducible in $\mathbb{Q}[x]$.

Proof. If $f(x)$ is reducible in $\mathbb{Q}[x]$, then by Gauss's Lemma and its corollaries we can express $f(x)$ as a product of two nonconstant polynomials $f(x) = G(x)H(x)$, with $G(x), H(x) \in \mathbb{Z}[x]$. But in that case, from (iii) we would conclude that $\overline{G(x)} = (x - \overline{a})^i$ with $i > 0$, and $\overline{H(x)} = (x - \overline{a})^j$ with $j > 0$, which yields a contradiction as in (v). Therefore, $f(x)$ must be irreducible in $\mathbb{Q}[x]$, as claimed. □