# Chapter 13
# How many Pythagorean triples are there?


In this chapter we determine an asymptotic formula for the number of primitive right triangles with bounded hypotenuse, giving a proof of a theorem of Lehmer from 1900. We start by relating the quantity we are interested in, namely the number of elements of the set

$$S(B) = \{(a, b, c) \in \mathbb{Z}^3 \mid a^2 + b^2 = c^2, \gcd(a, b, c) = 1, |a|, |b|, |c| \leq B\},$$

using our solution to the Pythagorean Equation, to the number of pairs of coprime integers satisfying certain conditions. Determining the latter number requires two inputs: an analogue of Gauss's Circle Theorem (Theorem 9.4) and a tool to ensure the coprimality of the integers; the tool we use to sieve out the non-coprime pairs is the function $\mu$ whose basic properties are collected in Lemmas 13.2 and 13.3. In the course of the proof we need to determine a quantity $C_2 = \sum_{\delta \text{ odd}} \mu(\delta)/\delta^2$. In §13.2 we show that the value $C_2$ is related to the value of the Riemann zeta function at 2, $\zeta(2)$, and explicitly calculate it. The main theorem of the chapter is Theorem 13.5. In the Notes to this chapter, we give some references for a conjecture of Manin that puts Lehmer's Theorem in a conceptual, geometric framework. The next item in the Notes is a disambiguation of the three number theorists with the last name of Lehmer (Hint: They were related!). The last part of the Notes is concerned with the Riemann zeta function, its analytic continuation, and the Riemann Hypothesis.

## 13.1 The asymptotic formula

It is clear that there are infinitely many right triangles with integer sides, but it still makes sense to obtain finer quantitative information about the set of right triangles. How many triples of integers $(a, b, c)$ are there such that $a^2 + b^2 = c^2$ and $|a|, |b|, |c|$ are bounded by a fixed number? What if we required that the numbers $a, b, c$ be coprime? For a positive real number $B$, we define



R. Takloo-Bighash, *A Pythagorean Introduction to Number Theory*,
Undergraduate Texts in Mathematics, https://doi.org/10.1007/978-3-030-02604-2_13

$$S(B) = \{(a, b, c) \in \mathbb{Z}^3 \mid a^2 + b^2 = c^2, \gcd(a, b, c) = 1, |a|, |b|, |c| \leq B\}.$$

and set $\mathcal{N}(B) = \#S(B)$. Can we find an exact formula for $\mathcal{N}(B)$? Or, in the absence of a useful explicit formula, can we study the behavior of the function, e.g., its asymptotic behavior as $B$ goes to infinity? And a related question, how many primitive right triangles are there with side lengths bounded by $B$? It will become clear in a moment that these questions are fairly easily tractable, and that one can give a beautiful formula describing the asymptotic behavior of the function $\mathcal{N}(B)$.

We start with some preliminary observations. By the proof of Theorem 3.1, if $(a, b, c) \in S(B)$, with $c > 0$, there are odd coprime integers $x, y$ such that

$$\begin{cases} a = \frac{x^2 - y^2}{2}; \\ b = xy; \\ c = \frac{x^2 + y^2}{2}, \end{cases}$$

if $a$ is even, and

$$\begin{cases} a = xy; \\ b = \frac{x^2 - y^2}{2}; \\ c = \frac{x^2 + y^2}{2}, \end{cases}$$

if $b$ is even. Also, since $|a|, |b|, |c| \leq |c|$, this means that we just need to require $(x^2 + y^2)/2 \leq B$. One needs to be careful about signs here. For examples, in these formulae $(x^2 + y^2)/2$ is always positive, whereas we wish to count *all* elements of $S(B)$. So, our first guess might be that $\mathcal{N}(B)$ is equal to

$$\mathcal{N}_1(B) = \#\{x, y \in \mathbb{Z} \mid x, y \text{ odd}, \gcd(x, y) = 1, x^2 + y^2 \leq 2B\}.$$

But this is not the whole story. For one, we need to multiply $\mathcal{N}_1(B)$ by 2 to account for the sign of $c$. Also, we need to multiply it by another factor of 2 to account for the odd and evenness of $a$ and $b$. But then we need to divide by 2, as changing $(x, y)$ to $(-x, -y)$ does not change the triple $(a, b, c)$. Consequently,

$$\mathcal{N}(B) = 2\mathcal{N}_1(B).$$

To study the function $\mathcal{N}_1(B)$ we introduce the related function

$$h(B) = \#\{(x, y) \neq (0, 0) \mid x, y \in \mathbb{Z}, \text{ odd}, \gcd(x, y) = 1, x^2 + y^2 \leq B\}.$$

Then clearly, $\mathcal{N}_1(B) = h(2B)$ and $\mathcal{N}(B) = 2h(2B)$.

To get an asymptotic formula for $h(B)$, first we relax the coprimality condition and define

$$\tilde{h}(B) = \#\{(x, y) \neq (0, 0) \mid x, y \in \mathbb{Z}, \text{ odd}, x^2 + y^2 \leq B\}.$$

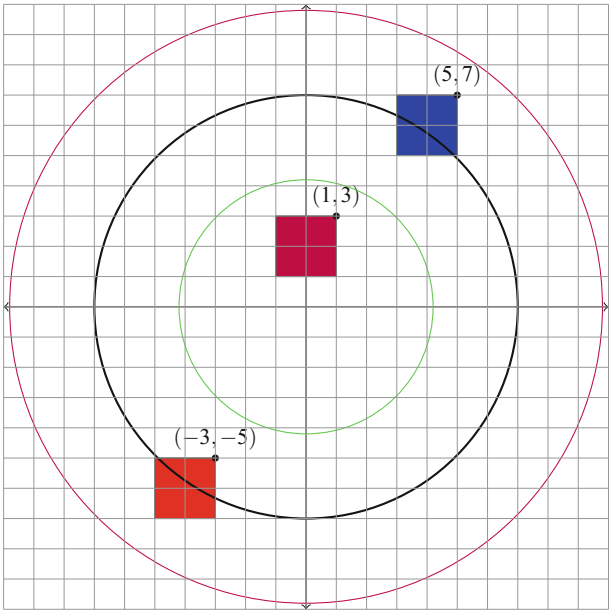


**Fig. 13.1** The diagram for the proof of Lemma 13.1

Then we have the following lemma:

**Lemma 13.1.** *As* $B \to \infty$,

$$\tilde{h}(B) = \frac{1}{4}\pi B + O(\sqrt{B}).$$

*Proof.* Our proof of this lemma is modeled on the proof of Theorem 9.4. In this case, for every integral point $(x, y)$ with $x, y$ inside the circle, we draw a $2 \times 2$ square whose upper right corner is $(x, y)$ as in Figure 13.1 with the point $(1, 3)$.

As in the proof of Theorem 9.4, not every square based on a point $(x, y)$ inside the circle will be completely within the circle, e.g., the red square whose upper right corner is the point $(-3, -5)$ is not entirely within the circle of radius 7; and also some integral points outside the circle of radius 7 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 $(5, 7)$. Since the diameter of a $2 \times 2$ square is $2\sqrt{2}$ and its area is 4, by emulating the proof of Theorem 9.4, we have

$$\pi(\sqrt{B} - 2\sqrt{2})^2 \leq 4\tilde{h}(B) \leq \pi(\sqrt{B} - 2\sqrt{2})^2.$$

This proves the lemma. □

We now relate the functions $h$ and $\tilde{h}$. Suppose $(x, y) \neq (0, 0)$ is an integral point such that $x^2 + y^2 \leq B$. Then we have

$$\left(\frac{x}{\gcd(x,y)}\right)^2+\left(\frac{y}{\gcd(x,y)}\right)^2\le\frac{B}{\gcd(x,y)^2}.$$

Clearly, if $x$, $y$ are odd numbers, $\gcd(x,y)$ is odd, and $\gcd(x/\gcd(x,y), y/\gcd(x,y)) = 1$. The map

$$(x,y)\mapsto(x/\gcd(x,y), y/\gcd(x,y))$$

establishes a one-to-one correspondence between the sets

$$\{(x,y)\neq(0,0)\mid x,y\in\mathbb{Z},\ \text{odd}, x^2+y^2\le B\}$$

and

$$\bigsqcup_{\delta\le B}\left\{(x,y)\neq(0,0)\mid x,y\in\mathbb{Z},\ \text{odd},\ \gcd(x,y)=1, x^2+y^2\le\frac{B}{\delta^2}\right\},$$

a disjoint union. As a result,

$$\tilde{h}(B)=\sum_{\substack{\delta^2\le B\\ \delta\ \text{odd}}}h\left(\frac{B}{\delta^2}\right).$$

We now express the function $h$ in terms of the function $\tilde{h}$. For $B<1$, $h(B)=0$. If $1\le B<9$, then since $\delta^2\le B$, with $\delta$ odd, means $\delta=1$, we see that

$$h(B)=\tilde{h}(B)$$

for $1\le B<9$. Next, let $9\le B<25$. Then

$$\tilde{h}(B)=h(B)+h\left(\frac{B}{9}\right).$$

Now we note that for $9\le B<25$, $1\le B/9<25/9<9$, and as a result $\tilde{h}(B/9)=h(B/9)$. Hence, for such $B$,

$$\tilde{h}(B)=h(B)-h\left(\frac{B}{9}\right).$$

We note that this formula is valid even if $B<9$, as in that case $B/9<1$, and $h(B/9)=0$. Now let's suppose $25\le B<49$. Then as before,

$$\tilde{h}(B)=h(B)+h\left(\frac{B}{9}\right)+h\left(\frac{B}{25}\right).$$

Since $1\le B/25<49/25<9$, we see that $\tilde{h}(\frac{B}{25})=h(\frac{B}{25})$. Also, $1\le B/9<16/9<4$, so again $\tilde{f}(\frac{B}{9})=f(\frac{B}{9})$. Hence, for $9\le B<16$ we have

$$h(B)=\tilde{h}(B)-\tilde{h}\left(\frac{B}{9}\right)-\tilde{h}\left(\frac{B}{25}\right).$$

Again, this identity is valid for all $1 \leq B < 49$. Further experimentation with intervals of the form $k^2 \leq B < (k+1)^2$ suggests that there should exist a function $u : \mathbb{N} \to \{+1, -1\}$ such that

$$h(B) = \sum_{\substack{\delta^2 \leq B \\ \delta \text{ odd}}} \tilde{h}\left(\frac{B}{\delta^2}\right) u(\delta).$$

Suppose for a moment that this is indeed true. Then we would have

$$\tilde{h}(B) = \sum_{\substack{\delta^2 \leq B \\ \delta \text{ odd}}} h\left(\frac{B}{\delta^2}\right) = \sum_{\substack{\delta^2 \leq B \\ \delta \text{ odd}}} \sum_{\substack{\eta^2 \leq B/\delta^2 \\ \eta \text{ odd}}} \tilde{h}\left(\frac{B/\delta^2}{\eta^2}\right) u(\eta)$$

$$= \sum_{\substack{\delta^2 \leq B \\ \delta \text{ odd}}} \sum_{\substack{\eta^2\delta^2 \leq B \\ \eta \text{ odd}}} \tilde{h}\left(\frac{B}{\delta^2\eta^2}\right) u(\eta).$$

Now we switch the order of summation by letting $\delta\eta = n$. It is clear that $n$ is odd and $n^2 \leq B$. Also, the $\eta$ summation is over all divisors of $n$. So the above sum is equal to

$$\sum_{n^2 \leq B} \tilde{h}\left(\frac{B}{n^2}\right) \sum_{\eta | n} u(\eta).$$

So, in order for the latter to be equal to $\tilde{h}(B)$ for all $B \geq 1$, it would be sufficient to find a function $u : \mathbb{N} \to \{+1, -1\}$ such that

$$\sum_{\eta | n} u(\eta) = \begin{cases} 1 & n = 1; \\ 0 & n > 1. \end{cases}$$

(For the purposes of the problem we are discussing here it is sufficient to define the function $u$ for odd numbers only, but this is a minor issue.) The interesting thing is that this last identity uniquely determines a function. In fact, it is clear that $u(1) = 1$. By setting $n = p$, a prime number, we see

$$u(1) + u(p) = 0$$

and, consequently, $u(p) = -1$. Next we try $n = pq$, with $p, q$ distinct prime numbers. We have

$$u(1) + u(p) + u(q) + u(pq) = 0.$$

This gives, $u(pq) = +1$. Similarly, $u(pqr) = -1$ with $p, q, r$ distinct primes. We can easily see using an easy inductive argument that if $p_1, \ldots, p_s$ are distinct prime numbers, then

$$u(p_1 \cdots p_s) = (-1)^s.$$

The function $u$ above is called the Möbius function, and it is usually denoted by $\mu(n)$. This is a very important function in analytic number theory. See the exercises

for the list of basic properties. In the sequel, we follow standard notation and use $\mu$ instead of $u$. We summarize this discussion as the following lemma:

**Lemma 13.2.** *If we define a function $\mu$ by*

$$\mu(n) = \begin{cases} 1 & n = 1; \\ (-1)^s & n = p_1 \cdots p_s, \text{ with } p_i \text{ distinct primes}; \\ 0 & n \text{ not square-free}, \end{cases}$$

*then for each natural number $n$*

$$\sum_{d|n} \mu(d) = \begin{cases} 1 & n = 1; \\ 0 & n \neq 1. \end{cases}$$

*Proof.* Exercise 13.1. □

Because of its importance we package the above discussion as the following lemma:

**Lemma 13.3.** *Suppose $F, G$ are functions defined on the set of positive real numbers. If for all $B > 0$,*

$$F(B) = \sum_{\substack{\delta \leq \sqrt{B} \\ \delta \text{ odd}}} G\left(\frac{B}{\delta^2}\right),$$

*then*

$$G(B) = \sum_{\substack{\delta \leq \sqrt{B} \\ \delta \text{ odd}}} F\left(\frac{B}{\delta^2}\right) \mu(\delta).$$

*Remark 13.4.* This lemma is still valid if we remove the oddness condition.

Now that we know how to express $h$ in terms of the function $\tilde{h}$, we can use Lemma 13.1 to find an asymptotic formula for the function $h$. By Lemma 13.3 and Lemma 13.1, we have

$$\begin{aligned} h(B) &= \sum_{\substack{\delta^2 \leq B \\ \delta \text{ odd}}} \tilde{h}\left(\frac{B}{\delta^2}\right) \mu(\delta) \\ &= \sum_{\substack{\delta^2 \leq B \\ \delta \text{ odd}}} \left(\frac{1}{4}\pi \frac{B}{\delta^2} + O(\sqrt{B/\delta^2})\right) \mu(\delta) \\ &= \frac{1}{4}\pi B \sum_{\substack{\delta^2 \leq B \\ \delta \text{ odd}}} \frac{\mu(\delta)}{\delta^2} + O\left(\sqrt{B} \sum_{\substack{\delta^2 \leq B \\ \delta \text{ odd}}} \frac{1}{\delta}\right). \end{aligned}$$

Note that we have replaced $O(\mu(\delta))$ by $O(1)$ in the last sum. We write the last sum as

$$= \frac{1}{4}\pi B \sum_{\substack{\delta=1 \\ \delta \text{ odd}}}^{\infty} \frac{\mu(\delta)}{\delta^2} - \frac{1}{4}\pi B \sum_{\substack{\delta^2 > B \\ \delta \text{ odd}}} \frac{\mu(\delta)}{\delta^2} + O\left(\sqrt{B} \sum_{\delta^2 \le B} \frac{1}{\delta}\right)$$

$$= \frac{1}{4}\pi B \sum_{\substack{\delta=1 \\ \delta \text{ odd}}}^{\infty} \frac{\mu(\delta)}{\delta^2} + O\left(B \sum_{\delta^2 > B} \frac{1}{\delta^2}\right) + O\left(\sqrt{B} \sum_{\delta^2 \le B} \frac{1}{\delta}\right).$$

By comparison with the convergent series $\sum_{\delta \ge 1} 1/\delta^2$ we see that the series $\sum_{\delta \text{ odd}} \mu(\delta)/\delta^2$ is convergent. Let's denote its value by $C_2$. We will calculate the exact value of $C_2$ in §13.2. Also,

$$\sum_{\delta^2 > B} \frac{1}{\delta^2} \le \int_{\sqrt{B}}^{\infty} \frac{dt}{t^2} \ll \frac{1}{\sqrt{B}},$$

and

$$\sum_{\delta^2 \le B} \frac{1}{\delta} \le \int_{1}^{\sqrt{B}} \frac{dt}{t} \ll \log B.$$

So we get

$$h(B) = \frac{1}{4}\pi C_2 B + O(\sqrt{B}) + O(\sqrt{B}\log B) = \frac{1}{4}\pi C_2 B + O(\sqrt{B}\log B). \quad (13.1)$$

We will show in §13.2 that $C_2 = 8/\pi^2$. Putting everything together, we get

**Theorem 13.5.** *As $B \to \infty$,*

$$\mathcal{N}(B) = \frac{4}{\pi} B + O(\sqrt{B}\log B)$$

**Corollary 13.6 (Lehmer, 1900).** *The number of primitive right triangles with hypotenuse bounded by $B$ is*

$$\frac{1}{2\pi} B + O(\sqrt{B}\log B)$$

*as $B \to \infty$.*

## 13.2 The computation of $C_2$

In this section we will prove the following identity:

$$C_2 = \frac{8}{\pi^2}.$$

In fact, we will prove a more general result. For each natural number $k \geq 1$, let

$$C_{2k} = \sum_{\substack{n=1 \\ n \text{ odd}}}^{\infty} \frac{\mu(n)}{n^{2k}},$$

and

$$\zeta(2k) = \sum_{n=1}^{\infty} \frac{1}{n^{2k}},$$

The series $\zeta(2k)$ is convergent absolutely, and comparison implies that $C_{2k}$ is absolutely convergent too.

**Lemma 13.7.** *For all natural numbers k,*

$$\left(1 - \frac{1}{2^{2k}}\right) C_{2k} \cdot \zeta(2k) = 1.$$

*Proof.* The first observation is that

$$\left(1 - \frac{1}{2^{2k}}\right) C_{2k} = \sum_{n=1}^{\infty} \frac{\mu(n)}{n^{2k}}.$$

Next, since all of our series are absolutely convergent we have

$$\left(1 - \frac{1}{2^{2k}}\right) C_{2k} \cdot \zeta(2k) = \sum_{n=1}^{\infty} \frac{\mu(n)}{n^{2k}} \sum_{m=1}^{\infty} \frac{1}{m^{2k}} = \sum_{n=1}^{\infty} \sum_{m=1}^{\infty} \frac{\mu(n)}{n^{2k} m^{2k}}$$

$$= \sum_{\delta=1}^{\infty} \sum_{mn=\delta} \frac{\mu(n)}{n^{2k} m^{2k}} = \sum_{\delta=1}^{\infty} \frac{1}{\delta^{2k}} \sum_{mn=\delta} \mu(n) = \sum_{\delta=1}^{\infty} \frac{1}{\delta^{2k}} \sum_{n|\delta} \mu(n).$$

Now by Lemma 13.2 whenever $\delta \neq 1$, the expression $\sum_{n|\delta} \mu(n)$ is equal to zero. Consequently, the only term that survives is $\delta = 1$, and the corresponding term is equal to 1. □

This means in order to compute $C_{2k}$ it suffices to compute $\zeta(2k)$.

The problem of computing the constant $\zeta(2)$, known as the *Basel Problem*, has a long history. Euler solved this problem in 1735 proving $\zeta(2) = \pi^2/6$. There are many proofs of this fact available in literature; see [64, 99]. Here we offer two proofs for Euler's identity using a product formula for the sine function. We will also suggest another approach using Fourier series in Exercise 13.20.

The starting point of both arguments is the infinite product formula

$$\sin z = z \prod_{n=1}^{\infty} \left(1 - \frac{z^2}{n^2 \pi^2}\right) \tag{13.2}$$

for the function $\sin z$; see [1, Ch. 5, §2.3].

We now give the first proof. We write the Taylor expansion of $\sin z/z$ to obtain

$$\sum_{k=0}^{\infty}(-1)^k\frac{z^{2k}}{(2k+1)!}=\prod_{n=1}^{\infty}\left(1-\frac{z^2}{n^2\pi^2}\right)$$

If we equate the coefficients of $z^2$ we obtain

$$-\frac{1}{6}=-\sum_{n=1}^{\infty}\frac{1}{n^2\pi^2}.$$

Consequently,

$$\zeta(2)=\sum_{n=1}^{\infty}\frac{1}{n^2}=\frac{\pi^2}{6}.$$

In the second proof we actually compute $\zeta(2k)$ for all $k\in\mathbb{N}$. Again we use the formula (13.2). Take the logarithm of both sides to obtain

$$\log\sin z=\log z+\sum_{n=1}^{\infty}\log\left(1-\frac{z^2}{n^2\pi^2}\right).$$

Differentiating gives

$$\begin{aligned}\frac{\cos z}{\sin z}&=\frac{1}{z}+\sum_{n=1}^{\infty}\frac{\frac{-2z}{n^2\pi^2}}{1-\frac{z^2}{n^2\pi^2}}\\&=\frac{1}{z}+\sum_{n=1}^{\infty}\frac{-2z}{n^2\pi^2}\sum_{k=0}^{\infty}\frac{z^{2k}}{n^{2k}\pi^{2k}}\\&=\frac{1}{z}-2\sum_{k=0}^{\infty}\frac{z^{2k+1}}{\pi^{2k+2}}\sum_{n=1}^{\infty}\frac{1}{n^{2k+2}}.\end{aligned}$$

Consequently,

$$z\frac{\cos z}{\sin z}=1-2\sum_{k=1}^{\infty}\frac{\zeta(2k)}{\pi^{2k}}z^{2k}. \tag{13.3}$$

On the other hand, by Theorem A.1

$$\cos z=\frac{e^{iz}+e^{-iz}}{2}$$

and

$$\sin z=\frac{e^{iz}-e^{iz}}{2i}.$$

So we have

$$z\frac{\cos z}{\sin z}=iz\frac{e^{iz}+e^{-iz}}{e^{iz}-e^{-iz}}=\frac{2iz}{e^{2iz}-1}+iz. \tag{13.4}$$

The function $t/(e^t - 1)$ whose value at $2iz$ appears in the above expression has a particularly well-known Taylor expansion with a long history. We define the *Bernoulli numbers* $B_m$, for $m \geq 0$, by

$$\frac{t}{e^t - 1} = \sum_{m=0}^{\infty} B_m \frac{t^m}{m!}.$$

It is not hard to see that $B_1 = -1/2$, and that for odd $m > 1$, $B_m = 0$. The first few non-zero $B_m$'s are $B_0 = 1$, $B_2 = 1/6$, $B_4 = -1/30$, $B_6 = 1/42$, .... Furthermore, for all $m$, $B_m$ is rational. See the exercises for more properties.

Going back to (13.4) we find that

$$z\frac{\cos z}{\sin z} = iz + \sum_{m=0}^{\infty} B_m \frac{(2iz)^m}{m!} = 1 + \sum_{k=1}^{\infty} (-1)^k \frac{2^{2k} B_{2k}}{(2k)!} z^{2k}.$$

Comparing this last expression with (13.3) gives:

**Theorem 13.8.** *For all natural numbers $k$,*

$$\zeta(2k) = (-1)^{k-1} \frac{2^{2k-1} B_{2k}}{(2k)!} \pi^{2k}.$$

Lemma 13.7 implies

**Corollary 13.9.** *With $C_2$ as above,*

$$C_2 = \frac{8}{\pi^2}.$$

## Exercises

13.1 Prove Lemma 13.2.

13.2 Prove Corollary 13.6.

13.3 An *arithmetic function* is a function $f : \mathbb{N} \to \mathbb{C}$. For arithmetic functions $f, g$, we define the arithmetic function $f * g$ by

$$(f * g)(n) = \sum_{d|n} f(d) g(\frac{n}{d}).$$

Show that for all arithmetic functions $f, g, h$ we have the following properties:

a. $f * (g * h) = (f * g) * h$;
b. $f * g = g * f$;
c. If $e(n) = \delta_{n0}$, Kronecker's delta, then $f * e = e * f = f$. Note that

$$e(n) = \begin{cases} 1 & n = 1; \\ 0 & n \neq 1. \end{cases}$$

13.4 Prove the claim in Remark 13.4.

13.5 (✠) Investigate the error term in Lemma 13.1.

13.6 (✠) Numerically verify the assertion of Theorem 13.5 and Corollary 13.6. Investigate the error terms in these results.

13.7 Define a function $\mathbf{1}$ by $\mathbf{1}(n) = 1$ for all $n$. Show that $\mathbf{1} * \mu = e$. Prove the *Möbius Inversion Formula*: If $f(n) = \sum_{d|n} g(d)$, then $g(n) = \sum_{d|n} \mu(d) f(\frac{n}{d})$.

13.8 Show that $\sum_{d|n} \varphi(d) = n$. Use this relation to derive a formula for the $\varphi$-function.

13.9 An arithmetic function $f$ is called *multiplicative* if for every $m, n$ with $\gcd(m, n) = 1$ we have $f(mn) = f(m)f(n)$. Show that if $f, g$ are multiplicative, then so is $f * g$.

13.10 For a natural number $n$ set $\sigma(n) = \sum_{d|n} d$. Find a formula for $\sigma(n)$ in terms of the prime factorization of $n$.

13.11 Show that for all $a, b \in \mathbb{N}$ with $a, b > 1$ we have

$$\frac{\sigma(a)}{a} < \frac{\sigma(ab)}{ab} < \frac{\sigma(a)\sigma(b)}{ab}.$$

13.12 Show that for $a, b > 1$,

$$\sigma(ab) > 2\sigma(a)^{1/2}\sigma(b)^{1/2}.$$

13.13 Show that for all $a, b \in \mathbb{N}$,

$$\sigma(a)\sigma(b) = \sum_{d|\gcd(a,b)} d\sigma\left(\frac{ab}{d^2}\right).$$

In particular, $\sigma$ is a multiplicative function.

13.14 Find an asymptotic formula for

$$\sum_{\substack{a,b \leq X \\ \gcd(a,b)=1}} ab$$

as $X \to \infty$.

13.15 Find an asymptotic formula for

$$\sum_{n \leq X} \varphi(n)$$

as $X \to \infty$.

13.16 Prove the following statement: Let $(c_n)_n$ be a sequence of complex numbers, and $f : [1, \infty) \to \mathbb{C}$ a function with continuous derivative. Then

$$\sum_{n\le x} c_n f(n) = \left(\sum_{n\le x} c_n\right) f(x) - \int_1^x \left(\sum_{n\le t} c_n\right) f'(t)\,dt.$$

13.17 Show

$$\sum_{d\le x} \frac{1}{d} = \log x + O(1).$$

13.18 Recall the notion of *average order* from Definition 9.3.

a. Let $d(n)$ be the number of divisors of $n$. Show that

$$\sum_{k\le n} d(k) = \sum_{k\le n} \left[\frac{n}{k}\right].$$

Conclude that $d(n)$ has average order $\log x$;

b. Let $\phi(n)$ be the Euler totient function. Show that the average order of $\phi(n)$ is $\zeta(2)x$;

c. Let $\omega(n)$ be the number of distinct prime divisors of $n$. Show that the average order of $\omega(n)$ is $\log\log x$.

13.19 Find a multiplicative function $f$ such that

$$\sum_{d|n} \frac{\mu(d)d^2 f(n/d)}{\phi(d)} = \sigma(n) f(n), \quad n \in \mathbb{N}.$$

13.20 Use Parseval's formula [41, Theorem 8.16] applied to the function $f(x) = x$ on the interval $[0, 1]$ to give another proof for Euler's identity, $\zeta(2) = \pi^2/6$.

13.21 Pick two natural numbers at random. What is the probably that they are coprime?

13.22 Prove that for each natural number $r$,

$$B_r = -\sum_{k=0}^{r-1} \binom{r}{k} \frac{B_k}{r-k+1}.$$

Use this relation to find the first few Bernoulli numbers.

13.23 Show that all Bernoulli numbers are rational.

13.24 Show that for each natural number $r$, $B_{2r+1} = 0$.

13.25 Find an asymptotic formula for the number of primitive right triangles with perimeter bounded by $X$ as $X \to \infty$.

## Notes

### *Lehmer's theorem and Manin's conjecture*

Lehmer [83] published a different proof of Corollary 13.6 in 1900. The argument we present here shows that any power saving improvement in the error term of Lemma 13.1 would improve the error terms in Theorem 13.5 and Corollary 13.6 to $O(\sqrt{B})$. The quantity considered in Corollary 13.6 appears in the *Online Encyclopedia of Integer Sequences*:

http://oeis.org/A156685

The question of counting integral solutions with bounded size to algebraic equations with infinitely many solutions is a very active area of research of current interest. Theorem 13.5 has now been greatly generalized. Yuri Manin has formulated several conjectures that connect the arithmetic features of some classes of equations where one expects a lot of solutions to the geometry of the resulting solution sets; see [104] for various questions and conjectures.

### *A family of number theorists*

The Lehmer of Corollary 13.6 is Derrick Norman Lehmer (July 27, 1867–September 8, 1938). He was the father of Derrick Henry Lehmer (February 23, 1905–May 22, 1991) who was a mathematician credited with many contributions to number theory. D. H. Lehmer was married to Emma Markovna Lehmer (née Trotskaia) (November 6, 1906–May 7, 2007) who was a number theorist herself with over 50 publications to her name, [84]. There have been several other families of mathematicians in history, most notably the Bernoulli family. And here is a joke: What was the most influential mathematician family in history? Clearly Gauss's family, because it doesn't matter what the rest of his family did.

### *The Riemann zeta function*

The complex function

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$$

is called the *Riemann zeta function*. This series converges absolutely for $\Re s > 1$. Riemann was certainly not the first person to study this function. In fact, by the time of the publication of Riemann's work in 1859 various mathematicians, Euler in particular, had studied the values of the zeta function for integer values of $s$ for at least two centuries; see [109] for a survey. The problem of computing $\zeta(2)$ which we

discussed in this chapter was posed by Pietro Mengoli in 1650 and solved by Euler in 1735. Riemann, in a spectacular paper [93], proved the analytic continuation of the zeta function, proved the functional equation, discussed the connection to the distribution of prime numbers, and formulated a conjecture about prime numbers, nowadays known as the *Riemann Hypothesis*.

First a word about analytic continuation. Suppose we have a function $f(s)$ which is holomorphic on an open subset $U$ of complex numbers, and suppose $V$ is an open set in $\mathbb{C}$ containing $U$. We call a function $g$, holomorphic on $V$, the *analytic continuation* of $f$ if the restriction of $g$ to $U$ is equal to $f$. It is not terribly hard to show that for $\Re s > 1$ we have

$$\zeta(s) = s \int_1^\infty \frac{[x]}{x^{s+1}}\, dx = \frac{s}{s-1} - s \int_1^\infty \frac{\{x\}}{x^{s+1}}\, dx.$$

The expression on the right-hand side is meromorphic on $\Re s > 0$ with a simple pole at $s = 1$, however, and this provides an analytic continuation for $\zeta(s)$ to a larger domain. But this is not where the analytic continuation stops. In fact, if we set

$$\xi(s) = s(s-1)\pi^{-s/2}\Gamma\left(\frac{s}{2}\right)\zeta(s),$$

then Riemann showed that $\xi(s)$ is holomorphic on $\Re s > 0$ and

$$\xi(1-s) = \xi(s). \tag{13.5}$$

Since $\xi(s)$ is holomorphic for $\Re s > 0$, and $\xi(1-s)$ is holomorphic for $\Re(1-s) > 0$, i.e., $\Re s < 1$, we obtain the holomorphy of $\xi(s)$ on the entire set of complex numbers. This further shows that $\zeta(s)$ has an analytic continuation to the entire complex plane to a meromorphic function with a unique simple pole at $s = 1$ with residue 1. Since we already have computed the value of $\zeta(s)$ for even positive integers $2k$, we can use the functional equation (13.5) to compute the values of the *analytic continuation* of $\zeta(s)$ for odd negative numbers. In fact, for $n \in \mathbb{N}$,

$$\zeta(1-2n) = -\frac{B_{2n}}{2n}.$$

For example, $\zeta(-1) = -1/12$. One can similarly compute the value of $\zeta(0)$ to be $-1/2$. Again, we should emphasize that these are the values of the analytically continued function, and they should not be taken to mean

$$1 + 1 + 1 + \cdots = -\frac{1}{2},$$

or

$$1 + 2 + 3 + \cdots = -\frac{1}{12}.$$

Let us illustrate what is happening here with an easy example. Suppose $U = \{s \in \mathbb{C} \mid |s| < 1\}$ and $f(s) = \sum_{k=0}^{\infty} s^k$. The series defining $f$ is absolutely convergent on $U$ and defines a holomorphic function there. By general properties of geometric series, for $|s| < 1$, we have

$$f(s) = \frac{1}{1-s}.$$

The function $g(s) = 1/(1-s)$ is holomorphic on the much larger domain $V = \{s \in \mathbb{C} \mid s \neq 1\}$. Note that outside the open set $U$ the function $g(s)$ is not given by the original series defining $f(s)$. This important point is the source of many paradoxes in the theory of infinite series. For example, the value of the function $g(s)$ at $s = 2$ is equal to $-1$. If we set $s = 2$ in the formula for $f(s)$ we formally get

$$1 + 2 + 4 + 8 + 16 + 32 + 64 + \ldots$$

Does this then mean

$$1 + 2 + 4 + 8 + 16 + 32 + 64 + \cdots = -1?$$

Absolutely not! In fact the series defining $f(s)$ is not even defined for $s = 2$.

We now turn to the connections between the zeta function and the distribution of prime numbers. Euler observed the product formula that now bears his name: For $\Re s > 1$ we have

$$\zeta(s) = \prod_{p \text{ prime}} \frac{1}{1 - p^{-s}}.$$

If we use this formula to compute $(d/ds) \log \zeta(s)$ we obtain

$$-\frac{\zeta'(s)}{\zeta(s)} = \sum_{k \geq 1} \sum_{p \text{ prime}} \frac{\log p}{p^{ks}} = \sum_{n=1}^{\infty} \frac{\Lambda(n)}{n^s}, \tag{13.6}$$

with $\Lambda(n)$ being the *von Mangoldt function* defined by

$$\Lambda(n) = \begin{cases} \log p & n = p^k, \, p \text{ prime}; \\ 0 & \text{otherwise.} \end{cases}$$

An idea that Riemann brought into this subject was *contour integration*. For a complex function $f(s)$ and a real number $c$ let us define

$$\int_{(c)} f(s)\, ds = \lim_{R \to \infty} \int_{c - iR}^{c + iR} f(s)\, ds.$$

Fix a real number $c > 1$. A contour integration computation shows that for $x > 1$, non-integer,

$$\sum_{n < x} \Lambda(n) = \frac{1}{2\pi i} \int_{(c)} \left( -\frac{\zeta'(s)}{\zeta(s)} \right) \frac{x^s}{s}\, ds.$$

The function $-\zeta'(s)/\zeta(s)$ has a simple pole at $s = 1$ with residue 1. Suppose we can shift the contour back to $(c')$, for a number $c' < 1$. Then we would obtain

$$\sum_{n<x} \Lambda(n) = x + \frac{1}{2\pi i} \int_{(c')} \left( -\frac{\zeta'(s)}{\zeta(s)} \right) \frac{x^s}{s}\, ds. \tag{13.7}$$

Riemann's idea then was to prove that this last integral contributes less than $x$ to the formula, and hence obtain

$$\sum_{n<x} \Lambda(n) \sim x, \quad x \to \infty. \tag{13.8}$$

Exercise 13.16 can now be used to prove

$$\#\{p \le x\} \sim \frac{x}{\log x} \tag{13.9}$$

which is the celebrated *Prime Number Theorem*, conjectured by Gauss. Also, knowing the specific value of $c'$ would lead to error estimates for the Prime Number Theorem. So, the question that Riemann was faced with was to determine how far back the contour could be moved. In general, the logarithmic derivative of a meromorphic function has poles whenever the function has poles or zeros. In particular in order to know the poles of $\zeta'(s)/\zeta(s)$ we need to know where the function $\zeta(s)$ is zero. Riemann computed several zeros of the zeta function in the domain $\Re s > 0$ and observed that they are all on the line $\Re s = 1/2$, and conjectured that this would be the case for all zeros. If one assumes the Riemann Hypothesis, then it follows that

$$\#\{p \le x\} = \operatorname{Li} x + O(x^{1/2+\varepsilon})$$

for all $\varepsilon > 0$, with

$$\operatorname{Li} x = \int_2^x \frac{dt}{\log t}.$$

At present, the Riemann Hypothesis appears out of reach.

Titchmarsh's classic [52] is a much recommended, comprehensive introduction to the theory of the Riemann zeta function.