Chapter 2

Congruences for $p(n)$ and $\tau(n)$

2.1. Historical Background

This chapter is primarily devoted to proving some of Ramanujan's congruences for $p(n)$ and $\tau(n)$. We begin with a remark on notation. Throughout the chapter, we shall see congruences of the sort

$$f(q) \equiv g(q) \pmod{m}, \tag{2.1.1}$$

where $f(q) = \sum a_n q^n$ and $g(q) = \sum b_n q^n$ are power series in q. The congruence (2.1.1) is equivalent to the condition $a_n \equiv b_n \pmod{m}$ for *every* integer n appearing as an index in either power series.

In 1919, Ramanujan [**188**], [**192**, pp. 210–213] announced that he had found three simple congruences satisfied by $p(n)$, namely,

$$p(5n+4) \equiv 0 \pmod{5}, \tag{2.1.2}$$

$$p(7n+5) \equiv 0 \pmod{7}, \tag{2.1.3}$$

$$p(11n+6) \equiv 0 \pmod{11}. \tag{2.1.4}$$

He gave proofs of (2.1.2) and (2.1.3) in [**188**] and later in a short one page note [**190**], [**192**, p. 230] announced that he had also found a proof of (2.1.4). He also remarks in [**190**] that "It appears that there are no equally simple properties for any moduli involving primes other than these three." In a posthumously published paper [**191**], [**192**,

pp. 232–238], Hardy extracted different proofs of (2.1.2)–(2.1.4) from an unpublished manuscript of Ramanujan on $p(n)$ and $\tau(n)$ [**194**, pp. 133–177], [**50**].

In [**188**], Ramanujan offered a more general conjecture. Let $\delta = 5^a 7^b 11^c$ and let λ be an integer such that $24\lambda \equiv 1 \pmod{\delta}$. Then

$$p(n\delta + \lambda) \equiv 0 \pmod{\delta}. \tag{2.1.5}$$

In his unpublished manuscript [**194**, pp. 133–177], [**50**], Ramanujan gave a proof of (2.1.5) for arbitrary a and $b = c = 0$. He also began a proof of his conjecture for arbitrary b and $a = c = 0$, but he did not complete it. If he had completed his proof, he would have noticed that his conjecture in this case needed to be modified. Ramanujan had formulated his conjectures after studying a table of values of $p(n), 0 \le n \le 200$, made by P. MacMahon. After Ramanujan died, H. Gupta extended MacMahon's table up to $n = 300$. Upon examining Gupta's table in 1934, S. Chowla [**75**] found that $p(243)$ is not divisible by 7^3, despite the fact that $24 \cdot 243 \equiv 1 \pmod{7^3}$. To correct Ramanujan's conjecture, define $\delta' = 5^a 7^{b'} 11^c$, where $b' = b$, if $b = 0, 1, 2$, and $b' = [(b+2)/2]$, if $b > 2$. Then

$$p(n\delta + \lambda) \equiv 0 \pmod{\delta'}. \tag{2.1.6}$$

In 1938, G. N. Watson [**218**] published a proof of (2.1.6) for $a = c = 0$ and gave a more detailed version of Ramanujan's proof of (2.1.6) in the case $b = c = 0$. It was not until 1967 that A. O. L. Atkin [**28**] proved (2.1.6) for arbitrary c and $a = b = 0$.

The tau function $\tau(n)$ was introduced by Ramanujan in his famous paper [**186**], [**192**, pp. 136–162]. Although he proved little about $\tau(n)$ in this paper, he did formulate some fundamental conjectures about $\tau(n)$. In [**190**], Ramanujan stated without proof congruences for $\tau(n)$ modulo 5, 7, and 23. In his unpublished manuscript on $p(n)$ and $\tau(n)$ [**194**, pp. 133–177], [**50**], he proved these congruences and several further results on $\tau(n)$.

2.2. Elementary Congruences for $\tau(n)$

First, we show that $\tau(n)$ is seldom odd.

Theorem 2.2.1. *The number of values of $n \leq x$ for which $\tau(n)$ is odd equals*

$$\left[\frac{1+\sqrt{x}}{2}\right], \tag{2.2.1}$$

where $[x]$ denotes the greatest integer less than or equal to x.

Proof. Observe that, for any positive integer j, by the binomial theorem,

$$(1-q^j)^8 = 1 - 8q^j + 28q^{2j} - \cdots + q^{8j} \equiv 1 + q^{8j} \equiv 1 - q^{8j} \pmod 2.$$

Hence,

$$(q;q)_\infty^8 \equiv (q^8;q^8)_\infty \pmod 2.$$

Therefore, using the definition of $\tau(n)$ in (1.1.10), the congruence above, and Jacobi's identity, Theorem 1.3.9, we find that

$$\begin{aligned}\sum_{n=1}^{\infty}\tau(n)q^n = q(q;q)_\infty^{24} &\equiv q(q^8;q^8)_\infty^3 \\ &= \sum_{n=0}^{\infty}(-1)^n(2n+1)q^{(2n+1)^2} \pmod 2.\end{aligned}$$

Thus, $\tau(n)$ is odd or even according as n is an odd square or not.

Exercise 2.2.2. *As an elementary exercise, show that the number of odd squares less than or equal to x is precisely* (2.2.1).

So the proof of Theorem 2.2.1 is complete. □

Theorem 2.2.3. *For each nonnegative integer n,*

$$\tau(7n), \tau(7n+3), \tau(7n+5), \tau(7n+6) \equiv 0 \pmod 7. \tag{2.2.2}$$

Proof. Applying the binomial theorem, as we did in the previous proof, we easily deduce that

$$(q;q)_\infty^7 \equiv (q^7;q^7)_\infty \pmod 7,$$

and so

$$\sum_{n=1}^{\infty}\tau(n)q^n = q(q;q)_\infty^{24} \equiv q(q;q)_\infty^3(q^7;q^7)_\infty^3 \pmod 7. \tag{2.2.3}$$

Since the powers in $(q^7;q^7)_\infty^3$ are all multiples of 7, we need only consider

$$q(q;q)_\infty^3 = \sum_{n=0}^{\infty}(-1)^n(2n+1)q^{1+n(n+1)/2}, \tag{2.2.4}$$

by Jacobi's identity, Theorem 1.3.9. Observe that $1+n(n+1)/2 \equiv 0,1,2,4 \pmod 7$. Moreover, $1+n(n+1)/2 \equiv 0 \pmod 7$ if and only if $n \equiv 3 \pmod 7$ or $2n+1 \equiv 0 \pmod 7$. It now follows from (2.2.3) and (2.2.4) that $\tau(7n) \equiv 0 \pmod 7$. It also follows that there are no powers of q on the right side of (2.2.4) that are congruent to either 3, 5, or 6 modulo 7. The latter three congruences in (2.2.2) thus follow from (2.2.3) and (2.2.4). □

For example, $\tau(3) = 252 \equiv 0 \pmod 7$, $\tau(5) = 4830 \equiv 0 \pmod 7$, $\tau(6) = -6048 \equiv 0 \pmod 7$, and $\tau(7) = -16744 \equiv 0 \pmod 7$. The reader will observe that 3, 5, and 6 are the quadratic nonresidues modulo 7 and that indeed the proof of Theorem 2.2.3 demonstrates this.

Theorem 2.2.4. *Let r, $0 \le r < 23$, denote any quadratic residue modulo 23. Then, for each positive integer n,*

$$\tau(23n-r) \equiv 0 \pmod{23}. \tag{2.2.5}$$

Proof. By the binomial theorem,

$$\sum_{n=1}^{\infty}\tau(n)q^n = q(q;q)_\infty^{24} \equiv q(q;q)_\infty(q^{23};q^{23})_\infty \pmod{23}.$$

Since the powers in $(q^{23};q^{23})_\infty$ are all multiples of 23, we need only consider

$$q(q;q)_\infty = \sum_{n=-\infty}^{\infty}(-1)^n q^{1+n(3n+1)/2}, \tag{2.2.6}$$

by Euler's pentagonal number theorem (1.3.18). Observe that

$$1+\frac{n(3n+1)}{2} = (6n+1)^2 - \frac{23n(3n+1)}{2} \equiv (6n+1)^2 \pmod{23}. \tag{2.2.7}$$

Thus, $\tau(m)$ will be a multiple of 23 when m is not congruent to a square modulo 23. In other words, if we set $m =: 23n+\ell = k^2, 0 \le \ell < 23$, for some integers n, ℓ, and k, then ℓ must be a quadratic

nonresidue modulo 23. Recall that r is a quadratic residue modulo 23. Since $23 \equiv -1 \pmod 4$, $-r, r \neq 0$, is a quadratic nonresidue modulo 23. It follows that

$$\tau(23n - r) \equiv 0 \pmod{23}, \qquad 0 < r < 23. \tag{2.2.8}$$

□

For example, 3 and 6 are quadratic residues modulo 23, and so $\tau(20) = -7109760 \equiv 0 \pmod{23}$ and $\tau(17) = -6905934 \equiv 0 \pmod{23}$.

We shall later examine congruences for $\tau(n)$ modulo 5. However, to establish these congruences, we first need to prove Ramanujan's famous congruence for $p(n)$ modulo 5.

2.3. Ramanujan's Congruence $p(5n + 4) \equiv 0 \pmod{5}$

In this monograph, we present four proofs of Ramanujan's congruence for $p(n)$ modulo 5. We offer three proofs in this section. The first and the second are more elementary than the third, but the third gives more information.

Theorem 2.3.1. *For each nonnegative integer n,*

$$p(5n + 4) \equiv 0 \pmod{5}. \tag{2.3.1}$$

First Proof of Theorem 2.3.1. Our first proof is taken from Ramanujan's paper [**188**], [**192**, pp. 210–213] and is reproduced in Hardy's book [**107**, pp. 87–88].

We begin by writing

$$q(q;q)_\infty^4 \frac{(q^5;q^5)_\infty}{(q;q)_\infty^5} = q\frac{(q^5;q^5)_\infty}{(q;q)_\infty} = (q^5;q^5)_\infty \sum_{m=0}^{\infty} p(m)q^{m+1}. \tag{2.3.2}$$

By the binomial theorem,

$$(q;q)_\infty^5 \equiv (q^5;q^5)_\infty \pmod 5 \qquad \text{or} \qquad \frac{(q^5;q^5)_\infty}{(q;q)_\infty^5} \equiv 1 \pmod 5. \tag{2.3.3}$$

Hence, by (2.3.2) and (2.3.3),

$$q(q;q)_\infty^4 \equiv (q^5;q^5)_\infty \sum_{m=0}^{\infty} p(m)q^{m+1} \pmod 5. \tag{2.3.4}$$

We now see from (2.3.4) that in order to show that $p(5n+4) \equiv 0 \pmod 5$ we must show that the coefficients of q^{5n+5} on the left side of (2.3.4) are multiples of 5.

By the pentagonal number theorem, Corollary 1.3.5, and Jacobi's identity, Theorem 1.3.9,

$$\begin{aligned} q(q;q)_\infty^4 &= q(q;q)_\infty (q;q)_\infty^3 \\ &= q \sum_{j=-\infty}^{\infty} (-1)^j q^{j(3j+1)/2} \sum_{k=0}^{\infty} (-1)^k (2k+1) q^{k(k+1)/2} \\ &= \sum_{j=-\infty}^{\infty} \sum_{k=0}^{\infty} (-1)^{j+k} (2k+1) q^{1+j(3j+1)/2+k(k+1)/2}. \end{aligned} \tag{2.3.5}$$

Our objective is to determine when the exponents on the right side are multiples of 5. Observe that

$$2(j+1)^2 + (2k+1)^2 = 8\left\{1 + \tfrac{1}{2}j(3j+1) + \tfrac{1}{2}k(k+1)\right\} - 10j^2 - 5.$$

Thus, $1 + \frac{1}{2}j(3j+1) + \frac{1}{2}k(k+1)$ is a multiple of 5 if and only if

$$2(j+1)^2 + (2k+1)^2 \equiv 0 \pmod 5. \tag{2.3.6}$$

It is easily checked that $2(j+1)^2 \equiv 0, 2,$ or 3 modulo 5 and that $(2k+1)^2 \equiv 0, 1,$ or 4 modulo 5. We therefore see that (2.3.6) is true if and only if

$$2(j+1)^2 \equiv 0 \pmod 5 \qquad \text{and} \qquad (2k+1)^2 \equiv 0 \pmod 5.$$

In particular, $2k+1 \equiv 0 \pmod 5$, which, by (2.3.5), implies that the coefficient of q^{5n+5}, $n \geq 0$, in $q(q;q)_\infty^4$ is a multiple of 5. The coefficient of q^{5n+5} on the right side of (2.3.4) is therefore also a multiple of 5, i.e., $p(5n+4)$ is a multiple of 5. □

We now give a second simple proof due to G. E. Andrews [**15**] and based on the simple lemma given below. See also an extensive generalization of this lemma by Andrews and R. Roy [**24**]. In particular, taking a special case of their general theorem, Andrews and Roy establish the congruence $p(7n+5) \equiv 0 \pmod 7$.

Lemma 2.3.2. *Let $\{a_n\}$, $n \geq 0$, be any sequence of integers. Then the coefficient of q^{5n+3}, $n \geq 0$, in*

$$L(q) := \frac{1}{(q;q)_\infty^2} \sum_{n=0}^{\infty} a_n q^{n^2} \tag{2.3.7}$$

is divisible by 5.

Proof. Write (2.3.7) in the form

$$L(q) = (q;q)_\infty^3 \frac{\sum_{m=0}^{\infty} a_m q^{m^2}}{(q;q)_\infty^5} \equiv (q;q)_\infty^3 \frac{\sum_{m=0}^{\infty} a_m q^{m^2}}{(q^5;q^5)_\infty} \pmod 5,$$

by the binomial theorem. Using Jacobi's identity, Theorem 1.3.9, we thus see that it suffices to examine the coefficient of q^{5n+3} in

$$(q;q)_\infty^3 \sum_{m=0}^{\infty} a_m q^{m^2} = \sum_{j=0}^{\infty} (-1)^j (2j+1) q^{j(j+1)/2} \sum_{m=0}^{\infty} a_m q^{m^2}. \tag{2.3.8}$$

We want those terms above for which $j(j+1)/2 + m^2 = 5n+3$, where $n \geq 0$. It is easy to see that this condition is equivalent to the congruence

$$(2j+1)^2 + 3m^2 \equiv 0 \pmod 5. \tag{2.3.9}$$

Since $(2j+1)^2 \equiv 0, \pm 1 \pmod 5$ and $3m^2 \equiv 0, 2, 3 \pmod 5$, we see that (2.3.9) holds only when

$$m \equiv 2j+1 \equiv 0 \pmod 5. \tag{2.3.10}$$

The coefficients of q^{5n+3} in (2.3.8) are then composed of terms of the sort $(-1)^j(2j+1)a_m$, which, by (2.3.10), are all multiples of 5. □

Exercise 2.3.3. *Use* (1.3.13) *to show that*

$$\varphi(-q) = \frac{(q;q)_\infty}{(-q;q)_\infty}. \tag{2.3.11}$$

Second Proof of Theorem 2.3.1. Using (2.3.11), we find that

$$\begin{aligned} \sum_{k=0}^{\infty} p(k) q^{2k} &= \frac{1}{(q^2;q^2)_\infty} = \frac{1}{(q;q)_\infty (-q;q)_\infty} = \frac{1}{(q;q)_\infty^2} \frac{(q;q)_\infty}{(-q;q)_\infty} \\ &= \frac{1}{(q;q)_\infty^2} \left(1 + 2 \sum_{m=1}^{\infty} (-1)^m q^{m^2} \right). \end{aligned}$$

By Lemma 2.3.2, the coefficients $p(k)$ on the left side above are multiples of 5 whenever $2k \equiv 5j + 3 \pmod 5$, i.e., whenever $k = 5n + 4$. This then completes our second proof. □

Our third proof is also due to Ramanujan in [**188**], but it is only briefly indicated in that paper. In his unpublished manuscript on $p(n)$ and $\tau(n)$, [**194**], [**50**], Ramanujan gives a more detailed sketch. In this proof, the congruence $p(5n + 4) \equiv 0 \pmod 5$ follows from a beautiful identity. Following Ramanujan, throughout the proof we let $J_k(q), k = 1, 2$, denote power series with integral powers and integral coefficients, not necessarily the same at each appearance. The precise identities of $J_1(q)$ and $J_2(q)$ are not important for the proof.

Theorem 2.3.4. *We have*

$$\sum_{n=0}^{\infty} p(5n+4)q^n = 5\frac{(q^5;q^5)_\infty^5}{(q;q)_\infty^6}. \tag{2.3.12}$$

Proof. We begin by writing

$$\frac{(q^{1/5};q^{1/5})_\infty}{(q^5;q^5)_\infty} = J_1(q) - q^{1/5} + J_2(q)q^{2/5}. \tag{2.3.13}$$

To see this, use the pentagonal number theorem (1.3.18) in the numerator on the left side of (2.3.13) and, if n is the index of summation, divide the terms into residue classes modulo 5. If $n \equiv 0, 2 \pmod 5$, then the powers are integral, and these, when divided by $(q^5;q^5)_\infty$, account for the terms in $J_1(q)$. If $n \equiv 3, 4 \pmod 5$, then the powers are of the form $k + 2/5$, where k is a positive integer, i.e., we obtain the terms $J_2(q)q^{2/5}$.

Exercise 2.3.5. *Lastly, when $n \equiv 1 \pmod 5$, use the pentagonal number theorem, Corollary* 1.3.5*, to show that these terms in $(q^{1/5};q^{1/5})_\infty$ are equal to $-q^{1/5}(q^5;q^5)_\infty$.*

Hence, we obtain the term $-q^{1/5}$ in (2.3.13). Now cube both sides of (2.3.13) to obtain

$$\begin{aligned}\frac{(q^{1/5};q^{1/5})_\infty^3}{(q^5;q^5)_\infty^3} &= (J_1^3 - 3J_2^2q) - q^{1/5}(3J_1^2 - J_2^3q) + 3J_1q^{2/5}(1 + J_1J_2) \\ &\quad - q^{3/5}(1 + 6J_1J_2) + 3J_2q^{4/5}(1 + J_1J_2),\end{aligned} \tag{2.3.14}$$

where for brevity we have deleted the argument q of J_1 and J_2. Next, we use Jacobi's identity, Theorem 1.3.9, in the numerator on the left side of (2.3.14) and repeat the same kind of argument that we applied with the pentagonal number theorem in (2.3.13). We subdivide the indices n of the sum in the numerator into residue classes modulo 5. As an exercise, readers should use Jacobi's identity (1.3.24) to show that the contributions of the terms with $n \equiv 2 \pmod 5$ are equal to $5(q^5;q^5)_\infty^3 q^{3/5}$. Thus, we obtain an equality of the sort

$$\frac{(q^{1/5};q^{1/5})_\infty^3}{(q^5;q^5)_\infty^3} = G_1(q) + G_2(q)q^{1/5} + 5q^{3/5}, \tag{2.3.15}$$

where $G_1(q)$ and $G_2(q)$ are power series with integral powers and integral coefficients. Hence, equating coefficients on the right sides of (2.3.14) and (2.3.15), we find that

$$J_1(1 + J_1J_2) = 0, \qquad 1 + 6J_1J_2 = -5, \qquad J_2(1 + J_1J_2) = 0.$$

From any one of these equalities, we deduce that

$$J_1J_2 = -1. \tag{2.3.16}$$

Our next task is to use (2.3.16), (2.3.13), and "rationalization" to show that

(2.3.17)

$$\begin{aligned}\frac{(q^5;q^5)_\infty}{(q^{1/5};q^{1/5})_\infty} &= \frac{1}{J_1 - q^{1/5} + J_2q^{2/5}} \\ &= \frac{(J_1^4 + 3J_2q) + q^{1/5}(J_1^3 + 2J_2^2q) + q^{2/5}(2J_1^2 + J_2^3q)}{J_1^5 - 11q + q^2J_2^5} \\ &\quad + \frac{q^{3/5}(3J_1 + J_2^4q) + 5q^{4/5}}{J_1^5 - 11q + q^2J_2^5}.\end{aligned}$$

We now demonstrate how to prove the second equality in (2.3.17).

Return to (2.3.13) and replace $q^{1/5}$ by $\omega q^{1/5}$, where ω is any fifth root of unity. Thus,

$$\frac{(\omega q^{1/5};\omega q^{1/5})_\infty}{(q^5;q^5)_\infty} = J_1(q) - \omega q^{1/5} + J_2(q)\omega^2 q^{2/5}. \tag{2.3.18}$$

Let ω run through all five fifth roots of unity and multiply all five such equalities (2.3.18) to obtain

$$\prod_{\omega} \frac{(\omega q^{1/5};\omega q^{1/5})_\infty}{(q^5;q^5)_\infty} = \prod_{\omega} \left\{ J_1(q) - \omega q^{1/5} + J_2(q)\omega^2 q^{2/5} \right\}. \tag{2.3.19}$$

First examine the product on the left side of (2.3.19). Using the fact that the sum of the five fifth roots of unity equals 0, we see that if n is not a multiple of 5, we obtain products of the form

$$(1-q^{n/5})(1-\omega q^{n/5})(1-\omega^2 q^{n/5})(1-\omega^3 q^{n/5})(1-\omega^4 q^{n/5}) = 1-q^n. \tag{2.3.20}$$

However, if $n = 5m$, then the corresponding terms are

$$(1-q^m)(1-q^m)(1-q^m)(1-q^m)(1-q^m) = (1-q^m)^5,$$

instead of $1-q^n$ that we obtained in (2.3.20). Thus, we find that

$$\prod_{\omega} \frac{(\omega q^{1/5};\omega q^{1/5})_\infty}{(q^5;q^5)_\infty} = \frac{(q;q)_\infty^6}{(q^5;q^5)_\infty^6}. \tag{2.3.21}$$

We now examine the product on the right side of (2.3.19). Since there are no fractional powers of q on the left side of (2.3.19) by (2.3.21), there are none on the right side as well. Thus, we only need to examine those terms in the product that give rise to integral powers of q. A brief inspection then convinces us that

$$\prod_{\omega} \left\{ J_1(q) - \omega q^{1/5} + J_2(q)\omega^2 q^{2/5} \right\} = J_1^5(q) - q + J_2^5(q)q^2 + C_1 q + C_2 q, \tag{2.3.22}$$

where C_1 is the sum of the $\binom{5}{1,3,1} = 20$ terms of the form $-J_1 J_2 \omega_1\omega_2\omega_3\omega_4^2 = \omega_1\omega_2\omega_3\omega_4^2$, and C_2 is the sum of the $\binom{5}{2,1,2} = 30$ terms of the form $-J_1^2 J_2^2 \omega_1\omega_2^2\omega_3^2 = -\omega_1\omega_2^2\omega_3^2$, since $J_1 J_2 = -1$. Here, for each j, ω_j is a fifth root of unity, and in each product $\omega_j \neq \omega_k$ if $j \neq k$. First, examine the terms $\omega_1\omega_2\omega_3\omega_4^2 = \omega_4\omega_5^{-1}$. Now,

$$\sum_{\omega_4 \neq \omega_5} \omega_4\omega_5^{-1} = -\omega_5\omega_5^{-1} = -1,$$

where the sum is over the four fifth roots of unity ω_4, except ω_5. Since there are five possibilities for ω_5, we conclude that $C_1 = -5$. Second,

examine the terms $-\omega_1\omega_2^2\omega_3^2$. Now,

$$-\sum_{\omega_1\neq\omega_2,\omega_3}\omega_1\omega_2^2\omega_3^2=(\omega_2+\omega_3)\omega_2^2\omega_3^2=\omega_2^3\omega_3^2+\omega_2^2\omega_3^3,$$

and

$$\sum_{\omega_2\neq\omega_3}(\omega_2^3\omega_3^2+\omega_2^2\omega_3^3)=-\omega_3^3\omega_3^2-\omega_3^2\omega_3^3=-2.$$

There are five possibilities for ω_3, and so it would seem that we obtain a contribution of -10 to the value of C_2. However, because of the symmetry of ω_2 and ω_3, we have counted each contribution to C_2 twice, i.e., in fact, $C_2=-5$. Using our values $C_1=-5=C_2$ in (2.3.22), we deduce that

$$\prod_{\omega}\left\{J_1(q)-\omega q^{1/5}+J_2(q)\omega^2q^{2/5}\right\}=J_1^5(q)-11q+J_2^5(q)q^2. \tag{2.3.23}$$

In summary, from (2.3.23), we have shown that

$$\begin{aligned}\frac{1}{J_1(q)-q^{1/5}+J_2(q)q^{2/5}}&=\frac{\prod_{\omega\neq1}\left\{J_1(q)-\omega q^{1/5}+J_2(q)\omega^2q^{2/5}\right\}}{\prod_{\omega}\left\{J_1(q)-\omega q^{1/5}+J_2(q)\omega^2q^{2/5}\right\}}\\&=\frac{\prod_{\omega\neq1}\left\{J_1(q)-\omega q^{1/5}+J_2(q)\omega^2q^{2/5}\right\}}{J_1^5(q)-11q+J_2^5(q)q^2}\\&=\frac{F(q)}{J_1^5(q)-11q+J_2^5(q)q^2},\end{aligned} \tag{2.3.24}$$

where

$$F(q)=\frac{J_1^5(q)-11q+J_2^5(q)q^2}{J_1(q)-q^{1/5}+J_2(q)q^{2/5}}.$$

If we consider the numerator and denominator above as polynomials in $q^{1/5}$ and use long division, we find that $F(q)$ indeed is the numerator on the right side of (2.3.17). Thus, by (2.3.24), the proof of (2.3.17) is complete.

Recalling that on the left side of (2.3.17) $1/(q^{1/5};q^{1/5})_\infty$ is the generating function for $p(n)$, we select those terms on both sides where the powers of q are congruent to $4/5$ modulo 1. We then divide both sides by $q^{4/5}$ to find that

$$(q^5;q^5)_\infty\sum_{n=0}^{\infty}p(5n+4)q^n=\frac{5}{J_1^5(q)-11q+J_2^5(q)q^2}. \tag{2.3.25}$$

However, from (2.3.19), (2.3.21), and (2.3.23), we also know that

$$\frac{(q^5;q^5)_\infty^6}{(q;q)_\infty^6} = \frac{1}{J_1^5(q) - 11q + J_2^5(q)q^2}. \tag{2.3.26}$$

Utilizing (2.3.26) in (2.3.25), we complete the proof of (2.3.12). □

Theorem 2.3.4 can be utilized to provide a proof of Ramanujan's congruence for $p(n)$ modulo 25.

Theorem 2.3.6. *For every nonnegative integer n,*

$$p(25n + 24) \equiv 0 \pmod{25}. \tag{2.3.27}$$

Proof. Applying the binomial theorem on the right side of (2.3.12), we find that

$$\sum_{n=0}^{\infty} p(5n+4)q^n \equiv 5\frac{(q^5;q^5)_\infty^4}{(q;q)_\infty} = 5(q^5;q^5)_\infty^4 \sum_{n=0}^{\infty} p(n)q^n \pmod{25}. \tag{2.3.28}$$

From Theorem 2.3.1 we know that the coefficients of $q^4, q^9, q^{14}, \ldots$, $q^{5n+4}, \ldots$ on the far right side of (2.3.28) are all multiples of 25. It follows that the coefficients of $q^{5n+4}, n \geq 0$, on the far left side of (2.3.28) are also multiples of 25, i.e.,

$$p(25n + 24) \equiv 0 \pmod{25}.$$

This completes the proof. □

Ramanujan's congruence in Theorem 2.3.1 yields a simple proof of Ramanujan's congruence for the tau function modulo 5, as we next demonstrate.

Theorem 2.3.7. *For each nonnegative integer n,*

$$\tau(5n) \equiv 0 \pmod{5}. \tag{2.3.29}$$

Proof. By the definition of $\tau(n)$ and the binomial theorem,

$$\sum_{n=1}^{\infty} \tau(n)q^n = q(q;q)_\infty^{24} = q\frac{(q;q)_\infty^{25}}{(q;q)_\infty} \equiv q(q^5;q^5)_\infty^5 \sum_{n=0}^{\infty} p(n)q^n \pmod{5}. \tag{2.3.30}$$

By Theorem 2.3.1, the coefficient of $q^{5n}, n \geq 1$, on the far right side of (2.3.30) is a multiple of 5. Thus, the coefficient of q^{5n} on the far left side of (2.3.30) is a multiple of 5, i.e., $\tau(5n) \equiv 0 \pmod 5$. □

2.4. Ramanujan's Congruence $p(7n+5) \equiv 0 \pmod 7$

We consider next Ramanujan's congruence for $p(n)$ modulo 7.

Theorem 2.4.1. *For each nonnegative integer n,*

$$p(7n+5) \equiv 0 \pmod 7. \tag{2.4.1}$$

Proof. Our proof is again taken from Ramanujan's paper [**188**] and was sketched by Hardy [**107**, p. 88].

First, by the binomial theorem,

$$q^2(q^7;q^7)_\infty \sum_{n=0}^{\infty} p(n)q^n = q^2\frac{(q^7;q^7)_\infty}{(q;q)_\infty} = q^2(q;q)_\infty^6 \frac{(q^7;q^7)_\infty}{(q;q)_\infty^7}$$

$$\equiv q^2(q;q)_\infty^6 \pmod 7. \tag{2.4.2}$$

Hence, if we can show that the coefficient of $q^{7n+7}, n \geq 0$, in $q^2(q;q)_\infty^6$ is a multiple of 7, it will follow from (2.4.2) that the coefficient of q^{7n+7} on the far left side is a multiple of 7, i.e., $p(7n+5) \equiv 0 \pmod 7$.

Applying Jacobi's identity, Theorem 1.3.9, we find that

$$q^2(q;q)_\infty^6 = q^2\{(q;q)_\infty^3\}^2$$

$$= \sum_{j=0}^{\infty}\sum_{k=0}^{\infty}(-1)^{j+k}(2j+1)(2k+1)q^{2+j(j+1)/2+k(k+1)/2}. \tag{2.4.3}$$

As we saw in the previous paragraph, we want to know when the exponents above are multiples of 7. Now observe that

$$(2j+1)^2 + (2k+1)^2 = 8\{2 + \tfrac{1}{2}j(j+1) + \tfrac{1}{2}k(k+1)\} - 14,$$

and so $2 + \frac{1}{2}j(j+1) + \frac{1}{2}k(k+1)$ is a multiple of 7 if and only if

$$(2j+1)^2 + (2k+1)^2 \equiv 0 \pmod 7. \tag{2.4.4}$$

We easily see that $(2j+1)^2, (2k+1)^2 \equiv 0, 1, 2, 4 \pmod 7$, and so the only way (2.4.4) can hold is if both $(2j+1)^2, (2k+1)^2 \equiv 0 \pmod 7$. In such cases, we trivially see that the coefficients on the right side of

(2.4.3) are multiples of 7. Hence, the coefficient of $q^{7n+7}, n \geq 1$, on the left side of (2.4.3) is a multiple of 7. As we demonstrated in the foregoing paragraph, this implies that $p(7n+5) \equiv 0 \pmod 7$. □

We now consider the analogue of Theorem 2.3.4 for $p(7n+5)$, which was stated without proof by Ramanujan in his paper [**188**]. In his unpublished manuscript on $p(n)$ and $\tau(n)$, he gives a very brief sketch of its proof [**194**, pp. 133–177], [**50**]. There are now several proofs of Theorem 2.4.2, but the details of Ramanujan's proof were worked out only recently by Berndt, A. J. Yee, and J. Yi [**54**]. Because the details are cumbersome, we provide only the central ideas and refer readers to [**54**] for a complete proof. Readers should not attempt to complete missing details but merely try to grasp the ideas behind Ramanujan's proof.

Theorem 2.4.2. *We have*

$$\sum_{n=0}^{\infty} p(7n+5)q^n = 7\frac{(q^7;q^7)_\infty^3}{(q;q)_\infty^4} + 49q\frac{(q^7;q^7)_\infty^7}{(q;q)_\infty^8}. \tag{2.4.5}$$

It is clear that Theorem 2.4.1 is an immediate corollary of Theorem 2.4.2.

Proof. Using (1.3.18) in both the numerator and denominator and then separating the indices of summation in the numerator into residue classes modulo 7, we readily find that

$$\frac{(q^{1/7};q^{1/7})_\infty}{(q^7;q^7)_\infty} = J_1 + q^{1/7}J_2 - q^{2/7} + q^{5/7}J_3, \tag{2.4.6}$$

where J_1, J_2, and J_3 are power series in q with integral coefficients, and where the pentagonal number theorem was used to calculate the coefficient of $q^{2/7}$. Cubing both sides of (2.4.6), we find that

$$\begin{aligned}
&\frac{(q^{1/7};q^{1/7})_\infty^3}{(q^7;q^7)_\infty^3} \\
&= (J_1^3 + 3J_2^2J_3q - 6J_1J_3q) + q^{1/7}(3J_1^2J_2 - 6J_2J_3q + J_3^2q^2) \\
&\quad + 3q^{2/7}(J_1J_2^2 - J_1^2 + J_3q) + q^{3/7}(J_2^3 - 6J_1J_2 + 3J_1J_3^2q) \\
&\quad + 3q^{4/7}(J_1 - J_2^2 + J_2J_3^2q) + 3q^{5/7}(J_2 + J_1^2J_3 - J_3^2q) \\
&\quad + q^{6/7}(6J_1J_2J_3 - 1).
\end{aligned} \tag{2.4.7}$$

On the other hand, using Jacobi's identity, Theorem 1.3.9, and separating the indices of summation in the numerator on the left side of (2.4.7) into residue classes modulo 7, we easily find that

$$\frac{(q^{1/7};q^{1/7})_\infty^3}{(q^7;q^7)_\infty^3} = G_1 + q^{1/7}G_2 + q^{3/7}G_3 - 7q^{6/7}, \tag{2.4.8}$$

where G_1, G_2, and G_3 are power series in q with integral coefficients, and where Jacobi's identity, Theorem 1.3.9, was used to determine the coefficient of $q^{6/7}$. Comparing coefficients in (2.4.7) and (2.4.8), we conclude that

$$\begin{cases} J_1J_2^2 - J_1^2 + J_3q &= 0, \\ J_1 - J_2^2 + J_2J_3^2q &= 0, \\ J_2 + J_1^2J_3 - J_3^2q &= 0, \\ 6J_1J_2J_3 - 1 &= -7. \end{cases} \tag{2.4.9}$$

Replace $q^{1/7}$ by $\omega q^{1/7}$ in (2.4.6), where ω is any seventh root of unity. Therefore,

$$\frac{(\omega q^{1/7};\omega q^{1/7})_\infty}{(q^7;q^7)_\infty} = J_1 + \omega q^{1/7}J_2 - \omega^2 q^{2/7} + \omega^5 q^{5/7}J_3. \tag{2.4.10}$$

Taking the products of both sides of (2.4.10) over all seven seventh roots of unity, we find that

$$\frac{(q;q)_\infty^8}{(q^7;q^7)_\infty^8} = \prod_\omega (J_1 + \omega q^{1/7}J_2 - \omega q^{2/7} + \omega q^{5/7}J_3). \tag{2.4.11}$$

Using the generating function for $p(n)$, (2.4.6), and (2.4.11), we find that

$$\begin{aligned} \sum_{n=0}^\infty p(n)q^n = \frac{1}{(q;q)_\infty} &= \frac{(q^{49};q^{49})_\infty^7}{(q^7;q^7)_\infty^8}\frac{(q^7;q^7)_\infty^8}{(q^{49};q^{49})_\infty^8}\frac{(q^{49};q^{49})_\infty}{(q;q)_\infty} \\ &= \frac{(q^{49};q^{49})_\infty^7}{(q^7;q^7)_\infty^8}\frac{\prod_\omega (J_1 + \omega qJ_2 - \omega q^2 + \omega q^5J_3)}{J_1 + qJ_2 - q^2 + q^5J_3} \\ &= \frac{(q^{49};q^{49})_\infty^7}{(q^7;q^7)_\infty^8}\left\{\prod_{\omega\neq 1}(J_1 + \omega qJ_2 - \omega q^2 + \omega q^5J_3)\right\}. \end{aligned} \tag{2.4.12}$$

We only need to compute the terms in $\prod_{\omega\neq 1}(J_1+\omega qJ_2-\omega q^2+\omega q^5J_3)$ where the powers of q are of the form $7n+5$ to complete the proof. In

order to do this, we need to prove several identities using the identities of (2.4.9). We do not give the details.

Choosing only those terms on each side of (2.4.12) where the powers of q are of the form $7n+5$ and using the omitted calculations, we find that

$$\sum_{\substack{n=0\\ n\equiv 5 \pmod 7}}^{\infty} p(n)q^n = q^5\frac{(q^{49};q^{49})_\infty^7}{(q^7;q^7)_\infty^8}\left(7\frac{(q^7;q^7)_\infty^4}{(q^{49};q^{49})_\infty^4}+49q^7\right),$$

or

$$\sum_{n=0}^{\infty} p(7n+5)q^{7n} = 7\frac{(q^{49};q^{49})_\infty^3}{(q^7;q^7)_\infty^4}+49q^7\frac{(q^{49};q^{49})_\infty^7}{(q^7;q^7)_\infty^8}. \tag{2.4.13}$$

Replacing q^7 by q in (2.4.13), we complete the proof of (2.4.5). □

Recall that the identity of Theorem 2.3.4 yielded in Theorem 2.3.6 a congruence for $p(n)$ modulo 5^2. Similarly, the identity in Theorem 2.4.2 yields a congruence for $p(n)$ modulo 7^2, as we now demonstrate.

Theorem 2.4.3. *For each nonnegative integer n,*

$$p(49n+47) \equiv 0 \pmod{49}. \tag{2.4.14}$$

Proof. Write (2.4.5) in the form

$$\sum_{n=0}^{\infty} p(7n+5)q^n = 7\frac{(q^7;q^7)_\infty^3(q;q)_\infty^3}{(q;q)_\infty^7}+49q\frac{(q^7;q^7)_\infty^7}{(q;q)_\infty^8}$$

$$\equiv 7(q^7;q^7)_\infty^2\sum_{m=0}^{\infty}(-1)^m(2m+1)q^{m(m+1)/2} \pmod{49}, \tag{2.4.15}$$

by the binomial theorem and Jacobi's identity (1.3.24). We now examine the terms on the right side of (2.4.15) where the powers of q are of the form $7n+6$. Separating the summands into residue classes modulo 7, we see that the only terms yielding such exponents are when $m \equiv 3 \pmod 7$. But then $2m+1 \equiv 0 \pmod 7$. Thus, the coefficient of the power $q^{7n+6}, n \geq 1$, on the right side of (2.4.15) is a multiple of 49. The same must be true, of course, on the left side of (2.4.15), i.e., the coefficient $p(49n+47)$ must be a multiple of 49, i.e., (2.4.14) has been established. □

We shall return to congruences for $p(n)$ after we introduce Eisenstein series in Chapter 4.

2.5. The Parity of $p(n)$

In contrast to Theorem 2.2.1 which provides a criterion for determining when $\tau(n)$ is either even or odd, we know much less about the parity of $p(n)$. It has long been conjectured that $p(n)$ is even approximately half of the time, or, more precisely,

$$\#\{n \leq N : p(n) \text{ is even}\} \sim \tfrac{1}{2}N, \tag{2.5.1}$$

as $N \to \infty$. T. R. Parkin and D. Shanks [**178**] undertook the first extensive computations, providing strong evidence that indeed (2.5.1) is most likely true. Despite the venerability of the problem, it was not even known that $p(n)$ assumes either even or odd values infinitely often until 1959, when O. Kolberg [**135**] established these facts. Other proofs of Kolberg's theorem were later found by J. Fabrykowski and M. V. Subbarao [**93**] and by M. Newman [**168**]. In 1983, L. Mirsky [**159**] established the first quantitative result by showing that

$$\#\{n \leq N : p(n) \text{ is even (odd)}\} > \frac{\log\log N}{2\log 2}. \tag{2.5.2}$$

An improvement was made by J.–L. Nicolas and A. Sárközy [**171**], who proved that

$$\#\{n \leq N : p(n) \text{ is even (odd)}\} > (\log N)^c, \tag{2.5.3}$$

for some positive constant c.

In the most recent investigations, the methods for finding lower bounds for the number of occurrences of even values of $p(n)$ have been somewhat different from those for odd values of $p(n)$. Greatly improving on previous results, Nicolas, I. Z. Ruzsa, and Sárközy [**170**] in 1998 proved that

$$\#\{n \leq N : p(n) \text{ is even }\} \gg \sqrt{N} \tag{2.5.4}$$

and, for each $\epsilon > 0$,

$$\#\{n \leq N : p(n) \text{ is odd }\} \gg \sqrt{N}e^{-(\log 2+\epsilon)\frac{\log N}{\log\log N}}. \tag{2.5.5}$$

(We pause to explain the notation $\gg$. We write $F(N) \gg G(N)$, if and only if there exists a positive constant c such that $F(N) \geq cG(N)$,

for all N sufficiently large.) In an appendix to their paper [**170**], J.–P. Serre used modular forms to prove that

$$\lim_{N\to\infty} \frac{\#\{n \le N : p(n) \text{ is even }\}}{\sqrt{N}} = \infty. \tag{2.5.6}$$

At present, this is the best known result for even values of $p(n)$. The lower bound (2.5.5) has been improved first by S. Ahlgren [**6**], who utilized modular forms, and second by Nicolas [**169**], who used more elementary methods, to prove that

$$\#\{n \le N : p(n) \text{ is odd }\} \gg \frac{\sqrt{N}(\log\log N)^K}{\log N}, \tag{2.5.7}$$

for some positive number K. Ahlgren proved (2.5.7) with $K = 0$. An elegant, elementary proof of (2.5.7) when $K = 0$ was established by D. Eichhorn [**86**]. The lower bound (2.5.7) is currently the best known result for odd values of $p(n)$.

Our goal in this section is to prove the results (2.5.5) and (2.5.4) of Nicolas, Ruzsa, and Sárközy [**170**] by relatively simple means. Our proof is a special instance of an argument devised by Berndt, Yee, and A. Zaharescu [**55**], who proved considerably more general theorems that are applicable to a wide variety of partition functions. Except for one step, when we must appeal to a theorem of S. Wigert [**223**] and Ramanujan [**185**], our proof is elementary and self-contained.

Theorem 2.5.1. *For each fixed c with $c > 2\log 2$ and N sufficiently large,*

$$\#\{n \le N : p(n) \text{ is odd}\} \ge N^{\frac{1}{2} - \frac{c}{\log\log N}}. \tag{2.5.8}$$

Theorem 2.5.2. *For each fixed constant c with $c < 1/\sqrt{6}$, and for N sufficiently large,*

$$\#\{n \le N : p(n) \text{ is even}\} \ge c\sqrt{N}. \tag{2.5.9}$$

Before we begin our proofs of Theorems 2.5.1 and 2.5.2, we need to establish some terminology. Although we shall use language from modern algebra, readers need not know any theorems from the subject. In fact, some of the information conveyed in the next two paragraphs will not be used in the sequel, but we think these facts are interesting in themselves.

Let $A := \mathbf{F}_2[[X]]$ be the ring of formal power series in one variable X over the field with two elements $\mathbf{F}_2 = \mathbf{Z}/2\mathbf{Z}$, i.e.,

$$A = \left\{ f(X) = \sum_{n=0}^{\infty} a_n X^n : a_n \in \mathbf{F}_2, \quad 0 \le n < \infty \right\}. \tag{2.5.10}$$

The ring A is an integral domain; note that an element $f(X) = \sum_{n=0}^{\infty} a_n X^n \in A$ is invertible if and only if $a_0 = 1$. Since 0 and 1 are the only elements of $\mathbf{F}_2$, we may write any element $f(X) \in A$ in the form

$$f(X) = X^{n_1} + X^{n_2} + \cdots, \tag{2.5.11}$$

where the sum may be finite or infinite and $0 \le n_1 < n_2 < \cdots$. For any $f(X) \in A$, observe that

$$f^2(X) = f(X^2). \tag{2.5.12}$$

In other words, if $f(X)$ is given by (2.5.11), then

$$f^2(X) = X^{2n_1} + X^{2n_2} + \cdots. \tag{2.5.13}$$

On A there exists a natural derivation which sends $f(X) \in A$ to $f'(X) = \frac{df}{dX} \in A$, i.e., if

$$f(X) = \sum_{n=0}^{\infty} a_n X^n, \quad \text{then} \quad f'(X) = \sum_{n=1}^{\infty} n a_n X^{n-1}. \tag{2.5.14}$$

Note that for any $f(X) \in A$,

$$f''(X) = 0. \tag{2.5.15}$$

We also remark that for any $f(X)$ given in the form (2.5.11), the condition

$$f'(X) = 0 \tag{2.5.16}$$

is equivalent to the condition that all the exponents n_j are even numbers.

In our proof of Theorem 2.5.2, we need to know the shape (2.5.11) of the series $f(X)/(1-X)$. For any integers $0 \le a < b$, we see that in A

$$\frac{X^a + X^b}{1-X} = \frac{X^a(1-X^{b-a})}{1-X} = X^a + X^{a+1} + \cdots + X^{b-1}. \tag{2.5.17}$$

We put together pairs of consecutive terms $X^{n_{2k+1}} + X^{n_{2k+2}}$ to obtain the equality

(2.5.18)
$$\begin{aligned}\frac{f(X)}{1-X} &= \frac{X^{n_1}+X^{n_2}}{1-X} + \frac{X^{n_3}+X^{n_4}}{1-X} + \cdots + \frac{X^{n_{2k+1}}+X^{n_{2k+2}}}{1-X} + \cdots \\ &= \left(X^{n_1} + X^{n_1+1} + \cdots + X^{n_2-1}\right) + \left(X^{n_3} + \cdots + X^{n_4-1}\right) + \cdots \\ &\quad + \left(X^{n_{2k+1}} + \cdots + X^{n_{2k+2}-1}\right) + \cdots .\end{aligned}$$

If the sum on the right side of (2.5.11) defining $f(X)$ is finite, say $f(X) = X^{n_1} + X^{n_2} + \cdots + X^{n_s}$, then

$$\begin{aligned}\frac{f(X)}{1-X} &= \left(X^{n_1} + X^{n_1+1} + \cdots + X^{n_2-1}\right) + \cdots \\ &\quad + \left(X^{n_{s-1}} + X^{n_{s-1}+1} + \cdots + X^{n_s-1}\right),\end{aligned} \tag{2.5.19}$$

if s is even, and

$$\begin{aligned}\frac{f(X)}{1-X} &= \left(X^{n_1} + \cdots + X^{n_2-1}\right) + \cdots \\ &\quad + \left(X^{n_{s-2}} + \cdots + X^{n_{s-1}-1}\right) + \sum_{n=n_s}^{\infty} X^n,\end{aligned} \tag{2.5.20}$$

if s is odd.

Before commencing our proofs of Theorems 2.5.1 and 2.5.2, we introduce some standard notation in analytic number theory. We say that $f(N) = O(g(N))$, as N tends to ∞, if there exists a positive constant $A > 0$ and a number $N_0 > 0$ such that $|f(N)| \le A|g(N)|$ for all $N \ge N_0$. To emphasize that this positive constant A above may depend upon another parameter c, we write $f(N) = O_c(g(N))$, as N tends to ∞.

Proof of Theorem 2.5.1. We begin with the pentagonal number theorem

$$\sum_{n=0}^{\infty} (-1)^n q^{n(3n-1)/2} + \sum_{n=1}^{\infty} (-1)^n q^{n(3n+1)/2} = (q;q)_\infty. \tag{2.5.21}$$

By reducing the coefficients modulo 2 and replacing q by X in (2.5.21), we find that, if $1/F(X)$ is the image of the infinite series of (2.5.21)

in A, then

$$1 = F(X)\left(1 + \sum_{n=1}^{\infty}\left(X^{n(3n-1)/2} + X^{n(3n+1)/2}\right)\right). \tag{2.5.22}$$

We write $F(X)$ in the form

$$F(X) = 1 + X^{n_1} + X^{n_2} + \cdots + X^{n_j} + \cdots, \tag{2.5.23}$$

where, of course, $n_1, n_2, \ldots$ are positive integers. Clearly, from the generating function of the partition function $p(n)$ and (2.5.23),

$$\#\{1 \le n \le N : p(n) \text{ is odd}\} = \#\{n_j \le N\} \tag{2.5.24}$$

and

$$\#\{1 \le n \le N : p(n) \text{ is even}\} = N - \#\{n_j \le N\}. \tag{2.5.25}$$

We first establish a lower bound for $\#\{n_j \le N\}$. Using (2.5.23), write (2.5.22) in the form

$$\left(\sum_{j=1}^{\infty} X^{n_j}\right)\left(1 + \sum_{n=1}^{\infty}\left(X^{n(3n-1)/2} + X^{n(3n+1)/2}\right)\right)$$

$$= \sum_{m=1}^{\infty}\left(X^{m(3m-1)/2} + X^{m(3m+1)/2}\right). \tag{2.5.26}$$

Asymptotically, there are $\sqrt{2N/3}$ terms of the form $X^{m(3m-1)/2}$ less than X^N on the right side of (2.5.26). For a fixed positive integer n_j, we determine how many of these terms appear in a series of the form

$$X^{n_j}\left(1 + \sum_{n=1}^{\infty}\left(X^{n(3n-1)/2} + X^{n(3n+1)/2}\right)\right), \tag{2.5.27}$$

arising from the left side of (2.5.26). Thus, for fixed $n_j < N$, we estimate the number of integral pairs (m, n) of solutions of the equation

$$n_j + \tfrac{1}{2}n(3n-1) = \tfrac{1}{2}m(3m-1), \tag{2.5.28}$$

which we put in the form

$$2n_j = (m-n)(3m+3n-1). \tag{2.5.29}$$

By a result of Wigert [**223**] and Ramanujan [**185**], [**192**, p. 80], the number of divisors of $2n_j$ is no more than $O_c\left(N^{\frac{c}{\log\log N}}\right)$ for any fixed $c > \log 2$. Thus, each of the numbers $m-n$ and $3m+3n-1$ can assume

at most $O_c\left(N^{\frac{c}{\log\log N}}\right)$ values. Since the pair $(m-n, 3m+3n-1)$ uniquely determines the pair (m,n), it follows that the number of solutions to (2.5.29) is $O_c\left(N^{\frac{c}{\log\log N}}\right)$, where c is any constant such that $c > 2\log 2$. A similar argument can be made for the terms in (2.5.26) of the form $X^{m(3m+1)/2}$.

Returning to (2.5.26) and (2.5.27), we see that each series of the form (2.5.27) has at most $O_c\left(N^{\frac{c}{\log\log N}}\right)$ terms $X^{m(3m-1)/2}$ up to X^N that appear on the right side of (2.5.26). It follows that there are at least $O_c\left(N^{\frac{1}{2}-\frac{c}{\log\log N}}\right)$ numbers $n_j \le N$ that are needed to match all the (asymptotically $\sqrt{2N/3}$) terms $X^{m(3m-1)/2}$ up to X^N on the right side of (2.5.26). Again, an analogous argument holds for terms of the form $X^{m(3m+1)/2}$. We have therefore completed the proof of Theorem 2.5.1. □

Proof of Theorem 2.5.2. Next, we provide a lower bound for $\#\{n \le N : p(n) \text{ is even}\}$. Let $\{m_1, m_2, \dots\}$ be the complement of the set $\{0, n_1, n_2, \dots\}$ in the set of natural numbers $\{0, 1, 2, \dots\}$, and define

$$G(X) := X^{m_1} + X^{m_2} + \cdots \in A. \tag{2.5.30}$$

Then

$$G(X) + F(X) = 1 + X + X^2 + \cdots + X^k + \cdots = \frac{1}{1-X}. \tag{2.5.31}$$

Since, by (2.5.25),

$$\#\{m_j \le N\} = N - \#\{n_j \le N\} = \{n \le N : p(n) \text{ is even}\}, \tag{2.5.32}$$

we need a lower bound for $\#\{m_j \le N\}$. Using (2.5.31) in (2.5.22), we find that

$$\begin{aligned} &1 + G(X)\left(1 + \sum_{n=1}^{\infty}\left(X^{n(3n-1)/2} + X^{n(3n+1)/2}\right)\right) \\ &= \frac{1}{1-X}\left(1 + \sum_{n=1}^{\infty}\left(X^{n(3n-1)/2} + X^{n(3n+1)/2}\right)\right) \\ &= \frac{1}{1-X}\left(1 + X + X^2 + X^5 + X^7 + \cdots\right) \end{aligned}$$

$$= \frac{1}{1-X}\Big((1+X)+(X^2+X^5)+\cdots$$
$$+(X^{(n-1)(3(n-1)+1)/2}+X^{n(3n-1)/2})$$
$$+(X^{n(3n+1)/2}+X^{(n+1)(3(n+1)-1)/2})+\cdots\Big). \tag{2.5.33}$$

By (2.5.18), we see that the right side of (2.5.33) equals

$$1+(X^2+X^3+X^4)+\cdots+(X^{(n-1)(3(n-1)+1)/2}+\cdots+X^{n(3n-1)/2-1})$$
$$+(X^{n(3n+1)/2}+\cdots+X^{(n+1)(3(n+1)-1)/2-1})+\cdots. \tag{2.5.34}$$

Observe that the gap between $X^{n(3n-1)/2-1}$ and $X^{n(3n+1)/2}$ contains n terms that are missing from the series (2.5.34). This gap comes after a segment of

$$\tfrac{1}{2}n(3n-1)-1-\tfrac{1}{2}(n-1)(3(n-1)+1)+1=2n-1$$

terms that do appear in (2.5.34). So we see that (2.5.34) contains asymptotically

$$\frac{2n-1}{n+(2n-1)}N=\frac{2n-1}{3n-1}N\sim\frac{2}{3}N$$

terms up to X^N. Now the sum in parentheses on the left side of (2.5.33) has asymptotically $2\sqrt{2N/3}$ nonzero terms up to X^N. Thus $G(X)$ must have at least $\sqrt{N/6}$ nonzero terms up to X^N in order for the left side of (2.5.33) to have at least $2N/3$ terms up to X^N to match those on the right side of (2.5.33). We have therefore completed the proof of Theorem 2.5.2. □

2.6. Notes

Theorem 2.2.1 has been slightly refined by M. R. Murty, V. K. Murty, and T. N. Shorey [**165**], using a more sophisticated argument. They also obtain lower bounds for the values of $\tau(n)$ when $\tau(n)$ is odd.

Another proof of Theorem 2.3.1, rivalling Ramanujan's first proof in simplicity, has been given by J. Drost [**84**]. See M. D. Hirschhorn's paper [**120**] for still another elementary proof. Many references to further proofs of both Theorem 2.3.1 and Theorem 2.3.4 can be found

in the latest edition of Ramanujan's *Collected Papers* [**192**, pp. 372–375]. These pages also contain references to other proofs of Theorems 2.4.1 and 2.4.2. Ramanujan himself summarized the congruences he proved and the methods he utilized to prove them in a letter to Hardy written from the nursing home, Fitzroy House, in the summer of 1918. In particular, he wrote [**51**, pp. 192–193], "Thus the divisibility by $5^a 7^b 11^c$ when $a = 0, 1, 2, 3$; $b = 0, 1, 2, 3$; $c = 0, 1, 2$ amounting to $4 \times 4 \times 3 - 1$ or 47 cases of the conjectured theorem are proved." This statement is interesting for several reasons. First, Ramanujan had evidently proved special cases of his general conjecture without leaving us proofs in these cases. Second, he claimed a proof for the modulus 7^3, but we had noted in the introduction to this chapter that Ramanujan's conjecture was false in this case. Third, Ramanujan's proof of his conjecture for arbitrary powers of 5 was obviously established after this letter was written.

We have not given a proof of Ramanujan's congruence $p(11n+6) \equiv 0 \pmod{11}$. The most elementary proof is due to L. Winquist [**227**] and uses *Winquist's Identity*. Further proofs of Winquist's identity have been found by Hirschhorn [**117**] and S.–Y. Kang [**133**]. Another elementary approach to proving that $p(11n+6) \equiv 0 \pmod{11}$ has been devised by Berndt, S. H. Chan, Z.–G. Liu, and H. Yesilyurt [**48**], who established a new identity for $(q;q)_\infty^{10}$. Hirschhorn [**118**] has devised a common approach to proving all three congruences (2.1.2)–(2.1.4).

Hirschhorn and D. C. Hunt [**126**] gave an alternative proof along classical lines to that of Ramanujan and Watson for Ramanujan's congruence modulo 5^a. Those readers intrigued by our sketch of Ramanujan's Theorem 2.4.2 might consult F. G. Garvan's [**95**] proof of the more general congruence modulo 7^b.

Ramanujan appeared to conjecture that the only congruences of the form $p(\ell n + B) \equiv 0 \pmod{\ell}$, where ℓ is a prime, are those when $\ell = 5, 7$, or 11. This was not proved until 2003, when Ahlgren and M. Boylan [**8**] proved that indeed these are the only three such congruences.

Suppose, however, that we drop the restriction that the moduli of the arithmetic progressions are the same as the moduli of the congruences. That is, are there congruences when the moduli are not the same or are not primes? The first theorems establishing lots of congruences for $p(n)$ were found by Atkin [**29**]. Then K. Ono [**175**] proved that, given any prime $\ell \geq 5$, there exist infinitely many congruences of the type $p(An + B) \equiv 0 \pmod{\ell}$. This was extended by Ahlgren [**7**] who established a similar result for any prime power ℓ^k. A consequence of their work is that if $\ell \geq 5$ is prime, then for a positive proportion of positive integers n, $p(n) \equiv 0 \pmod{\ell}$. Nonetheless, finding concrete examples illustrating their theorems is not easy. Atkin and J. N. O'Brien [**30**] had earlier found a couple of such congruences; one is

$$p(17303n + 237) \equiv 0 \pmod{13}.$$

R. Weaver [**219**] devised an algorithm based on Ono's work and found over 76,000 explicit examples, all with $\ell \leq 31$.

Define

$$\delta_\ell := \frac{\ell^2 - 1}{24}.$$

Except for a couple of sporadic examples, it turns out that for all of the congruences $p(An + B) \equiv 0 \pmod{\ell}$ found by Ramanujan, Ono, Ahlgren, and others, $B \equiv -\delta_\ell \pmod{\ell}$. In another breakthrough, Ahlgren and Ono [**10**], proved that this residue class is only one of $(\ell+1)/2$ residue classes where $p(n)$ possesses many such congruences. An informative historical description of the quest for congruences for the partition function has been given by Ahlgren and Ono [**9**].

Subbarao [**211**] first conjectured that in every arithmetic progression $n \equiv r \pmod{t}$ there are infinitely many values of n such that $p(n)$ is even and that there are infinitely many values of n for which $p(n)$ is odd. The most extensive results pointing toward the truth of this conjecture have been found by Ono [**173**], [**174**] and Ahlgren [**6**], with a summary of previous results provided in these papers. The best lower bounds for the number of even and odd values of $p(n)$ in arithmetic progressions are (2.5.6) [**170**] and (2.5.7) [**6**], respectively, while the most general theorems of this sort are found in [**55**] and [**56**].

In his unpublished manuscript on $p(n)$ and $\tau(n)$, Ramanujan asserted and, in some cases, proved further congruences for $\tau(n)$, most involving divisor functions. References to most of the many papers written on this subject can be found in Berndt and Ono's account of Ramanujan's manuscript [**50**]. We now have a complete understanding of congruences for $\tau(n)$ through the theory of ℓ-adic representations, and an account of this with many references can be found in H. P. F. Swinnerton-Dyer's survey paper [**213**]. There are, in essence, only six congruences for $\tau(n)$, with the largest modulus being 691.

Z.–H. Sun and K. S. Williams [**212**] have established a refinement of Theorem 2.2.4. To describe their theorem, we first need to define the order of an integer. Let p denote a prime. Then the unique nonnegative integer α such that $p^{\alpha}|n$ but $p^{\alpha+1} \nmid n$ is called the order of n modulo p and is denoted by $\operatorname{ord}_p n$.

Theorem 2.6.1. *For any positive integer n,*

$$\tau(n) \equiv \begin{cases} 0 \pmod{23}, & \text{if there exists a prime } p \text{ such that} \\ & \left(\frac{p}{23}\right) = -1 \text{ and } 2 \nmid \operatorname{ord}_p n, \\ 0 \pmod{23}, & \text{if there exists a prime } p \text{ such that} \\ & p = 2x^2 + xy + 3y^2 \text{ and } \operatorname{ord}_p n \equiv 2 \pmod{3}, \\ (-1)^{\mu} \displaystyle\prod_{p=2x^2+xy+3y^2 \neq 23} & (1 + \operatorname{ord}_p n) \pmod{23}, \quad \text{otherwise}, \end{cases}$$

where

$$\mu := \sum_{\substack{p=2x^2+xy+3y^2 \\ \operatorname{ord}_p n \equiv 1 \pmod 3}} 1,$$

where p runs over all primes represented by $2x^2 + xy + 3y^2$.

As mentioned in the Historical Background beginning this chapter, Ramanujan introduced his arithmetical function $\tau(n)$ in [**186**], [**192**, pp. 136–16], which was to become one of the most important papers in the history of number theory. In this paper, Ramanujan made three important conjectures about $\tau(n)$.

(a) $\tau(n)$ is multiplicative, i.e., $\tau(m)\tau(n) = \tau(mn)$, whenever $(m, n) = 1$.

(b) If p is any prime and n is any integer exceeding 1, then

$$\tau(p^{n+1}) = \tau(p)\tau(p^n) - p^{11}\tau(p^{n-1}).$$

(c) For each prime p,

$$|\tau(p)| \leq 2p^{11/2}.$$

The first two conjectures were first proved by L. J. Mordell [**161**] in 1917 and then greatly generalized by E. Hecke [**113**], beginning one of the most important chapters in the theory of modular forms. Conjecture (c) was also considerably generalized and was one of the most famous unproved conjectures in number theory until it was proved by P. Deligne [**81**] in 1974.

Readers wanting to learn more about $\tau(n)$ might begin by reading two expository papers, one by R. A. Rankin [**197**], and the other by M. R. Murty [**164**]. See also a paper by V. K. Murty [**166**].