CHAPTER 4

MODULO ARITHMETIC

4.1. As we will see, modulo arithmetic aids in testing the irreducibility of polynomials and even in completely factoring polynomials in $\mathbb{Z}[x]$. If we expect a polynomial $f(x)$ is irreducible, for example, it is not unreasonable to try to find a prime p such that $f(x)$ is irreducible modulo p. If we can find such a prime p and p does not divide the leading coefficient of $f(x)$, then $f(x)$ is irreducible in $\mathbb{Z}[x]$ (see Problem (1.6)). It is the case that there exist polynomials which are irreducible in $\mathbb{Z}[x]$ but are reducible modulo every prime (see Problem (4.1)), but as it turns out, one can show that such polynomials are rare and verifying that a polynomial $f(x)$ is irreducible by trying to find a prime p for which $f(x)$ is irreducible modulo p will almost always work rather quickly (see Chapter 6). This is already strong motivation for looking into the idea of using modulo arithmetic, but in this chapter, we plan to explore other aspects of modulo arithmetic as well.

We begin with a definition. Let p be a prime, and let $f(x) \in \mathbb{Z}[x]$. Suppose further that $f(x) \not\equiv 0 \pmod{p}$. We say that $u(x) \equiv v(x)$ (modd p, $f(x)$), where $u(x)$ and $v(x)$ are in $\mathbb{Z}[x]$, if there exist $g(x)$ and $h(x)$ in $\mathbb{Z}[x]$ such that $u(x) = v(x) + f(x)g(x) + ph(x)$. (In other words, $u(x) \equiv v(x)$ (modd p, $f(x)$) if $u(x) - v(x)$ is in the ideal generated by p and $f(x)$ in the ring $\mathbb{Z}[x]$.) One easily checks that if $u(x) \equiv v(x)$ (modd p, $f(x)$) and $v(x) \equiv w(x)$ (modd p, $f(x)$), then $u(x) \equiv w(x)$ (modd p, $f(x)$). Suppose that $u_1(x) \equiv v_1(x)$ (modd p, $f(x)$) and $u_2(x) \equiv v_2(x)$ (modd p, $f(x)$). Then $u_1(x) \pm u_2(x) \equiv v_1(x) \pm$

$v_2(x)$ (modd p, $f(x)$). Also, using

$$u_1(x)u_2(x) - v_1(x)v_2(x) = u_1(x)\left(u_2(x) - v_2(x)\right) + v_2(x)\left(u_1(x) - v_1(x)\right),$$

we easily see that $u_1(x)u_2(x) \equiv v_1(x)v_2(x)$ (modd p, $f(x)$). We note that if $u(x) \equiv v(x)$ (mod p), then $u(x) \equiv v(x)$ (modd p, $f(x)$) (by taking $g(x) \equiv 0$), and if $u(x) \equiv v(x)$ (mod $f(x)$), then $u(x) \equiv v(x)$ (modd p, $f(x)$) (by taking $h(x) \equiv 0$). Also, if $u(x) \equiv 0$ (modd p, $f(x)$), then $f(x)$ is a factor of $u(x)$ modulo p.

Let $f(x)$ be monic. If $u(x)$ and $v(x)$ are in $\mathbb{Z}[x]$ and $u(x) \equiv v(x)$ (modd p, $f(x)$), then there are polynomials $g_0(x)$ and $h_0(x)$ in $\mathbb{Z}[x]$ such that $u(x) - v(x) = f(x)g_0(x) + ph_0(x)$. Recall (see the last remarks of Section 1.2) that when dividing a polynomial in $\mathbb{Z}[x]$ by a monic polynomial in $\mathbb{Z}[x]$, the quotient and remainder will be in $\mathbb{Z}[x]$. It follows that there are polynomials $q(x)$ and $r(x)$ in $\mathbb{Z}[x]$ with $r(x) \equiv 0$ or $\deg r < \deg f$ such that $h_0(x) = f(x)q(x) + r(x)$. Taking $g(x) = g_0(x) + pq(x)$ and $h(x) = r(x)$, we deduce that if $u(x) \equiv v(x)$ (modd p, $f(x)$), then there are polynomials $g(x)$ and $h(x)$ in $\mathbb{Z}[x]$ with $h(x) \equiv 0$ or $\deg h < \deg f$ such that $u(x) - v(x) = f(x)g(x) + ph(x)$. A simple argument shows further that such a $g(x)$ and $h(x)$ are unique (given $u(x)$, $v(x)$, $f(x)$, and p).

We will also make use of the following convention. Let p be a prime, and suppose $f(x) = \sum_{j=0}^{n} a_j x^j \in \mathbb{Z}[x]$ (with $f(x) \not\equiv 0 \pmod{p}$). Then we refer to the degree of $f(x)$ modulo p as the largest positive integer $k \le n$ for which p does not divide a_k. Thus, for example, $2x^3 + 3x^2 + 4$ is a polynomial of degree 2 modulo 2. With the added condition that $a_n = 1$, we easily see that any $g(x) \in \mathbb{Z}[x]$ is congruent (modd p, $f(x)$) to one of the p^n polynomials of degree $\le n-1$ with coefficients from $\{0, 1, \dots, p-1\}$. Also, each of these p^n polynomials are incongruent (modd p, $f(x)$). In other words, we can view these p^n polynomials as representatives of the p^n distinct residue classes (modd p, $f(x)$). Consider now the possibility that $a_n \ne 1$, and let k denote the degree of $f(x)$ modulo p. Problem (4.7) implies that arithmetic (modd p, $f(x)$) is the same as arithmetic (modd p, $f_1(x)$) where $f_1(x) \equiv f(x) \pmod{p}$ and $\deg f_1(x) = k$. Problem (4.4) further implies that arithmetic (modd p, $f_1(x)$) is the same as arithmetic (modd p, $f_2(x)$) where $f_2(x)$ is monic and

$\deg f_2(x) = k$. It follows that there are precisely p^k distinct residue classes (modd p, $f(x)$) with representatives given by the polynomials of degree $\le k-1$ with coefficients from $\{0, 1, \dots, p-1\}$.

Theorem 16. *Let p be a prime. If $f(x) \in \mathbb{Z}[x]$ is of degree n modulo p and $f(x)$ is irreducible modulo p, then*

$$x^{p^n} \equiv x \pmod{p,\ f(x)}.$$

We clarify that in Theorem 16, as is usual,

$$x^{p^n} = x^{(p^n)}.$$

Before we prove this theorem, we consider an example. We show that $f(x) = x^p - x - 1$ is irreducible modulo p (and hence irreducible over $\mathbb{Z}$). Consider $u(x)$ and $v(x)$ in $\mathbb{Z}[x]$, with $u(x)$ irreducible modulo p and with $f(x) \equiv u(x)v(x) \pmod{p}$. Observe that $1 \le \deg u(x) \le p$. We further suppose, as we may, that $u(x)$ is monic (for if a is the leading non-zero coefficient modulo p of $u(x)$, then we can consider $f(x) \equiv (a^{-1}u(x))(av(x)) \pmod{p}$). It suffices to show $\deg u(x) = p$. Note that

$$x^p \equiv x + 1 \pmod{p,\ f(x)}.$$

Hence,

$$x^{p^2} \equiv (x^p)^p \equiv (x+1)^p \equiv x^p + 1 \equiv x + 2 \pmod{p,\ f(x)}.$$

For any integer a, Fermat's Little Theorem gives us that $a^p \equiv a \pmod{p}$. An easy induction argument shows that for every positive integer r,

$$x^{p^r} \equiv x + r \pmod{p,\ f(x)}. \tag{4.1}$$

Since $u(x)$ divides $f(x)$ modulo p, we may replace $f(x)$ with $u(x)$ in (4.1). Let $m = \deg u(x)$. Then by Theorem 16 and (4.1),

$$x \equiv x^{p^m} \equiv x + m \pmod{p,\ u(x)}.$$

Hence, $m \equiv 0$ (modd p, $u(x)$). Recalling that this implies there are polynomials $g(x)$ and $h(x)$ in $\mathbb{Z}[x]$ with $\deg h < \deg u$ such that $m = u(x)g(x) + ph(x)$, we obtain that $g(x) \equiv 0$, $\deg h = 0$, and $p|m$. On the other hand, $1 \le m \le p$; thus, $m = p$, implying that $f(x)$ is irreducible modulo p.

We now turn to the proof of Theorem 16.

Lemma. *Let p be a prime, and let $f(x)$ be irreducible modulo p. Let $a(x) \in \mathbb{Z}[x]$ with $a(x) \not\equiv 0$ (modd p, $f(x)$). Then there exists $b(x) \in \mathbb{Z}[x]$ such that $a(x)b(x) \equiv 1$ (modd p, $f(x)$).*

Proof. Let $n = \deg f(x)$. Making use of Problems (4.7) and (4.4) as before, we may suppose (and do suppose) that $f(x)$ is monic. Observe that there exists a $w(x) \in \mathbb{Z}[x]$ with $\deg w < n$ such that $a(x) \equiv w(x) \pmod{f(x)}$. Thus, $a(x) \equiv w(x)$ (modd p, $f(x)$). Since $a(x) \not\equiv 0$ (modd p, $f(x)$), we deduce that $w(x) \not\equiv 0 \pmod{p}$. Hence, there exists an integer m and a monic polynomial $v(x) \in \mathbb{Z}[x]$ such that $w(x)m \equiv v(x) \pmod{p}$ so that $a(x)m \equiv v(x)$ (modd p, $f(x)$). Here, $\deg v \le \deg w < n$. Fix $u(x)$ and $v(x)$ in $\mathbb{Z}[x]$ with $a(x)u(x) \equiv v(x)$ (modd p, $f(x)$), with $v(x)$ monic, and with $\deg v(x)$ as small as possible. We deduce that $\deg v(x) < n$ and $v(x) \not\equiv 0$ (modd p, $f(x)$). Since $v(x)$ is monic, there exist $q(x)$ and $r(x)$ in $\mathbb{Z}[x]$ such that

$$f(x) = q(x)v(x) + r(x) \tag{4.2}$$

and such that either $r(x) \equiv 0$ or $\deg r(x) < \deg v(x)$. Observe that

$$a(x)u(x)q(x) \equiv v(x)q(x) \equiv -r(x) \quad (\text{modd } p,\ f(x)).$$

From the minimality of $\deg v(x)$, we deduce $r(x) \equiv 0 \pmod{p}$ (otherwise, we could multiply through by a constant in the above congruence to obtain a monic polynomial on the right-hand side, leading to a contradiction). Since $\deg v(x) < n = \deg f(x)$ and $f(x)$ is irreducible modulo p, we get from (4.2) that $\deg v(x) = 0$. Since $v(x)$ is monic, we deduce that $v(x) \equiv 1$ and the lemma follows. ■

Proof of Theorem 16. As before, using Problem (4.4), we may suppose that $f(x)$ is monic and do so. Suppose $f(x) \equiv x \pmod{p}$. Then $n = 1$ and

$$x^{p^n} \equiv 0 \equiv x \quad (\text{modd } p,\ f(x)).$$

Now, suppose that $f(x) \not\equiv x \pmod{p}$. From the lemma, we get that x has an inverse (modd p, $f(x)$). Let $k = p^n - 1$, and let $a_1(x), \dots, a_k(x)$ denote incongruent non-zero polynomials (modd p, $f(x)$). Then every non-zero polynomial (modd p, $f(x)$) is congruent to one of $a_1(x), \dots, a_k(x)$. It follows that $xa_1(x), \dots, xa_k(x)$ are congruent to $a_1(x), \dots, a_k(x)$ in some order (modd p, $f(x)$). Hence,

$$a_1(x) \cdots a_k(x) \equiv (xa_1(x)) \cdots (xa_k(x)) \equiv x^k a_1(x) \cdots a_k(x) \quad (\text{modd } p,\ f(x)).$$

Observe that $a_1(x) \cdots a_k(x) \not\equiv 0$ (modd p, $f(x)$); otherwise, there would exist a $g(x) \in \mathbb{Z}[x]$ such that $f(x)g(x) \equiv a_1(x) \cdots a_k(x) \pmod{p}$, contradicting Theorem 3. Using the lemma with $a(x) = a_1(x) \cdots a_k(x)$, we get that

$$x^{p^n - 1} \equiv x^k \equiv 1 \quad (\text{modd } p,\ f(x)) \tag{4.3}$$

from which it follows that

$$x^{p^n} \equiv x \quad (\text{modd } p,\ f(x)),$$

completing the proof. ■

Given the lemma above, it is easy to see that the p^n incongruent representatives (modd p, $f(x)$) together with the operations modulo (modd p, $f(x)$) form a field. Thus, the $p^n - 1$ non-zero elements (modd p, $f(x)$) form a multiplicative group. Theorem 16 (or, more precisely, (4.3)) is merely asserting that in this group (as with any group) an element raised to the order of the group is equal to the identity element in the group.

4.2. In this section, we generalize Theorem 16 and show how we can deduce from the generalization a formula for the number of irreducible polynomials of a given degree n

modulo a prime p. We shall make use of this result later in the book when we discuss the density of $f(x) \in \mathbb{Z}[x]$ which are irreducible modulo some prime. Let p be a prime, and let $f(x) \in \mathbb{Z}[x]$. Suppose that $f(x)$ is of degree n modulo p and that $f(x)$ is irreducible modulo p. We use the concluding remark of the previous section that the p^n incongruent representatives (modd p, $f(x)$) together with addition and multiplication (modd p, $f(x)$) form a field. If we denote this field by F, then we can deduce from Theorem 4 that the polynomial $y^{p^k} - y$ has at most p^k roots in F. We begin by showing that if $k < n$, then x is not a root of $y^{p^k} - y$ in F. Suppose x is a root of $y^{p^k} - y$ in F. Then letting $g(x) = \sum_{j=0}^{r} b_j x^j$ represent an element in F, we get (by applying the multinomial theorem k times)

$$g(x)^{p^k} \equiv \left(\sum_{j=0}^{r} b_j x^j \right)^{p^k} \equiv \sum_{j=0}^{r} b_j^{p^k} x^{p^k j} \equiv \sum_{j=0}^{r} b_j x^j \equiv g(x) \pmod{p,\ f(x)}.$$

Thus, if x is a root of $y^{p^k} - y$ in F, then so is every element of F. Hence, by Theorem 4, $p^k \geq |F| = p^n$ so that $k \geq n$. Therefore, if $k < n$, then x is not a root of $y^{p^k} - y$ in F.

It is easy to see that since $x^{p^n} \equiv x$ (modd p, $f(x)$), we can obtain for every non-negative integer m,

$$x^{p^{mn}} \equiv x \pmod{p,\ f(x)}.$$

In other words, if k is a non-negative integer which is divisible by n, then

$$x^{p^k} \equiv x \pmod{p,\ f(x)}. \tag{4.4}$$

We now show that the converse of this statement is also true. In other words, if (4.4) holds, then k is divisible by n. Suppose then that (4.4) holds. By the previous paragraph, we know that $k \geq n$. Write $k = qn + r$, where q and r are non-negative integers with $0 \leq r < n$. Taking $m = q$ above, we see that $x^{p^{qn}} \equiv x$ (modd p, $f(x)$). Therefore, by (4.4),

$$x^{p^r} \equiv \left(x^{p^{qn}} \right)^{p^r} \equiv x^{p^{qn+r}} \equiv x^{p^k} \equiv x \pmod{p,\ f(x)}.$$

This implies $r = 0$ by the result of the previous paragraph. Thus, we obtain the following improvement of Theorem 16.

Theorem 17. *Let p be a prime, and let n be a positive integer. Let $f(x)$ be an irreducible polynomial modulo p, and suppose that p does not divide the leading coefficient of $f(x)$. Then*

$$x^{p^n} \equiv x \pmod{p,\ f(x)}$$

holds if and only if $\deg f(x)$ *divides n.*

Observe that $x^{p^n} \equiv x$ (modd p, $f(x)$) if and only if $f(x)$ is a factor of $x^{p^n} - x$ modulo p. Derivative considerations easily imply that $x^{p^n} - x$ cannot be divisible by $f(x)^2$ modulo p. When factoring $x^{p^n} - x$ modulo p, we need only consider monic factors. Therefore, by Theorem 17, $x^{p^n} - x$ factors modulo p as the product of all monic irreducible polynomials modulo p of degree dividing n with each irreducible factor occuring once and only once. Hence,

$$x^{p^n} - x \equiv \prod_{k|n} \left({\prod}^{*} f(x) \right) \pmod{p},$$

where the $*$ indicates that the product (or sum below) is over those $f(x)$ modulo p which are monic, irreducible, and of degree k. Thus,

$$\begin{aligned} p^n &= \sum_{k|n} \left({\sum}^{*} \deg f(x) \right) = \sum_{k|n} \left({\sum}^{*} k \right) \\ &= \sum_{k|n} k {\sum}^{*} 1 = \sum_{k|n} k M_k, \end{aligned}$$

where $M_k = M_k(p)$ denotes the number of incongruent monic irreducible polynomials of degree k modulo p. We state this as

Lemma 1. *If M_k denotes the number of monic irreducible polynomials modulo a prime p, then*

$$p^n = \sum_{k|n} k M_k.$$

We now obtain an exact formula for M_n and for the number of incongruent irreducible polynomials of degree n modulo a prime p. We denote this last quantity by $I_n = I_n(p)$

and observe that in fact $I_n = (p-1)M_n$. To obtain a formula for M_n, we introduce the Möbius $\mu-$function which is defined by

$$\mu(n) = \begin{cases} (-1)^r & \text{if } n = p_1 \dots p_r \text{ where the } p_j \text{ are distinct primes} \\ 0 & \text{otherwise,} \end{cases}$$

where we interpret the above to mean that $\mu(1) = 1$. In particular, it is immediate from this definition that

$$\mu(ab) = \mu(a)\mu(b) \qquad \text{for } a \text{ and } b \in \mathbb{Z} \text{ with } \gcd(a,b) = 1.$$

In other words, μ is a multiplicative function.

Lemma 2. *Let n be a positive integer. Then*

$$\sum_{d|n} \mu(d) = \begin{cases} 1 & \textit{if } n = 1 \\ 0 & \textit{otherwise.} \end{cases}$$

Proof. If $n = 1$, then $\sum_{d|n} \mu(d) = \mu(1) = 1$. If $n > 1$, then we can write n in the form,

$$n = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r},$$

where $p_1, \dots, p_r$ are distinct primes with $r \geq 1$ and where $e_1, \dots, e_r$ are positive integers. Observing that $\mu(d) = 0$ if d is not squarefree, we get that

$$\sum_{d|n} \mu(d) = \sum_{d|p_1 \cdots p_r} \mu(d).$$

Recalling that μ is a multiplicative function and that $r \geq 1$, we deduce that if $n > 1$, then

$$\sum_{d|n} \mu(d) = \prod_{j=1}^{r} (1 + \mu(p_j)) = \prod_{j=1}^{r} (1-1) = 0,$$

completing the proof. ■

Observe that

$$\sum_{d|n} \mu(d) = \sum_{d|n} \mu\left(\frac{n}{d}\right)$$

so that we can use the sum on the right above in Lemma 2 rather than the sum on the left. From Lemma 1, we get that

$$\sum_{d|n} \mu\left(\frac{n}{d}\right) p^d = \sum_{d|n} \mu\left(\frac{n}{d}\right) \sum_{k|d} kM_k.$$

For each d and k in this last expression, we have that $d = kd'$ for some integer d'. Thus, rearranging the order of summation and using Lemma 2, we obtain that

$$\sum_{d|n} \mu\left(\frac{n}{d}\right) p^d = \sum_{k|n} \sum_{d'|(n/k)} \mu\left(\frac{n}{kd'}\right) kM_k = \sum_{k|n} kM_k \sum_{d'|(n/k)} \mu\left(\frac{n/k}{d'}\right) = nM_n.$$

Therefore, we have established

Theorem 18. *Let p be a prime, and let n be a positive integer. Then*

$$M_n(p) = \frac{1}{n} \sum_{d|n} \mu\left(\frac{n}{d}\right) p^d \quad \text{and} \quad I_n(p) = \frac{p-1}{n} \sum_{d|n} \mu\left(\frac{n}{d}\right) p^d.$$

Example 1. Consider $n = 12$ and $p = 2$. Then

$$\frac{1}{12} \sum_{d|12} \mu\left(\frac{12}{d}\right) 2^d = \frac{1}{12}\left(2^{12} - 2^6 - 2^4 + 2^2\right) = 335.$$

Thus, there are exactly 335 incongruent (monic) irreducible polynomials of degree 12 modulo 2.

Example 2. Consider $n = 3$ and $p = 5$. Then

$$\frac{4}{3} \sum_{d|3} \mu\left(\frac{3}{d}\right) 5^d = \frac{4}{3}\left(5^3 - 5\right) = 160.$$

Thus, there are exactly 160 incongruent irreducible polynomials of degree 3 modulo 5.

The proof above that Theorem 18 follows from Lemma 1 is simply an application of the Möbius inversion formula. The argument presented is based on a derivation of the Möbius inversion formula which can be found in almost every if not every introductory Number Theory text.

If p is a prime and n is a positive integer, then the existence of a finite field of order p^n is a consequence of the fact that $I_n(p) > 0$. The latter follows from Theorem 18. To see this, observe that if $n = k\ell$, where k is the largest squarefree factor of n, then $(1/p^\ell)\sum_{d|n}\mu(n/d)p^d$ is an integer $\equiv \pm 1 \pmod p$. Thus, $\sum_{d|n}\mu(n/d)p^d$ and, hence, $I_n(p)$ are non-zero.

4.3. In this section, we give another approach to establishing Theorem 18. More precisely, we shall establish Lemma 1 of the previous section using formal power series. For this approach, we follow Berlekamp [1]. We begin with a general discussion of formal power series. Formal power series are used to obtain results by manipulating series without concern for their convergence or divergence. In fact, one can discuss these series with their coefficients coming from an arbitrary field so that the concepts of convergence or divergence may not even be defined. For our purposes, the reader may assume that the coefficients are rational. A formal power series is of the form

$$f(z) = a_0 + a_1 z + a_2 z^2 + \cdots .$$

If

$$g(z) = b_0 + b_1 z + b_2 z^2 + \cdots \qquad \text{and} \qquad h(z) = c_0 + c_1 z + c_2 z^2 + \cdots$$

are two formal power series, then we say that $g(z) = h(z)$ if $b_j = c_j$ for every $j \in \{0, 1, 2, \dots\}$. If $f(z)$, $g(z)$, and $h(z)$ are as above, then we say $f(z) = g(z) \pm h(z)$ if $a_k = b_k \pm c_k$ for every $k \in \{0, 1, 2, \dots\}$ and we say $f(z) = g(z)h(z)$ if

$$a_k = \sum_{i+j=k} b_i c_j = \sum_{j=0}^{k} b_{k-j} c_j \qquad \text{for every } k \in \{0, 1, 2, \dots\}.$$

If $g(z)h(z) = 1$, then we will sometimes write $g(z) = 1/h(z)$ and refer to $g(z)$ as an inverse of $h(z)$. In this case, we must have that $b_0 c_0 = 1$. Thus, a formal power series $g(z) = b_0 + b_1 z + \cdots$ does not have an inverse if $b_0 = 0$. If $b_0 \neq 0$, then $g(z)$ does have an inverse (Problem (4.5)). If $g(z)$ and $h(z)$ are non-zero, then the definition of $g(z)h(z)$

above implies that the coefficient of $z^{k+\ell}$ in $g(z)h(z)$ is non-zero where k is the minimal j such that $b_j \neq 0$ and ℓ is the minimal j such that $c_j \neq 0$. Hence, if $g(z)h(z) \equiv 0$, then either $g(z) \equiv 0$ or $h(z) \equiv 0$. If $g_1(z)$, $g_2(z)$, and $h(z)$ are formal power series, then the above definitions imply that

$$(g_1(z) \pm g_2(z))\, h(z) = g_1(z)h(z) \pm g_2(z)h(z).$$

It now follows that the inverse of a formal power series is unique (if it exists). For example, the inverse of $1-z$ as a formal power series with coefficients from any field is $1+z+z^2+z^3+\cdots$. Whenever we use the notation $g(z)/h(z)$, we shall mean that $h(z)$ has an inverse and $g(z)/h(z)$ represents the product of $g(z)$ with the inverse of $h(z)$. It is not difficult to see that addition and multiplication of formal power series are commutative and associative operations. In particular, if $g_1(z), \ldots, g_r(z)$ are formal power series, then what we mean by the product $g_1(z) \cdots g_r(z)$ is understood.

We define the derivative of a formal power series $f(z) = a_0 + a_1 z + a_2 z^2 + \cdots$ as

$$f'(z) = a_1 + 2a_2 z + 3a_3 z^2 + \cdots = \sum_{k=1}^{\infty} k a_k z^{k-1}.$$

It is easy to check that if $g(z)$ and $h(z)$ are formal power series, then

$$(g(z) \pm h(z))' = g'(z) \pm h'(z).$$

Using the notation for $g(z)$ and $h(z)$ above, we see that the derivative of $g(z)h(z)$ is

$$\begin{aligned}
(g(z)h(z))' &= \left(\sum_{k=0}^{\infty} \left(\sum_{j=0}^{k} b_{k-j} c_j \right) z^k \right)' \\
&= \sum_{k=1}^{\infty} k \left(\sum_{j=0}^{k} b_{k-j} c_j \right) z^{k-1} \\
&= \sum_{k=1}^{\infty} \left(\sum_{j=0}^{k} (k-j) b_{k-j} c_j \right) z^{k-1} + \sum_{k=1}^{\infty} \left(\sum_{j=0}^{k} b_{k-j} j c_j \right) z^{k-1} \\
&= g'(z)h(z) + g(z)h'(z).
\end{aligned}$$

If $h(z) = 1/g(z)$, then we get that

$$0 = \frac{g'(z)}{g(z)} + g(z)\left(\frac{1}{g(z)}\right)'$$

so that

$$\left(\frac{1}{g(z)}\right)' = -\frac{g'(z)}{g(z)^2}.$$

If $g_1(z), \ldots, g_r(z)$ are formal power series, then we also get that

$$(g_1(z)\cdots g_r(z))' = \sum_{k=1}^{r} \frac{g_k'(z)}{g_k(z)} \prod_{j=1}^{r} g_j(z)$$

so that

$$\frac{(g_1(z)\cdots g_r(z))'}{g_1(z)\cdots g_r(z)} = \sum_{k=1}^{r} \frac{g_k'(z)}{g_k(z)}.$$

Thus, we get the usual Calculus rules for derivatives of sums (or differences), for derivatives of products, for derivatives of reciprocals, and for logarithmic derivatives of products. All of these hold regardless of the field of coefficients for the formal power series.

We now restrict our attention to formal power series with rational coefficients. We recall the notation $M_n(p)$ of the previous section for the number of monic irreducible polynonmials modulo a prime p. The total number of monic polynomials (including reducible ones) of degree n modulo p is p^n, and each of these by Theorem 3 can be written uniquely as a product of monic irreducible polynomials modulo p (without regard to the order in which the factors appear). This implies that if $n \leq m$, then p^n will be the coefficient of z^n in the formal power series product

$$\prod_{k=1}^{m} \left(1 + z^k + z^{2k} + \cdots\right)^{M_k} = \prod_{k=1}^{m} \left(\frac{1}{1 - z^k}\right)^{M_k}.$$

On the other hand, if n is any non-negative integer, then p^n is the coefficient of z^n in $1/(1 - pz)$. Hence, we can find a formal power series $g(z)$ such that

$$\frac{1}{1 - pz} = \prod_{k=1}^{m} \left(\frac{1}{1 - z^k}\right)^{M_k} + z^{m+1} g(z).$$

Let L denote the left-hand side above and R denote the right-hand side. Also, let P denote the product in R. Since inverses are unique, it follows that the inverse of R exists and is $1-pz$. Observe also that P has the inverse $\prod_{k=1}^{m}(1-z^k)^{M_k}$. It follows that we can write the inverse of R as

$$\frac{1-z^{m+1}g(z)(1-pz)}{P}.$$

Since $L=R$, we get that $L'/L = R'/R$. Hence, we get that there is a formal power series $h(z)$ such that

$$\begin{aligned}
\frac{p}{1-pz} &= \frac{P' + (m+1)z^m g(z) + z^{m+1}g'(z)}{R} \\
&= \frac{P'}{P}\left(1-z^{m+1}g(z)(1-pz)\right) + \left((m+1)z^m g(z) + z^{m+1}g'(z)\right)(1-pz) \\
&= \frac{P'}{P} + z^m h(z).
\end{aligned}$$

Using our previous formula for the logarithmic derivative of a product and multiplying through by z, we obtain that

$$\begin{aligned}
\sum_{d=1}^{\infty} p^d z^d &= \frac{pz}{1-pz} \\
&= \sum_{k=1}^{m} \frac{M_k k z^k}{1-z^k} \; + \; z^{m+1}h(z) \\
&= \sum_{k=1}^{m} kM_k \sum_{\substack{d\geq 1 \\ k|d}} z^d \; + \; z^{m+1}h(z) \\
&= \sum_{d=1}^{\infty} \left(\sum_{\substack{1\leq k\leq m \\ k|d}} kM_k \right) z^d \; + \; z^{m+1}h(z).
\end{aligned}$$

If we consider any positive integer n and take $m=n$ above, we deduce Lemma 1 of the previous section by comparing the coefficients of z^n above.

Problems

(4.1) (a) Let p be an odd prime. Show that if a is a non-zero square modulo p, then a is a root of $x^{(p-1)/2} - 1$ modulo p; and if a is not a square modulo p, then a is a root of $x^{(p-1)/2} + 1$ modulo p.

(b) Prove that if a and b are not squares modulo a prime p, then $a \times b$ is a square modulo p.

(c) From part (b), we know that for every prime p, either -1, 2, or -2 is a square modulo p. Prove that $x^4 + 1$ is reducible modulo every prime p.

(4.2) Let a and b be integers. Prove that $x^4 + ax^2 + b$ is reducible modulo every prime.

(4.3) Let p be a prime, and let a be an integer which is not divisible by p. Prove that $x^p - x - a$ is irreducible modulo p.

(4.4) Let p be a prime, and let $f(x) \in \mathbb{Z}[x]$ with leading coefficient a modulo p (in other words, a is the coefficient of the highest degree term in $f(x)$ which is non-zero modulo p). Then we can write $f(x) \equiv ag(x) \pmod{p}$ for some monic polynomial $g(x) \in \mathbb{Z}[x]$. Let $u(x)$ and $v(x)$ be in $\mathbb{Z}[x]$. Prove that $u(x) \equiv v(x)$ (modd p, $f(x)$) if and only if $u(x) \equiv v(x)$ (modd p, $g(x)$).

(4.5) Let $g(z) = b_0 + b_1 z + \cdots$ represent a formal power series with $b_0 \neq 0$. Prove that $g(z)$ has an inverse.

(4.6) Let $f(x) = ax^2 + bx + c$, where a, b, and c are odd integers. Using arithmetic modulo 2, explain why $f(x)$ is irreducible over the rationals.

(4.7) Let p be a prime, and let $f(x)$ and $g(x)$ be in $\mathbb{Z}[x]$ with $f(x) \equiv g(x) \pmod{p}$. Let $u(x)$ and $v(x)$ be in $\mathbb{Z}[x]$. Prove that $u(x) \equiv v(x)$ (modd p, $f(x)$) if and only if $u(x) \equiv v(x)$ (modd p, $g(x)$).