Theory of Equations

Chapter 5 Appendix

Polynomials over $\mathbb{Z}_p$

by

Barry H. Dayton
Northeastern Illinois University
Chicago, IL 60625, USA

www.neiu.edu/~bhdayton/theq/

1 Modular Arithmetic

Modular arithmetic was first explicitly given by Gauss in 1801 in his famous book *Disquisitiones Arithmeticae* where he was studying the cyclotomic polynomial $x^p - 1$. In 1829 Galois showed the importance of finite fields in understanding polynomial equations. As we will see, modular arithmetic plays a particularly important role in the study of factoring.

Let n be a fixed integer, $n > 1$. Two integers a, b are said to be *congruent modulo* n if the difference $a - b$ is divisible by n, we write this $a \equiv b \pmod{n}$. Alternatively, the Division Algorithm for $\mathbb{Z}$ says that given $a \in \mathbb{Z}$ and $n > 1$ there exist a unique quotient q and remainder r with $a = nq + r$ with $0 \leq r < n$. Given integers a, b write $a = nq + r$ and $b = nq' + s$, then $a \equiv b \pmod{n}$ if and only if $r = s$, i.e. two numbers are congruent if and only if they have the same remainder after division by n. Note that if $n = 2, a \equiv b \pmod{n}$ says that either both a, b are even or both a, b are odd. Thus congruence modulo n is a generalization of the idea of "even" or "odd".

Congruence modulo n is an *equivalence relation*, that is, a weak type of equality. In particular we have

1) $a \equiv a \pmod{n}$ for all a (reflexivity)
2) if $a \equiv b \pmod{n}$ then $b \equiv a \pmod{n}$ (symmetry)
3) if $a \equiv b$ and $b \equiv c \pmod{n}$ then $a \equiv c \pmod{n}$ (transitivity)

One can easily prove that if $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$ then

$$a + c \equiv b + d \pmod{n} \quad (1)$$
$$ac \equiv bd \pmod{n} \quad (2)$$

from which it follows that

$$a - c \equiv b - d \pmod{n}$$
$$a^k \equiv b^k \pmod{n} \text{ if } k \geq 0$$

In particular the relation of congruence respects all arithmetic operations. For example if we have $f(x) = a_0 + a_1 x + \cdots + a_n x^n, c \in \mathbb{Z}$ and we wish to find the remainder of $f(c)$ after division by n we can do all arithmetic and then divide by n and take the remainder, we can divide c by n and take the remainder before doing the arithmetic, or we can divide by n and take the remainder after each step.

For fixed n and $a \in \mathbb{Z}$ we denote by $[a] = \{b \in \mathbb{Z} | a \equiv b \pmod{n}\}$, i.e. $[a]$ is the set of all integers which have the same remainder after division by n as a. For example if $n = 5$ then $[3] = \{\ldots, -12, -7, -2, 3, 8, 13, 18, \ldots\}$. Or if $n = 2$ then $[0] = [2] = [4] = [-6] = \cdots$ is the set of even integers and $[1] = [3] = [-5] = \cdots$ is

the set of odd integers. $[a]$ is called the *congruence class* of a modulo n. For a given n the congruence classes $[0], [1], \ldots, [n-1]$ *partition* $\mathbb{Z}$, i.e., each integer is in one of these congruence classes and no integer is in more than one. If $a = nq + r, 0 \leq r < n$ then $a \in [r]$ and $[a] = [r]$. More generally,

$$a \equiv b \pmod{n} \text{ if and only if } [a] = [b].$$

Thus the congruence classes allow us to trade *equivalence* of integers for *equality* of classes.

Equation 1 and Equation 2 above can be restated as saying that if $[a] = [b]$ and $[c] = [d]$ then $[a+c] = [b+d]$ and $[ac] = [bd]$. Thus $[a]+[b] = [a+b]$ and $[a]*[b] = [ab]$ give well defined operations of addition and multiplication on the set of congruence classes modulo n. It is easy to check that from Equations 1 and 2 the commutative, associative and distributive laws of $\mathbb{Z}$ hold for congruence classes. Further $[0]+[a] = [0+a] = [a]$ and $[1]*[a] = [1*a] = [a]$, so $[0], [1]$ are the zero and the multiplicative identity. Finally $[a] + [-a] = [0]$ so we have additive inverses and can write $-[a] = [-a]$. Thus laws C1, C2 as well as R1 - R8 hold for this modular arithmetic.

Thus we write $\mathbb{Z}_n = \{[0], [1], ..., [n-1]\}$ and call this set the *ring of integers modulo* n, as we have a ring in the sense of §1.1. (Many books use the notation $\mathbb{Z}_n$ to mean something else, a more standard notation for the ring of integers modulo n is $\mathbb{Z}/n\mathbb{Z}$.) $\mathbb{Z}_n$ is an arithmetic with n elements. Unfortunately $\mathbb{Z}_n$ in general does not even satisfy the integral domain axiom I1 in general, for instance if $n = 6$ then $[2] * [3] = [6] = [0]$ but neither $[2] = [0]$ nor $[3] = [0]$. However Gauss discovered the following wonderful fact:

Theorem 1.1 *Let p be a prime number. Then $\mathbb{Z}_p$ is a field. That is, given $[a] \in \mathbb{Z}_p, [a] \neq [0]$ then there exists $[b] \in \mathbb{Z}_p$ with $[a] * [b] = [1]$.*

Proof: Let $[a] \neq [0]$, then p does not divide a and so $\gcd(a, p) = 1$. Modifying the proof of Theorem 1.8.2 (or using the Euclidean Algorithm) substituting absolute value for degree, there exist integers s, t so that $sa + tp = 1$. But then $[s] * [a] = [sa] + [0] = [sa] + [tp] = [sa + tp] = [1]$ so $[a]^{-1} = [s]$.

There is one other wonderful theorem about $\mathbb{Z}_p$ which we will need, this one originally due to Fermat.

Theorem 1.2 (Fermat's Little Theorem) *Let p be a prime number. Then for every $[a] \in \mathbb{Z}_p, [a]^p = [a]$.*

Proof: This is usually proved as a consequence of Lagrange's Theorem, alluded to in §4.9. There is a nice simple proof by induction: For $a = 0$ the result is obvious, $[0]^p = [0]$. Suppose $[a]^p = [a]$ then by the binomial theorem $(a+1)^p = a^p + pa^{p-1} + C(p,2)a^{p-2} + \cdots + pa + 1$ where $C(p,k)$ is the binomial coefficient. It is not hard to see that $C(p,k)$ is divisible by p for $k = 1, 2, \ldots, p-1$ so $(a+1)^p \equiv a^p + 1 \pmod{p}$ giving $[a+1]^p = [a+1]$ which finishes the induction step.

If $[a] \in \mathbb{Z}_p$ we write $[a] + [a] = 2[a], [a] + [a] + [a] = 3[a]$, etc. It is not hard to see that for each non-negative m that $m[a] = [ma]$, so we can extend this notation for negative m as well. An important property of Z/p is that $p[a] = [pa] = [0]$ for every $[a] \in \mathbb{Z}_p$. A field which satisfies this property is said to have *characteristic* p.

We finally mention that there is a function $\sigma : \mathbb{Z} \to \mathbb{Z}_p$ given by $\sigma(a) = [a]$. We have $\sigma(a+b) = [a+b] = [a] + [b] = \sigma(a) + \sigma(b)$ and likewise $\sigma(a * b) = \sigma(a) * \sigma(b)$. It follows that σ preserves arithmetic, or in other words, we may do our arithmetic in $\mathbb{Z}$ and then apply σ or we may apply σ and then do our arithmetic in $\mathbb{Z}_p$, in either case getting the same result. In modern algebra we say σ is a *homomorphism*.

2 Polynomials over $\mathbb{Z}_p$

Having more or less carefully developed the arithmetic of $\mathbb{Z}_p$ in the last section we will now allow ourselves to get sloppy and write a for $[a]$ when it is clear from context that we are in $\mathbb{Z}_p$ and not $\mathbb{Z}$. Since $\mathbb{Z}_p$ satisfies the field properties we can talk about polynomials with coefficients in $\mathbb{Z}_p$. However there is one technical detail which we briefly alluded to in §1.7 which becomes important here, the difference between a polynomial *form* and a polynomial *function*. For a more complete discussion on this topic see either of the abstract algebra texts by Birkoff and Mac Lane.

A *polynomial form* with coefficients in $\mathbb{Z}_p$ is an expression $f = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n$ where the $a_j \in \mathbb{Z}_p$ and x is a formal *place holder*. Alternatively, x can be considered a special element of a larger integral domain. The important property is that polynomials $f = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n$ and $g = b_0 + b_1 x + \cdots + b_m x^m$ are *equal* if and only if $a_j = b_j$ for all $j = 0, 1, 2, \ldots$.

A *polynomial function* on the other hand is a function $f : \mathbb{Z}_p \to \mathbb{Z}_p$ given by a formula $f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n$ where here x is considered to be a *variable*. The important property here is that polynomial functions $f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n$ and $g(x) = b_0 + b_1 x + \cdots + b_m x^m$ are *equal* if and only if $f(c) = g(c)$ for every $c \in \mathbb{Z}_p$.

In previous chapters where we considered polynomials with coefficients in $\boldsymbol{Q}$, $\boldsymbol{R}$

or $\boldsymbol{C}$, there was no problem as Theorem 1.7.3 applied to say that polynomial forms and polynomial functions are essentially the same thing. But with coefficients in $\mathbb{Z}_p$ this is not true, for one thing there are only p^p possible functions $\mathbb{Z}_p \to \mathbb{Z}/p$, all of them being polynomial functions! (This can be proven by Lagrange interpolation.) However the polynomial forms $x, x^2, x^3, x^4, \ldots$ are all distinct, i.e. there are infinitely many polynomial forms.

Given a polynomial form $f = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$ there is a corresponding polynomial function $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$. What can happen over $\mathbb{Z}_p$ is that different polynomial forms can correspond to the same polynomial function. For instance the polynomial forms $f = x$ and $g = x^p$ are different but by Fermat's Little Theorem the polynomial functions $f(x) = g(x)$.

Polynomial forms can be added and multiplied by the formulas for the coefficients given in §1.4. As $\mathbb{Z}_p$ satisfies all the field properties it is not difficult to show that many of the theorems in §1.5, 1.6, 1.7, 1.8 and 1.9 hold for $\mathbb{Z}_p[x]$, the ring of polynomial forms. In particular, Theorems 1.5.1, 1.6.1, 1.6.2, 1.7.1, 1.7.2, (not 1.7.3 or 1.7.4) 1.8.2 (and the Euclidean Algorithm), 1.9.3, 1.9.4 and 1.9.7 hold for polynomial forms over $\mathbb{Z}_p$.

Polynomial functions can be added and multiplied as functions. The correspondence $f \mapsto f(x)$ respects the two different sets of operations and is another example of a *homomorphism.* However the above mentioned theorems do not apply to polynomial functions over $\mathbb{Z}_p$, for instance 1.5.1, 1.6.1 do not make sense as there is no notion of degree, theorems such as 1.9.3, 1.9.4 are simply nonsense when applied to functions.

> *Thus, for the remainder of this chapter, the word* **polynomial** *will mean* **polynomial form**.

As noted above, the Euclidean Algorithm holds for polynomials over $\mathbb{Z}_p$. Applying this algorithm over $\boldsymbol{Q}$ can get messy, and floating point approximations may change the aspect of the problem drastically – all polynomials are "approximately" relatively prime. Since there are only p elements of $\mathbb{Z}/p$ the numbers don't get messy. Thus if one wants to check rational polynomials to see if they are relatively prime (eg. if one is checking for multiple roots) it is recommended that one first try the Euclidean algorithm over $\mathbb{Z}_p$ for one or more suitable p. We now explore the relationship between gcd's over $\mathbb{Z}[x]$ and over $\mathbb{Z}_p[x]$.

Given a polynomial $f = a_0 + a_1x + \cdots + a_nx^n$ in $\mathbb{Z}[x]$ we write $[f] = [a_0] + [a_1]x + \cdots + [a_n]x^n$ in $\mathbb{Z}_p[x]$. The correspondence $f \mapsto [f]$ extends the function $\sigma : \mathbb{Z} \to \mathbb{Z}_p$ of the previous section and is again a homomorphism. We have

Theorem 2.1 *Let $f = a_0 + a_1x + \cdots + a_nx^n$, $h = b_0 + b_1x + \cdots + b_mx^m \in \mathbb{Z}[x]$ and let p be a prime integer. Let g be a gcd of f and h in $\mathbb{Z}[x]$. Then $[g]$ divides $\gcd([f],[h])$ in $\mathbb{Z}_p[x]$. In particular, if $[f],[h]$ are relatively prime, and either a_n or b_m is not divisible by p, then f, h are relatively prime in $\boldsymbol{Q}[x]$. Moreover, if in addition to $[g] = 1$, f, h are primitive in $\mathbb{Z}[x]$ then f, h are relatively prime in $\mathbb{Z}[x]$.*

Proof: By the homomorphism property, $[g]|[f]$ and $[g]|[h]$ so by definition of greatest common divisor, $[g]|\gcd([f],[h])$. Now suppose $g = c_0 + c_1x + \cdots + c_kx^k$, $c_k \neq 0$, and $[g] = 1$. By Theorem 5.2.1 $c_k|a_n$ and $c_k|b_m$ so our hypothesis on a_n, b_m assures that c_k is not divisible by p, i.e. $[c_k] \neq 0$. Thus $\deg g = \deg[g] = 0$ so f, h are relatively prime in $\boldsymbol{Q}[x]$. If in addition f, h are primitive then by Theorem 5.1.6 f, h are relatively prime in $\mathbb{Z}[x]$.

We end this section with a brief discussion of quadratic equations over $\mathbb{Z}_p$. As long as $p \neq 2$, and $a \neq 0$, then $ax^2 + bx + c = 0$ can be rewritten by completing the square as first $x^2 + (b/a)x + (c/a) = 0$ and then

$$(x + \frac{b}{2a})^2 = (\frac{b}{2a})^2 - \frac{c}{a} = \frac{b^2 - 4ac}{4a^2}$$

Thus, as in the usual case, there is a root to ax^2+bx+c if and only if b^2-4ac is a square in $\mathbb{Z}/p$. Solving an equation $[y]^2 = [d]$ in $\mathbb{Z}_p$ is equivalent to solving a congruence $y^2 \equiv d \pmod{p}$ in $\mathbb{Z}$. Integers d which satisfy this congruence for some y are called *quadratic residues modulo p*. The study of quadratic residues has been an important topic in Number Theory and there have been important and elegant contributions to this study by Euler, Legendre, Gauss and Jacobi. We refer the interested reader to any Number Theory text. The results of this theory say that about half of the integers $n, 1 < n < p$ are quadratic residues modulo p, and there are fairly easy algorithms to determine which ones. Thus, about half of the quadratic equations in $\mathbb{Z}_p[x]$ have roots in $\mathbb{Z}_p$. In §5.10 we will discuss the topic of roots of possibly higher degree polynomials in $\mathbb{Z}_p[x]$.

3 Factoring in $\mathbb{Z}_p[x]$

Factoring in $\mathbb{Z}_p[x]$ has been studied extensively, partly because it is, as we will see, considerably easier than factoring over $\mathbb{Z}[x]$ and partly because there are a number of commercially important applications to coding theory and communications theory. For one thing, $\mathbb{Z}_p[x]$ has only finitely many polynomials in any given degree, and hence

only finitely many monic irreducible polynomials. If p is a small prime and d is a small number it is practical to make a table of all monic irreducible polynomials of degree d in $\mathbb{Z}_p[x]$.

For example for $p = 2$ we have

Irreducible polynomials of degree 1

$$x, x + 1$$

Irreducible polynomials of degree 2

$$x^2 + x + 1$$

Irreducible polynomials of degree 3

$$x^3 + x + 1, x^3 + x^2 + 1$$

Irreducible polynomials of degree 4

$$x^4 + x + 1, x^4 + x^3 + 1, x^4 + x^3 + x^2 + x + 1$$

The connection between factoring in $\mathbb{Z}_p[x]$ and $\mathbb{Z}[x]$ is given by the following theorem:

Theorem 3.1 *Let $f = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n \in \mathbb{Z}[x]$ and p be a prime number. If $[f]$ is irreducible in $\mathbb{Z}_p[x]$ and a_n is not divisible by p then f is irreducible in $\mathbb{Z}[x]$. More specifically, if p does not divide a_n and $[f]$ has no factor (irreducible or otherwise) of degree d then f has no factors of degree d.*

Proof: This follows from the homomorphism property, and the fact that the hypothesis on a_n and Theorem 5.2.1 insure that the degree of f and its factors are preserved under the homomorphism $\mathbb{Z}[x] \to \mathbb{Z}_p[x]$.

As an application, it is follows from our table of irreducible polynomials in $\mathbb{Z}_2$ that $3x^2 + 5x + 7, x^3 + 7x^2 + 4x + 3$ and $x^3 + 2x^2 + 5x + 7$ are all irreducible in $\mathbb{Z}[x]$.

As another application, it can be shown, by methods to be discussed below, that $f = x^8 + x^6 - 3x^4 - 3x^3 + 8x^2 + 2x - 5$ factors as a product of a degree 1, degree 3 and degree 4 polynomial in $\mathbb{Z}_{13}$ and a degree 2 times degree 6 in $\mathbb{Z}/2$. In $\mathbb{Z}_2$ there is no linear factor, so f has no linear factor, in $\mathbb{Z}_{13}$ there is no quadratic factor, so f has no quadratic factor, in $\mathbb{Z}_2$ there are no factors of degree 3 or 4 so f has no factors of degree 3 or 4. Since f is of degree 8 it follows that f is irreducible in $\mathbb{Z}[x]$. It appears that this

f is not irreducible over any $\mathbb{Z}_p$ but is irreducible over $\mathbb{Z}$, at any rate x^4+1 satisfies this condition. Thus there is no converse, or partial converse, to 3.1.

In recent years several very efficient algorithms for factoring polynomials over $\mathbb{Z}_p$ have been developed. Perhaps the most efficient and best known is one due to E. Berlekamp in 1967. Berlekamp's algorithm uses some advanced ideas and linear algebra, so we will not discuss it here. Instead we will explain another algorithm called *distinct-degree factorization* which is somewhat simpler. This method had a somewhat mysterious origin in the late 1950's It is implemented, for instance, in MAPLE as a subroutine for MAPLE's integer factoring program factor. Before describing this method we breifly discuss the idea of congruence of polynomials.

Let F denote one of the fields $\boldsymbol{Q}$, $\boldsymbol{R}$, $\boldsymbol{C}$, or $\mathbb{Z}_p$ and consider the ring of polynomials with coefficients F. Let $u(x)$ be a fixed polynomial. We say $f(x), g(x)$ are *congruent modulo* $u(x)$, written $f(x) \equiv g(x) \pmod{u(x)}$ if $f(x) - g(x)$ is divisible by $u(x)$, alternatively if $f(x), g(x)$ have the same remainder after division by $u(x)$. This notion of congruence has the properties of congruence modulo n discussed earlier in this chapter. In particular, congruence respects addition, subtraction and multiplication. Further, if $u(x)$ has degree n, by the Division Theorem, each polynomial $f(x)$ is congruent to a unique polynomial of degree $< n$.

The distinct-degree factorization method is based on the following amazing theorem the proof of which is beyond the scope of this book.

Theorem 3.2 *Let $g(x)$ be an irreducible polynomial of degree d. Then $g(x)$ divides $x^{p^d} - x$ but does not divide $x^{p^c} - x$ for $c < d$.*

Thus the method of the distinct-degree algorithm to find factors of $u(x)$ is basically to take the gcd of $u(x)$ and $x^{p^d} - x$ where d is the degree of the desired factor. The problem is that p^d can be quite large and a direct computation of the gcd would make this method impractical, in fact no easier than dividing each of the p^d polynomials of degree d into $u(x)$ directly. We are saved by the following simple fact, more or less a restatement of Lemma 1.8.3.

Theorem 3.3 *Suppose* $g(x) \equiv h(x) \pmod{u(x)}$. *Then* $\gcd(g(x), u(x)) = \gcd(h(x), u(x))$.

Thus we may replace x^n by $g(x)$ where $\deg g(x) < \deg u(x)$ and $g(x) \equiv x^n \pmod{u(x)}$. But the nice thing, is if we have calculated $g(x)$ for $n = p^d$, then $x^{p^d+1} \equiv g(x)^p \pmod{u(x)}$. But even this calculation is easy due to the following suprising theorem in $\mathbb{Z}_p$.

Theorem 3.4 *If $f = a_0 + a_1x + \cdots + a_nx^n \in \mathbb{Z}_p[x]$ then $f^p = a_0 + a_1x^p + a_2x^2p + \cdots + a^nx^{np}$. In other notation, $f(x)^p = f(x^p)$.*

Proof: First from the binomial formula, using the fact that the binomial coefficients $C(p,r) \equiv 0 \pmod{p}$ for $0 < r < p$, we have the "Freshman Binomial Theorem" $(a+b)^p = a^p + b^p$. By induction we have $f^p = (a_0)^p + (a_1x)^p + (a_2x^2)^p + \cdots + (a_nx^n)^p$. The result follows from Fermat's Little Theorem. Note since we are dealing with polynomial forms, not functions, Fermat's theorem does not apply to $(x^j)^p$ which is not equal to x^j.

The distinct-degree algorithm to find irreducible factors of $u(x) \in \mathbb{Z}_p[x]$ of degree n now proceeds as follows:

1. Calculate $\gcd(u(x), u'(x))$ over $\mathbb{Z}_p$ and divide out any multiple factors, the rest of the algorithm does not work as well with multiple factors present.
2. Initialize $d = 0$ and $g(x) = x$.
3. If $d > n/2$, stop, $u(x)$ is irreducible. Otherwise replace d by $d+1$ and raise $g(x)$ to the pth power modulo $u(x)$, i.e. replace $g(x)$ by a polynomial of degree $< n$ congruent to $g(x)^p \pmod{u(x)}$. Note by 3.4 only one division is required and the polynomial never has degree greater than $(n-1) * p$. With more divisions we can arrange our arithmetic so the degree never exceeds n.
4. Find $h(x) = \gcd(g(x) - x, u(x))$. If not 1, $h(x)$ is the product of all irreducible factors of degree d.
5. Divide $u(x)$ by $h(x)$ and replace $u(x)$ by the quotient and n by the degree of this quotient. Go back to step 3.

Note that this algorithm does not necessarily find all the irreducible factors but only the product of the irreducible factors of each degree. With additional work one can actually find all the factors, see [D. Knuth, *Seminumerical Algorithms*, §4.6.2]. However, for many purposes, eg. proving irreducibility, it is not the actual factors but the number of factors of each degree that is important. The algorithm above finds this quite nicely.

4 Roots of Polynomials in $\mathbb{Z}_n$

In this last optional section we discuss the problem of counting the number of roots of a polynomial in the ring $\mathbb{Z}_n$ where n may not be a prime number. There are several

surprises, one being the appearance of Newtons method, even though we are doing modular arithmetic and not numerical analysis! The material in this section is based on §3.4 of the book *Fundamentals of Number Theory* by W.J. LeVeque, 1977, which was most recently available from Dover Publications.

We start with the case $n = p$ is a prime number. The main result is

Theorem 4.1 *Let $f(x) \in \mathbb{Z}_p[x]$ where p is a prime number. The number of distinct solutions to the equation $f(x) = 0$ in $\mathbb{Z}_p$ is the degree of $\gcd(f(x), x^p - x)$. In particular, if $f(x)$ has degree d then $f(x)$ has d distinct roots in $\mathbb{Z}_p$ if and only if $f(x)|(x^p - x)$.*

Proof: Fermat's Little Theorem says that each element of $\mathbb{Z}_p$ is a root of $x^p - x$ from which it follows from the root Theorem that

$$x^p - x = x(x - [1])(x - [2]) \cdots (x - [p - 1]) \tag{3}$$

Each root of $f(x)$ corresponds to a linear factor $(x - [m])$ so counting the number of roots amounts to counting the distinct linear factors, i.e. the degree of $\gcd(f(x), x^p - x)$.

As a corollary of this we get a quick proof of a famous theorem of number theory:

Corollary 4.2 (Wilson's Theorem) *If p is a prime number, then $(p-1)! \equiv -1 \pmod{p}$.*

Proof: The result is true by inspection if $p = 2$. Now suppose p is an odd prime. By the theory of symmetric polynomials (Theorem 4.8.1) the coefficient of x on the right of Equation 3 is $(p - 1)!$ since $p - 1$ is even. But the coefficent of x on the left is -1.

We now consider general n. We first remind the reader that if n is not prime most of the theorems of Chapter 1 do not hold.

Example 4.3 Let $n = 15$ and $f(x) = x^2 + 3x + 2 \in \mathbb{Z}_{15}[x]$. Then by inspection one sees that $f(x)$ has roots $x = 4, 8, 13$ and $14 \pmod{15}$ violating Theorem 1.7.2.

Example 4.4 Let $n = 8$, $f(x) = 1+2x+4x^2$ and $g(x) = 1-2x$. Then $f(x)*g(x) = 1$ in $\mathbb{Z}_8$ violating Theorem 1.5.1. Note that $f(x)$ is a non-constant polynomial which has a multiplicative inverse!

An application of the Chinese Remainder Theorem (see any number theory book) gives

Theorem 4.5 *Let $f(x) \in \mathbb{Z}[x]$ and m, n integers with $\gcd(m, n) = 1$. Then the number of roots of $[f]$ in $\mathbb{Z}_{mn}$ is the number of roots of $[f]$ in $\mathbb{Z}_m$ multiplied by the number of roots of $[f]$ in $\mathbb{Z}_n$.*

Proof: Given $f(x_1) \equiv 0 \pmod{m}$ and $f(x_2) \equiv 0 \pmod{n}$ by the Chinese remainder theorem there is a unique y with $0 \leq y < nm$ and

$$\begin{aligned} y &\equiv x_1 \pmod{m} \\ y &\equiv x_2 \pmod{n} \end{aligned}$$

then $f(y) \equiv 0 \pmod{m}$ so $m|f(y)$ and $f(y) \equiv 0 \pmod{n}$ so $n|f(y)$. Since $\gcd(m, n) = 1$ then $mn|f(y)$ so $f(y) \equiv 0 \pmod{mn}$. Conversely if $f(y) \equiv 0 \pmod{mn}$ then $mn|f(y)$ so $f(y) \equiv 0 \pmod{m}$ and $f(y) \equiv 0 \pmod{n}$ so every root in $\mathbb{Z}_{mn}$ is of this form.

Now we note that if $n > 1$ then n factors in $\mathbb{Z}$ as $n = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$ so as a corollary we get

Theorem 4.6 *Let $n = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$ be an integer greater than 1. Let $f(x) \in \mathbb{Z}[x]$. Then the number of roots of $[f(x)] \in \mathbb{Z}_n[x]$ is the product over the number of roots of $[f(x)]$ in each ring $\mathbb{Z}_{p_j^{e_j}}$.*

Thus, to understand the general case, it suffices to understand the special case $n = p^e$ where p is prime and $e \geq 1$. Of course if $e = 1$ this is just Theorem 4.1. We will show, inductively, how to treat the case $n = p^{e+1}$ assuming the case $n = p^e$ is known.

The key is that if x is a solution to $f(x) \equiv 0 \pmod{p^{e+1}}$ then $p^{e+1}|f(x)$ so in particular $p^e|f(x)$ and hence x is also a solution to $f(x) \equiv 0 \pmod{p^e}$. Thus we will start with a fixed solution x_0 to $f(x_0) \equiv 0 \pmod{p^e}$ and show how to find all solutions to $f(x) \equiv 0 \pmod{p^{e+1}}$ which are congruent to $x_0 \bmod p^e$.

But if $0 \leq x < p^{e+1}$ and $x \equiv x_0 \pmod{p^e}$ then $x = x_0 + tp^e$ where $0 \leq t < p$. Now by using Horner's process of §2.3 and Theorem 5.1.1 we see that if $f(x) \in \mathbb{Z}[x]$ and $c \in \mathbb{Z}$ that we have a Taylor series

$$f(x) = f(c) + f'(c)(x - c) + \frac{f''(c)}{2!}(x - c)^2 + \cdots$$

where the coefficients $f^{(j)}(c)/j!$ are integers. Now letting $x = x_0 + tp^e$ and $c = x_0$ then $x - c = tp^e$ so this becomes

$$f(x) = f(x_0) + f'(x_0)tp^e + \frac{f''(x_0)}{2}t^2p^{2e} + \cdots$$

but we will be reducing this modulo p^{e+1} and $p^{e+1}|p^{2e}$ so we actually have

$$f(x) \equiv f(x_0) + f'(x_0)tp^e + sp^{e+1}$$

for some integer s.

Now recalling that we chose x_0 so that $f(x_0) \equiv 0 \pmod{p^e}$ and we want x to satisfy $f(x) \equiv 0 \pmod{p^{e+1}}$ we have the integer equation

$$p\frac{f(x)}{p^{e+1}} = \frac{f(x_0)}{p^e} + f'(x_0)t + sp$$

which gives the congruence

$$0 \equiv \frac{f(x_0)}{p^e} + f'(x_0)t \pmod{p}$$

or

$$f'(x_0)t = -\frac{f(x_0)}{p^e} \pmod{p} \tag{4}$$

Now we have two cases. The less common *singular* case is when $f'(x_0) \equiv 0 \pmod{p}$. In this case if $\frac{f(x_0)}{p^e} \not\equiv 0 \pmod{p}$ there are no solutions to Equation 4 and the solution x_0 of $f(x_0) \equiv 0 \pmod{p^e}$ produces no solutions to $f(x) \equiv 0 \pmod{p^{e+1}}$. On the other hand if also $\frac{f(x_0)}{p^e} \equiv 0 \pmod{p}$ then Equation 4 becomes $0 * t \equiv 0 \pmod{p}$ and every t is a solution, $0 \leq t < p$, so the solution x_0 produces p distinct solutions to $f(x) \equiv 0 \pmod{p^{e+1}}$.

The more common and interesting case is the *non-singular* case when $f'(x_0) \not\equiv 0 \pmod{p}$. Since $\mathbb{Z}_p$ is a field we can divide Equation 4 by $[f'(x_0)]$ to get

$$t = -\left[\frac{f(x_0)}{p^e f'(x_0)}\right]$$

Now plugging this value of t into the equation $x = x_0 + tp^e$ we get the equation (in $\mathbb{Z}_{p^{e+1}}$)

$$x = x_0 - \frac{f(x_0)}{f'(x_0)}$$

which the astute reader notes is just the iteration formula for Newton's method!

One technicality we should mention is that $\mathbb{Z}_{p^{e+1}}$ is not a field so we must be careful using division. But since $f'(x_0) \not\equiv 0 \pmod{p}$ then $\gcd(p^{e+1}, f'(x_0)) = 1$ so $1 = rp^{e+1} + sf'(x_0)$ for some $r, s \in \mathbb{Z}$ so $[f'(x_0)]^{-1} = [s]$ in $\mathbb{Z}_{p^{e+1}}$. In practice, s can be found by the extended Euclidean Algorithm as in §1.8.

Example 4.7 We end these notes by finding the unique solution to $x^2-2 \equiv 0 \pmod{2401}$, i.e. the square root of 2 modulo 7^4. By inspection, trying all possibilities, we see that the unique solution to $x^2 - 2 \equiv 0 \pmod 7$ is $x_0 \equiv 4 \pmod 7$

Now if $f(x) = x^2 - 2$ then $f'(x) = 2x$ so an application of Newtons method gives

$$x_1 \equiv x_0 - \frac{f(x_0)}{f'(x_0)} = 4 - \frac{[14]}{[8]} \pmod{49}$$

where $\frac{[14]}{[8]}$ is calculated in $\mathbb{Z}_{49}$ where $[8]^{-1} = [43]$ so $\frac{[14]}{[8]} = [14][43] = [602] = [14]$ so $x_1 = [4] - [14] = [4] + [35] = [39]$ and hence the solution is $x_1 \equiv 39 \pmod{49}$

Next we have

$$x_2 \equiv x_1 - \frac{f(x_1)}{f'(x_1)} = 39 - \frac{[1519]}{[78]} \pmod{343}$$

Now in $\mathbb{Z}_{343}$ we have $\frac{1519]}{[78]} = \frac{[147]}{[78]} = [147][22] = [3234] = [147]$ so $x_2 = [39] - [147] = [39] + [196] = [235]$ and hence $x_2 \equiv 235 \pmod{343}$.

Finally

$$x_3 \equiv x_2 - \frac{f(x_2)}{f'(x_2)} = 235 - \frac{[55223]}{[470]} \pmod{2401}$$

However here we are lucky in that $2401|55223$ so $[55223] = 0$ in $\mathbb{Z}_{2401}$. Thus $x_3 \equiv 235 \pmod{2401}$ is our desired answer!