Chapter 27
Irreducible Polynomials

We find a formula for the number of irreducible polynomials of degree n in $\mathbb{F}_p[x]$ for any p and n, and use it to show that in some sense, almost every polynomial in $\mathbb{Z}[x]$ is irreducible in $\mathbb{Q}[x]$.

A. Irreducible Polynomials in $\mathbb{F}_p[x]$

We begin by showing

Theorem 1. *$x^{p^n} - x$ is the product of all monic irreducible polynomials in $\mathbb{F}_p[x]$ of degree d, for all d dividing n.*

We prove this in two parts.

Theorem 2. *If $q(x)$ is an irreducible polynomial of degree d and d divides n, then $q(x)$ divides $x^{p^n} - x$.*

Proof. Let $F = \mathbb{F}_p[x]/(q(x)) = \mathbb{F}_p[\alpha]$, where $\alpha = [x]_{q(x)}$. Then $q(x)$ is the minimal polynomial over $\mathbb{F}_p$ of α. Now F is a field with p^d elements. So by Fermat's theorem, $\alpha^{p^d} = \alpha$. Since $de = n$ for some integer e,

$$\alpha^{p^n} = \alpha^{p^{de}} = \alpha,$$

so α is a root of $x^{p^n} - x$.

Now $q(x)$ is irreducible in $\mathbb{F}_p[x]$, so either $q(x)$ divides $x^{p^n} - x$ or (by Bezout's identity),

$$s(x)q(x) + t(x)(x^{p^n} - x) = 1$$

for some polynomials $s(x)$, $t(x)$ in $\mathbb{F}_p[x]$. But if the second condition held, then setting $x = \alpha$ would yield $0 = 1$, impossible. Hence $q(x)$ divides $x^{p^n} - x$, as claimed. □

L.N. Childs, *A Concrete Introduction to Higher Algebra*, Undergraduate Texts in Mathematics, © Springer Science+Business Media LLC 2009

Theorem 3. *If $q(x)$ is an irreducible factor of $x^{p^n} - x$ and has degree d, then d divides n.*

Proof. This proof uses the Isomorphism Theorem of Section 24A.

Let K be a splitting field over $\mathbb{F}_p$ of $x^{p^n} - x$, and let F be the subfield consisting of all of the p^n roots of $x^{p^n} - x$ described in Theorem 6 of Section 24C. Since $q(x)$ divides $x^{p^n} - x$, there is a root β of $q(x)$ in F. Since $q(x)$ is irreducible, $q(x)$ is the minimal polynomial of β over $\mathbb{F}_p$.

Let $\phi_\beta : \mathbb{F}_p[x] \to F$ be the "evaluation at β" homomorphism. Since $q(x)$ is the minimal polynomial of β, the homomorphism ϕ_β induces a 1-1 homomorphism $\overline{\phi}$ from $E = \mathbb{F}_p[x]/(q(x))$ to F by sending $[x]$ to β.

Let L be the image of E in F; L is then a subfield of F isomorphic to E.

Let α be a primitive element of F. Let $s(x)$ be the minimal polynomial of α over L. Then the evaluation homomorphism ϕ_α from $L[x]$ to F sending x to α induces a 1-1 homomorphism ϕ' from $L[x]/s(x)$ to F, which is onto because every non-zero element of F is a power of α. So ϕ' is an isomorphism from $L[x]/(s(x))$ onto F. So $L[x]/(s(x))$ and F have the same number of elements.

How many elements are in $L[x]/(s(x))$? If $s(x)$ has degree e, and L has q elements, then $L[x]/(s(x))$ has q^e elements. But $q = p^d$ and F has p^n elements. So $(p^d)^e = p^n$. So $de = n$, and d, the degree of $q(x)$, divides n. That completes the proof. □

Let $N_n(p)$ be the number of irreducible polynomials of degree n in $\mathbb{F}_p[x]$. We'll write N_n if the prime p is understood.

Using Theorem 1, we will find an explicit formula for $N_n(p)$.

To obtain such a formula, we use the Mobius function, a classical tool in number theory and combinatorics.

Definition. The Mobius function $\mu(n)$ is defined for $n \geq 1$ by

$$\mu(n) = \begin{cases} 1 \text{ if } n = 1, \\ 0 \text{ if } n \text{ is not squarefree} \\ (-1)^r \text{ if } n \text{ is the product of } r \text{ distinct primes.} \end{cases}$$

The formula we want is

$$N_n = \frac{1}{n} \sum_{d|n} \mu\left(\frac{n}{d}\right) p^d.$$

This formula is a special case of the Mobius inversion formula, which we now derive. We begin with two facts about the Mobius function.

Proposition 4. *If $(m,n) = 1$, then $\mu(mn) = \mu(m)\mu(n)$.*

This is easy to verify.

A function such as μ that satisfies Proposition 4 is called *multiplicative*. Another example of a multiplicative function is Euler's ϕ function.

Proposition 5. $\sum_{d|n} \mu(d) = 0$ *unless* $n = 1$.

The proof of this is an exercise in manipulating sums. Before doing the proof in general we illustrate with $n = 36 = 2^2 3^2$: then the divisors of n are 1, 2, 4, 3, 6, 12, 9, 18 and 36, and we have

$$\begin{aligned}\sum_{d|36} \mu(d) &= [\mu(1)+\mu(2)+\mu(2^2)] \\ &\quad +[\mu(3)+\mu(2\cdot 3)+\mu(2^2\cdot 3)] \\ &\quad +[\mu(3^2)+\mu(2\cdot 3^2)+\mu(2^2\cdot 3^2)] \\ &= \mu(1)[1+\mu(2)+\mu(2^2)] \\ &\quad +\mu(3)[1+\mu(2)+\mu(2^2)] \\ &\quad +\mu(3^2)[1+\mu(2)+\mu(2^2)].\end{aligned}$$

Now $\mu(d) = 0$ if d is divisible by the square of a prime, and $\mu(1) = 1$, so this sum reduces to

$$\begin{aligned}&= \mu(1)[\mu(1)+\mu(2)]+\mu(3)[\mu(1)+\mu(2)] \\ &= [\mu(1)+\mu(3)][\mu(1)+\mu(2)].\end{aligned}$$

Now $\mu(1) = 1$, $\mu(3) = -1$, so $\mu(1)+\mu(3) = 0$. Hence $\sum_{d|36} \mu(d) = 0$.
The proof in general works in a similar way.

Proof. Write $n = p^e q$ with $(p,q) = 1$. Then

$$\begin{aligned}\sum_{d|n} \mu(d) &= \sum_{r=0}^{e} \sum_{b|q} \mu(p^r b) \\ &= \sum_{r=0}^{e} \sum_{b|q} \mu(p^r)\mu(b).\end{aligned}$$

Since $\mu(p^r) = 0$ for $r \geq 2$, this reduces to

$$\begin{aligned}&= \sum_{b|q} \mu(1)\mu(b) + \sum_{b|q} \mu(p)\mu(b) \\ &= \mu(1)\sum_{b|q} \mu(b) + \mu(p)\sum_{b|q} \mu(b) \\ &= [\mu(1)+\mu(p)]\sum_{b|q} \mu(b) = 0\end{aligned}$$

since $\mu(1)+\mu(p) = 0$. □

With Proposition 5 we can prove the useful

Proposition 6 (Mobius Inversion Formula). *Let f be a function defined on the natural numbers. If we set*

$$F(n) = \sum_{d|n} f(d) \text{ for every } n \geq 1,$$

then

$$f(n) = \sum_{d|n} \mu(\frac{n}{d}) F(d) = \sum_{e|n} \mu(e) F(\frac{n}{e}).$$

Proof. If we substitute $e = n/d, d = n/e$, then as d runs through all divisors of n, so does e. Hence the last two sums are equal.

Now by definition of F,

$$\sum_{e|n} \mu(e) F(\frac{n}{e}) = \sum_{e|n} \mu(e) (\sum_{d|(n/e)} f(d)) = \sum_{e|n} \sum_{d|(n/e)} (\mu(e) f(d).$$

Interchanging the order of summation (if $d|(n/e)$, then $de|n$ so $e|(n/d)$), we get

$$\sum_{e|n} \mu(e) F(\frac{n}{e}) = \sum_{d|n} \left(\sum_{e|(n/d)} \mu(e) \right) f(d). \tag{27.1}$$

Now by Proposition 5, for each $m > 1$,

$$\sum_{e|m} \mu(e) = 0.$$

So the coefficient of $f(d)$ is 0 unless $n/d = 1$, that is, $d = n$. Hence the sum (1) reduces to the single term $f(n)$, as was to be shown. □

With these generalities out of the way, we can get the desired formula for N_n^p. We shall write N_n^p as N_n if p is understood.

Theorem 7. *Let N_n be the number of irreducible polynomials of degree n in $\mathbb{F}_p[x]$. Then*

$$N_n = \frac{1}{n} \sum_{d|n} \mu\left(\frac{n}{d}\right) p^d.$$

Proof. Theorem 1 describes the complete factorization of $x^{p^n} - x$ in $\mathbb{F}_p$ for any n. Since $x^{p^n} - x$ is the product of all the N_d irreducible polynomials of degree d for all d dividing n, we obtain the formula

$$p^n = \sum_{d|n} dN_d$$

by summing the degrees of all the irreducible factors of $x^{p^n} - x$. Now apply the Mobius inversion formula with $F(n) = p^n$, $f(d) = dN_d$. We get

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

Dividing both sides by n yields the desired formula. □

With that formula we can give another proof of Corollary 7 of Chapter 24, that for every prime p and every $n > 0$ there is an irreducible polynomial in $\mathbb{F}_p[x]$ of degree n.

Proposition 8. *For every prime p and every $n > 0$, $N_n > 0$.*

Proof. Since $\mu(n/n) = 1$ and $\mu(n/d) \geq -1$ for all $d|n$, $d < n$, we have that

$$\begin{aligned} N_n &= \frac{1}{n}p^n + \frac{1}{n}\sum_{d|n,d<n}\mu(\frac{n}{d})p^d \\ &\geq \frac{1}{n}p^n - \frac{1}{n}\sum_{d|n,d<n}p^d \\ &\geq \frac{1}{n}\left(p^n - \sum_{d=0}^{n-1}p^d\right) \end{aligned}$$

Now

$$\sum_{d=0}^{n-1}p^d = \frac{p^n - 1}{p-1} < p^n,$$

so

$$\frac{1}{n}\left(p^n - \sum_{d=0}^{n-1}p^d\right) > 0.$$

Hence $N_n > 0$. □

The number $N_n(p)$ of irreducible monic polynomials over $\mathbb{F}_p$ of degree n for $n = 1, \ldots, 10$ is given by the following formulas

n	$N_n(p)$	$N_n(2)$	$N_n(3)$	$N_n(5)$	$N_n(7)$
1	p	2	3	5	7
2	$(p^2-p)/2$	1	3	10	21
3	$(p^3-p)/3$	2	8	40	112
4	$(p^4-p^2)/4$	3	18	150	588
5	$(p^5-p)/5$	6	48	624	3360
6	$(p^6-p^2-p^3+p)/6$	9	116	2580	19544
7	$(p^7-p)/7$	18	312	11160	117648
8	$(p^8-p^4)/8$	30	810	48750	720300
9	$(p^9-p^3)/9$	56	2184	217000	4483696
10	$(p^{10}-p^5-p^2+p)/10$	99	5880	976248	28245840

Every irreducible polynomial in $\mathbb{F}_7[x]$ of degree n gives rise to infinitely many different irreducible polynomials of degree n in $\mathbb{Q}[x]$. So there are many irreducible polynomials in $\mathbb{Q}[x]$. We'll get an idea of how many in the next section.

For more discussion on Mobius inversion, see Bender and Goldman (1975).

Exercises.

1. If F is a function defined on natural numbers and f is defined by

$$f(n) = \sum_{d|n} \mu(d) F(n/d),$$

prove that

$$F(n) = \sum_{d|n} f(d).$$

2. If f is a multiplicative function defined on natural numbers and $F(n) = \sum_{d|n} f(d)$, prove that F is multiplicative.

3. Prove Proposition 4.

4. What are the 8 monic irreducible polynomials of degree 3 in $\mathbb{F}_3[x]$?

5. Find the formula for $N_{12}(p)$. Find $N_{12}(2)$.

6. Find the formula for $N_{30}(p)$.

7. If n is divisible by g distinct primes, how many different powers of p appear in the formula for $N_n(p)$?

8. Show that

$$\left(\frac{p^n}{n}\right)(1-\varepsilon) < N_n < \frac{p^n}{n}$$

for some quantity $\varepsilon = \varepsilon(n)$ where $\varepsilon \to 0$ as $n \to \infty$. Conclude that for n large, approximately one of every n monic polynomials in $\mathbb{F}_p[x]$ of degree n is irreducible. (Asking about the size of N_n for n large is the analogue in $\mathbb{F}_p[x]$ of the Prime Number Theorem discussed in Section 4C.)

9. If d divides n, prove that every irreducible polynomial of degree d in $\mathbb{F}_p[x]$ has a root in every field F with p^n elements.

10. Show that if $q(x)$ in $\mathbb{F}_p[x]$ is irreducible and has degree d, and F is a field with p^n elements, where $d|n$, then F is a splitting field of $q(x)$.

11. Factor $x^{16} - x$ in $\mathbb{F}_2[x]$.

12. Factor $x^9 - x$ in $\mathbb{F}_3[x]$.

13. Factor $x^{25} - x$ in $\mathbb{F}_5[x]$.

14. Show that if p, q are primes, then $x^{p^q} - x = (x^p - x)h(x)$ in $\mathbb{F}_p[x]$, where $h(x)$ is the product of all monic irreducible polynomials in $\mathbb{F}_p[x]$ of degree q.

15. Show that $\mathbb{F}_{16}$ is a splitting field for $x^4 - x$ in $\mathbb{F}_2[x]$. If $\mathbb{F}_{16} = \mathbb{F}_2[\alpha]$ where $\alpha^4 + \alpha + 1 = 0$ (as in Table 2 of Chapter 25A), what are the roots in $\mathbb{F}_{16}$ of $x^4 - x$?

16. Prove Rabin's irreducibility test [Rabin (1980b)] for polynomials $m(x)$ of degree n in $\mathbb{F}_p[x]$: $m(x)$ is irreducible if

(i) $m(x)$ divides $x^{p^n} - x$; and

(ii) for any prime divisor d of n, the greatest common divisor of $m(x)$ and $x^{p^{n/d}} - x$ is 1.

17. Suppose $m(x)$ in $\mathbb{F}_p[x]$ has degree d. Call $m(x)$ *Carmichael* if $m(x)$ is composite, and for every polynomial $a(x)$ in $\mathbb{F}_p[x]$, coprime to $m(x)$,

$$a(x)^{p^d} = a(x) \pmod{m(x)}.$$

(i) Show that if $m(x)$ is irreducible, then for every $a(x)$ coprime to $m(x)$,

$$a(x)^{p^d} = a(x) \pmod{m(x)}.$$

(ii) Prove that the following are equivalent:

(a) $m(x)$ is Carmichael;

(b) $m(x)$ divides $x^{p^d} - x$;

(c) $m(x) = q_1(x) \cdots q_g(x)$, a product of distinct irreducible polynomials, where for each i, if d_i is the degree of $q_i(x)$, then $p^{d_i} - 1$ divides $p^d - 1$;

(d) $m(x) = q_1(x) \cdots q_g(x)$, a product of distinct irreducible polynomials, where for each i, if d_i is the degree of $q_i(x)$, then d_i divides d.

B. Most Polynomials in $\mathbb{Z}[x]$ are Irreducible

In the last section, we computed the number $N_n(p)$ of monic irreducible polynomials of degree n in $\mathbb{Z}_p[x]$ for any n and p. We showed that

$$N_n(p) = \frac{1}{n} \sum_{d|n} \mu\left(\frac{n}{d}\right) p^d,$$

where $\mu(e)$ is the Mobius function. Thus we have

Lemma 9.

$$N_n(p) > \frac{p^n}{2n}.$$

Proof. Since $\mu(n/d)$ is either 1, -1 or 0, and $\mu(1) = 1$, the formula

$$N_n(p) = \frac{1}{n} \sum_{d|n} \mu\left(\frac{n}{d}\right) p^d,$$

yields

$$nN_n(p) = p^n - \sum_{d|n, d<n} p^d.$$

Since every proper divisor of n is $<n/2$, we have

$$\sum_{d|n,d<n} p^d \leq \sum_{d\leq n/2} p^d < p^{\lfloor n/2\rfloor+1}$$

where $\lfloor a\rfloor$ denotes the greatest integer $<a$. Hence

$$nN_n(p) > (p^n - p^{\lfloor n/2\rfloor+1}).$$

If $n > 2$, then $\lfloor n/2\rfloor + 1 \leq n-1$, so

$$N_n(p) > \frac{1}{n}(p^n - p^{n-1}) = \frac{p^n}{n}\left(1-\frac{1}{p}\right) \geq \frac{p^n}{n}\left(\frac{1}{2}\right).$$

For $n = 2$,

$$N_2(p) = \frac{1}{2}(p^2 - p) = \frac{p^2}{2}\left(1-\frac{1}{p}\right) \geq \frac{p^2}{2}\left(\frac{1}{2}\right).$$

□

Using this lower bound for N_n^p we will show that almost all monic polynomials in $\mathbb{Z}[x]$ of degree $n \geq 1$ are irreducible. The main idea of the argument is that if $f(x)$ is a monic polynomial in $\mathbb{Z}[x]$ whose image in $\mathbb{F}_p[x]$ is irreducible for some prime p, then $f(x)$ is irreducible in $\mathbb{Z}[x]$.

What do we mean by "almost all"?

The way we will interpret this is as follows.

Pick a bound M. Consider the set $P_n(M)$ of all monic polynomials $f(x)$ in $\mathbb{Z}[x]$,

$$f(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_2x^2 + a_1x + a_0,$$

so that each coefficient a_k satisfies $-M < a_k \leq M$. This is a finite set of polynomials: the number of such polynomials is $(2M)^n$, since there are $2M$ possibilities for each of the n coefficients $a_{n-1},\ldots,a_0$.

We will find a lower bound on the number of irreducible polynomials in the set $P_n(M)$, and show that for a suitable increasing sequence of numbers M, the proportion of irreducible polynomials goes to 1. More precisely,

Theorem 10. *For every $n \geq 2$ and every $g \geq 1$ let M_g be the product of the first g odd primes. Let*

$$I_n(M_g) = \{f(x) \text{ in } P_n(M_g) | f(x) \text{ is irreducible}\}.$$

Then

$$\lim_{g\to\infty} \frac{|I_n(M_g)|}{|P_n(M_g)|} = 1.$$

Proof. For every $M \geq 2$, if

$$f(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_2x^2 + a_1x + a_0,$$

is in $P_n(M)$, then each coefficient a_k satisfies $-M < a_k \leq M$ for $0 \leq k \leq n-1$. Since the integers a with $-M < a \leq M$ is a complete set of representatives for $\mathbb{Z}/(2M)\mathbb{Z}$, we have a one-to-one correspondence between $P_n(M)$ and monic polynomials of degree n with coefficients in the ring $\mathbb{Z}/(2M)\mathbb{Z}$.

Now assume $M = M_g = 3 \cdot 5 \cdots p_g$ is the product of the first g odd primes.

By the Chinese remainder theorem, there is an isomorphism

$$\mathbb{Z}/(2M)\mathbb{Z}) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \cdots \times \mathbb{Z}/p_g\mathbb{Z}$$

given by mapping $[a]_{2M}$ to the $(g+1)$-tuple $([a]_2, [a]_3, \ldots, [a]_{p_g})$. This map induces a one-to-one correspondence between polynomials in $P_n(M)$ and $(g+1)$-tuples $([f(x)]_2, [f(x)]_3, \ldots, [f(x)]_{p^g})$ of monic polynomials of degree n in

$$\mathbb{Z}/2\mathbb{Z}[x] \times \mathbb{Z}/3\mathbb{Z}[x] \times \cdots \times \mathbb{Z}/p_g\mathbb{Z}[x].$$

Here if $f(x)$ is in $P_n(M)$, then $[f(x)]_p$ denotes the image of $f(x)$ in $\mathbb{Z}/p\mathbb{Z}[x]$ obtained by replacing the coefficients of $f(x)$ by their congruence classes modulo p.

Under this correspondence between $P_n(M)$ and

$$\mathbb{Z}/2\mathbb{Z}[x] \times \mathbb{Z}/3\mathbb{Z}[x] \times \cdots \times \mathbb{Z}/p_g\mathbb{Z}[x].$$

a polynomial $f(x)$ is irreducible in $\mathbb{Z}[x]$ if for some prime p among $2, 3, \ldots, p_g$, the image $[f(x)]_p$ of $f(x)$ in $\mathbb{Z}/p\mathbb{Z}[x]$ is irreducible.

Thus $|I_n(M)| \geq$ the number of $(g+1)$-tuples of monic polynomials of degree n, $(h_0(x), h_1(x), \ldots, h_g(x))$, with $h_0(x)$ in $\mathbb{Z}/2\mathbb{Z}[x]$, $h_1(x)$ in $\mathbb{Z}/3\mathbb{Z}[x]$, ..., $h_g(x)$ in $\mathbb{Z}/p_g\mathbb{Z}[x]$, such that at least one of $h_0(x), \ldots, h_g(x)$ is irreducible.

How many $(g+1)$-tuples of polynomials

$$(h_0(x), h_1(x), \ldots, h_g(x)) \text{ in } \mathbb{Z}/2\mathbb{Z}[x] \times \mathbb{Z}/3\mathbb{Z}[x] \times \cdots \times \mathbb{Z}/p_g\mathbb{Z}[x]$$

have the property that none of them is irreducible?

By Lemma 9 above, the number N_n of monic irreducible polynomials of degree n in $\mathbb{Z}/p\mathbb{Z}[x]$ satisfies $N_n^p > p^n/2n$. Thus the number of monic polynomials of degree n in $\mathbb{Z}/p\mathbb{Z}[x]$ that are not irreducible is less than

$$p^n - \frac{p^n}{2n} = p^n\left(1 - \frac{1}{2n}\right).$$

Hence the number of $(g+1)$-tuples of monic degree n polynomials in $\mathbb{Z}/2\mathbb{Z}[x] \times \mathbb{Z}/3\mathbb{Z}[x] \times \cdots \times \mathbb{Z}/p_g\mathbb{Z}[x]$ such that none of the $(g+1)$-polynomials is irreducible, is at most

$$2^n\left(1 - \frac{1}{2n}\right)3^n\left(1 - \frac{1}{2n}\right)\cdots p_g^n\left(1 - \frac{1}{2n}\right)$$
$$= (2M)^n\left(1 - \frac{1}{2n}\right)^{g+1}.$$

Thus the number of $(g+1)$-tuples of monic degree n polynomials such that at least one of the $g+1$ polynomials is irreducible is at least

$$(2M)^n - (2M)^n\left(1-\frac{1}{2n}\right)^{g+1} = (2M)^n\left(1-\left(1-\frac{1}{2n}\right)^{g+1}\right).$$

But then, since $|P_n(M)| = (2M)^n$, we have

$$\frac{|I_n(M)|}{|P_n(M)|} \geq 1-\left(1-\frac{1}{2n}\right)^{g+1}.$$

Letting the number g of primes $p_1, p_2, \ldots, p_g$ increase (recall that $M = M_g = p_1 p_2 \cdot \ldots \cdot p_g$), we have

$$\begin{aligned} 1 &\geq \lim_{g\to\infty} \frac{|I_n(M)|}{|P_n(M)|} \\ &\geq 1 - \lim_{g\to\infty}\left(1-\frac{1}{2n}\right)^{g+1}. \end{aligned}$$

Since the degree n is fixed while g (hence M) goes off to infinity,

$$\lim_{g\to\infty}\left(1-\frac{1}{2n}\right)^{g+1} = 0.$$

Hence

$$\lim_{g\to\infty} 1-\left(1-\frac{1}{2n}\right)^{g+1} = 1.$$

and so

$$\lim_{g\to\infty} \frac{|I_n(M)|}{|P_n(M)|} = 1,$$

as we wished to show. □

As a numerical example, if we consider monic polynomials of degree 5 and let M be the product of the first 30 odd primes, then among the $(2M)^5$ such polynomials with coefficients a_k satisfying $-M < a_k \leq M$, at least 95.7% of them are irreducible. Here M is slightly larger than 3×10^{52}.

We noted in Section 16C that there are monic irreducible polynomials in $\mathbb{Z}[x]$ that factor modulo every prime. Thus

$$\frac{|I_n(M)|}{|P_n(M)|}$$

is closer to 1 than the estimate of Theorem 2 indicates.

Theorem 2 is a special case of a theorem of Van der Waerden (1934).

Exercises.

18. Let $M = 3 \cdot 5 = 15$ and $n = 2$. Let $\mathscr{S}$ be the set consisting of the $900 = 30^2$ monic polynomials $x^2 + bx + c$ in $\mathbb{Z}[x]$ with coefficients satisfying $-14 \leq b, c \leq 15$. How many polynomials in $\mathscr{S}$ are irreducible? (A polynomial of degree 2 is irreducible if and only if it has no roots, so count the number of polynomials in $\mathscr{S}$ that have a root in $\mathbb{Z}$.)

19. Same question with $n = 3$.