CHAPTER 6

DENSITY RESULTS

A weaker man might be moved to re-examine his faith,
if in nothing else at least in the law of probability.

– Guildenstern
Rosencrantz and Guildenstern are Dead
by Tom Stoppard

"Let's count our pebbles," said Pooh.
Piglet emptied the sock. He counted very slowly.
Then he said, "One."
Pooh Bear was puzzled. "Are you sure?" he asked.
"Please count them again, Piglet. More slowly this time."
Piglet took a deep breath and counted as slowly as he could.
"One pebble," he said at last. "I counted very slowly."

– Walt Disney's
Winnie-the-Pooh and the Pebble Hunt

6.1. With all the irreducibility criteria at our disposal, we might be surprised to find that there even exists one reducible polynomial. Although such a statement should not be taken seriously, the reader might want to consider some random sequences of polynomials in $\mathbb{Z}[x]$ and test the irreducibility of the polynomials. For example, it is commonly accepted that no particular pattern exists among the digits of π (though the author has on occasion told his students that he knows all the digits of π ... all 10 of them). Consider

$$P_n(x) = 3 + x + 4x^2 + \cdots,$$

where, for $j \in \{0, \ldots, n\}$, the coefficient of x^j is the $(j+1)$th digit of π. What would be a good estimate for the number of irreducible (or reducible) $P_n(x)$ with $n \leq t$? We may or may not be able to answer such a question in the near future. A quick computational check indicates that $P_n(x)$ is irreducible for $0 \leq n \leq 150$. There is no result in the literature to justify that $P_n(x)$ is usually irreducible or, more generally, that most polynomials with a non-zero constant term and a fixed bound on their coefficients are irreducible. For example, an open problem (due to Odlyzko and Poonen) is to determine whether

$$\lim_{n\to\infty} \frac{|\{f(x) = \sum_{j=0}^{n} \epsilon_j x^j : \epsilon_0 = 1, \epsilon_j \in \{0,1\} \text{ for } j = 1, \ldots, n, \text{ and } f(x) \text{ irreducible}\}|}{2^n} = 1.$$

Simply showing that the limit on the left-hand side above exists or showing that the limit supremum is positive seems to be difficult.

We can, however, obtain some density results if we fix a bound on the degree n of the polynomials we wish to consider and examine what happens as the absolute value of their coefficients are allowed to get large. For the purposes of this chapter, then, we define

$$S_n(B) = \left\{ f(x) = \sum_{j=0}^{n} a_j x^j \in \mathbb{Z}[x] : |a_j| \leq B \text{ for } j = 0, 1, \ldots, n \right\}.$$

Thus, $S_n(B)$ is the set of all polynomials in $\mathbb{Z}[x]$ of degree $\leq n$ with coefficients in the interval $[-B, B]$. Note that the total number of polynomials $f(x) \in S_n(B)$ is $(2[B] + 1)^{n+1} \sim (2B)^{n+1}$ as $B \to \infty$. We say that the proportion of polynomials in $\mathbb{Z}[x]$ of degree n satisfying a given property $\mathcal{P}$ is c if

$$\lim_{B\to\infty} \frac{|\{f(x) \in S_n(B) : f(x) \text{ satisfies } \mathcal{P}\}|}{(2B)^{n+1}} = c$$

where c is a constant possibly depending on n. If c does not depend on n and if for every sufficiently large positive integer n, the proportion of the polynomials in $\mathbb{Z}[x]$ of degree n

satisfying $\mathcal{P}$ is c, then we say that the proportion of the polynomials in $\mathbb{Z}[x]$ satisfying $\mathcal{P}$ is c. We will use the terminology "almost all" in the case that $c = 1$. Thus, almost all polynomials satisfy property $\mathcal{P}$ if for all sufficiently large n,

$$\lim_{B\to\infty} \frac{|\{f(x) \in S_n(B) : f(x) \text{ satisfies } \mathcal{P}\}|}{(2B)^{n+1}} = 1.$$

We say that a positive proportion of the polynomials in $\mathbb{Z}[x]$ of degree n have a given property $\mathcal{P}$ (and the proportion is at least c) if

$$\liminf_{B\to\infty} \frac{|\{f(x) \in S_n(B) : f(x) \text{ satisfies } \mathcal{P}\}|}{(2B)^{n+1}} > c$$

for some constant $c > 0$ (possibly depending on n). If for every sufficiently large positive integer n, the proportion of the polynomials in $\mathbb{Z}[x]$ of degree n satisfying $\mathcal{P}$ is at least $c > 0$ where c is independent of n, then we say that a positive proportion of the polynomials in $\mathbb{Z}[x]$ satisfy $\mathcal{P}$.

We are now ready to establish

Theorem 20. *Almost all polynomials in $\mathbb{Z}[x]$ are irreducible over the rationals.*

Proof. Fix a positive integer n. We will show that there are $\ll_n B^n \log^2 B$ reducible $f(x) \in S_n(B)$ over the rationals from which the theorem will follow. Observe that there are $2[B] + 1 \ll B$ constant polynomials in $S_n(B)$, which by definition are not irreducible; we need not concern ourselves with these as $B \ll_n B^n \log^2 B$. Each non-zero polynomial $f(x) \in S_n(B)$ can have at most n roots so that there are at least $n+1$ integers a (depending on $f(x)$) with absolute value $\leq n$ such that $f(a) \neq 0$. Let U be the set of $n+1$ element subsets of $\{-n, -n+1, \dots, n-1, n\}$. Thus, $|U| = \binom{2n+1}{n+1}$. For each $T \in U$, let $V(T)$ be the set of $f(x) \in S_n(B)$ such that $f(a) \neq 0$ for every $a \in T$. Hence, every non-zero $f(x) \in S_n(B)$ belongs to $V(T)$ for at least one $T \in U$. Fix $T = \{a_0, a_1, \dots, a_n\} \in U$. We will find an upper bound for the number of $f(x)$ in $V(T)$ which are reducible over the rationals. Let $f(x) \in V(T)$, and suppose that $f(x)$ is reducible over the rationals. Then there are polynomials $g(x)$ and $h(x)$ in $\mathbb{Z}[x]$ such that

$$f(x) = g(x)h(x) \quad \text{and} \quad 1 \leq \deg g(x) \leq \deg h(x) \leq n-1.$$

For every $a \in T$, we get that

$$|g(a)||h(a)| = |f(a)| \leq c_n B \quad \text{where} \quad c_n = n^n + n^{n-1} + \cdots + n + 1. \tag{6.1}$$

Furthermore, $|g(a)||h(a)| \neq 0$. Observe that (6.1) is true for any $f(x) \in V(T)$ and $g(x)$ and $h(x) \in \mathbb{Z}[x]$ with $f(x) = g(x)h(x)$. We get from (6.1) that for each $j \in \{0, \ldots, n\}$, the total number of values for the pair $(g(a_j), h(a_j))$ is bounded by

$$\begin{aligned} 4 \sum_{k \leq c_n B} \sum_{d|k} 1 = 4 \sum_{d \leq c_n B} \sum_{\substack{k \leq c_n B \\ d|k}} 1 &\leq 4 \sum_{d \leq c_n B} \frac{c_n B}{d} \\ &\leq 4 c_n B \left(1 + \int_1^{c_n B} \frac{1}{t}\, dt \right) \ll_n B \log B, \end{aligned}$$

where the 4 appears above since each of $g(a_j)$ and $h(a_j)$ may be either positive or negative. Fix integers r and s with $1 \leq r \leq s \leq n - r$, and consider now those $f(x) \in V(T)$ which factor as a product of a polynomial $g(x)$ of degree r and a polynomial $h(x)$ of degree s. Thus, as $f(x)$ runs through those elements in $V(T)$, there are $\ll_n (B \log B)^{r+1}$ values for $(g(a_0), h(a_0)), (g(a_1), h(a_1)), \ldots, (g(a_r), h(a_r))$. Since $g(x)$ is completely determined by the values of $g(a_0), \ldots, g(a_r)$ and since once $g(x)$ is determined (6.1) implies that each of $h(a_{r+1}), \ldots, h(a_s)$ can have at most $\leq 2c_n B$ different values, we get that there are

$$\ll_n (B \log B)^{r+1} B^{s-r} \ll_n B^{s+1} \log^{r+1} B$$

different possibilities for the pair $(g(x), h(x))$. Therefore, there are $\ll_n B^{s+1} \log^{r+1} B$ polynomials $f(x) \in V(T)$ that factor as a product of a polynomial of degree r times a polynomial of degree s. Observe that this bound is maximized when $r = 1$ and $s = n - 1$ (given that $1 \leq r \leq s \leq n - r$). Since there are $\binom{2n+1}{n+1}$ choices for $T \in U$ and $\leq n^2$ choices for r and s, we get that there are $\ll_n B^n \log^2 B$ polynomials $f(x) \in S_n(B)$ which are reducible over the rationals. The theorem easily follows. ■

Observe that we have actually proven a result stronger than Theorem 20. We have shown that if n is a positive integer, then the number of reducible $f(x) \in S_n(B)$ is $\ll_n B^n \log^2 B$.

It also follows as a consequence of the above proof that the number of $f(x) \in S_n(B)$ which can be written as a product of a polynomial of degree r times a polynomial of degree s with $s \geq r$ is $\ll_n B^{s+1} \log^{r+1} B$.

6.2. Another related theorem is due to Van der Waerden [1]. Van der Waerden's Theorem is the earliest known density theorem in this chapter. We state it as follows:

Theorem 21. *Almost all polynomials in $\mathbb{Z}[x]$ are irreducible modulo some prime.*

Before proving Theorem 21, we make some further remarks. First, it should be noted that Van der Waerden actually established a stronger version of this theorem. He showed that almost all polynomials $f(x) \in \mathbb{Z}[x]$ have their associated Galois group equal to the symmetric group on $\deg f(x)$ letters. He stated his result (in German) by referring to "100 %" of the polynomials rather than "almost all" of the polynomials. This result is mentioned in Van der Waeden's classical *Algebra* [2] (however, not in the earliest editions). The translations of Van der Waerden's *Algebra* into English (cf. [3]) have improperly stated the result as being that all polynomials $f(x) \in \mathbb{Z}[x]$ have their associated Galois group equal to the symmetric group on $\deg f(x)$ letters. The latter would imply that every polynomial in $\mathbb{Z}[x]$ is irreducible over the rationals. (Now is a good time to reread the first sentence of this chapter.)

Observe that Theorem 21 neither implies nor is implied by Theorem 20 (at least not directly); see Problems (1.6) and (4.1). On the other hand, it can be shown that if $f(x)$ is irreducible over $\mathbb{Q}$ and $f(x)$ is of prime degree, then $f(x)$ is irreducible modulo infinitely many primes; thus, Theorem 20 implies Theorem 21 when one considers polynomials of prime degree. In general, from Problem (1.6), we see that Theorem 20 would follow from the assertion that almost all polynomials $f(x)$ in $\mathbb{Z}[x]$ are irreducible modulo some prime not dividing the leading coefficient of $f(x)$. This assertion can in fact be obtained by modifying our argument for Theorem 21.

To prove Theorem 21, we recall Lemma 1 to Theorem 18. Let n be a positive integer.

Define, as in that theorem, $M_n = M_n(p)$ as the number of incongruent monic irreducible polynomials modulo p of degree n and $I_n = I_n(p)$ as the number of incongruent irreducible polynomials of degree n modulo p. Then

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

In the sum above, $M_k \leq p^k$ and if $k \neq n$, then $k \leq n/2$. Thus, we easily get that each term in the sum other than nM_n is $\leq np^{n/2}$. In particular,

$$\sum_{\substack{1 \leq k < n \\ k|n}} kM_k \leq \sum_{\substack{1 \leq k < n \\ k|n}} np^{n/2} \leq n^2 p^{n/2}.$$

Hence, we get that

$$M_n = \frac{1}{n}\Bigg(p^n - \sum_{\substack{1 \leq k < n \\ k|n}} kM_k\Bigg) = \frac{p^n}{n} + O(np^{n/2}).$$

Observe that we could have used Theorem 18 directly to obtain the above formula. Since $I_n = (p-1)M_n$, we deduce

$$I_n(p) = \frac{p^n(p-1)}{n} + O(np^{(n+2)/2}). \tag{6.2}$$

Define

$$I'_n(B,p) = |\{f(x) \in S_n(B) : f(x) \text{ is irreducible mod } p\}|.$$

Next, we obtain an upper bound for $I'_n(B,p)$ as follows. We divide the integers in the interval $[-B,B]$ into $\ell = [(2[B]+1)/p] + 1$ disjoint sets (where the last expression involves two uses of the greatest integer function [ ]) with the first $[(2[B]+1)/p]$ sets, say $S_1, \ldots, S_{\ell-1}$, each consisting of p consecutive integers and with the final set, say S_ℓ, consisting of the remaining unspecified number of consecutive integers. In particular, S_ℓ has ≥ 0 elements and $\leq p-1$ elements. There are $\leq (n+1)(p-1)(2[B]+1)^n \ll_n pB^n$ polynomials $f(x) \in S_n(B)$ which have a coefficient in S_ℓ. We consider now the polynomials $f(x) \in S_n(B)$ which have all their coefficients in $S_1 \cup S_2 \cup \cdots \cup S_{\ell-1}$. Fix

$f_0(x) = \sum_{j=0}^{n} a'_j x^j \in \mathbb{Z}[x]$. We count the number of $f(x) = \sum_{j=0}^{n} a_j x^j \in S_n(B)$ with coefficients in $S_1 \cup S_2 \cup \cdots \cup S_{\ell-1}$ and with $f(x) \equiv f_0(x) \pmod{p}$. For each fixed $j \in \{0, \ldots, n\}$ and for each fixed set S_i of p consecutive integers, there is a unique value of $a_j \in S_i$ such that $a_j \equiv a'_j \pmod{p}$. Thus, for each $j \in \{0, \ldots, n\}$, there are $[(2[B]+1)/p]$ values of $a_j \equiv a'_j \pmod{p}$ among the $\ell - 1$ sets $S_1, \ldots, S_{\ell-1}$ (one value for each set). Hence, we get that there are $(\ell-1)^{n+1} = [(2[B]+1)/p]^{n+1}$ polynomials $f(x)$ as above with $f(x) \equiv f_0(x) \pmod{p}$. If $f(x) \in S_n(B)$ is irreducible modulo p, then $f(x)$ has degree $\leq n$ and is congruent to one of the $\sum_{k \leq n} I_k(p)$ different irreducible polynomials modulo p of degree $\leq n$. Recalling our bound on the number of polynomials in $S_n(B)$ which have a coefficient in S_ℓ, we get that

$$I'_n(B, p) = [(2[B]+1)/p]^{n+1} \sum_{k \leq n} I_k(p) \ + \ O_n\left(pB^n\right).$$

We set

$$c_n(p) = \frac{\sum_{k \leq n} I_k(p)}{p^{n+1}}.$$

Using the trivial bound of $I_k(p) \leq p^{n+1}$ for $k \leq n$, we easily get that

$$I'_n(B, p) = c_n(p)(2B)^{n+1} + O_n\left(p^{n+1}B^n\right). \tag{6.3}$$

There is a generalization of (6.3) that we will want. Let $P = \{p_1, \ldots, p_r\}$ be a set of r primes, and define $I_n(P)$ as the number of incongruent polynomials modulo $p_1 \cdots p_r$ of degree $\leq n$ which are irreducible when considered modulo p for every $p \in P$. Observe that this definition differs from our use of $I_n(p)$ in that the latter only concerns itself with polynomials of degree equal to n. In particular, if p is a prime and $P = \{p\}$, then

$$I_n(P) = I_n(\{p\}) = \sum_{k \leq n} I_k(p).$$

We let

$$I'_n(B, P) = |\{f(x) \in S_n(B) : f(x) \text{ is irreducible mod } p \text{ for every } p \in P\}|.$$

We will make use of the following version of the Chinese Remainder Theorem.

Lemma. *Let $f_1(x), \ldots, f_r(x)$ be polynomials with integer coefficients, and let $p_1, \ldots, p_r$ be r distinct primes. Then there exists a unique polynomial $w(x)$ modulo $p_1 \cdots p_r$ such that*

$$w(x) \equiv f_j(x) \pmod{p_j} \quad \text{for every } j \in \{1, \ldots, r\}. \tag{6.4}$$

Proof. For each $j \in \{1, \ldots, r\}$, let $N_j = \left(\prod_{i=1}^{r} p_i\right)/p_j$ and let N_j' be an integer satisfying $N_j N_j' \equiv 1 \pmod{p_j}$. Consider

$$w(x) = \sum_{j=1}^{r} f_j(x) N_j N_j'.$$

Then it is easily verified that (6.4) holds, and therefore the existence of $w(x)$ as in the lemma is established. If $u(x) \in \mathbb{Z}[x]$ and $u(x) \equiv f_j(x) \pmod{p_j}$ for every $j \in \{1, \ldots, r\}$, then each p_j divides the coefficients of $w(x) - u(x)$ (since $w(x) \equiv f_j(x) \equiv u(x) \pmod{p_j}$) and, hence, $w(x) \equiv u(x) \pmod{p_1 \cdots p_r}$. This proves the uniqueness of $w(x)$ modulo $p_1 \cdots p_r$ and completes the proof. ■

Corollary. $I_n(P) = \prod_{j=1}^{r} \left(\sum_{k \leq n} I_k(p_j)\right)$.

Proof. The lemma implies that there is a one-to-one correspondence between the $r-$tuples $(f_1(x), \ldots, f_r(x))$ where $f_j(x)$ is an irreducible polynomial of degree $\leq n$ modulo p_j for each $j \in \{1, \ldots, r\}$ and the polynomials $f(x)$ modulo $p_1 \cdots p_r$ of degree $\leq n$ which are irreducible when considered modulo each p_j. Thus,

$$I_n(P) = \prod_{j=1}^{r} I_n(\{p_j\}),$$

and the result follows. ■

We can divide the integers in the interval $[-B, B]$ into $[(2[B]+1)/(p_1 \cdots p_r)] + 1$ disjoint sets and use the argument given for obtaining (6.3) to get that

$$I_n'(B, P) = \left(\prod_{j=1}^{r} c_n(p_j)\right)(2B)^{n+1} + O_n\left(p_1^{n+1} \cdots p_r^{n+1} B^n\right). \tag{6.5}$$

We are now ready to prove Theorem 21. Fix $n \geq 1$ and define $R(n, B, z)$ as the number of polynomials $f(x)$ in $S_n(B)$ such that $f(x)$ is reducible modulo p for every prime $p \leq z$. Thus, if $f(x)$ is not among the polynomials counted by $R(n, B, z)$, then it is irreducible modulo some prime. Hence, it suffices to show that for every $\epsilon > 0$ and for every $B \geq B_0(n, \epsilon)$ and $z \geq z_0(n, \epsilon, B)$, we have that

$$R(n, B, z) \leq \epsilon B^{n+1}. \tag{6.6}$$

To get such a bound, we can use the method of inclusion and exclusion. If we were to take away from the polynomials in $S_n(B)$ all of those polynomials which are irreducible modulo some prime $\leq z$, then we would be left with

$$|S_n(B)| - \sum_{p \leq z} I'_n\left(B, \{p\}\right)$$

polynomials except that this last sum over counts the number of polynomials which are irreducible modulo some prime $\leq z$. More specifically, if a polynomial $f(x)$ in $S_n(B)$ is irreducible modulo several primes $\leq z$, then it is counted several times in the last sum (once for each prime $p \leq z$ such that $f(x)$ is irreducible modulo p). Thus, we need to modify the expression above. For this purpose, we consider $f(x) \in S_n(B)$ and define

$$\alpha(f(x)) = 1 - \sum_{p_1 \leq z}^{*} 1 + \sum_{p_1 < p_2 \leq z}^{*} 1 - \sum_{p_1 < p_2 < p_3 \leq z}^{*} 1 + \cdots,$$

where the $*$ in a summation indicates that each prime p_j in the sum is such that $f(x)$ is irreducible modulo p_j. Suppose that there are exactly k primes $p \leq z$ such that $f(x)$ is irreducible modulo p. If $k = 0$, then we get that $\alpha(f(x)) = 1$. If $k > 0$, then we get that

$$\alpha(f(x)) = 1 - \binom{k}{1} + \binom{k}{2} - \binom{k}{3} + \cdots = (1-1)^k = 0.$$

Thus, $\alpha(f(x)) = 0$ if $f(x)$ is irreducible modulo some prime $\leq z$ and otherwise $\alpha(f(x)) = 1$.

We get that

$$\begin{aligned}
R(n,B,z) &= \sum_{f(x)\in S_n(B)} \alpha(f(x)) \\
&= \sum_{f(x)\in S_n(B)} \left(1 - \sum_{p_1\le z}^{*} 1 + \sum_{p_1<p_2\le z}^{*} 1 - \sum_{p_1<p_2<p_3\le z}^{*} 1 + \cdots\right) \\
&= |S_n(B)| - \sum_{f(x)\in S_n(B)} \sum_{p_1\le z}^{*} 1 + \sum_{f(x)\in S_n(B)} \sum_{p_1<p_2\le z}^{*} 1 - \sum_{f(x)\in S_n(B)} \sum_{p_1<p_2<p_3\le z}^{*} 1 + \cdots .
\end{aligned}$$

Rearranging the summations and using the definition of $I_n'(B,P)$, we get that

$$\begin{aligned}
R(n,B,z) = |S_n(B)| - \sum_{p_1\le z} I_n'(B,\{p_1\}) &+ \sum_{p_1<p_2\le z} I_n'(B,\{p_1,p_2\}) \\
&- \sum_{p_1<p_2<p_3\le z} I_n'(B,\{p_1,p_2,p_3\}) + \cdots .
\end{aligned}$$

Observe that this gives an exact formula for $R(n,B,z)$ and that there are only a finite number of sums above since $\pi(z)$ (the number of primes $\le z$) is finite. Indeed, there are $\le z$ primes which are $\le z$. Hence, from (6.5), we get that

$$\begin{aligned}
R(n,B,z) = (2B)^{n+1} - \sum_{p_1\le z} c_n(p_1)(2B)^{n+1} &+ \sum_{p_1<p_2\le z} c_n(p_1)c_n(p_2)(2B)^{n+1} \\
- \sum_{p_1<p_2<p_3\le z} & c_n(p_1)c_n(p_2)c_n(p_3)(2B)^{n+1} + \cdots + E \\
= (2B)^{n+1} \prod_{p\le z} (1 - c_n(p)) \ + \ E,
\end{aligned}$$

where

$$\begin{aligned}
|E| &\ll_n B^n \left(1 + \binom{\pi(z)}{1} z^{n+1} + \binom{\pi(z)}{2} z^{2(n+1)} + \binom{\pi(z)}{3} z^{3(n+1)} + \cdots\right) \\
&\ll_n \left(1 + \binom{\pi(z)}{1} + \binom{\pi(z)}{2} + \binom{\pi(z)}{3} + \cdots\right) z^{z(n+1)} B^n \ll_n 2^z z^{z(n+1)} B^n.
\end{aligned}$$

Taking $z = \log\log B$, one gets that

$$|E| \ll_n e^z z^{z(n+1)} B^n \ll_n (\log B)(\log\log B)^{(n+1)\log\log B} B^n.$$

For B sufficiently large, we get that

$$|E| \leq \frac{\epsilon}{2} B^{n+1}.$$

From (6.2) and the definition of $c_n(p)$, we get that

$$\begin{aligned} c_n(p) &= \frac{1}{p^{n+1}} \sum_{k \leq n} I_k(p) \\ &\geq \frac{1}{p^{n+1}} I_n(p) = \frac{p-1}{pn} + O(np^{-n/2}) \\ &\geq \frac{1}{2n} + O(np^{-1/2}). \end{aligned}$$

For any constant c' and for $p \geq 16(c')^2 n^4$, we get that

$$c' n p^{-1/2} \leq \frac{1}{4n}.$$

Thus, if p is sufficiently large, then $c_n(p) \geq 1/(4n)$. This easily implies that if B is sufficiently large (so that z consequently is large), then

$$\prod_{p \leq z} (1 - c_n(p)) < \frac{\epsilon}{2^{n+2}}.$$

Combining the above estimates, (6.6) and, hence, Theorem 21 follows.

The technique used in establishing Theorem 21 is a sieve technique, more precisely the sieve of Eratosthenes. A more general consequence of the approach described above is

Theorem 22. *Let T be a set of polynomials in $\mathbb{Z}[x]$ of degree $\leq n$. Let D be a set of positive integers. For each $d \in D$, suppose that we have associated with it a subset $T(d)$ of T. For any $d_1, \ldots, d_r$ in D, define*

$$T(\{d_1, \ldots, d_r\}) = \bigcap_{j=1}^{r} T(d_j).$$

For $d \in D$, let $c(d)$ and $R(d, B)$ (possibly depending on n) be such that

$$|T(d) \cap S_n(B)| = c(d)(2B)^{n+1} + R(d, B).$$

For $d_1, \ldots, d_r$ in D, define $R(\{d_1, \ldots, d_r\}, B)$ by

$$|T(\{d_1, \ldots, d_r\}) \cap S_n(B)| = c(d_1) \cdots c(d_r)(2B)^{n+1} + R(\{d_1, \ldots, d_r\}, B).$$

Then for every $z > 0$,

$$|\{f(x) \in S_n(B) : \text{ for each } d \in D \text{ with } d \leq z, f(x) \notin T(d)\}|$$

$$= \prod_{\substack{d \in D \\ d \leq z}} (1 - c(d))\,(2B)^{n+1} + O\Bigg(\sum_{\substack{D' \subseteq D \\ d \in D' \implies d \leq z}} |R(D', B)| \Bigg) + O\left(B^n\right).$$

The sieve of Eratosthenes has been extended and elaborated on considerably to provide a very powerful and useful tool in Number Theory. We will use sieve methods again later in this book. For an excellent reference on this subject see Halberstam and Richert [1]. In particular, if in trying to apply Theorem 22, the reader unfamiliar with sieve techniques finds the value of z he wishes to use is sufficiently large so that the first error term above exceeds the main term, then he may wish to consider using the Brun sieve or the Selberg sieve instead of the sieve of Eratosthenes. The book by Halberstam and Richert [1] can be consulted for this purpose.

The proof of Theorem 21 implies that not only is almost every $f(x) \in \mathbb{Z}[x]$ irreducible modulo some prime but also that almost every $f(x) \in \mathbb{Z}[x]$ is irreducible modulo some *small* prime. More specifically, it is possible to modify the proof slightly to obtain that if $\psi(t)$ is any function that tends to infinity with t, then for almost all $f(x) = \sum_{j=0}^{n} a_j x^j \in \mathbb{Z}[x]$, there is a prime $p \leq \psi(\max_{0 \leq j \leq n}\{|a_j|\})$ such that $f(x)$ is irreducible modulo p. This implies that a fast probabilistic test for irreducibility over the rationals can be formulated which simply tests a given $f(x) \in \mathbb{Z}[x]$ for irreducibility modulo small primes. If $f(x)$ is irreducible modulo a small prime and the prime does not divide the leading coefficient of $f(x)$, then $f(x)$ is irreducible over the rationals; and if $f(x)$ is reducible modulo every small prime used, then the test is inconclusive. If one fixes a function $\psi(t)$ and defines "small" as above, then the test will correctly deduce the irreducibility over the rationals of almost every $f(x) \in \mathbb{Z}[x]$. There is an even quicker algorithm which correctly predicts the irreducibility over the rationals of almost every polynomial $f(x) \in \mathbb{Z}[x]$. In fact, the second algorithm is so quick that its running time is faster than the running time it takes to input most polynomials. The second algorithm is to disregard the polynomial and simply print a note claiming the polynomial is irreducible over the rationals. By Theorem 20, we know the second algorithm will correctly predict the irreducibility over $\mathbb{Q}$ of almost all $f(x) \in \mathbb{Z}[x]$. The difference, however, in these two irreducibility algorithms is that the first never produces misinformation; in other words, it never claims that a reducible polynomial is irreducible (over $\mathbb{Q}$).

6.3. In this section, we show that if $f(x) \in \mathbb{Z}[x]$ is irreducible over the rationals, then usually the Eisenstein-Schönemann Criterion does not help in determining its irreducibility. To be more precise, we let E denote the set of polynomials in $\mathbb{Z}[x]$ which are Eisenstein. We will prove that e_n approaches 0 as n approaches infinity where

$$e_n = \limsup_{B\to\infty} \frac{|\{f(x) \in S_n(B) : f(x) \in E\}|}{|\{f(x) \in S_n(B) : f(x) \text{ irreducible over } \mathbb{Q}\}|}.$$

Since from Theorem 20

$$\lim_{B\to\infty} \frac{|\{f(x) \in S_n(B) : f(x) \text{ irreducible over } \mathbb{Q}\}|}{(2B)^{n+1}} = 1,$$

we see that

$$e_n = \limsup_{B\to\infty} \frac{|\{f(x) \in S_n(B) : f(x) \in E\}|}{(2B)^{n+1}}.$$

We consider $n \ge 10$. Recall that if $f(x)$ is an Eisenstein polynomial of degree m with respect to some prime p, then there are integers a and b such that $f(x) \equiv b(x-a)^m \pmod{p}$. We let T be the set of all $f(x) \in \mathbb{Z}[x]$ such that $f(x) \equiv b(x-a)^m \pmod{p}$ holds for some prime p and some integers a, b, and m (with $m \ge 0$). Thus, $E \subseteq T$. We set

$$t_n = \limsup_{B\to\infty} \frac{|\{f(x) \in S_n(B) : f(x) \in T\}|}{(2B)^{n+1}}.$$

Thus, $e_n \le t_n$, and it suffices to show that $\lim_{n\to\infty} t_n = 0$. We use Theorem 22 with D being the set of primes. For each prime p, we set $T(p)$ to be the set $f(x) \in \mathbb{Z}[x]$ such that $f(x) \equiv b(x-a)^m \pmod{p}$ for some choice of integers a, b, and m (with $m \geq 0$). In particular, if $f(x)$ is a constant modulo p, then $f(x) \in T(p)$. The number of other incongruent $f(x)$ modulo p in $T(p) \cap S_n(B)$ is $(p-1)pn$. Hence, there are a total of $(np-n+1)p$ incongruent $f(x)$ modulo p in $T(p) \cap S_n(B)$. In a manner similar to that used to obtain (6.3) in the previous section, we deduce that

$$|T(p) \cap S_n(B)| = c(p)(2B)^{n+1} + O_n\left(p^2 B^n\right) \tag{6.7}$$

where $c(p) = (np-n+1)/p^n$. Furthermore, if $P = \{p_1, \dots, p_r\}$ is a set of primes, then

$$|T(P) \cap S_n(B)| = c(p_1) \cdots c(p_r)(2B)^{n+1} + O_n\left(p_1^2 \cdots p_r^2 B^n\right).$$

Thus,

$$R(P, B) \ll p_1^2 \cdots p_r^2 B^n$$

and (along the lines of estimating $|E|$ in the previous section)

$$\sum_{\substack{P=\{p_1,\dots,p_r\} \\ p_j \leq z \text{ for each } j}} |R(P, B)| \ll 2^z z^{2z} B^n.$$

Taking $z = \log\log B$, we deduce from Theorem 22 that

$$\begin{aligned}|\{f(x) \in S_n(B) : \text{for each prime } p \leq z, f(x) \notin T(p)\}| \\ = \prod_{p \leq z} (1 - c(p))\,(2B)^{n+1} + O_n\left(B^{(2n+1)/2}\right).\end{aligned}$$

Since we are considering $n \geq 10$, the product

$$\prod_p (1 - c(p)) = \prod_p \left(1 - \frac{np-n+1}{p^n}\right)$$

converges. We are almost ready to claim that t_n is no larger than the value of this product; however, T is the union of the sets $T(p)$ as p varies over all the primes, and we have thus far only established an estimate for the number of $f(x) \in S_n(B)$ with $f(x) \notin T(p)$ for $p \leq \log\log B$.

Suppose now that $f(x) \in T(p) \cap S_n(B)$ and $p > z = \log\log B$. We recall Problem (2.7) (a). Although the problem there dealt with Eisenstein polynomials rather than polynomials in T, for the purposes of that problem, the conclusion is the same. In other words, $p^{n-1}|R(f,f')$. On the other hand, if $m = \deg f(x) \geq 1$, then $R(f,f')$ is the determinant of a $(2m-1)\times(2m-1)$ matrix all of whose entries are $\leq mB$. Since $m \leq n$, we easily deduce that $|R(f,f')| = O_n(B^{2n-1})$. If $R(f,f') = 0$, then recall that (2.2) implies that $f(x)$ and $f'(x)$ have a root in common so that one can deduce that $f(x)$ is reducible. We have already shown in the proof of Theorem 20 that there are at most $O_n(B^n \log^2 B)$ such $f(x) \in S_n(B)$. If $R(f,f') \neq 0$, then $p^{n-1}|R(f,f')$ and $|R(f,f')| = O_n(B^{2n-1})$ imply that $p \leq B^3$ (where we consider here, as we may, B to be large compared to n). Therefore, we have $z < p \leq B^3$. For each such p, we use that

$$|T(p) \cap S_n(B)| \leq (np - n + 1)p\left(\frac{2B+1}{p} + 1\right)^{n+1}.$$

This inequality can be deduced along the lines of (6.7). From this we obtain

$$|T(p) \cap S_n(B)| = O_n\left(c(p)B^{n+1}\right) + O_n\left(p^2\right).$$

We now deduce that the number of $f(x) \in T(p) \cap S_n(B)$ for some $p > z$ is

$$O_n\left(\sum_{z<p\leq B^3} c(p)B^{n+1}\right) + O_n\left(\sum_{z<p\leq B^3} p^2\right) + O_n\left(B^n \log^2 B\right).$$

Using $c(p) = (np - n + 1)/p^n$ and $n \geq 10$, we conclude that the number of such $f(x)$ is $O_n(B^{n+1}/\log\log B)$.

Combining the above, we obtain

$$|\{f(x) \in S_n(B) : f(x) \notin T\}| = \prod_{p \leq \log\log B} (1 - c(p))\,(2B)^{n+1} + O_n\left(B^{n+1}/\log\log B\right).$$

Hence,

$$\lim_{B\to\infty} \frac{|\{f(x) \in S_n(B) : f(x) \notin T\}|}{(2B)^{n+1}} = \prod_p \left(1 - \frac{np-n+1}{p^n}\right) \geq \prod_p \left(1 - \frac{n}{p^{n-1}}\right).$$

We leave it now to the reader to verify that $\lim_{n\to\infty} t_n = 0$.

Problems

(6.1) Modify the proof of Theorem 20 to show that for every positive integer n, almost all monic polynomials are irreducible. In other words, show that if $n \ge 1$, then

$$\lim_{B\to\infty} \frac{|\{f(x) \in S_n(B) : f(x) \text{ is monic and irreducible}\}|}{(2B)^n} = 1.$$

(6.2) Let n be a positive integer. What proportion of the polynomials of degree n are irreducible over the *integers*? More specifically, evaluate

$$\lim_{B\to\infty} \frac{|\{f(x) \in S_n(B) : f(x) \text{ is irreducible}\}|}{(2B)^{n+1}}.$$

(6.3) Given two properties $\mathcal{P}_1$ and $\mathcal{P}_2$, we say that almost all polynomials $f(x) \in \mathbb{Z}[x]$ which satisfy property $\mathcal{P}_1$ have property $\mathcal{P}_2$ if

$$\lim_{B\to\infty} \frac{|\{f(x) \in S_n(B) : f(x) \text{ satisfies } \mathcal{P}_1 \text{ and } \mathcal{P}_2\}|}{|\{f(x) \in S_n(B) : f(x) \text{ satisfies } \mathcal{P}_1\}|} = 1$$

for every sufficiently large positive integer n.

(a) Using the comments after the proof of Theorem 20, explain why almost all $f(x) \in \mathbb{Z}[x]$ which are reducible over the rationals have a linear factor in $\mathbb{Z}[x]$.

(b) Let k be a positive integer. Consider the $f(x) \in \mathbb{Z}[x]$ which have a factor over the rationals of degree $\ge k$ but which have no factor over the rationals of degree ℓ for $1 \le \ell < k$. Show that almost all such $f(x)$ have a factor over the rationals of degree exactly k.

(6.4) Observe that both $f(x) = 2x + 2$ and $f(x) = x^2 + x + 2$ have the property that if m is an integer, then $f(m)$ is even. We say that $f(x) \in \mathbb{Z}[x]$ has a fixed prime divisor if for some prime p and every integer m, $f(m)$ is divisible by p. Show that the density of $f(x) \in \mathbb{Z}[x]$ of degree n which do not have a fixed prime divisor is $\prod_{p\le n}(1 - (1/p^p))$. (Hint: First resolve why the product is only over the primes which are $\le n$.)

(6.5) (a) Let $f(x) \in \mathbb{Z}[x]$. Suppose that for some integer a, $f(x + a) = \sum_{j=0}^{n} a_j x^j$ with $a_n = 1$, $a_0 \ne 0$, and $|a_{n-1}| > 1 + \sum_{j=0}^{n-2} |a_j|$. By Perron's Theorem (Theorem 8) and

Problem (1.1), we can deduce that $f(x)$ is irreducible. Call such an $f(x)$ irreducible by Perron's Theorem. The argument for establishing Perron's Theorem implies that such an $f(x)$ has $n-1$ roots within 1 of a in the complex plane. Write $f(x) = \sum_{j=0}^{n} b_j x^j$, and suppose that $f(x) \in S_n(B)$. By considering the relations b_0 and b_1 have with the roots of $f(x)$, show that if $B \geq 2$, $n \geq 4$, and $|a| \geq n$, then $|a| \leq 2B^{1/3} + 1$.

(b) With the notation in part (a), show that

$$|b_{n-1}| \leq (n-1)(|a|+1) + \frac{B}{(|a|-1)^{n-1}}.$$

(c) In the above situation, suppose that B is sufficiently large (possibly depending on n). Show that there are at most $4B$ possible values for the pair (a, a_{n-1}). Furthermore, establish that $|a_{n-1}| \leq 2B$.

(d) In part (c), show that there are at most $(6^{n-1}/(n-1)!)B^{n-1}$ possible values for the $(n-1)$–tuple $(a_{n-2}, \dots, a_1, a_0)$.

(e) Prove that if $f(x) \in \mathbb{Z}[x]$ is a monic irreducible polynomial, then one cannot usually determine its irreducibility by using Perron's Theorem. In other words, establish that if

$$p_n = \limsup_{B \to \infty} \frac{|\{f(x) \in S_n(B) : f(x) \text{ irreducible by Perron's Theorem}\}|}{|\{f(x) \in S_n(B) : f(x) \text{ monic and irreducible}\}|},$$

then $\lim_{n \to \infty} p_n = 0$.

(6.6) Explain how

$$\left| \left\{ f(x) = \sum_{j=0}^{n} \epsilon_j x^j : \epsilon_0 = 1, \epsilon_j \in \{0,1\} \text{ for } j = 1, \dots, n, \text{ and } f(x) \text{ irreducible} \right\} \right| \gg \frac{2^n}{n}$$

follows as a consequence of a theorem from Chapter 4.

(6.7) Recall the polynomials $P_n(x) = 3 + x + 4x^2 + \cdots$, in Section 6.1. Think of what might likely be a factor of $P_n(x)$ and find (computationally) a positive integer n for which $P_n(x)$ is reducible. (Hint: If one flips a coin patiently for years and years, what is the probability that eventually the number of heads flipped equals the number of tails flipped?)