ROOTS AND IRREDUCIBLES

KEITH CONRAD

1. Introduction

This handout discusses relationships between roots of irreducible polynomials and field extensions. Throughout, the letters K, L, and F are fields and $\mathbf{F}_p = \mathbf{Z}/(p)$ is the field of p elements. When $f(X) \in K[X]$, we will say $f(X)$ is a polynomial "over" K. Sections 2 and 3 describe some general features of roots of polynomials. In the later sections we look at roots to polynomials over the finite field $\mathbf{F}_p$.

2. Roots in larger fields

For most fields K, there are polynomials in $K[X]$ without a root in K. Consider $X^2 + 1$ in $\mathbf{R}[X]$ or $X^3 - 2$ in $\mathbf{F}_7[X]$. If we are willing to enlarge the field, then we can discover some roots. This is due to Kronecker, by the following argument.

Theorem 2.1. *Let K be a field and $f(X)$ be nonconstant in $K[X]$. There is a field extension of K containing a roof of $f(X)$.*

Proof. It suffices to prove the theorem when $f(X) = \pi(X)$ is irreducible (why?).

Set $F = K[t]/(\pi(t))$, where t is an indeterminate. Since $\pi(t)$ is irreducible in $K[t]$, F is a field. Inside of F we have K as a subfield: the congruence classes represented by constants. There is also a root of $\pi(X)$ in F, namely the class of t. Indeed, writing $\overline{t}$ for the congruence class of t in F, the congruence $\pi(t) \equiv 0 \bmod \pi(t)$ becomes the equation $\pi(\overline{t}) = 0$ in F. $\square$

Example 2.2. Consider $X^2 + 1 \in \mathbf{R}[X]$, which has no root in $\mathbf{R}$. The ring $\mathbf{R}[t]/(t^2 + 1)$ is a field containing $\mathbf{R}$. In this field $\overline{t}^2 = -1$, so the polynomial $X^2 + 1$ has the root $\overline{t}$ in the field $\mathbf{R}[t]/(t^2 + 1)$. The reader should recognize $\mathbf{R}[t]/(t^2 + 1)$ as an algebraic version of the complex numbers: congruence classes are represented by $a + bt$ with $\overline{t}^2 = -1$.

When an irreducible polynomial over a field K picks up one root in a larger field, there need not be more roots in that field. *This is an important point to keep in mind.* A simple example is $X^3 - 2$ in $\mathbf{Q}[X]$, which has only one root in $\mathbf{R}$, namely $\sqrt[3]{2}$. There are two more roots in $\mathbf{C}$, but they do not live in $\mathbf{R}$. (Incidentally, the field extension of $\mathbf{Q}$ constructed by Theorem 2.1 which contains a root of $X^3 - 2$, namely $\mathbf{Q}[t]/(t^3 - 2)$, is much smaller than the real numbers, *e.g.*, it is countable.)

By repeating the construction in the proof of Theorem 2.1 several times, we can always create a field with a full set of roots for our polynomial. We state this as a corollary, and give a proof by induction on the degree.

Corollary 2.3. *Let K be a field and $f(X) = c_m X^m + \cdots + c_0$ be in $K[X]$ with degree $m \geq 1$. There is a field $L \supset K$ such that in $L[X]$,*

$$f(X) = c_m(X - \alpha_1) \cdots (X - \alpha_m). \tag{2.1}$$

Proof. We induct on the degree m. The case $m = 1$ is clear, using $L = K$. By Theorem 2.1, there is a field $F \supset K$ such that $f(X)$ has a root in F, say α_1. Then in $F[X]$,

$$f(X) = (X - \alpha_1)g(X),$$

where $\deg g(X) = m - 1$. The leading coefficient of $g(X)$ is also c_m.

Since $g(x)$ has smaller degree than $f(X)$, by induction on the degree there is a field $L \supset F$ (so $L \supset K$) such that $g(X)$ decomposes into linear factors in $L[X]$, so we get the desired factorization of $f(X)$ in $L[X]$. □

Corollary 2.4. *Let $f(X)$ and $g(X)$ be nonconstant in $K[X]$. They are relatively prime in $K[X]$ if and only if they do not have a common root in any extension field of K.*

Proof. Assume $f(X)$ and $g(X)$ are relatively prime in $K[X]$. Then we can write

$$f(X)u(X) + g(X)v(X) = 1$$

for some $u(X)$ and $v(X)$ in $K[X]$. If there were an α in an field extension of K which is a common root of $f(X)$ and $g(X)$, then substituting α for X in the above polynomial identity makes the left side 0 while the right side is 1. This is a contradiction, so $f(X)$ and $g(X)$ have no common root in any field extension of K.

Now assume $f(X)$ and $g(X)$ are not relatively prime in $K[X]$. Say $h(X) \in K[X]$ is a (nonconstant) common factor. There is a field extension of K in which $h(X)$ has a root, and this root will be a common root of $f(X)$ and $g(X)$. □

Although adjoining one root of an irreducible in $\mathbf{Q}[X]$ to the rational numbers does not always produce the other roots in the same field (such as with $X^3 - 2$), the situation in $\mathbf{F}_p[X]$ is much simpler. We will see later (Theorem 5.4) that for an irreducible in $\mathbf{F}_p[X]$, a larger field which contains one root must contain *all* the roots. Here are two examples.

Example 2.5. The polynomial $X^3 - 2$ is irreducible in $\mathbf{F}_7[X]$. It has a root in $F = \mathbf{F}_7[t]/(t^3 - 2)$, namely $\bar{t}$. It also has two other roots in F, $2\bar{t}$ and $4\bar{t}$.

Example 2.6. The polynomial $X^3 + X^2 + 1$ is irreducible in $\mathbf{F}_5[X]$. In the field $F = \mathbf{F}_5[t]/(t^3 + t^2 + 1)$, the polynomial has the root $\bar{t}$ and also the roots $2\bar{t}^2 + 3\bar{t}$ and $3\bar{t}^2 + \bar{t} + 4$.

3. Divisibility and roots in $K[X]$

There is an important connection between roots of a polynomial and divisibility by *linear* polynomials. For $f(X) \in K[X]$ and $\alpha \in K$, $f(\alpha) = 0 \Longleftrightarrow (X - \alpha)|f(X)$. The next result is an analogue for divisibility by higher degree polynomials in $K[X]$, provided they are irreducible. (All linear polynomials are irreducible.)

Theorem 3.1. *Let $\pi(X)$ be irreducible in $K[X]$ and let α be of a root of $\pi(X)$ in some larger field. For $h(X)$ in $K[X]$, $h(\alpha) = 0 \Longleftrightarrow \pi(X)|h(X)$ in $K[X]$.*

Proof. If $h(X) = \pi(X)g(X)$, then $h(\alpha) = \pi(\alpha)g(\alpha) = 0$.

Now assume $h(\alpha) = 0$. Then $h(X)$ and $\pi(X)$ have a common root, so by Corollary 2.4 they have a common factor in $K[X]$. Since $\pi(X)$ is irreducible, this means $\pi(X)|h(X)$ in $K[X]$. To see this argument more directly, suppose $h(\alpha) = 0$ and $\pi(X)$ does not divide $h(X)$. Then (because π is irreducible) the polynomials $\pi(X)$ and $h(X)$ are relatively prime in $K[X]$ so we can write

$$\pi(X)u(X) + h(X)v(X) = 1$$

for some $u(X), v(X) \in K[X]$. Substitute α for X and the left side vanishes. The right side is 1 so we have a contradiction. □

Example 3.2. Take $K = \mathbf{Q}$ and $\pi(X) = X^2 - 2$. It has a root $\sqrt{2} \in \mathbf{R}$. For any $h(X) \in \mathbf{Q}[X]$, $h(\sqrt{2}) = 0 \iff (X^2 - 2)|h(X)$. This equivalence breaks down if we allow $h(X)$ to come from $\mathbf{R}[X]$: try $h(X) = X - \sqrt{2}$.

The following theorem, which we will not explicitly use further in this handout, shows that divisibility relations in $K[X]$ can be checked by working over any larger field.

Theorem 3.3. *Let K be a field and L be a larger field. For $f(X)$ and $g(X)$ in $K[X]$, $f(X)|g(X)$ in $K[X]$ if and only if $f(X)|g(X)$ in $L[X]$.*

Proof. It is clear that divisibility in $K[X]$ implies divisibility in the larger $L[X]$. Conversely, suppose $f(X)|g(X)$ in $L[X]$. Then

$$g(X) = f(X)h(X)$$

for some $h(X) \in L[X]$. By the division algorithm in $K[X]$,

$$g(X) = f(X)q(X) + r(X),$$

where $q(X)$ and $r(X)$ are in $K[X]$ and $r(X) = 0$ or $\deg r < \deg f$. Comparing these two formulas for $g(X)$, the uniqueness of the division algorithm in $L[X]$ implies $q(X) = h(X)$ and $r(X) = 0$. Therefore $g(X) = f(X)q(X)$, so $f(X)|g(X)$ in $L[X]$. $\square$

Notice how the uniqueness in the division algorithm for polynomials (over any field) played a role in the proof.

4. Raising to the p-th power in characteristic p

The rest of this handout is concerned with applications of the preceding ideas to polynomials in $\mathbf{F}_p[X]$. What we see will be absorbed later into the general ideas of Galois theory, but already at this point some interesting results can be made rather explicit (*e.g.*, Corollary 4.5 and Theorem 5.4) without a lot of general machinery.

The most important operation in characteristic p is the p-th power map $x \mapsto x^p$ because is not just multiplicative, but also additive:

Lemma 4.1. *Let A be a commutative ring with prime characteristic p. Pick any a and b in A.*

a) $(a + b)^p = a^p + b^p$.

b) When A is a domain, $a^p = b^p \Longrightarrow a = b$.

Proof. a) By the binomial theorem,

$$(a + b)^p = a^p + \sum_{k=1}^{p-1} \binom{p}{k} a^{p-k} b^k + b^p.$$

For $1 \leq k \leq p - 1$, the integer $\binom{p}{k}$ is a multiple of p (why?), so the intermediate terms are 0 in A.

b) Now assume A is a domain and $a^p = b^p$. Then $0 = a^p - b^p = (a - b)^p$. (Note $(-1)^p = -1$ for $p \neq 2$, and also for $p = 2$ since $2 = 0 \Longrightarrow -1 = 1$ in A.) Since A is a domain, $a - b = 0$, so $a = b$. $\square$

Lemma 4.2. *Let $F \supset \mathbf{F}_p$. For $c \in F$, $c \in \mathbf{F}_p \iff c^p = c$.*

Proof. Every element c of $\mathbf{F}_p$ satisfies the equation $c^p = c$. Conversely, solutions to this equation are the roots of $X^p - X$, which has at most p roots in F. The elements of $\mathbf{F}_p$ already fulfill this upper bound, so there are no further roots in characteristic p. $\square$

Theorem 4.3. *For any $f(X) \in \mathbf{F}_p[X]$, $f(X)^{p^r} = f(X^{p^r})$ for $r \geq 0$. If F is a field of characteristic p other than $\mathbf{F}_p$, this is not always true in $F[X]$.*

Proof. Writing
$$f(X) = c_m X^m + c_{m-1}X^{m-1} + \cdots + c_1 X + c_0,$$
Lemma 4.1a with $A = \mathbf{F}_p[X]$ gives
$$\begin{aligned} f(X)^p &= (c_m X^m + c_{m-1}X^{m-1} + \cdots + c_1 X + c_0)^p \\ &= c_m^p X^{mp} + c_{m-1}^p X^{p(m-1)} + \cdots + c_1^p X^p + c_0^p \\ &= c_m (X^p)^m + c_{m-1}(X^p)^{m-1} + \cdots + c_1 X^p + c_0, \end{aligned}$$
since $c^p = c$ for any $c \in \mathbf{F}_p$. The last expression is $f(X^p)$. Applying this result r times, we find $f(X)^{p^r} = f(X^{p^r})$.

If F has characteristic p and is not $\mathbf{F}_p$, then F contains an element c which is not in $\mathbf{F}_p$. Then $c^p \neq c$ by Lemma 4.2, so the constant polynomial $f(X) = c$ (or any monomial cX^d) does not satisfy $f(X)^p = f(X^p)$. □

Remark 4.4. Theorem 4.3 is false if the coefficients of $f(X)$ are in a field of characteristic p larger than $\mathbf{F}_p$ itself. The proof required $c^p = c$ for all coefficients c, and this equation is true only for the elements of $\mathbf{F}_p$ (Lemma 4.2).

Let $f(X) \in \mathbf{F}_p[X]$ be nonconstant, with degree m. Let $L \supset \mathbf{F}_p$ be a field over which $f(X)$ decomposes into linear factors, *i.e.*, (2.1) holds. It is possible that some of the roots of $f(X)$ are multiple roots. As long as that does not happen, the following corollary says something about the p-th powers of the roots.

Corollary 4.5. *When $f(X) \in \mathbf{F}_p[X]$ has distinct roots, raising all roots of $f(X)$ to the p-th power permutes the roots:*
$$\{\alpha_1^p, \ldots, \alpha_m^p\} = \{\alpha_1, \ldots, \alpha_m\}.$$

Proof. Let $S = \{\alpha_1, \cdots, \alpha_m\}$. Since $f(X)^p = f(X^p)$ by Theorem 4.3, the p-th power of each root of $f(X)$ is again a root of $f(X)$. Therefore raising to the p-th power defines a function $\varphi\colon S \to S$. By Lemma 4.1b, φ takes different values on different elements of S. Since S is a finite set, φ must assume each element of S as a value (in the language of set theory, a one-to-one function from a finite set to itself is onto), so φ is a permutation of S. □

Example 4.6. Consider $X^3 + X^2 + 1 \in \mathbf{F}_5[X]$. In Example 2.6, we found a field $F \supset \mathbf{F}_5$ in which the polynomial has roots $\alpha_1 = \bar{t}$, $\alpha_2 = 2\alpha_1^2 + 2\alpha_1$, and $\alpha_3 = 3\alpha_1^2 + \alpha_1 + 4$. Check that $\alpha_1^5 = \alpha_3$, $\alpha_2^5 = \alpha_1$, and $\alpha_3^5 = \alpha_2$.

5. Roots of irreducibles in $\mathbf{F}_p[X]$

All the roots of an irreducible polynomial in $\mathbf{Q}[X]$ are not generally expressible in terms of a particular root, with $X^3 - 2$ being a typical example. (The field $\mathbf{Q}(\sqrt[3]{2})$ contains only one root to this polynomial, not all 3 roots.) However, the situation is markedly simpler over finite fields. In this section we will make explicit the relations among the roots of an irreducible polynomial in $\mathbf{F}_p[X]$. In short, we can obtain all roots from any one root by repeatedly taking p-th powers. The precise statement is in Theorem 5.4.

Lemma 5.1. *For $h(X)$ in $\mathbf{F}_p[X]$ with degree m, $\mathbf{F}_p[X]/(h(X))$ has size p^m.*

Proof. By the division algorithm in $\mathbf{F}_p[X]$, every congruence class modulo $h(X)$ contains a unique remainder from division by $h(X)$. These remainders are the polynomials

$$c_{m-1}X^{m-1} + \cdots + c_1 X + c_0,$$

with $c_j \in \mathbf{F}_p$. (Note $c_{m-1} = 0$ if the remainder has small degree.) There are p^m such representatives. □

Lemma 5.2. *When F is a finite field with size q, $c^q = c$ for all c in F.*

Proof. For $c \neq 0$ in F, $c^{q-1} = 1$ (since $F^\times$ is a group of size $q-1$) so multiplying through by c shows $c^q = c$. This last equation is obviously satisfied also by $c = 0$. □

Theorem 5.3. *Let $\pi(X)$ be irreducible of degree d in $\mathbf{F}_p[X]$.*
a) In $\mathbf{F}_p[X]$, $\pi(X)|(X^{p^d} - X)$.
b) For $n \geq 0$, $\pi(X)|(X^{p^n} - X) \iff d|n$.

Proof. The divisibility in (a) in the same as the congruence $X^{p^d} \equiv X \bmod \pi(X)$, or equivalently the equation $\overline{X}^{p^d} = \overline{X}$ in $\mathbf{F}_p[X]/(\pi(X))$. Such an equation follows immediately from Lemmas 5.1 and 5.2, using the field $\mathbf{F}_p[X]/(\pi(X))$.

To prove ($\Longleftarrow$) in (b), write $n = kd$. Starting with $X \equiv X^{p^d} \bmod \pi(X)$ (from (a)) and applying the p^d-th power to both sides k times, we obtain

$$X \equiv X^{p^d} \equiv X^{p^{2d}} \equiv \cdots \equiv X^{p^{(k-1)d}} \equiv X^{p^{kd}} = X^{p^n} \bmod \pi(X).$$

Thus $\pi(X)|(X^{p^n} - X)$ in $\mathbf{F}_p[X]$.

Now we prove ($\Longrightarrow$) in (b). We assume

$$X^{p^n} \equiv X \bmod \pi(X) \tag{5.1}$$

and want to show $d|n$. Write $n = dq + r$ with $0 \leq r < d$. We will show $r = 0$.

We have $X^{p^n} = X^{p^{dq}p^r} = (X^{p^{dq}})^{p^r}$. Since $d|dq$, $X^{p^{dq}} \equiv X \bmod \pi(X)$ by ($\Longleftarrow$), so $X^{p^n} \equiv X^{p^r} \bmod \pi(X)$. Thus, by (5.1),

$$X^{p^r} \equiv X \bmod \pi(X). \tag{5.2}$$

This tells us that one particular element of $\mathbf{F}_p[X]/(\pi(X))$, the class of X, is equal to its own p^r-th power. Let's extend this property to all elements of $\mathbf{F}_p[X]/(\pi(X))$. For any $f(X) \in \mathbf{F}_p[X]$, $f(X)^{p^r} = f(X^{p^r})$ by Theorem 4.3. Combining with (5.2),

$$f(X)^{p^r} \equiv f(X) \bmod \pi(X).$$

Therefore in $\mathbf{F}_p[X]/(\pi(X))$ the congruence class of $f(X)$ is equal to its own p^r-th power. As $f(X)$ is a general polynomial in $\mathbf{F}_p[X]$, we have proved every element of $\mathbf{F}_p[X]/(\pi(X))$ is its own p^rth power (in $\mathbf{F}_p[X]/(\pi(X))$).

Consider now the polynomial $T^{p^r} - T$. When $r > 0$, this is a polynomial with degree $p^r > 1$, and we have found p^d different roots of this polynomial in $\mathbf{F}_p[X]/(\pi(X))$ (namely, every element of this field is a root). Therefore $p^d \leq p^r$, so $d \leq r$. But, recalling where r came from, $r < d$. This is a contradiction, so $r = 0$. That proves $d|n$. □

Theorem 5.4. *Let $\pi(X)$ be irreducible in $\mathbf{F}_p[X]$ with degree d and $F \supset \mathbf{F}_p$ be a field in which $\pi(X)$ has a root, say α. Then $\pi(X)$ has roots $\alpha, \alpha^p, \alpha^{p^2}, \cdots, \alpha^{p^{d-1}}$. These d roots are distinct; more precisely, when i and j are nonnegative, $\alpha^{p^i} = \alpha^{p^j} \iff i \equiv j \bmod d$.*

Proof. Since $\pi(X)^p = \pi(X^p)$ by Theorem 4.3, we see α^p is also a root of $\pi(X)$, and likewise $\alpha^{p^2}, \alpha^{p^3}$, and so on by iteration. Once we reach α^{p^d} we have cycled back to the start: $\alpha^{p^d} = \alpha$ by Theorem 5.3a. (Write the divisibility in Theorem 5.3a as an equation in $\mathbf{F}_p[X]$ and then substitute α for X.)

Now we will show for $i, j \geq 0$ that $\alpha^{p^i} = \alpha^{p^j} \iff i \equiv j \bmod d$. Since $\alpha^{p^d} = \alpha$, the implication ($\Longleftarrow$) is straightforward. To argue in the other direction, we may suppose without loss of generality that $i \leq j$, say $j = i + k$ with $k \geq 0$. Then

$$\alpha^{p^i} = \alpha^{p^{i+k}} = (\alpha^{p^k})^{p^i}.$$

Applying Lemma 4.1b to this equality i times, with $A = F$, we have $\alpha = \alpha^{p^k}$. Therefore α is a root of $X^{p^k} - X$, so $\pi(X)|(X^{p^k} - X)$ in $\mathbf{F}_p[X]$ by Theorem 3.1. We conclude $d|k$ by Theorem 5.3b, so $i \equiv j \bmod d$. □

Since $\pi(X)$ has at most $d = \deg \pi$ roots in any field, Theorem 5.4 tells us $\alpha, \alpha^p, \ldots, \alpha^{p^{d-1}}$ are a complete set of roots of $\pi(X)$ and these roots are distinct.

Example 5.5. The polynomial $X^3 + X + 1$ is irreducible in $\mathbf{F}_2[X]$. In the field $F = \mathbf{F}_2[t]/(t^3 + t + 1)$, one root of the polynomial is $\bar{t}$. The other two roots are $\bar{t}^2$ and $\bar{t}^4$.

If we wish to write the third root without going beyond the second power of $\bar{t}$, note $t^4 \equiv t^2 + t \bmod t^3 + t + 1$. Therefore, the roots of $X^3 + X + 1$ in F are $\bar{t}$, $\bar{t}^2$, and $\bar{t}^2 + \bar{t}$.

Now we can remove the mystery behind the discovery of the roots in Example 2.6. There was no guessing or brute-force searching involved. The roots are $\bar{t}$, $\bar{t}^5$, and $\bar{t}^{25}$. Then remainders modulo $t^3 + t^2 + 1$ (in $\mathbf{F}_5[t]$) were computed for t^5 and t^{25}.

6. Finding irreducibles in $\mathbf{F}_p[X]$

A nice application of Theorem 5.3 is the next result, which is due to Gauss. It describes all irreducible polynomials of a given degree in $\mathbf{F}_p[X]$ as factors of a certain polynomial.

Theorem 6.1. *Let $n \geq 1$. In $\mathbf{F}_p[X]$,*

$$X^{p^n} - X = \prod_{d|n} \prod_{\substack{\deg \pi = d \\ \pi \text{monic}}} \pi(X), \tag{6.1}$$

where $\pi(X)$ is irreducible.

Let's look at some examples to understand what the theorem is telling us, before giving the proof.

Example 6.2. We factor $X^{2^n} - X$ in $\mathbf{F}_2[X]$ for $n = 1, 2, 3, 4$. We have

$$X^2 - X = X(X + 1),$$

$$X^4 - X = X(X + 1)(X^2 + X + 1),$$

$$X^8 - X = X(X + 1)(X^3 + X + 1)(X^3 + X^2 + 1),$$

$$X^{16} - X = X(X - 1)(X^2 + X + 1)(X^4 + X + 1)(X^4 + X^3 + 1)(X^4 + X^3 + X^2 + X + 1).$$

The following table lists all the irreducibles of each small degree in $\mathbf{F}_2[X]$:

n	Irreducibles of degree n in $\mathbf{F}_2[X]$
1	X, $X+1$
2	X^2+X+1
3	X^3+X+1, X^3+X^2+1
4	X^4+X+1, X^4+X^3+1, $X^4+X^3+X^2+X+1$

Proof. From Theorem 5.3, the irreducible factors of $X^{p^n} - X$ in $\mathbf{F}_p[X]$ are the irreducibles with degree dividing n. What remains is to show that each monic irreducible factor of $X^{p^n} - X$ appears only once in the factorization. Let $\pi(X)$ be an irreducible factor of $X^{p^n} - X$ in $\mathbf{F}_p[X]$. We want to show $\pi(X)^2$ does not divide $X^{p^n} - X$.

There is a field F in which $\pi(X)$ has a root, say α. We will work in $F[X]$. Since $\pi(X)|(X^{p^n} - X)$, $X^{p^n} - X = \pi(X)k(X)$, so $\alpha^{p^n} = \alpha$. Then in $F[X]$,

$$\begin{aligned} X^{p^n} - X &= X^{p^n} - X - 0 \\ &= X^{p^n} - X - (\alpha^{p^n} - \alpha) \\ &= (X-\alpha)^{p^n} - (X-\alpha) \quad \text{by Lemma 4.1a} \\ &= (X-\alpha)((X-\alpha)^{p^n-1} - 1). \end{aligned}$$

The second factor in this last expression does not vanish at α, so $(X-\alpha)^2$ does not divide $X^{p^n} - X$. Therefore $\pi(X)^2$ does not divide $X^{p^n} - X$ in $\mathbf{F}_p[X]$. $\square$

Let $\mathrm{N}_p(n)$ be the number of monic irreducibles of degree n in $\mathbf{F}_p[X]$. For instance, $\mathrm{N}_p(1) = p$. On the right side of (6.1), for each d dividing n there are $\mathrm{N}_p(d)$ different monic irreducible factors of degree d. Taking degrees of both sides of (6.1),

$$p^n = \sum_{d|n} d\mathrm{N}_p(d) \tag{6.2}$$

for all $n \geq 1$. Looking at this formula over all n lets us invert it to get a formula for $\mathrm{N}_p(n)$.

Example 6.3. $\mathrm{N}_p(2) = \dfrac{p^2-p}{2}$, $\quad \mathrm{N}_p(3) = \dfrac{p^3-p}{3}$, $\quad \mathrm{N}_p(12) = \dfrac{p^{12}-p^6-p^4+p^2}{12}$.

A general formula for $\mathrm{N}_p(n)$ can be written down from (6.1) using the Möbius inversion formula, which we omit.