Chapter 9
How many lattice points are there on a circle or a sphere?

A point in $\mathbb{R}^n$ with integral coordinates is called a *lattice point*. In this chapter we study the distribution of lattice points on circles and spheres in $\mathbb{R}^n$. We start by finding a formula for the number $r(n)$ of points with integral coordinates on the circle $x^2 + y^2 = n$ for a natural number n. We then prove a famous theorem of Gauss that gives an expression for the sum $\sum_{n=1}^{k} r(n)$. We then state similar theorems for the number of points on higher dimensional spheres. At the end we state and prove a theorem of Jarnik (Theorem 9.9), and a recent generalization due to Cilleruelo and Córdoba (Theorem 9.10), about integral points on arcs. In the Note, we discuss the error term in Gauss' theorem mentioned above.

9.1 The case of two squares

For a natural number n, we let $r(n)$ be the number of representations of n as a sum of two integral squares, i.e., the number of integral points on the circle $x^2 + y^2 = n$. By Theorem 5.7 we know that if we write

$$n = m \cdot 2^{\alpha} \prod_{p \equiv 1 \bmod 4} p^{\beta_p}$$

with m a product of primes of the form $4k + 3$, then $r(n) = 0$ unless m is a square.

Theorem 9.1. *If m is a square,*

$$r(n) = 4 \prod_{p} (1 + \beta_p).$$

Proof. If $n = x^2 + y^2$, then $n = N(x + iy)$. So we need to determine the number of Gaussian integers z such that $n = N(z)$. By Theorem 5.10 any such z is a product

$$z = uk(1+i)^a \prod_{p \equiv 1 \bmod 4} \varpi_p^{e_p} \overline{\varpi}_p^{f_p}.$$

R. Takloo-Bighash, *A Pythagorean Introduction to Number Theory*,
Undergraduate Texts in Mathematics, https://doi.org/10.1007/978-3-030-02604-2_9

Here u is one of the four units in $\mathbb{Z}[i]$; $k \in \mathbb{N}$ is a product of primes of the form $4k+3$; and all but finitely many of the non-negative integers e_p, f_p are zero, meaning the product is finite. Then we have

$$N(z) = N(k)N(1+i)^a \prod_{p\equiv 1 \bmod 4} N(\varpi_p)^{e_p} N(\overline{\varpi}_p)^{f_p}$$

$$= k^2 2^a \prod_{p\equiv 1 \bmod 4} p^{e_p} p^{f_p} = k^2 2^a \prod_{p\equiv 1 \bmod 4} p^{e_p+f_p}.$$

Consequently, since $N(z) = n$ we get

$$m2^\alpha \prod_j p_j^{\beta_j} = k^2 2^a \prod_{p\equiv 1 \bmod 4} p^{e_p+f_p}.$$

This implies $m = k^2$, $a = \alpha$, and for each p of the form $4k+1$, $e_p + f_p = \beta_p$. The number of such e_p, f_p is $1 + \beta_p$. Since there are four possibilities for the unit u, i.e., ± 1, $\pm i$, we get a total of

$$4 \prod_p (1 + \beta_p)$$

choices for z. This finishes the proof. □

For example, we have

$$180 = 3^2 \cdot 2^2 \cdot (2+i) \cdot (2-i).$$

So we get the following numbers as the list of numbers z that have the property that $N(z) = 180$:

$$u \cdot 3 \cdot (1+i)^2 \cdot (2+i) = u(-6+12i)$$

and

$$u \cdot 3 \cdot (1+i)^2 \cdot (2-i) = u(6+12i)$$

for $u \in \{+1, -1, i, -i\}$. This means that the possibilities for the ordered pairs (a, b) such that $180 = a^2 + b^2$ are:

$$(\pm 6, \pm 12), \quad (\pm 12, \pm 6),$$

a total of eight possibilities.

Now that we have a formula for $r(n)$ one could ask natural statistical questions about it. For example, one could ask what the average behavior of $r(n)$ is like. Let us make this notion precise.

Definition 9.2. Suppose $f : \mathbb{N} \to \mathbb{C}$ is a function. We say f has *average value* equal to c if the limit

$$\lim_{N\to\infty} \frac{1}{N} \sum_{n=1}^{N} f(n)$$

exists and is equal to c.

It should be clear that not every function has an average value, see Exercise 9.3. There is a more general concept which is the following:

Definition 9.3. For functions $f, g : \mathbb{N} \to \mathbb{C}$, we say f, g have the same average order, or that g is an average order of f, if

$$\lim_{X\to\infty} \frac{\sum_{n\le X} f(n)}{\sum_{n\le X} g(n)} = 1.$$

In applications, one of the functions, say f, is the one we are interested in, and the idea is to find a nice function g which imitates the function f on average.

In the case of $r(n)$, the sum $\sum_{n=1}^{N} r(n)$ that appears in the definition of the average value has a neat geometric interpretation. Indeed, we have

$$\begin{aligned}\sum_{n=1}^{N} r(n) &= \sum_{n=1}^{N} \#\{(x, y) \in \mathbb{Z}^2 \mid x^2 + y^2 = n\}\\ &= \#\{(x, y) \in \mathbb{Z}^2 \mid x^2 + y^2 \le N\}.\end{aligned}$$

This means that $\sum_{n=1}^{N} r(n)$ is the number of integral points inside the circle of radius $\sqrt{N}$. Intuitively, the number of integral points inside the circle of radius $\sqrt{N}$ should be about the area of the circle. One way to see this is to associate a unit square to each integral point as shown in Figure 9.1 for the point (3, 2).

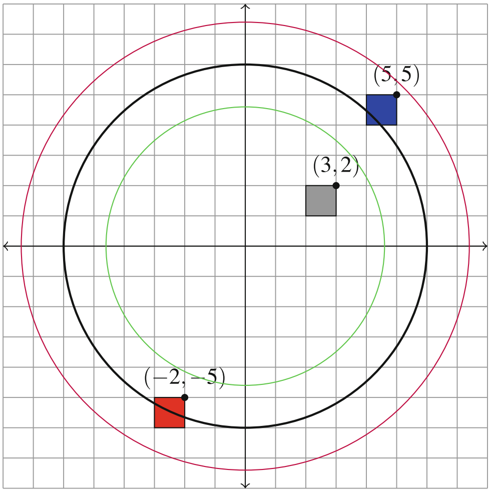

Fig. 9.1 The grey square is completely within the circle of radius 6. The point (5, 5) is outside the circle of radius 6 but the blue square to its lower left intersects the circle. The point (−2, −5) is within the circle of radius 6 but the red square to its lower left is not contained in the circle of radius 6

The trouble here is that not every square based on a point inside the circle will be completely within the circle, e.g., the red square in Figure 9.1 whose upper right corner is the point $(-2, -5)$ is not entirely within the circle of radius 6; and also some integral points outside the circle of radius 6 shown in the picture will have squares associated with them that intersect the circle, e.g., the blue square to the lower left of the point $(5, 5)$. The key point, however, is that the troublesome squares cannot stray too much from the boundary of the circle with radius $\sqrt{N}$. In fact, since the diagonal of a unit square is $\sqrt{2}$, each square to the lower left of an integral point within the circle of radius $\sqrt{N}$ will be fully contained in a circle of radius $\sqrt{N}+\sqrt{2}$. For $\sqrt{N} = 6$, the purple circle in the figure has radius $6 + \sqrt{2}$. Consequently, the total area of all unit squares, which is equal to $\sum_{n=1}^{N} r(n)$, is at most the area of the circle with radius $\sqrt{N} + \sqrt{2}$. Hence,

$$\sum_{n=1}^{N} r(n) \leq \pi(\sqrt{N} + \sqrt{2})^2 = \pi N + 2\pi\sqrt{2}\sqrt{N} + 2\pi.$$

Similarly, the entire area of the circle with radius $\sqrt{N} - \sqrt{2}$ is covered by unit squares to the lower left of integral points within the circle of radius $\sqrt{N}$. In the figure above the green circle is the one that has radius $6 - \sqrt{2}$. This means,

$$\sum_{n=1}^{N} r(n) \geq \pi(\sqrt{N} - \sqrt{2})^2 = \pi N - 2\pi\sqrt{2}\sqrt{N} + 2\pi.$$

Putting these inequalities together, we get

$$\pi N - 2\pi\sqrt{2} \cdot \sqrt{N} + 2\pi \leq \sum_{n=1}^{N} r(n) \leq \pi N + 2\pi\sqrt{2}\sqrt{N} + 2\pi.$$

These inequalities imply

$$\left| \sum_{n=1}^{N} r(n) - \pi N - 2\pi \right| \leq 2\pi\sqrt{2}\sqrt{N}.$$

We can write this inequality in terms of the *big O* notation. For real functions f, g, we write $f(x) = O(g(x))$ if there is a constant $C > 0$ such that for all x large enough, $|f(x)| \leq C|g(x)|$. We use the big O notation if we do not have to worry about the specific constants. Using this notation we can write

$$\sum_{n=1}^{N} r(n) = \pi N + 2\pi + O(\sqrt{N}) = \pi N + O(\sqrt{N}).$$

This last identity is a famous result of Gauss which for ease of reference we record as a theorem:

Theorem 9.4 (Gauss). *As $N \to \infty$,*

$$\sum_{n=1}^{N} r(n) = \pi N + O(\sqrt{N}).$$

This theorem has the following rather curious corollary:

Corollary 9.5. *The average value of* $r(n)$ *is* π.

Remark 9.6. We will prove a variation of Theorem 9.4 in §13.1.

9.2 More than two squares

It is clear that the geometric argument of the proof of Theorem 9.4 can be adapted to every dimension. For $k \geq 2$ and $n \in \mathbb{N}$, we set

$$r_k(n) = \# \left\{ (x_1, \ldots, x_k) \in \mathbb{Z}^k \mid \sum_{i=1}^{k} x_i^2 = n \right\},$$

the number of integral points on the sphere in the k-dimensional space. We have $r_2(n) = r(n)$. Then we have:

Theorem 9.7. *As* $N \to \infty$,

$$\sum_{n=1}^{N} r_k(n) = \frac{\pi^{\frac{k}{2}}}{\Gamma\left(\frac{k}{2}+1\right)} N^{\frac{k}{2}} + O(N^{\frac{k-1}{2}}).$$

For the definition and basic properties of the Gamma function Γ see [4] or [41, Chapter 8]. We review some basic properties in Exercise 9.2. The proof of Theorem 9.7 is sketched in Exercises 9.4–9.6 below.

Note that Theorem 9.7 shows that for $k > 2$, the limit

$$\lim_{N\to\infty} \frac{1}{N} \sum_{n=1}^{N} r_k(N)$$

is not finite, and consequently $r_k(N)$ does not have an average value.

Now we state an extension of Theorem 5.7 for $k > 2$.

Theorem 9.8. *For* $n \in \mathbb{N}$, $r_3(n) \neq 0$ *if and only if* n *is not of the form* $4^a(8n+7)$. *If* $k > 3$, *for all* n, $r_k(n) \neq 0$, *i.e., every natural number is the sum of four integral squares.*

We will give a proof of this fact in Chapter 10 using a theorem of Minkowski. We will give other proofs in Chapters 11 and 12. The most challenging part of the theorem is the statement for sums of three squares. We present two proofs for this theorem in §10.5 and §12.4, but unfortunately, both of these proofs rely in substantial ways on Dirichlet's Arithmetic Progression Theorem, Theorem 5.11 in Notes to Chapter 5.

In Chapter 5 we referred to Theorem 5.2 as the *Two Squares Theorem*. Throughout the text we refer to the portion of Theorem 9.8 that deals with sums of three squares as the *Three Squares Theorem*, and to the part about the expressibility of every natural number as the sum of four squares as the *Four Squares Theorem* often without explicit reference to Theorem 9.8.

Generalizing Theorem 9.1 for $k > 2$ is far more problematic. Computing $r_3(n)$ already poses a serious challenge, [113]. Erdös [73] claims that there is a constant $c > 0$ such that

$$r_3(n) \geq c\sqrt{n} \log \log n$$

but does not provide a proof. For $k = 4$ there is a beautiful explicit formula, due to Jacobi (1834), that says

$$r_4(n) = 8 \sum_{d|n, 4\nmid d} d.$$

The short paper [80] contains an elementary proof of this fact. For $k > 5$, the question of determining r_k has a long history. We refer the reader to [79] and [74] for some early works.

9.3 Integral points on arcs

In §3.2 we studied the rational points on the unit circle. If we have a rational point $(a/c, b/c)$ on the unit circle, $a, b, c \in \mathbb{Z}$, we obtain an integral point (a, b) on the circle $x^2 + y^2 = c^2$ of radius $|c|$, an integer. In general, if we have an integral point (a, b) on some circle with equation $x^2 + y^2 = R^2$, R need not be an integer, e.g., the point (2, 1) is on the circle with radius $\sqrt{5}$. As we noted above, Theorem 9.1 counts the number of integral points on the circle $x^2 + y^2 = n$ for a natural number n. As we will see below, it is in general difficult to gain a complete understanding of the distribution of these integral points on the circle, and there are still open problems that we do not know to solve. We learned the material of this section and Theorems 9.9 and 9.10 from Lillian Pierce (private communication).

Suppose we have three integral points A, B, C on a circle of radius R and let L be an arc containing the three points, e.g., $\widehat{ACB}$, as in Figure 9.2 . Let a, b, c be the lengths of the three sides of the triangle ABC and S the area of the triangle formed by the points.

By Exercise 9.8 we have $abc = 4SR$. Then since $a, b, c \leq \max\{a, b, c\}$ we have

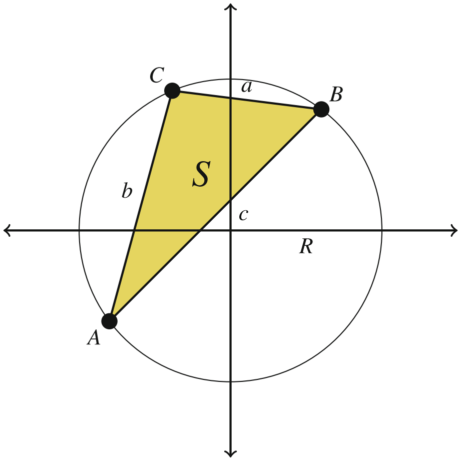

Fig. 9.2 Triangle ABC with area S whose vertices are on a circle of radius R

$$4SR = abc \leq \max\{a, b, c\}^3.$$

But since any triangle with three vertices that are integral points has area at least $1/2$ we have

$$\max\{a, b, c\}^3 \geq 2R$$

and consequently,

$$\max\{a, b, c\} \geq (2R)^{1/3}.$$

But the maximum of a, b, c is less than the length of the arc L. This means

$$L \geq (2R)^{1/3}.$$

We state this as the following important theorem:

Theorem 9.9 (Jarnik). *An arc of length less than $(2R)^{1/3}$ in a circle of radius R contains at most two integral points.*

In the case where we have more than three points the situation becomes complicated very quickly. The following is a fairly recent result that gives a non-trivial bound for any number of points.

Theorem 9.10 (Cilleruelo and Córdoba, [67]). *On a circle of radius R centered at the origin, an arc of length*

$$\sqrt{2}R^{\frac{1}{2}-\frac{1}{4[m/2]+2}}$$

contains at most m integral points.

At the time of this writing the bound obtained in the theorem seems to be the best available in literature; see [68, §5] for several comments on this theorem. The bound is sharp for $m = 3$, but it is not clear whether for $m \geq 4$ it provides the best bound possible. For $m = 4$ the theorem gives the exponent $2/5$, and *ibid.* lists the following as a non-trivial problem:

Question 9.11. Can the exponent $2/5$ be improved?

Proof of Theorem 9.10. We use the notations of the proof of Theorem 9.1. If the circle of radius R contains no lattice points, there is nothing to prove. So we assume that $R = \sqrt{n}$ for some natural number n, and by Theorem 9.1, we may further assume

$$n = k^2 2^\alpha \prod_{p \equiv 1 \bmod 4} p_j^{\beta_p}$$

with k a product of primes of the form $4k+3$. Then the total number of lattice points on the circle is

$$r(n) = 4 \prod_p (1 + \beta_p).$$

This number $r(n)$ corresponds to the various representations $N(a + ib) = n$, and in fact one can write any such $a + ib$ in the form

$$uk(1+i)^\alpha \prod_{p \equiv 1 \bmod 4} \varpi_p^{e_p} \overline{\varpi}_p^{f_p}.$$

for a unit $u \in \{\pm 1, \pm i\}$ and $e_p + f_p = \beta_p$ with $e_p, f_p \geq 0$. Here for each prime $p \equiv 1 \bmod 4$, write

$$\varpi_p = \sqrt{p} e^{2\pi i \phi_p}$$

and

$$\overline{\varpi}_p = \sqrt{p} e^{-2\pi i \phi_p}.$$

Then

$$\varpi_p^{e_p} \overline{\varpi}_p^{f_p} = p^{\frac{\beta_p}{2}} e^{2\pi i (e_p - f_p)\phi_p} = p^{\frac{\beta_p}{2}} e^{2\pi i (\beta_p - 2f_p)\phi_p}.$$

Also each unit in $\mathbb{Z}[i]$ can be written as

$$e^{2\pi i \frac{t}{4}}, \quad t \in \{0, 1, 2, 3\}.$$

Consequently, every $a + ib$ with $N(a + ib) = n$ can be written as

$$\sqrt{n} e^{2\pi i (\phi_2 + \sum_p \gamma_p \phi_p + \frac{t}{4})} \tag{9.1}$$

for $t \in \{0, 1, 2, 3\}$, $|\gamma_p| \leq \beta_p$ and $\gamma_p \equiv \beta_p \mod 2$, and the sum in the exponent is over primes p with $p \equiv 1 \bmod 4$, and $\phi_2 = \begin{cases} 0 & \alpha \text{ even;} \\ 1 & \alpha \text{ odd.} \end{cases}$

We divide the remainder of the proof into three steps.

Step One. Suppose we have $m + 1$ lattice points on an arc of length $\sqrt{2} R^\theta$. We write these points as

$$a_s + ib_s = \sqrt{n} e^{2\pi i (\phi_2 + \sum_p \gamma_p^s \phi_p + \frac{t^s}{4})},$$

$s \in \{1, \ldots, m+1\}$, with γ_p^s, t^s integers as above. For $s, s' \in \{1, \ldots, m+1\}$, $\gamma_p^s \equiv \gamma_p^{s'} \bmod 2$. Define

$$\psi^{s,s'} = \sum_p \frac{\gamma_p^s - \gamma_p^{s'}}{2}\phi_p + \frac{t^s - t^{s'}}{8}.$$

Note that $2\pi|||\psi^{s,s'}|||$ is one half of the central angle between $a_s + ib_s$ and $a_{s'} + ib_{s'}$ in radians (Here and elsewhere, for a real number x, $|||x|||$ is the distance from x to the closest integer). If the length of the arc connecting $a_s + ib_s$ and $a_{s'} + ib_{s'}$ is η, then we have

$$2\pi|||\psi^{s,s'}||| = \frac{\eta}{2R} \leq \frac{\sqrt{2}R^\theta}{2R} = \frac{1}{\sqrt{2}}R^{\theta-1}.$$

We obtain the first main inequality of this proof:

$$|||\psi^{s,s'}||| \leq \frac{1}{2\pi\sqrt{2}}R^{\theta-1}. \tag{9.2}$$

Step two. Now we proceed to obtain a lower bound for $|||\psi^{s,s'}|||$. Comparing this lower bound with Equation (9.2) gives the result. We recognize two cases:

- If $t^s \equiv t^{s'} \bmod 2$, then $(t^s - t^{s'})/8 = t^{s,s'}/4$ for some integer $t^{s,s'}$. In this case, $2\pi\psi^{s,s'}$ is the angle corresponding to a representation of the number

$$\prod_p p^{\frac{|\gamma_p^s - \gamma_p^{s'}|}{2}}$$

  as a sum of two squares;
- if $t^s \not\equiv t^{s'} \bmod 2$, then $(t^s - t^{s'}) = 1/8 + t^{s,s'}/4$ for some integer $t^{s,s'}$. In this case, $2\pi\psi^{s,s'}$ is the angle corresponding to a representation of the number

$$2\prod_p p^{\frac{|\gamma_p^s - \gamma_p^{s'}|}{2}}$$

  as a sum of two squares.

Note that if $\psi^{s,s'}$ is an integer, then the linear independence of

$$1, \phi_2, \phi_3, \phi_5, \ldots$$

over the rationals (Exercise 9.16) implies that $t^s = t^{s'}$ and $\gamma_p^s = \gamma_p^{s'}$ for every p. This means $a_s + ib_s = a_{s'} + ib_{s'}$. Consequently, if $s \neq s'$, then $|||\psi^{s,s'}||| > 0$. By the above discussion, $\psi := 2\pi|||\psi^{s,s'}|||$ is the angle of a lattice point $P(x_0, y_0)$ not on the x axis and on a circle of radius

$$R_{s,s'} := 2^{\nu/2}\prod_p p^{\frac{|\gamma_p^s - \gamma_p^{s'}|}{4}}$$

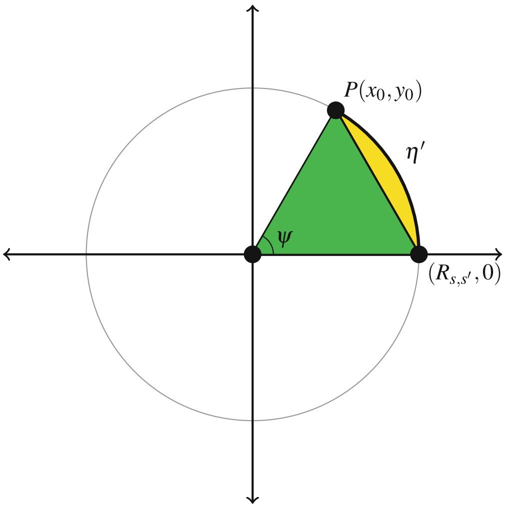

Fig. 9.3 In this diagram, η' is the length of the arc connecting $P(x_0, y_0)$ to $(R_{s,s'}, 0)$

with $\nu = 0$ or 1, depending on whether $t_s \equiv t_{s'}$ mod 2 or not. Let η' be the length of the arc connecting the P to the point $(R_{s,s'}, 0)$ as in Figure 9.3. Then η' is longer than the straight line distance between P and $(R_{s,s'}, 0)$.

This means,

$$\eta' > \sqrt{(x_0 - R_{s,s'})^2 + y_0^2} \geq \sqrt{y_0^2} \geq 1.$$

Then, in the circle of radius $R_{s,s'}$ we have

$$2\pi\,|||\psi^{s,s'}|||= \frac{\eta'}{R_{s,s,}} > \frac{1}{R_{s,s'}} \geq \frac{1}{\sqrt{2}\prod_p p^{\frac{|\gamma_p^s - \gamma_p^{s'}|}{4}}}.$$

We have then obtained our second main inequality:

$$|||\psi^{s,s'}||| > \frac{1}{2\pi\sqrt{2}\prod_p p^{\frac{|\gamma_p^s - \gamma_p^{s'}|}{4}}} \tag{9.3}$$

for $s \neq s'$.

Step three. Comparing (9.2) and (9.3) gives the following inequality: For all $s \neq s'$ we have

$$\frac{1}{\prod_p p^{\frac{|\gamma_p^s - \gamma_p^{s'}|}{4}}} < R^{\theta - 1}. \tag{9.4}$$

Step four. There are $m(m+1)/2$ choices for the unordered pairs of numbers s, s'. Multiplying inequalities (9.4) over all of these choices gives

$$\frac{1}{\prod_{s,s'} \prod_p p^{\frac{|\gamma_p^s - \gamma_p^{s'}|}{4}}} < R^{(\theta-1)m(m+1)/2}.$$

We would like to find a lower bound for the left hand side of the above inequality. In order to do this we need to maximize

$$\prod_{s,s'} \prod_p p^{\frac{|\gamma_p^s - \gamma_p^{s'}|}{4}} = \left(\prod_p p^{\sum_{s,s'} |\gamma_p^s - \gamma_p^{s'}|} \right)^{\frac{1}{4}}.$$

In order to do this, we need to maximize

$$\sum_{s,s'} |\gamma_p^s - \gamma_p^{s'}|$$

subject to the following conditions: for each s, $|\gamma_p^s| \leq \beta_p$ and $\gamma_p^s \equiv \beta_p \bmod 2$. By Exercise 9.17, the maximum value of this expression is

$$\frac{(m+1)^2 - \delta(m+1)}{2} \beta_p,$$

with the function δ being given by

$$\delta(n) = \frac{1 - (-1)^n}{2} = \begin{cases} 0 & n \text{ even;} \\ 1 & n \text{ odd.} \end{cases}$$

Putting everything together, we obtain

$$R^{(\theta-1)m(m+1)/2} > \left(\prod_p p^{\frac{(m+1)^2 - \delta(m+1)}{2} \beta_p} \right)^{-\frac{1}{4}} \geq R^{-\frac{(m+1)^2 + \delta(m+1)}{4}}.$$

This inequality implies

$$\theta > 1 - \frac{(m+1)^2 - \delta(m+1)}{2m(m+1)} = \frac{1}{2} - \frac{1}{4[m/2] + 2}. \tag{9.5}$$

This finishes the proof of the theorem. □

We finish this chapter with the following conjecture:

Conjecture 9.12 ([68], Conjecture 14). The number of lattice points on an arc of length $R^{1-\theta}$ on the circle with equation $x^2 + y^2 = R^2$ is bounded uniformly in R.

Exercises

9.1 (✠) Investigate the error term in the asymptotic formula of Theorem 9.4.

9.2 In this exercise we assume the reader is familiar with basic complex analysis.

a. Show that for each $s \in \mathbb{C}$ with $\Re s > 0$, the integral

$$\Gamma(s) := \int_0^\infty t^{s-1} e^{-t}\, dt$$

is absolutely convergent.

b. Show that the for all s with $\Re s > 0$ we have

$$\Gamma(s+1) = s\Gamma(s).$$

c. Conclude that the function $\Gamma(s)$, originally defined on $\Re s > 0$, has an analytic continuation to a meromorphic function on all of $\mathbb{C}$ with simple poles at $s = 0, -1, -2, -3, \ldots$. Compute the residues at the poles.

d. Show that $1/\Gamma(s)$ is entire.

e. Show that for each natural number n, $\Gamma(n) = (n-1)!$.

f. Show that for all s_1, s_2 with $\Re s_1, \Re s_2 > 0$, we have

$$\int_0^1 t^{s_1-1}(1-t)^{s_2-1}\, dt = \frac{\Gamma(s_1)\Gamma(s_2)}{\Gamma(s_1+s_2)}.$$

9.3 Find an easy function $f : \mathbb{N} \to \mathbb{C}$ which does not have an average value.

9.4 Compute the volume of the sphere of radius R in $\mathbb{R}^k$.

9.5 Compute the diameter of the unit hypercube in $\mathbb{R}^k$.

9.6 Prove Theorem 9.7.

9.7 Show that the function r_k for $k > 2$ does not have an average value. Find a continuous function $f : \mathbb{R} \to \mathbb{R}$ with the same average order as r_k.

9.8 Prove that for a triangle with side lengths a, b, c with area S which is inscribed in a circle of radius R we have

$$abc = 4RS.$$

9.9 Show that if a circle of radius r in $\mathbb{R}^2$ has three points A, B, C such that the distances AB, AC, BC are rational numbers, then r is a rational number.

9.10 Show that every circle in $\mathbb{R}^2$ with rational radius contains infinitely many points every two of which have rational distance.

9.11 Justify Equation (9.1).

9.12 Show that for all real numbers ξ, $|||\xi||| = |\xi + [\xi] - [2\xi]|$.

9.13 Show that for all real numbers ξ, η,

$$|||\xi + \eta||| \leq |||\xi||| + |||\eta|||.$$

9.14 Show that for all $\xi \in \mathbb{R}$ and $n \in \mathbb{Z}$, $|||n\xi||| \leq |n| \cdot |||\xi|||$.

9.15 Show that for all natural numbers n,

$$n \cdot |||n\sqrt{2}||| \geq 2 \cdot |||2\sqrt{2}||| = 6 - 4\sqrt{2}.$$

9.16 Show that the real numbers $1, \phi_2, \phi_3, \phi_5, \ldots$ appearing in the proof of Theorem 9.10 are linearly independent over the rational numbers.

9.17 Suppose β is a positive integer, and k a natural number. Show that for each choice of $\gamma_1, \ldots, \gamma_k$ such that for i, $|\gamma_i| \leq \beta$ and $\gamma_i \equiv \beta$ mod 2, we have

$$\sum_{1 \leq i < j \leq k} |\gamma_i - \gamma_j| \leq \frac{k^2 - \delta(k)}{2}\beta$$

where $\delta(k) = \begin{cases} 0 & k \text{ even;} \\ 1 & k \text{ odd.} \end{cases}$. Show that equality is attained if

a. k even: $k/2$ of the γ_i's are equal to β and the other $k/2$ are equal to $-\beta$;
b. k odd: $(k+1)/2$ of the γ_i's are equal to β and the remaining $(k-1)/2$ are equal to $-\beta$.

9.18 Prove inequality (9.5).

9.19 Show that for every natural number m there are infinitely many circles centered at the origin with precisely m integral points on their perimeters.

9.20 Show that for each natural number n, there are infinitely many circles in $\mathbb{R}^2$ which contain exactly n lattice points.

9.21 This problem is about the celebrated theorem of Georg Pick (1859–1942, Theresienstadt Concentration Camp). A simple proof of this theorem appears in [103].

a. Suppose T is a triangle in the plane all of whose vertices are lattice points. Let S be the area of the triangle, E the number of lattice points on the edges, and I the number of lattice points inside the triangle. Show that

$$S = I + \frac{1}{2}E - 1.$$

b. Prove Pick's theorem: Let P be a closed non self-intersecting polygon in $\mathbb{R}^2$ whose vertices are lattice points. Let S be the area, E the number of lattice points on the edges, and I the number of lattice points inside P. Then we have

$$S = I + \frac{1}{2}E - 1.$$

9.22 (✠) Investigate Question 9.11.

9.23 (✠) Do you believe Conjecture 9.12?

9.24 (✠) For each natural number n, consider the sphere S_n defined by

$$x^2 + y^2 + z^2 = n$$

in $\mathbb{R}^3$, and define $S_n(\mathbb{Z})$ to be the collection of points on S_n that have integral coordinates. If $(x, y, z) \in S_n(\mathbb{Z})$, then

$$(\frac{x}{\sqrt{n}}, \frac{y}{\sqrt{n}}, \frac{z}{\sqrt{n}}) \in S_1.$$

Investigate the distribution of the resulting points on the sphere S_1. Experiment with restricting the sequence of n's, e.g., squares, primes, etc.

Notes

Gauss' Circle Theorem

In Theorem 9.4 we showed that if we have a circle of radius r, then the number of lattice points inside the circle is $\pi r^2 + O(r)$. There is a famous conjecture [23, Section F1] asserting that the error term in Gauss' Circle Theorem is $O(r^{1/2+\epsilon})$ for any $\varepsilon > 0$. Richard Guy describes the problem of proving this conjecture as *very difficult*. The best result in this direction is due to Martin Huxley who around the year 2000 proved that the error is $O(r^{131/208})$ improving his own earlier result of $O(r^{46/73})$. Note that $46/73 - 131/208 = 0.000329....$