LECTURE NOTES

KARL DILCHER

Lecture 1

1. Continued Fractions

1.1. **Introduction.** Let me begin with the expression

$$1+\cfrac{1}{1+\cfrac{1}{1+\cfrac{1}{1+\cfrac{1}{1+\cfrac{1}{1+\ddots}}}}} \tag{1.1}$$

which you may find rather curious. This first obvious questions that arise are: What is this? How is this to be interpreted? And given that this is apparently an infinite object, does this make sense at all?

Let us for a moment assume that this object represents a well-defined quantity, and denote it by x. Now note that the above expression is "self-replicating", in the sense that we have

$$x = 1 + \frac{1}{x}.$$

If we multiply both sides of this by x, we obtain the quadratic equation

$$x^2 - x - 1 = 0,$$

which has the two solutions

$$\frac{1+\sqrt{5}}{2}, \quad \frac{1-\sqrt{5}}{2}.$$

The second solution is negative, while one may assume that the object (5.1) represents (if anything) something positive. So we come to the conclusion that

$$x = \frac{1+\sqrt{5}}{2}.$$

You may recognize this number as the *golden mean* which is closely related to the *Fibonacci numbers*.

The purpose of this lecture is to give all this some meaning, and to put it on a firm foundation. In the process it will turn out that what we did above is indeed correct, and that there is a close connection to Fibonacci and related number sequences. You will also see that this is more than just a curiosity.

For representing (i.e., just "writing down") arbitrary real numbers, continued fractions present an alternative to the decimal representation. In addition to some

basic properties, in this lecture you will see that continued fractions enable us to find the best rational approximation of a given real number.

1.2. **Finite continued fractions.** Given the fraction $\frac{u_0}{u_1}$ with $(u_0, u_1) = 1$ and $u_1 > 0$, we use the Euclidean algorithm:

$$\begin{aligned} u_0 &= u_1a_0 + u_2, && 0 < u_2 < u_1 \\ u_1 &= u_2a_1 + u_3, && 0 < u_3 < u_2 \\ &\vdots \\ u_{j-1} &= u_ja_{j-1} + u_{j+1}, && 0 < u_{j+1} < u_j \\ u_j &= u_{j+1}a_j. \end{aligned}$$

If we write $q_i := \frac{u_i}{u_{i+1}}$, $0 \le i \le j$, then

$$\begin{aligned} q_i &= a_i + \frac{1}{q_{i+1}}, \quad 0 \le i \le j-1, \\ q_j &= a_j. \end{aligned}$$

Example: Start with 67/24. Then

$$\begin{aligned} 67 &= 2 \cdot 24 + 19, & \tfrac{67}{24} &= 2 + \tfrac{19}{24}; \\ 24 &= 1 \cdot 19 + 5, & \tfrac{24}{19} &= 1 + \tfrac{5}{19}; \\ 19 &= 3 \cdot 5 + 4, & \tfrac{19}{5} &= 3 + \tfrac{4}{5}; \\ 5 &= 1 \cdot 4 + 1, & \tfrac{5}{4} &= 1 + \tfrac{1}{4}. \end{aligned}$$

Substituting each equation in the second column into the one above, we obtain the expression

$$\frac{67}{24} = 2 + \cfrac{1}{1 + \cfrac{1}{3 + \cfrac{1}{1 + \cfrac{1}{4}}}}$$

Such an expression is called a *finite continued fraction*. In general,

$$\frac{u_0}{u_1} = q_0 = a_0 + \cfrac{1}{a_1 + \ddots + \cfrac{1}{a_{j-1} + \cfrac{1}{a_j}}} \tag{1.2}$$

The a_i are called *partial quotients*. a_0 may be positive, negative, or zero. Since $0 < u_2 < u_1$, we have $a_1 > 0$. Similarly, $a_2, a_3, \ldots, a_j$ are also positive integers.

Notation: We denote the continued fraction (1.2) by

$$\langle a_0, a_1, \ldots, a_j \rangle.$$

Remarks. (1) We have

$$\langle a_0, a_1, \ldots, a_j \rangle = a_0 + \frac{1}{\langle a_1, a_2, \ldots, a_j \rangle}. \tag{1.3}$$

(2) In greater generality than in (1.2), let $x_0, x_1, \ldots, x_j$ be any *real* numbers, with $x_1, \ldots, x_j > 0$. Then we can define

$$\langle x_0, x_1, \ldots, x_j \rangle = x_0 + \cfrac{1}{x_1 + \ddots + \cfrac{1}{x_{j-1} + \cfrac{1}{x_j}}}$$

If all the x_i are positive integers (with x_0 allowed to be negative or zero), the continued fraction is said to be *simple*. In this course we will only be dealing with simple continued fractions. However, the *analytic theory* of continued fractions is also a fascinating and important subject; you can read more about it, e.g., in the classical book [7].

For the remainder of this section we will be concerned with the uniqueness of finite continued fractions. We begin with the following simple example:

$$\frac{51}{22} = 2 + \cfrac{1}{3 + \cfrac{1}{7}} = 2 + \cfrac{1}{3 + \cfrac{1}{6 + \cfrac{1}{1}}}$$

This obvious lack of uniqueness, which can always be created, is easy to avoid if we require the final partial quotient to be greater than 1, namely $a_j > 1$. If this is done, we have the following result:

Theorem 1.1. *If*

$$\langle a_0, a_1, \ldots, a_j \rangle = \langle b_0, b_1, \ldots, b_n \rangle$$

are simple continued fractions and if $a_j > 1$ and $b_n > 1$ then $j = n$ and $a_i = b_i$ for $i = 0, 1, \ldots, n$.

Proof. We set $y_i := \langle b_i, b_{i+1}, \ldots, b_n \rangle$ and observe that

$$y_i = b_i + \frac{1}{\langle b_{i+1}, b_{i+2}, \ldots, b_n \rangle} = b_i + \frac{1}{y_{i+1}}.$$

Hence $y_i > b_i$ and

$$\begin{aligned} y_i &> 1 \quad \text{for} \quad i = 1, 2, \ldots, n-1, \\ y_n &= b_n > 1, \end{aligned}$$

which means that

$$b_i = \lfloor y_i \rfloor \quad \text{for all} \quad i = 1, 2, \ldots, n.$$

Let the q_i be defined as in the beginning of this section. By hypothesis we have $y_0 = q_0$, and we saw before that

$$q_i = a_i + \frac{1}{q_{i+1}}.$$

By definition we have $q_i = \frac{u_i}{u_{i+1}} > 1$ for all $i \geq 1$, hence

$$a_i = \lfloor q_i \rfloor \quad \text{for all} \quad i = 0, 1, \ldots, j.$$

Now we proceed by induction.

(i) $y_0 = q_0$ implies $b_0 = \lfloor y_0 \rfloor = \lfloor q_0 \rfloor = a_0$.

(ii) $\frac{1}{q_1} = q_0 - a_0 = y_0 - b_0 = \frac{1}{y_1}$

(iii) Now we make the assumption that $q_i = y_i$, $a_i = b_i$. Then

$$\frac{1}{q_{i+1}} = q_i - a_i = y_i - b_i = \frac{1}{y_{i+1}},$$

i.e., $q_{i+1} = y_{i+1}$, which implies

$$a_{i+1} = \lfloor q_{i+1} \rfloor = \lfloor y_{i+1} \rfloor = b_{i+1}.$$

This proves by induction that the partial quotients are unique. It remains to show that $j = n$. To obtain a contradiction, we suppose that $j < n$. Then we have, from above, that $q_j = y_j$ and $a_j = b_j$. But $q_j = a_j$ (last element), while $y_j > b_j$ (not the last element), and this is a contradiction. Similarly for $j > n$. Hence $j = n$, and we are done. □

The following result is an easy consequence; it shows how rational numbers are characterized by continued fractions.

Theorem 1.2. *Any finite continued fraction represents a rational number. Conversely, any rational number can be expressed as a finite simple continued fraction in a unique way.*

Proof. (1) Use the formula (1.3) repeatedly; it terminates after a finite number of steps.

(2) The second part follows from Euclid's algorithm, as developed at the beginning of this section. Uniqueness follows from Theorem 1.1. □

1.3. **Infinite continued fractions.** In this section we will give meaning to continued fractions such is the introductory example (1.1). As is the case with all infinite objects, we have to proceed quite carefully.

Let $a_0, a_1, a_2, \ldots$ be an infinite sequence of integers, all positive, with the possible exception of a_0. We define the two sequences $\{h_n\}$, $\{k_n\}$ by

$$h_{-2} = 0, \quad h_{-1} = 1, \quad h_i = a_i h_{i-1} + h_{i-2} \quad (i \geq 0); \tag{1.4}$$

$$k_{-2} = 1, \quad k_{-1} = 0, \quad k_i = a_i k_{i-1} + k_{i-2} \quad (i \geq 0). \tag{1.5}$$

It follows immediately that $k_0 = 1$, $k_1 = a_1 k_0 \geq k_0$, $k_2 > k_1$, $k_3 > k_2, \ldots$, in other words,

$$1 \leq k_1 < k_2 < k_3 < \ldots < k_n < \ldots \tag{1.6}$$

With the help of these two recurrence sequences we can write a finite continued fraction as a plain fraction:

Theorem 1.3. *For any $x \in \mathbb{R}$, $x > 0$, we have*

$$\langle a_0, a_1, \ldots, a_{n-1}, x \rangle = \frac{x h_{n-1} + h_{n-2}}{x k_{n-1} + k_{n-2}}.$$

Proof. We prove this by induction. For $n = 0$ the statement reduces to

$$x = \frac{x h_{-1} + h_{-2}}{x k_{-1} + k_{-2}},$$

which follows immediately from (1.4) and (1.5). For $n = 1$, the result is

$$\langle a_0, x \rangle = \frac{x h_0 + h_{-1}}{x k_0 + k_{-1}};$$

this is again easy to verify, using the fact that $\langle a_0, x \rangle = a_0 + \frac{1}{x}$.

Now we assume that the result holds for $\langle a_0, a_1, \ldots, a_{n-1}, x\rangle$. Then

$$\begin{aligned}\langle a_0, a_1, \ldots, a_{n-1}, a_n, x\rangle &= \langle a_0, a_1, \ldots, a_{n-1}, a_n + \tfrac{1}{x}\rangle \\ &= \frac{\left(a_n + \frac{1}{x}\right) h_{n-1} + h_{n-2}}{\left(a_n + \frac{1}{x}\right) k_{n-1} + k_{n-2}} \\ &= \frac{x(a_n h_{n-1} + h_{n-2}) + h_{n-1}}{x(a_n k_{n-1} + k_{n-2}) + k_{n-1}} \\ &= \frac{x h_n + h_{n-1}}{x k_n + k_{n-1}},\end{aligned}$$

where we have used the recurrence relations (1.4) and (1.5). This completes the proof by induction. □

As a special case we obtain:

Theorem 1.4. *If $r_n := \langle a_0, a_1, \ldots, a_n\rangle$ for $n \geq 0$, then $r_n = \frac{h_n}{k_n}$.*

Proof. Use Theorem 1.3, and replace x by a_n:

$$r_n := \langle a_0, a_1, \ldots, a_n\rangle = \frac{a_n h_{n-1} + h_{n-2}}{a_n k_{n-1} + k_{n-2}} = \frac{h_n}{k_n},$$

where the last equation follows again by the recurrence relations (1.4) and (1.5). □

The following theorem is a collection of properties of the three new sequences we have defined so far, all based on the given sequence $\{a_n\}$.

Theorem 1.5. (*i*) *For $i \geq 1$,*

$$h_i k_{i-1} - h_{i-1} k_i = (-1)^{i-1}, \tag{1.7}$$

$$r_i - r_{i-1} = \frac{(-1)^{i-1}}{k_i k_{i-1}}. \tag{1.8}$$

(*ii*) *For $i \geq 2$,*

$$h_i k_{i-2} - h_{i-2} k_i = (-1)^i a_i, \tag{1.9}$$

$$r_i - r_{i-2} = \frac{(-1)^i a_i}{k_i k_{i-2}}. \tag{1.10}$$

(*iii*) *The fraction $\frac{h_i}{k_i}$ is reduced, i.e., $(h_i, k_i) = 1$.*

Proof. (i) We prove (1.7) by induction. By (1.4) and (1.5) we have

$$h_{-1} k_{-2} - h_{-2} k_{-1} = 1,$$

which is our induction beginning. We assume now that we have

$$h_{i-1} k_{i-2} - h_{i-2} k_{i-1} = (-1)^{i-2}.$$

Again using (1.4) and (1.5), we have

$$\begin{aligned} h_i k_{i-1} - h_{i-1} k_i &= (a_i h_{i-1} + h_{i-2}) k_{i-1} - h_{i-1}(a_i k_{i-1} + k_{i-2}) \\ &= -(h_{i-1} k_{i-2} - h_{i-2} k_{i-1}) \\ &= -(-1)^{i-2} = (-1)^{i-1}.\end{aligned}$$

This completes the proof of (1.7). To obtain (1.8), we divide both sides of (1.7) by $k_i k_{i-1}$:

$$\frac{h_i}{k_i} - \frac{h_{i-1}}{k_{i-1}} = \frac{(-1)^{i-1}}{k_i k_{i-1}};$$

identity (1.8) now follows from the definition of r_i.

(ii) Exercise. (Proceed as in the proof of (i)).

(iii) If $d \mid h_i$ and $d \mid k_i$ then (1.7) implies that $d \mid (-1)^{i-1}$. Hence $d = 1$. □

The following limit results are the key to putting infinite continued fractions on a firm foundation. The numbers r_n are as defined in Theorem 1.4.

Theorem 1.6. (*i*) *We have the chain of inequalities*

$$r_0 < r_2 < r_4 < r_6 < \ldots < r_7 < r_5 < r_3 < r_1.$$

(*ii*) $\lim_{n\to\infty} r_n$ *exists, and for all* $j \geq 0$ *we have*

$$r_{2j} < \lim_{n\to\infty} r_n < r_{2j+1}.$$

Proof. By (1.8) and (1.10) we have

$$r_{2j} < r_{2j+2}, \quad r_{2j-1} > r_{2j+1}, \quad r_{2j} < r_{2j-1},$$

since $k_i > 0$ for $i \geq 0$ and $a_i > 0$ for $i \geq 1$. Hence

$$r_0 < r_2 < r_4 < \ldots, \quad \text{and} \quad r_1 > r_3 > r_5 > \ldots$$

and also

$$r_{2n} < r_{2n+2j} < r_{2n+2j-1} \leq r_{2j-1}.$$

This proves part (i).

(ii) The sequence $\{r_0, r_2, \ldots\}$ is monotonically increasing and bounded above by r_1; hence it has a limit. Similarly, the sequence $\{r_1, r_3, \ldots\}$ is monotonically decreasing and bounded below by r_0, so it also has a limit.

Now, according to (1.8) we have $r_i - r_{i-1} \to 0$ as $i \to \infty$ since the integers k_i form a strictly increasing sequence by (1.6). Hence the two limits in question are equal. □

Definition 1.7. *Let* $a_0, a_1, a_2, \ldots$ *be an infinite sequence of integers with* $a_j > 0$ *for* $j \geq 1$. *Then the infinite simple continued fraction* $\langle a_0, a_1, a_2, \ldots\rangle$ *is defined by*

$$\lim_{n\to\infty} \langle a_0, a_1, \ldots a_n\rangle.$$

Remark. The rational number

$$\langle a_0, a_1, \ldots a_n\rangle = r_n = \frac{h_n}{k_n}$$

is called the nth *convergent* of the infinite continued fraction. (This is also defined for finite continued fractions.)

Theorem 1.8. *The value of any infinite simple continued fraction* $\langle a_0, a_1, a_2, \ldots\rangle$ *is irrational.*

Proof. Let $\theta := \langle a_0, a_1, a_2, \ldots\rangle$. Then by Theorem 1.6 we have

$$r_n < \theta < r_{n+1} \quad \text{or} \quad r_n > \theta > r_{n+1}.$$

Subtracting r_n, we obtain

$$0 < |\theta - r_n| < |r_{n+1} - r_n|,$$

and multiplying by k_n,

$$0 < |k_n\theta - h_n| < k_n|r_{n+1} - r_n| = \frac{k_n}{k_n k_{n+1}} = \frac{1}{k_{n+1}}, \tag{1.11}$$

where the second-last equation comes from (1.8).

To obtain a contradiction we assume that θ is rational, say $\theta = \frac{a}{b}$, with $a, b \in \mathbb{Z}$, $b > 0$. Now multiply (1.11) by b:

$$0 < |k_n a - h_n b| < \frac{b}{k_{n+1}}.$$

By (1.6), the integers k_n become arbitrarily large, hence $\frac{b}{k_{n+1}} < 1$ if n is sufficiently large. So finally,

$$0 < |k_n a - h_n b| < 1,$$

but this is impossible since the term in the middle is always an integer. Our assumption was therefore false, and θ is irrational. □

The following is an auxiliary result, needed in later proofs.

Lemma 1.9. *If $\theta := \langle a_0, a_1, a_2, \ldots\rangle$ then $a_0 = \lfloor\theta\rfloor$. If $\theta_1 := \langle a_1, a_2, \ldots\rangle$ then $\theta = a_0 + \frac{1}{\theta_1}$.*

Proof. By Theorem 1.6 we have $r_0 < \theta < r_1$, which means

$$a_0 < \theta < a_0 + \frac{1}{a_1}.$$

But $a_1 \geq 1$, hence $a_0 < \theta < a_0 + 1$, which implies $a_0 = \lfloor\theta\rfloor$.

To prove the second statement, we use Remark (1) in Section 1.2:

$$\begin{aligned}
\theta &= \lim_{n\to\infty} \langle a_0, a_1, a_2, \ldots a_n\rangle \\
&= \lim_{n\to\infty} \left(a_0 + \frac{1}{\langle a_1, a_2, \ldots a_n\rangle}\right) \\
&= a_0 + \frac{1}{\lim_{n\to\infty}\langle a_1, a_2, \ldots a_n\rangle} \\
&= a_0 + \frac{1}{\theta_1}.
\end{aligned}$$

□

The last two results in this section deal with questions of uniqueness.

Theorem 1.10. *Two distinct infinite simple continued fractions converge to different values.*

Proof. Suppose that

$$\langle a_0, a_1, a_2, \ldots\rangle = \langle b_0, b_1, b_2, \ldots\rangle = \theta.$$

By Lemma 1.9 we have $\lfloor\theta\rfloor = a_0 = b_0$, and

$$\theta = a_0 + \frac{1}{\langle a_1, a_2, \ldots\rangle} = b_0 + \frac{1}{\langle b_1, b_2, \ldots\rangle},$$

which implies $\langle a_1, a_2, \ldots\rangle = \langle b_1, b_2, \ldots\rangle$ Now repeat the process. We get (by induction) $a_n = b + n$ for all n. □

Theorem 1.11. *Any irrational number x can be uniquely expressed as an infinite simple continued fraction $\langle a_0, a_1, a_2, \ldots\rangle$.*

Proof. We set $x = x_0$ and define consecutively

$$\begin{aligned} a_0 &= \lfloor x_0 \rfloor, \quad x_1 = \frac{1}{x_0 - a_0}, \quad \left(x_0 = a_0 + \frac{1}{x_1} \right), \\ a_1 &= \lfloor x_1 \rfloor, \quad x_2 = \frac{1}{x_1 - a_1}, \quad \left(x_1 = a_1 + \frac{1}{x_2} \right), \end{aligned}$$

and in general,

$$a_i = \lfloor x_i \rfloor, \quad x_{i+1} = \frac{1}{x_i - a_i}, \quad \left(x_i = a_i + \frac{1}{x_{i+1}} \right). \tag{1.12}$$

It is clear that the a_i are all integers, and all x_i are irrational. In particular,

$$a_{i-1} < x_{i-1} < a_{i-1} + 1, \quad \text{i.e.,} \quad 0 < x_{i-1} - a_{i-1} < 1 \tag{1.13}$$

and therefore

$$x_i = \frac{1}{x_{i-1} - a_{i-1}} > 1,$$

which means that

$$a_i = \lfloor x_i \rfloor \geq 1. \tag{1.14}$$

Now we apply (1.12) repeatedly, to obtain

$$\begin{aligned} x = x_0 &= \langle a_0, x_1 \rangle \\ &= \langle a_0, a_1 + \frac{1}{x_2} \rangle \\ &= \langle a_0, a_1, x_2 \rangle \\ &\vdots \\ &= \langle a_0, a_1, \ldots, a_{m-2}, a_{m-1} + \frac{1}{x_m} \rangle \\ &= \langle a_0, a_1, \ldots, a_{m-2}, a_{m-1}, x_m \rangle. \end{aligned}$$

Claim: $x = \langle a_0, a_1, a_2, \ldots \rangle$.

Proof: By Theorem 1.3 we have

$$\langle a_0, a_1, \ldots, a_{n-1}, x_n \rangle = \frac{x_n h_{n-1} + h_{n-2}}{x_n k_{n-1} + k_{n-2}}, \tag{1.15}$$

and by Theorem 1.5,

$$\begin{aligned} x - r_{n-1} = x - \frac{h_{n-1}}{k_{n-1}} &= \frac{x_n h_{n-1} + h_{n-2}}{x_n k_{n-1} + k_{n-2}} - \frac{h_{n-1}}{k_{n-1}} \\ &= \frac{-(h_{n-1}k_{n-2} - h_{n-2}k_{n-1})}{k_{n-1}(x_n k_{n-1} + k_{n-2})} \\ &= \frac{(-1)^{n-1}}{k_{n-1}(x_n k_{n-1} + k_{n-2})}. \end{aligned}$$

But this tends to 0 since the k_n are strictly increasing integers (by (1.6)), and $x_n > 0$. Therefore $x - r_n \to 0$ as $n \to \infty$, and finally

$$x = \lim_{n \to \infty} \langle a_0, a_1, a_2, \ldots, a_n \rangle = \langle a_0, a_1, a_2, \ldots \rangle.$$

This proves our claim, and we are done. □

We note that the proof of Theorem 1.11 is *constructive*; the method can be used to actually find a continued fraction expansion of a given number.

Example: $x = x_0 = \sqrt{6}$. We give two methods, the first one more numerical. By consecutive subtracting and taking the reciprocal, we find

$$\begin{aligned}
\sqrt{6} \simeq 2.4494897 &= 2 + 0.4494897 \\
&= 2 + \frac{1}{2.2247449} \\
&= 2 + \frac{1}{2 + 0.2247449} \\
&= 2 + \frac{1}{2 + \dfrac{1}{4.4494897}} \\
&= 2 + \frac{1}{2 + \dfrac{1}{4 + 0.4494897}}
\end{aligned}$$

and now we see that we have repetition, so that

$$\sqrt{6} = \langle 2, 2, 4, 2, 4, \ldots \rangle = \langle 2, \overline{2, 4} \rangle.$$

However, it should be noted that rounding errors will be a serious problem after only a few steps, so that the result obtained above has to be verified with the method used after example (1.1).

This problem is avoided if we use the second method:

$$\begin{aligned}
\sqrt{6} &= 2 + (\sqrt{6} - 2); \\
\frac{1}{\sqrt{6} - 2} &= \frac{\sqrt{6} + 2}{6 - 4} = 2 + \left(\frac{1}{2}\sqrt{6} - 1 \right); \\
\frac{1}{\frac{1}{2}\sqrt{6} - 1} &= \frac{\frac{1}{2}\sqrt{6} + 1}{\frac{6}{4} - 1} = 4 + (\sqrt{6} - 2).
\end{aligned}$$

Now we see that we have a repetition, and putting everything together, we get the same expansion as before, only this time there is no need for verification.

1.4. **Approximations to irrational numbers.** In this section we will deal with the first of the two main results mentioned at the beginning of this chapter. Let x be an irrational number, and $\frac{h_n}{k_n}$ its nth convergent, as defined in the previous section. We will show that the quotients $\frac{h_n}{k_n}$ are, in a certain sense, best possible approximations to x.

Theorem 1.12. *For all $n \geq 0$ we have*

$$\left| x - \frac{h_n}{k_n} \right| < \frac{1}{k_n k_{n+1}}.$$

Proof. As before, we set $r_n = h_n/k_n$. In the proof of Theorem 1.11 we saw that

$$|x - r_n| = \frac{1}{k_n(x_{n+1}k_n + k_{n-1})},$$

and using the fact that $a_{n+1} = \lfloor x_{n+1} \rfloor < x_{n+1}$, we get

$$\left| x - \frac{h_n}{k_n} \right| < \frac{1}{k_n(a_{n+1}k_n + k_{n-1})} = \frac{1}{k_n k_{n+1}},$$

where the last equality follows from (1.5). □

Theorem 1.13. *The convergents get successively closer to x, i.e.,*

$$\left| x - \frac{h_n}{k_n} \right| < \left| x - \frac{h_{n-1}}{k_{n-1}} \right|.$$

Proof. Again from the proof of Theorem 1.11 we have

$$\left| x - \frac{h_{n-1}}{k_{n-1}} \right| = \frac{1}{k_{n-1}(x_n k_{n-1} + k_{n-2})}.$$

Since $a_n + 1 > x_n$ (by (1.13)), we have

$$\begin{aligned} x_n k_{n-1} + k_{n-2} &< (a_n + 1)k_{n-1} + k_{n-2} \\ &= k_n + k_{n-1} \qquad \text{(by (1.5))} \\ &\le a_{n+1}k_n + k_{n-1} \qquad \text{(by (1.14))} \\ &= k_{n+1} \qquad \text{(by (1.5))}. \end{aligned}$$

Hence

$$\left| x - \frac{h_{n-1}}{k_{n-1}} \right| \ge \frac{1}{k_{n-1}k_{n+1}} > \frac{1}{k_n k_{n+1}} > \left| x - \frac{h_n}{k_n} \right|,$$

where the middle inequality follows from (1.6), and the right one from Theorem 1.12. □

The following is the main result of this lecture. To put it in perspective, let us first recall that the rational numbers are dense in the reals, in other words, any real number, rational or irrational, can be arbitrarily closely approximated by rational. Thus, for instance, the decimal expansion of a real number (say, of $x = \pi = 3.1415926\ldots$) gives a sequence of rational approximations to x that become arbitrarily close. (In our example, we have the sequence

$$\frac{3}{1}, \frac{31}{10}, \frac{314}{100}, \frac{3141}{1000}, \frac{31415}{10000}, \frac{314159}{100000}, \ldots).$$

What the following theorem says is that, given a convergent of x, there is no better approximation to x with denominator equal to, or smaller than, that of the convergent. Thus the nth convergents give us a sequence of *best rational approximations*. For specific examples, see the homework assignments.

Theorem 1.14. *If $\frac{a}{b} \in \mathbb{Q}$, $b > 0$, and if*

$$\left| x - \frac{a}{b} \right| < \left| x - \frac{h_n}{k_n} \right|$$

for some $n \ge 1$, then $b > k_n$.

Proof. We will prove the following somewhat stronger
Claim: If

$$|xb - a| < |xk_n - h_n| \tag{1.16}$$

for some $n \ge 0$, then $b \ge k_{n+1}$.

To derive the theorem from this, we assume that the statement of the theorem is false, i.e., there exists $a/b \in \mathbb{Q}$ with

$$\left|x - \frac{a}{b}\right| < \left|x - \frac{h_n}{k_n}\right| \quad \text{and} \quad b \leq k_n.$$

Multiplying these two inequalities together, we get

$$|xb - a| < |xk_n - h_n|.$$

Now the Claim gives $b \geq k_{n+1}$, and this is a contradiction since by (1.6) we have $k_n < k_{n+1}$ for $n \geq 1$. This proves the theorem.

Proof of the Claim: To obtain a contradiction, we assume that

$$|xb - a| < |xk_n - h_n| \quad \text{and} \quad b < k_{n+1}.$$

We consider the linear equations

$$\begin{aligned} yk_n + zk_{n+1} &= b, \\ yh_n + zh_{n+1} &= a. \end{aligned}$$

The determinant of this system is

$$k_n h_{n+1} - h_n k_{n+1} = \pm 1,$$

by (1.7). Hence there is an integer solution y, z. We will now derive a few properties of this solution.

(i) Neither y nor z are 0.

Indeed, if $y = 0$ then $b = zk_{n+1}$ which implies $z > 0$; but z is an integer, and therefore $b \geq k_{n+1}$. This, however, contradicts our assumption $b < k_{n+1}$.

If $z = 0$ then $a = yh_n$, $b = yk_n$, and

$$|xb - a| = |xyk_n - yh_n| = |y| \cdot |xk_n - h^n| \geq |xk_n - h_n|$$

since $|y| \geq 1$; this is again a contradiction to our assumption.

(ii) y and z have opposite signs.

Indeed, if $z < 0$ then $yk_n = b - zk_{n+1}$, hence $y > 0$.

If $z > 0$ then $b < k_{n+1}$ implies $b < zk_{n+1}$, hence $yk_n = b - zk_{n+1} < 0$, so finally $y < 0$.

(iii) Since by Theorem 1.6 x is always between r_n and r_{n+1}, the terms $xk_n - h_n$ and $xk_{n+1} - h_{n+1}$ have opposite signs, and therefore, by (ii), $y(xk_n - h_n)$ and $z(xk_{n+1} - h_{n+1})$ have the same sign. Now

$$xb - a = y(xk_n - h_n) + z(xk_{n+1} - h_{n+1}),$$

It is, once again, important to note that the two terms on the right-hand side above have the same sign; because of this the second equality below is true (which would otherwise not be the case!):

$$\begin{aligned} |xb - a| &= |y(xk_n - h_n) + z(xk_{n+1} - h_{n+1})| \\ &= |y(xk_n - h_n)| + |z(xk_{n+1} - h_{n+1})| \\ &> |y(xk_n - h_n)| \\ &= |y| \cdot |(xk_n - h_n)| \\ &\geq |(xk_n - h_n)|. \end{aligned}$$

This final contradiction proves our Claim, and the proof of the theorem is complete. □

1.5. **Examples of various continued fractions.**

$$e = \langle 2,1,2,1,1,4,1,1,6,1,1,8,\ldots\rangle$$

$$= 2+\cfrac{1}{1+\cfrac{1}{2+\cfrac{1}{1+\cfrac{1}{1+\cfrac{1}{4+\ddots}}}}} \tag{1.17}$$

$$\frac{\pi}{2} = 1+\cfrac{1}{1+\cfrac{1}{\frac{1}{2}+\cfrac{1}{\frac{1}{3}+\cfrac{1}{\frac{1}{4}+\ddots}}}} \tag{1.18}$$

$$\frac{4}{\pi} = 1+\cfrac{1}{2+\cfrac{3^2}{2+\cfrac{5^2}{2+\cfrac{7^2}{2+\ddots}}}} \tag{1.19}$$

$$e^z = 1+\cfrac{z}{1-\cfrac{z}{2+\cfrac{z}{1-\cfrac{z}{3+\cfrac{z}{1-\ddots}}}}} \tag{1.20}$$

The continued fraction (1.17) is simple and has a very nice and simple pattern, but it is not periodic (note that the number e is transcendental).

(1.18)–(1.20) are not simple continued fractions. Note the pattern in the expression (1.18) for $\pi/2$. A certain *simple* continued fraction expansion for π has now been computed to several billion terms, without any pattern having become apparent; the situation is similar to that of the decimal expansion of π. (Compare, however, with (1.17)).

(1.19) is another expansion involving π. This is our first example of a continued fraction with numerators different from 1.

Finally, (1.20) is the expansion of a well-known *function* in terms of a continued fraction. This is part of the *analytic* theory of continued fractions.

More on continued fractions from an elementary point of view can be found in [5] or [3].

Lecture 2

2. Periodic continued fractions and Pell's equation

2.1. **Periodic continued fractions.** This subsection will be concerned with the second of the two main results in the theory of simple continued fractions, namely the characterization of quadratic irrationals. We begin with a definition.

Definition 2.1. *An infinite simple continued fraction $\langle a_0, a_1, a_2, \ldots\rangle$ is said to be periodic if there is an integer n such that $a_j = a_{j+n}$ for all sufficiently large j.*

This means that we can write a periodic continued fraction as

$$\begin{aligned}&\langle b_0, b_1, \ldots, b_r, a_0, a_1, \ldots, a_{n-1}, a_0, a_1, \ldots, a_{n-1}, \ldots\rangle\\ &= \langle b_0, b_1, \ldots, b_r, \overline{a_0, a_1, \ldots, a_{n-1}}\rangle\end{aligned}$$

A periodic continued fraction is called *purely periodic* if it has the form

$$\langle \overline{a_0, a_1, \ldots, a_{n-1}}\rangle.$$

Example: $\langle \overline{2,3}\rangle = \langle 2, 3, 2, 3, \ldots\rangle$.

If we set $\theta = \langle \overline{2,3}\rangle$, then we have

$$\theta = 2 + \frac{1}{3 + \dfrac{1}{\theta}},$$

which can be rewritten as a quadratic equation:

$$\begin{aligned}\theta\left(3 + \frac{1}{\theta}\right) &= 2\left(3 + \frac{1}{\theta}\right),\\ 3\theta^2 + \theta &= 6\theta + 2 + \theta,\\ 3\theta^2 - 6\theta - 2 &= 0,\end{aligned}$$

which has the solution

$$\theta = \frac{3 + \sqrt{15}}{3}.$$

Any given periodic continued fraction can be evaluated in this way (see also (1.1) in Lecture 1), and you will notice that you always get a quadratic irrational. The question arises whether this is always true. The following result answers this in the affirmative. Much more is actually shown, as you will see in the statement of the theorem.

Theorem 2.2 (Lagrange)**.** *Any periodic simple continued fraction is a quadratic irrational, and conversely.*

Proof. The two directions have to be proven separately.

"⇒": Let x be the value of the full continued fraction, and let θ be its periodic part:

$$\begin{aligned}\theta &= \langle \overline{a_0, a_1, \ldots, a_{n-1}}\rangle\\ &= \langle a_0, a_1, \ldots, a_{n-1}, \theta\rangle.\end{aligned}$$

From the proof of Theorem 1.11 we have

$$\theta = \frac{\theta h_{n-1} + h_{n-2}}{\theta k_{n-1} + k_{n-2}};$$

this is clearly a quadratic equation in θ. Hence θ is either rational or a quadratic irrational. However, by Theorem 1.8 it can not be rational since we have an infinite continued fraction. Now we consider the full continued fraction

$$x = \langle b_0, b_1, \ldots, b_r, \theta\rangle = \frac{\theta m + m'}{\theta q + q'},$$

where $m'/q', m/q$ are the last two convergents to $\langle b_0, b_1, \ldots, b_r\rangle$. But we know that $\theta = (a + \sqrt{b})/c$, so x must be of a similar form; also, $x \notin \mathbb{Q}$.

"$\Leftarrow$": Suppose that x is a quadratic irrational; we want to show that it can be written as a periodic continued fraction. We divide the proof into several parts. The new notation $b \neq \square$ means "b is not a square".

(1) We can write

$$x = x_0 = \frac{a + \sqrt{b}}{c}, \quad a, b, c \in \mathbb{Z}, \quad b > 0, \quad c \neq 0, \quad b \neq \square.$$

Multiplying numerator and denominator by $|c|$, we get

$$x_0 = \frac{ac + \sqrt{bc^2}}{c^2} \quad \text{or} \quad x_0 = \frac{-ac + \sqrt{bc^2}}{-c^2}$$

(when $c > 0$, resp. $c < 0$). Hence we can always write

$$x_0 = \frac{m_0 + \sqrt{d}}{q_0}, \quad \text{where} \quad q_0 \mid (d - m_0^2),$$

and where $d, m_0, q_0 \in \mathbb{Z}$, $q_0 \neq 0$, $d \neq \square$.

(2) We define recursively

$$\begin{aligned} m_{i+1} &= a_i q_i - m_i, \\ q_{i+1} &= \frac{d - m_{i+1}^2}{q_i}, \\ x_i &= \frac{m_i + \sqrt{d}}{q_i}, \qquad a_i = \lfloor x_i \rfloor. \end{aligned} \tag{2.1}$$

Beginning with the initial values x_0, m_0, q_0 from part (1), we see that $x_i, m_i, q_i \in \mathbb{R}$ (at least).

(3) *To show:* $m_i, q_i \in \mathbb{Z}$, $q_i \neq 0$, $q_i \mid (d - m_i^2)$.

Proof: We do this by induction. The case $i = 0$ is just part (1). Now assume that what we wish to show is true for some i; we want to show it for $i + 1$, using (2.1). First,

$$m_{i+1} = a_i q_i - m_i \in \mathbb{Z},$$

and with this we get

$$q_{i+1} = \frac{d - m_{i+1}^2}{q_i} = \frac{d - m_i^2}{q_i} + 2a_i m_i - a_i^2 q_i \in \mathbb{Z}.$$

Next, we have $q_{i+1} \neq 0$ for otherwise we'd have $d = m_{i+1}^2$, but $d \neq \square$. Finally, rewriting (2.1), we get

$$q_i = \frac{d - m_{i+1}^2}{q_{i+1}}, \quad \text{i.e.,} \quad q_{i+1} \mid (d - m_{i+1}^2).$$

This completes part (3).

(4) From (2.1) we get

$$\begin{aligned} x_i - a_i &= \frac{-a_i q_i + m_i + \sqrt{d}}{q_i} = \frac{\sqrt{d} - m_{i+1}}{q_i} \\ &= \frac{d - m_{i+1}^2}{q_i(d + m_{i+1}^2)} \\ &= \frac{q_{i+1}}{q_i(d + m_{i+1}^2)} = \frac{1}{x_{i+1}}. \end{aligned}$$

Hence we have

$$x = x_0 = \langle a_0, a_1, \ldots \rangle, \tag{2.2}$$

where the a_i are as defined in (2.1).

(5) Before we show that the continued fraction (2.2) is periodic, we need some preparatory observations. Let

$$x_i' = \frac{m_i - \sqrt{d}}{q_i}$$

be the conjugate of x_i. From the proof of Theorem 1.11 (and taking conjugates) we have

$$x_0' = \frac{x_n' h_{n-1} + h_{n-2}}{x_n' k_{n-1} + k_{n-2}}.$$

Solving this for x_n', we get

$$x_n' = -\frac{k_{n-2}}{k_{n-1}} \left(\frac{x_0' - \frac{h_{n-2}}{k_{n-2}}}{x_0' - \frac{h_{n-1}}{k_{n-1}}} \right). \tag{2.3}$$

Since by definition of infinite continued fractions we have

$$\frac{h_{n-2}}{k_{n-2}} \to x_0, \quad \frac{h_{n-1}}{k_{n-1}} \to x_0,$$

but $x_0' \neq x_0$ (otherwise x_0 would be rational), the large fraction in parentheses in (2.3) approaches 1 as $n \to \infty$. Hence $x_n' < 0$ if n is sufficiently large. But we know that $x_n > 0$ for $n \geq 1$, and therefore

$$x_n - x_n' > 0 \quad \text{for} \quad n > N, \tag{2.4}$$

for a sufficiently large $N \in \mathbb{N}$. From (2.1) we get

$$x_n - x_n' = \frac{m_n + \sqrt{d}}{q_n} - \frac{m_n - \sqrt{d}}{q_n} = \frac{2\sqrt{d}}{q_n}.$$

By (2.4) this is positive, and therefore

$$q_n > 0 \quad \text{for} \quad n > N. \tag{2.5}$$

(6) We are now ready to show that the continued fraction (2.2) is periodic. From (2.1) and (2.5) we have for $n > N$,

$$q_n q_{n+1} = d - m_{n+1}^2 \leq d,$$

hence

$$q_n \leq q_n q_{n+1} \leq d \quad \text{for} \quad n > N,$$

and also

$$m_{n+1}^2 < m_{n+1}^2 + q_n q_{n+1} = d, \quad \text{i.e.,} \quad |m_{n+1}| < \sqrt{d}.$$

But d is a fixed positive integer, and therefore q_n, m_{n+1} can assume only a fixed number of possible values for $n > N$. This means that (m_n, q_n) can assume only a fixed number of possible pairs of values for $n > N$. As a consequence, there exist integers $j < k$ such that $m_j = m_k$ and $q_j = q_k$. By (2.1) this means that $x_j = x_k$, so finally

$$x_0 = \langle a_0, a_1, \ldots, a_{j-1}, \overline{a_j, a_{j+1}, \ldots, a_k}\rangle,$$

and the proof is complete. □

2.2. **Some special cases.** The two results in this section are required for the following section.

Theorem 2.3. *The continued fraction expansion of the real quadratic irrational number x is purely periodic if and only if $x > 1$ and $-1 < x' < 0$, where x' is the conjugate of x,*

A proof of this result can be found, for instance, in [4]. I should mention that much of the material in this chapter was taken from that excellent book.

Theorem 2.4. *Let $d > 1$ be an integer, not a perfect square. Then*
(1) *the simple continued fraction expansion of $\sqrt{d}$ has the form*

$$\sqrt{d} = \langle a_0, \overline{a_1, a_2, \ldots, a_{r-1}, 2a_0}\rangle, \qquad a_0 = \lfloor\sqrt{d}\rfloor.$$

(2) *With $x_0 = \sqrt{d}, q_0 = 1, m_0 = 0$ in (2.1) we have $q_i = 1$ if and only if $r \mid i$, while $q_i = -1$ holds for no i.*

Proof. (i) Consider the irrational number $\sqrt{d} + \lfloor\sqrt{d}\rfloor$. It satisfies the conditions of Theorem 2.3, and so its continued fraction is purely periodic,

$$\sqrt{d} + \lfloor\sqrt{d}\rfloor = \langle\overline{a_0, a_1, \ldots, a_{r-1}}\rangle = \langle a_0, \overline{a_1, \ldots, a_{r-1}, a_0}\rangle, \tag{2.6}$$

where r is chosen to be the smallest period. Note that

$$x_i = \langle a_i, a_{i+1}, \ldots\rangle$$

is purely periodic for all values of i, and that

$$x_0 = x_r = x_{2r} = \cdots$$

Furthermore, $x_1, x_2, \ldots, x_{r-1}$ are all different from x_0 since otherwise there would be a smaller period. Thus $x_i = x_0$ if and only if $i = mr$ for some m.

(ii) Now we can start with

$$x_0 = \sqrt{d} + \lfloor\sqrt{d}\rfloor, \quad q_0 = 1, \quad , m_0 = \lfloor\sqrt{d}\rfloor$$

in (2.1) because $1 \mid (d - \lfloor\sqrt{d}\rfloor^2)$. Then for all $j \geq 0$ we have

$$\frac{m_{jr} + \sqrt{d}}{q_{jr}} = x_{jr} = x_0 = \frac{m_0 + \sqrt{d}}{q_0} = \lfloor\sqrt{d}\rfloor + \sqrt{d}, \tag{2.7}$$

$$m_{jr} - q_{jr}\lfloor\sqrt{d}\rfloor = (q_{jr} - 1)\sqrt{d}, \tag{2.8}$$

and so $q_{jr} = 1$ since the left side of (2.8) is rational, while $\sqrt{d}$ is irrational.

(iii) Next we show that $q_i = 1$ for no other values of i. To do so, we note that, by (2.1), $q_i = 1$ implies $x_i = m_i + \sqrt{d}$; but x_i has a purely periodic expansion, so by Theorem 2.3 we have

$$-1 < m_i - \sqrt{d} < 0, \quad \text{that is,} \quad \sqrt{d} - 1 < m_i < \sqrt{d},$$

and hence $m_i = \lfloor\sqrt{d}\rfloor$. Thus $x_i = x_0$, and i is a multiple of r.

(iv) We also show that $q_i = -1$ does not hold for any i. Indeed, by (2.1), $q_i = -1$ implies $x_i = -m_i - \sqrt{d}$, and by Theorem 2.3 we would have

$$-m_i - \sqrt{d} > 1 \quad \text{and} \quad -1 < -m_i + \sqrt{d} < 0.$$

But this implies $\sqrt{d} < m_i < -\sqrt{d} - 1$, which is impossible.

(v) Finally we note that $a_0 = \lfloor \sqrt{d} + \lfloor \sqrt{d} \rfloor \rfloor = 2\lfloor \sqrt{d} \rfloor$, and we turn to the case $x = \sqrt{d}$. Using (2.6), we have

$$\begin{aligned} \sqrt{d} &= -\lfloor \sqrt{d} \rfloor + (\sqrt{d} + \lfloor \sqrt{d} \rfloor) \\ &= -\lfloor \sqrt{d} \rfloor + \langle 2\lfloor \sqrt{d} \rfloor, \overline{a_1, a_2, \ldots, a_{r-1}, a_0} \rangle \\ &= \langle \lfloor \sqrt{d} \rfloor, \overline{a_1, a_2, \ldots, a_{r-1}, a_0} \rangle, \end{aligned}$$

with $a_0 = 2\lfloor \sqrt{d} \rfloor$. This completes the proof. □

2.3. **Pell's equation.** The equation

$$x^2 - d\,y^2 = N, \qquad d, N, \in \mathbb{Z}, \tag{2.9}$$

with integer unknowns x and y, is usually called *Pell's equation*, although the English mathematician John Pell had little to do with it. Some remarks:

– The original case is $N = 1$.
– The equation has important applications in algebraic number theory.
– If d is negative, then (2.9) can only have finitely many solutions.
– If d is a perfect square, say $d = a^2$, then (2.9) reduces to

$$(x - ay)(x + ay) = N,$$

which again can only have finitely many solutions. Therefore we assume that $d > 1$, not a perfect square.

We expand $\sqrt{d}$ into a continued fraction as in Theorem 2.4, with convergents h_n/k_n, and with q_n defined by (2.1), with $x_0 = \sqrt{d}$, $q_0 = 1$, $m_0 = 0$.

Theorem 2.5. *If d is a positive integer not a perfect square, then for all integers $n \geq -1$ we have*

$$h_n^2 - d \cdot k_n^2 = (-1)^{n-1} q_{n+1}.$$

Proof. (Sketch) From (1.15) and (2.1) we have

$$\sqrt{d} = x_0 = \frac{x_{n+1}h_n + h_{n+1}}{x_{n+1}k_n + k_{n+1}} = \frac{(m_{n+1} + \sqrt{d})h_n + q_{n+1}h_{n-1}}{(m_{n+1} + \sqrt{d})k_n + q_{n+1}k_{n-1}}.$$

Now simplify this equation and separate into rational and purely irrational parts. Each part must be 0, so we get two equations; eliminate m_{n+1} from them (Exercise). The final result is

$$h_n^2 - d \cdot k_n^2 = (h_n k_{n-1} - h_{n-1}k_n)q_{n+1} = (-1)^{n-1} q_{n+1},$$

where we have used Theorem 1.5 in the last step. □

Corollary 2.6. *Let r be the period length of the expansion of $\sqrt{d}$ in Theorem 2.4. Then for $n \geq 0$ we have*

$$h_{nr+1}^2 - d \cdot k_{nr+1}^2 = (-1)^{nr} q_{nr} = (-1)^{nr}. \tag{2.10}$$

Proof. This follows immediately from Theorem 2.5 with n replaced by $nr - 1$, and then using Theorem 2.4(2). □

We can now see: (2.10) gives us infinitely many solutions of the equations

$$x^2 - d \cdot y^2 = 1 \quad \text{and} \quad x^2 - d \cdot y^2 = -1.$$

Next we'll show that *every* solution of these equations can be obtained from the continued fraction expansion of $\sqrt{d}$. Before we do so, we note that it is sufficient to consider the positive solutions $x > 0$, $y > 0$. First we need two other result that are of independent interest.

Theorem 2.7. *Let x be an irrational number. If there is a rational number r/s with $(r, s) = 1$ and $s \geq 1$ such that*

$$\left| x - \frac{r}{s} \right| < \frac{1}{2s^2},$$

then r/s is one of the convergents of the simple continued fraction expansion of x.

Proof. Let h_j/k_j be the convergents of the simple continued fraction expansion of x, and suppose that r/s is not a convergent. Let $n \in \mathbb{N}$ be such[1] that $k_n \leq s < k_{n+1}$. For this n, the inequality $|xs - r| < |xk_n - h_n|$ is impossible because of (1.16). Therefore we have

$$|xk_n - h_n| \leq |xs - r| < \frac{1}{2s},$$

that is,

$$\left| x - \frac{h_n}{k_n} \right| < \frac{1}{2sk_n}.$$

Using the assumption that $r/s \neq h_n/k_n$ and the fact that $sh_n - rk_n \in \mathbb{Z}$, we find

$$\frac{1}{sk_n} \leq \frac{|sh_n - rk_n|}{sk_n} = \left| \frac{h_n}{k_n} - \frac{r}{s} \right| \leq \left| x - \frac{h_n}{k_n} \right| + \left| x - \frac{r}{s} \right| < \frac{1}{2sk_n} + \frac{1}{2s^2}.$$

This implies $s < k_n$, which is a contradiction to how we chose n. Hence the assumption that r/s is not a convergent was false, which proves the theorem. □

Theorem 2.8. *Let $x > 1$ be a real number. Then the nth convergent of $1/x$ is the reciprocal of the $(n-1)$st convergent of x.*

Proof. (Sketch) We have $x = \langle a_0, a_1, \ldots \rangle$ and $1/x = \langle 0, a_0, a_1, \ldots \rangle$. Now use the identities (1.4) and (1.5), and proceed by induction. □

Theorem 2.9. *Let d be a positive integer not a perfect square, and let the convergents of the simple continued fraction expansion of $\sqrt{d}$ be h_n/k_n. Suppose the integer N satisfies $|N| < d$. Then any positive solution $x = s$, $y = t$ of*

$$x^2 - d \cdot y^2 = N \quad \textit{with} \quad (s, t) = 1$$

satisfies $s = h_n$, $t = k_n$ for some positive integer n.

Proof. Let E and M be positive integers such that $(E, M) = 1$ and $E^2 - \rho M^2 = \sigma$, where $\sqrt{\rho}$ is irrational and $0 < \sigma < \sqrt{\rho}$. (Here $\rho, \sigma \in \mathbb{R}$, not necessarily integers). Then

$$\frac{E}{M} - \sqrt{\rho} = \frac{\sigma}{M(E + M\sqrt{\rho})},$$

and therefore

$$0 < \frac{E}{M} - \sqrt{\rho} < \frac{\sigma}{M(E + M\sqrt{\rho})} = \frac{1}{M^2(\frac{E}{M\sqrt{\rho}} + 1)}.$$

[1] In these lectures, $\mathbb{N}$ denotes the natural numbers $1, 2, 3, \ldots$

Also, $0 < E/M - \sqrt{\rho}$ implies $E/(M\sqrt{\rho}) > 1$, and thus

$$\left|\frac{E}{M} - \sqrt{\rho}\right| < \frac{1}{2M^2}.$$

By Theorem 2.7, E/M is a convergent in the continued fraction expansion of $\sqrt{\rho}$. Now we distinguish between two cases.

If $N > 0$, we take $\sigma = N, \rho = d, E = s$, and $M = t$; the theorem holds in this case.

If $N < 0$, then we rewrite the original equation as

$$t^2 - \frac{1}{d}s^2 = -\frac{N}{d},$$

and we take $\sigma = -N/d, \rho = 1/d, E = t$, and $M = s$. Then t/s is a convergent in the expansion of $1/\sqrt{d}$. Finally, Theorem 2.8 shows that s/t is a convergent in the expansion of $\sqrt{d}$, and we are done. □

Combining the results of Theorems 2.4, 2.5, and 2.9, we get the following result.

Theorem 2.10. *Let $d > 1$ be an integer not a perfect square, let h_n/k_n be the convergents of the continued fraction expansion of $\sqrt{d}$, and let r be the period of the expansion of $\sqrt{d}$ as given in Theorem 2.4. Then*

1. *all positive solutions of $x^2 - d\,y^2 = \pm 1$ can be found among $x = h_n$, $y = k_n$;*
2. *if r is even, then $x^2 - d\,y^2 = -1$ has no solution, and all positive solutions of $x^2 - d\,y^2 = 1$ are given by $x = h_{nr-1}$, $y = k_{nr-1}$ for $n = 1, 2, 3, \ldots$;*
3. *if r is odd, then $x = h_{nr-1}$, $y = k_{nr-1}$ give all positive solutions of $x^2 - d\,y^2 = -1$ for $n = 1, 3, 5, \ldots$, and all positive solutions of $x^2 - d\,y^2 = 1$ for $n = 2, 4, 6, \ldots$.*

We conclude this lecture with an example.

Example: Consider $x^2 - 73y^2 = -1$. We first find the continued fraction expansion $\sqrt{73} = \langle 8, \overline{1, 1, 5, 5, 1, 1, 16}\rangle$ which, by the way, is consistent with Theorem 2.4. Hence $r = 7$, and by Theorem 2.10 the given equation has solutions, and moreover, the least positive solution is given by h_6/k_6. We use the recurrences (1.4) and (1.5) to obtain successive h_j/k_j, starting with h_0/k_0:

$$\frac{8}{1}, \quad \frac{9}{1}, \quad \frac{17}{2}, \quad \frac{94}{11}, \quad \frac{487}{57}, \quad \frac{561}{68}, \quad \frac{1068}{125}.$$

Therefore $x = 1068$, $y = 125$ is the smallest positive solution of the given equation.

In a similar way we can find the smallest positive solution of the related equation $x^2 - 73y^2 = 1$. In this case we need to compute recursively the fraction h_{13}/k_{13}, which leads to the solution $x = 2\,281\,249$, $y = 267\,000$. All other solutions can also be found in this way.

In closing I note that there is another, simpler, way of obtaining higher solutions from a given smallest positive solution; see [4, p. 354].

Lecture 3

3. Chebyshev's prime number theorem

3.1. **Introduction.** We begin with a basic definition.

Definition 3.1. *An integer $p > 1$ is called a prime number, or simply a prime, if it has only 1 and itself as divisors. An integer that is not a prime number is called composite.*

The first question that arises is, *how many primes are there?*

Theorem 3.2 (Euclid)**.** *There are infinitely many primes.*

Proof. Suppose there were only a finite number of primes, namely $p_1 = 2, p_2 = 3, p_3 = 5, \ldots, p_r$. Now form the number

$$n = p_1 p_2 \cdots p_r + 1.$$

n is not divisible by any of the primes $p_1, p_2, \ldots, p_r$ since in each case we have remainder 1 upon division. Hence any prime divisor of n must be distinct from the $p_1, p_2, \ldots, p_r$, but this is a contradiction. □

Remark: A great deal can be said about the theory and applications of prime numbers. Here we have to restrict ourselves to a few results about their distributions. Further to Euclid's theorem, the following is noteworthy.

(a) Variants of Euclid's proof can be used to show that, for instance, there are infinitely many primes of the for $4k + 1$, or $4k - 1$, or $6k - 1$.

(b) More generally, what about $p = ak + b$, where $(a, b) = 1$? It turns out that there are infinitely many primes in each class. This was first proved by P. G. Lejeune-Dirichlet in 1837; this remarkable proof marked the beginning of analytic number theory.

(c) The prime numbers are both very regularly and very irregularly distributed. Let me explain this seemingly contradictory statement. To support the "irregularity" claim, I will give two extreme situations.

First, there are "gaps" of arbitrary length between primes: Consider the integers

$$k! + 2, k! + 3, \ldots, k! + k - 1, k! + k;$$

all these $k - 1$ consecutive integers are composite because clearly

$$j \mid k! + j \quad \text{for} \quad j = 2, 3, \ldots, k.$$

Second, there are the *twin primes*, namely pairs $p, p + 2$ of primes, such as

$$3, 5 \quad 5, 7 \quad 11, 13 \quad 17, 19 \quad \ldots$$

Are there infinitely many such pairs? This is not known, and the conjecture that there are infinitely many pairs of twin primes is the so-called *twin-prime conjecture*, one of the most notorious unsolved problems in number theory.

(d) On the other hand, the *prime number theorem* shows that the primes are very regularly behaved "in the large". More exactly, we define the function

$$\pi(x) = \sum_{p \le x} 1 = \#\{p \le x \mid p \text{ prime}\}.$$

It was proved by Jacques Hadamard (1865–1963) and (independently) Charles de la Vallée Poussin (1866–1962) in 1896 that

$$\pi(x) \sim \frac{x}{\log x} \text{ as } x \to \infty,$$

which is a short form for writing[2]

$$\lim_{x\to\infty} \pi(x)\frac{\log x}{x} = 1.$$

The proof of the important prime number theorem relies heavily on complex analysis and is beyond the scope of these lectures. However, a somewhat weaker version, which still shows how the primes behave "in the large", is easier to obtain. This will be the main objective of this lecture.

3.2. **Chebyshev's prime number theorem.** Before the eventual proof in 1896 of the Prime Number Theorem, the most important advance occurred when the great Russian mathematician Pavnutii Lvovich Chebyshev (1821–1894) proved a weaker version in 1850. Although the existence of the limit was not yet established, it does give the correct "order of growth" of the function $\pi(x)$. Here is a version of Chebyshev's theorem with a different, easier, proof.

Theorem 3.3. *For all $n \geq 2$,*

$$\frac{1}{8} \leq \frac{\pi(n)}{n/\log n} \leq 12.$$

To prove this theorem, we first state another one:

Theorem 3.4. *For all $n \geq 2$,*

$$\frac{1}{8} \leq \pi(n)\frac{H(n)}{n} < 6,$$

where

$$H(n) = \sum_{j=2}^{n} \frac{1}{j}.$$

In other words: $\pi(n)$ is of the same order of magnitude as the reciprocal of the average of $(\frac{1}{2}, \frac{1}{3}, \frac{1}{4}, \ldots, \frac{1}{n})$. The numbers $H(n)$ are closely related to the *harmonic numbers* $1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n}$.

Before proving Theorem 3.4, we use it to prove Chebyshev's theorem, Theorem 3.3.

Proof of Theorem 3.3. For $n \geq 2$ we have

$$\log\frac{n}{2} = \int_2^n \frac{dt}{t} < \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n} < \int_1^n \frac{dt}{t} = \log n.$$

For $n \geq 4$ we have

$$\log\frac{n}{2} \geq \frac{1}{2}\log n,$$

and also

$$\frac{1}{2}\log 3 \leq \frac{1}{2} + \frac{1}{3}, \qquad \frac{1}{2}\log 2 \leq \frac{1}{2}.$$

[2]As is usual in pure mathematics, $\log x$ denotes the *natural logarithm*, often denoted by $\ln x$.

Hence for all $n \geq 2$,

$$\frac{1}{2}\log n \leq H(n) \leq \log n,$$

and therefore Theorem 3.3 follows from Theorem 3.4. □

Remark: In view of the first line of the above proof it is of interest to note that the limit

$$\gamma := \lim_{n\to\infty}\left(1+\frac{1}{2}+\frac{1}{3}+\cdots+\frac{1}{n}-\log n\right)$$

actually exists. γ is called *Euler's constant*, also known as the *Euler-Mascheroni constant*. After the numbers π and e it is probably the most important special constant in mathematics, and it is also closely related to the ubiquitous *Gamma function* $\Gamma(x)$.

In preparation for the proof of Theorem 3.4, we first prove several lemmas.

Lemma 3.5.

$$\pi\left(2^{k+1}\right) \leq 2^k.$$

Proof. Even numbers cannot be primes, with the exception of 2. For $n > 9$ we clearly have $\pi(n) \leq n/2$. For the smaller cases we count the primes: $\pi(2) = 1 = 2^0$, $\pi(4) = 2 = 2^1$, $\pi(8) = 4 = 2^2$. □

Lemma 3.6.

$$\frac{1}{2}l \leq H(2^l) \leq l.$$

Proof. We group the terms of the sum $H(2^l)$ in two different ways. First,

$$\begin{aligned} H(2^l) &= \frac{1}{2}+\left(\frac{1}{3}+\frac{1}{4}\right)+\left(\frac{1}{5}+\frac{1}{6}+\frac{1}{7}+\frac{1}{8}\right)+\cdots \\ &\quad +\left(\frac{1}{2^{l-1}+1}+\cdots+\frac{1}{2^l}\right) \\ &\geq \frac{1}{2}+\left(\frac{1}{4}+\frac{1}{4}\right)+\left(\frac{1}{8}+\frac{1}{8}+\frac{1}{8}+\frac{1}{8}\right)+\cdots+\left(\frac{1}{2^l}+\cdots+\frac{1}{2^l}\right) \\ &= \frac{1}{2}l. \end{aligned}$$

On the other hand,

$$\begin{aligned} H(2^l) &= \left(\frac{1}{2}+\frac{1}{3}\right)+\left(\frac{1}{4}+\frac{1}{5}+\frac{1}{6}+\frac{1}{7}\right)+\cdots+\frac{1}{2^l} \\ &\leq \left(\frac{1}{2}+\frac{1}{2}\right)+\left(\frac{1}{4}+\frac{1}{4}+\frac{1}{4}+\frac{1}{4}\right)+\cdots+\left(\frac{1}{2^{l-1}}+\cdots+\frac{1}{2^{l-1}}+\frac{1}{2^l}\right) \\ &\leq l. \end{aligned}$$

□

Lemma 3.7. *The canonical factorization of* $n!$ *is*

$$n! = \prod_{p\leq n} p^{\lfloor n/p\rfloor+\lfloor n/p^2\rfloor+\cdots}.$$

Proof. Only primes $p \le n$ can occur in the factorization of $n!$. Fix such a prime p. In the sequence of factors

$$1,\ 2,\ 3,\ \dots, n-1,\ n \quad \text{of} \quad n!,$$

– every pth number (namely $p, 2p, \dots$) is divisible by p; there are $\lfloor n/p \rfloor$ of them;
– every p^2th number (namely $p, 2p, \dots$) is divisible by a second copy of p; there are $\lfloor n/p^2 \rfloor$ of them;
– and so on, so that the power of p in $n!$ is

$$\lfloor \frac{n}{p} \rfloor + \lfloor \frac{n}{p^2} \rfloor + \lfloor \frac{n}{p^3} \rfloor + \cdots,$$

which completes the proof of the lemma. □

Lemma 3.8. *The power of a prime p in $\binom{N}{n}$ is*

$$\sum_{m \ge 1} \left(\left\lfloor \frac{N}{p^m} \right\rfloor - \left\lfloor \frac{n}{p^m} \right\rfloor - \left\lfloor \frac{N-n}{p^m} \right\rfloor \right).$$

Proof. We use the fact that $\binom{N}{n} = \frac{N!}{n!(N-n)!}$ and apply Lemma 3.7. □

Proof of Theorem 3.4. (i) We begin with the following assertion:

$$\prod_{n < p \le 2n} p \,\Big|\, \binom{2n}{n} \qquad \text{and} \qquad \binom{2n}{n} \,\Big|\, \prod_{p^r \le 2n < p^{r+1}} p^r. \tag{3.1}$$

Proof: We use the fact that

$$\binom{2n}{n} = \frac{(2n!)}{n!n!}.$$

If $n < p \le 2n$ then $p \mid (2n)!$, while $p \nmid n!$. This proves the left part of (3.1).

On the other hand, by Lemma 3.8 the power of p in $\frac{2n}{n}$ is

$$\sum_{m=1}^{r} \underbrace{\left(\left\lfloor \frac{2n}{p^n} \right\rfloor - 2 \left\lfloor \frac{n}{p^n} \right\rfloor \right)}_{\le 1} \le r.$$

This proves the right part of (3.1).

(ii) Changing divisibility in (3.1). into inequalities, we obtain for $n \ge 1$,

$$n^{\pi(2n)-\pi(n)} < \prod_{n < p \le 2n} p \le \binom{2n}{n} \le \prod_{p^r \le 2n < p^{r+1}} p^r \le (2n)^{\pi(2n)}, \tag{3.2}$$

where the left-most inequality follows from the fact that there are $\pi(2n) - \pi(n)$ primes between n and $2n$, and the smallest one is at least n; similarly, the right-most inequality follows from the fact that the number of p in the preceding product is $\pi(2n)$, while each factor p^r is at most $2n$. Now

$$\begin{aligned} \binom{2n}{n} &= \frac{2n(2n-1)\cdots(n+1)}{n(n-1)\cdots 1} \\ &= 2\left(2 + \frac{1}{n-1}\right) \cdots \left(2 + \frac{j}{n-j}\right) \cdots \left(2 + \frac{n-1}{1}\right) \\ &\ge 2^n, \end{aligned}$$

and

$$\binom{2n}{n} \le (1+1)^{2n} = 2^{2n}.$$

Hence, with (3.2) we get for $n \ge 1$,

$$n^{\pi(2n)-\pi(n)} < 2^{2n}, \qquad 2^{2n} \le (2n)^{\pi(2n)}.$$

Now let $n = 2^k$, $k = 0, 1, 2, \ldots$. Then the last inequalities become

$$2^{k(\pi(2^{k+1})-\pi(2^k))} < 2^{2^{k+1}}, \qquad 2^{2^k} \le 2^{(k+1)\pi(2^{k+1})},$$

or

$$k(\pi(2^{k+1}) - \pi(2^k)) < 2^{k+1}, \qquad 2^k \le (k+1)\pi(2^{k+1}). \tag{3.3}$$

Now

$$(k+1)\pi(2^{k+1}) - k\pi(2^k) < 2^{k+1} + \pi(2^{k+1}) \le 3 \cdot 2^k,$$

where the first inequality follows from (3.3), and the second one from Lemma 3.5. Replace k successively by $0, 1, \ldots, k$ and add. On the left we have a "telescoping sum" so that

$$(k+1)\pi(2^{k+1}) < 3\left(2^0 + 2^1 + \cdots + 2^k\right) < 3 \cdot 2^{k+1}.$$

Using this and (3.3), we find

$$\frac{1}{2} \cdot \frac{2^{k+1}}{k+1} \le \pi(2^{k+1}) < 3\frac{2^{k+1}}{k+1}.$$

Now let $n \in \mathbb{N}$, $n > 1$, be such that

$$2^{k+1} \le n < 2^{k+2}.$$

Then

$$\pi(n) \le \pi(2^{k+2}) < 3\frac{2^{k+2}}{k+2} \le 6\frac{2^{k+1}}{H(2^{k+2})} \le 6\frac{n}{H(n)},$$

where we have used Lemma 3.6 in the third inequality. On the other hand,

$$\begin{aligned}\pi(n) \ge \pi(2^{k+1}) &\ge \frac{1}{2} \cdot \frac{2^{k+1}}{k+1} = \frac{1}{8} \cdot \frac{2^{k+2}}{\frac{1}{2}(k+1)} \\ &\ge \frac{1}{8} \cdot \frac{2^{k+2}}{H(2^{k+1})} \ge \frac{1}{8} \cdot \frac{n}{H(n)},\end{aligned}$$

where we have used Lemma 3.6 for the second-last inequality. Putting the last two strings of inequalities together, we finally obtain the statement of Theorem 3.4. □

In concluding this lecture, let me remark that Chebyshev's theorem easily leads to a proof of a famous and at that time unsolved problem, namely

Bertrand's Postulate: (J. L. F. Bertrand, 1845)
If $x \in \mathbb{R}$, $x > 1$, then there is at least one prime in the open interval $(x, 2x)$.

The proof is left as an exercise.

Lecture 4

4. The Riemann zeta function

4.1. **Introduction.** We begin with the definition of one of the most important functions in analytic number theory.

Definition 4.1. *For a complex variable s the Riemann zeta function is defined by*

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} \qquad (\mathrm{Re}(s) > 1).$$

This function was studied already by Leonhard Euler (1707–1783), but it was Bernhard Riemann (1826–1866) who first investigated deeper connections between the zeta function and the distribution of primes.

Is this function well-defined as stated? As is customary in analytic number theory, we denote a complex variable by $s \in \mathbb{C}$, where $s = \sigma + it$. If $\mathrm{Re}(s) > 1$, we have

$$\frac{1}{n^s} = \frac{1}{n^{\sigma+it}} = \frac{1}{n^\sigma} \cdot \frac{1}{n^{it}}.$$

Now note that

$$|n^{it}| = |e^{it \log n}| = 1, \qquad \text{so} \quad \left|\frac{1}{n^s}\right| = \frac{1}{n^\sigma},$$

and that the series $\sum_{n=1}^{\infty} 1/n^\sigma$ is absolutely convergent for $\sigma > 1$. Therefore Definition 4.1 does make sense.

For now, and until further notice, we assume that s is real, $s > 1$.

Theorem 4.2. *For $s > 1$ we have*

$$\zeta(s) = \prod_p \frac{1}{1 - p^{-s}},$$

where the product is taken over all primes p.

Proof. For $s > 1$ we have $p^s < 1$, and therefore

$$\begin{aligned}
\frac{1}{1-2^{-s}} &= 1 + 2^{-s} + 2^{-2s} + 2^{-3s} + \cdots, \\
\frac{1}{1-3^{-s}} &= 1 + 3^{-s} + 3^{-2s} + 3^{-3s} + \cdots, \\
\frac{1}{1-5^{-s}} &= 1 + 5^{-s} + 5^{-2s} + 5^{-3s} + \cdots, \\
&\vdots
\end{aligned}$$

By unique factorization we have

$$\prod_{p \le N} \frac{1}{1-p^{-s}} = \sum_{n \le N} n^{-s} + R_N(s),$$

where $R_N(s)$ is a remainder term which satisfies

$$R_N(s) \le \sum_{n=N+1}^{\infty} \frac{1}{n^s}.$$

But $\zeta(s)$ is a convergent series for $s > 1$; therefore $R_N(s) \to 0$ as $N \to \infty$. This completes the proof. □

The product in this theorem is called an *Euler product*. As a consequence of Theorem 4.2 we obtain a second very interesting proof of the infinitude of the primes.

Corollary 4.3 (Euler)**.** *There are infinitely many primes.*

Proof. By Definition 4.1 and the fact that the harmonic series diverges, $\zeta(s)$ does not stay bounded as $s \to 1^+$, which by Theorem 4.2 means that

$$\prod_p \frac{1}{1-p^{-s}} \to \infty \quad \text{as} \quad s \to 1^+.$$

However, if there were only finitely many primes, then

$$\lim_{s\to 1^+} \prod_p \frac{1}{1-p^{-s}} = \prod_p \frac{1}{1-p^{-1}}$$

would be finite. This contradiction proves the corollary. □

Before we state a second consequence of Theorem 4.2, we define one of the most important number theoretic functions, which is also of great importance in combinatorics. It is named after August Ferdinand Möbius (1790–1868), well known also for the famous "Möbius strip".

Definition 4.4. *The Möbius function $\mu(n)$ is defined for $n \in \mathbb{N}$ by*

$$\mu(n) = \begin{cases} 1 & \text{if } n = 1, \\ 0 & \text{if } a^2 \mid n \text{ for some } a \in \mathbb{N}, a > 1, \\ (-1)^r & \text{if } n = p_1 \cdots p_r, p_i \text{ distinct primes.} \end{cases}$$

We recall that a number theoretic function f, that is, a function $f : \mathbb{N} \to \mathbb{C}$, is *multiplicative* if

$$f(mn) = f(m)f(n) \quad \text{whenever} \quad (m,n) = 1.$$

Lemma 4.5. *The Möbius function is multiplicative, and*

$$\sum_{d\mid n} \mu(d) = \begin{cases} 1 & \text{if } n = 1, \\ 0 & \text{if } n > 1. \end{cases}$$

Proof. The multiplicativity of $\mu(n)$ follows from the definition and the simple fact that $(-1)^r \cdot (-1)^s = (-1)^{r+s}$.

Now, since $\mu(n)$ is multiplicative, it suffices to consider $n = p^\alpha$, for some integer $\alpha \geq 1$. But then

$$\sum_{d\mid p^\alpha} \mu(d) = \mu(1) + \mu(p) + \mu(p^2) + \cdots + \mu(p^\alpha) = 1 + (-1) + 0 + \cdots + 0 = 0,$$

which completes the proof. □

The Möbius function has other interesting and important properties, which we cannot pursue in the confines of these lectures.

Corollary 4.6. *For $s > 1$ we have*

$$\sum_{n=1}^{\infty} \frac{\mu(n)}{n^s} = \prod_p \left(1 - \frac{1}{p^s}\right) = \frac{1}{\zeta(s)}.$$

Proof. The second equality is simply the Euler product (Theorem 4.2). The first inequality can be proved in two different ways:

First proof: Consider the product

$$\left(1-\frac{1}{2^s}\right)\left(1-\frac{1}{3^s}\right)\cdots\left(1-\frac{1}{p_k^s}\right),$$

and expand it, using the definition of the Möbius function. There will be an error term which can be estimated as in the proof of Theorem 4.2.

Second proof: We multiply two functions and rearrange:

$$\begin{aligned}\zeta(s)\sum_{n=1}^{\infty}\frac{\mu(n)}{n^s} &= \sum_{m=1}^{\infty}\frac{1}{m^s}\sum_{n=1}^{\infty}\frac{\mu(n)}{n^s} = \sum_{m,n=1}^{\infty}\frac{\mu(n)}{(mn)^s}\\ &= \sum_{t=1}^{\infty}\frac{1}{t^s}\sum_{d|t}\mu(d) = 1,\end{aligned}$$

where in the last step we have used Lemma 4.5. □

We have already seen that $\zeta(s)\to\infty$ as $s\to 1^+$. This gives rise to the question as to how exactly $\zeta(s)$ behaves as s approaches 1.

Theorem 4.7. *We have the following limit:*

$$\lim_{s\to 1^+}(s-1)\zeta(s) = 1.$$

Proof. We note that for a fixed s, t^{-s} is monotone decreasing as a function of t. Therefore

$$(n+1)^{-s} < \int_n^{n+1} t^{-s}dt < n^{-s}.$$

Now we sum all three expressions for all n from 1 to ∞, obtaining

$$\zeta(s)-1 < \int_1^{\infty} t^{-s}dt < \zeta(s),$$

and note that the improper integral in the middle evaluates to $1/(s-1)$. Multiplying everything by $s-1$, we then get

$$(s-1)(\zeta(s)-1) < 1 < (s-1)\zeta(s),$$

or, equivalently,

$$1-s < 1-(s-1)\zeta(s) < 0, \quad \Leftrightarrow \quad s > (s-1)\zeta(s) > 1.$$

Finally, taking the limit as $s\to 1^+$, we obtain the desired result. □

Remark: Though not part of this lecture, it should be mentioned at this point that $\zeta(s)$, seen as a function in $s\in\mathbb{C}$, has an analytic continuation to all of $\mathbb{C}$, with the exception of $s=1$. Theorem 4.7 indicates that $\zeta(s)$ has a simple pole at $s=1$, with residue 1.

The following result gives another connection between the Riemann zeta function and prime numbers.

Theorem 4.8.

$$\log \zeta(s) = \sum_p \frac{1}{p^s} + R(s),$$

where the sum is taken over all primes, and the function $R(s)$ remains bounded as $s \to 1^+$.

Proof. By Theorem 4.2 we have

$$\zeta(s) = \prod_{p \le N} \frac{1}{1-p^{-s}} \lambda_N(s),$$

where $\lambda_N(s) \to 1$ as $N \to \infty$. Taking logarithms, we obtain

$$\log \zeta(s) = \sum_{p \le N} \log \frac{1}{1-p^{-s}} + \log \lambda_N(s).$$

Now we use the fact that for $-1 < x < 1$ we have

$$\log \frac{1}{1-x} = x + \frac{x^2}{2} + \frac{x^3}{3} + \cdots,$$

so that

$$\log \zeta(s) = \sum_{p \le N} \sum_{m=1}^{\infty} \frac{p^{-ms}}{m} + \log \lambda_N(s).$$

Now we take the limit as $N \to \infty$ and note that $\log \lambda_N(s) \to 0$. Then we get

$$\log \zeta(s) = \sum_p \sum_{m=1}^{\infty} \frac{p^{-ms}}{m} = \sum_p p^{-s} + \sum_p \sum_{m=2}^{\infty} \frac{p^{-ms}}{m}.$$

Finally, we estimate the second term on the right, noting that it is less than

$$\sum_p \sum_{m=2}^{\infty} p^{-ms} = \sum_p p^{-2s} \frac{1}{1-p^{-s}} \le \frac{1}{1-2^{-s}} \sum_p p^{-2s} \le 2\,\zeta(s).$$

This completes the proof. □

4.2. **Bernoulli numbers.** This brief section is devoted to the *Bernoulli numbers*, a sequence of numbers that has important applications in number theory, combinatorics, and numerical analysis, among other areas.

Definition 4.9. *The numbers B_n, $n = 0, 1, 2, \ldots$, defined by the generating function*

$$\frac{t}{e^t - 1} = \sum_{n=0}^{\infty} B_n \frac{t^n}{n!} \qquad (|t| < 2\pi),$$

are called Bernoulli numbers.

By expanding the fraction on the left in a Taylor series, we can easily obtain the first few values $B_0 = 1$, $B_1 = -1/2$, $B_2 = 1/6$, $B_3 = 0$, $B_4 = -1/30$. A more convenient way of computing Bernoulli numbers is given by the following recurrence relation:

Theorem 4.10. *For all $k \ge 1$ we have*

$$(k+1)B_k = -\sum_{j=0}^{k-1} \binom{k+1}{j} B_j.$$

Proof. We use the identity

$$t = (e^t - 1)\frac{t}{e^t - 1} = \left(t + \frac{t^2}{2!} + \frac{t^3}{3!} + \cdots\right)\left(1 + \frac{B_1}{1!}t + \frac{B_2}{2!}t^2 + \frac{B_3}{3!}t^3 + \cdots\right),$$

where we have used Definition 4.9 and the Taylor expansion of the exponential function. Now we take the Cauchy product of the last line and equate coefficients of equal powers of t, obtaining

$$\frac{B_k}{k!} + \frac{B_{k-1}}{2!(k-1)!} + \frac{B_{k-2}}{3!(k-2)!} + \cdots + \frac{B_1}{k!} + \frac{1}{(k+1)!} = 0,$$

for $k \geq 1$. Finally we multiply this identity by $(k+1)!$ and use $\binom{k+1}{j} = \frac{(k+1)!}{j!(k+1-j)!}$, which leads to the desired identity. □

Example: We can use Theorem 4.10 to successively compute the first few Bernoulli numbers:

$$\begin{aligned} 2B_1 + 1 = 0 &\longrightarrow B_1 = -\frac{1}{2}, \\ 3B_2 + 3B_1 + 1 = 0 &\longrightarrow B_2 = \frac{1}{6}, \\ 4B_3 + 6B_2 + 4B_1 + 1 = 0 &\longrightarrow B_3 = 0, \\ 5B_4 + 10B_3 + 10B_2 + 5B_1 + 1 = 0 &\longrightarrow B_4 = -\frac{1}{30}, \end{aligned}$$

and so on, obtaining $B_5 = 0, B_6 = \frac{1}{42}, B_7 = 0, B_8 = -\frac{1}{30}, B_9 = 0, B_{10} = \frac{5}{66}$.

The fact that all these numbers appear to be small is a bit misleading; we will soon see that Bernoulli numbers increase very rapidly. However, it is obvious from the recurrence relation in Theorem 4.10 that all Bernoulli numbers are rational numbers. Another observation from the above example is that after B_1, all odd-index Bernoulli numbers are 0. This fact is not difficult to prove:

Theorem 4.11. *For all $k \geq 1$ we have $B_{2k+1} = 0$.*

Proof. Since $B_1 = -1/2$, we get with Definition 4.9,

$$S(t) := 1 + \sum_{n=2}^{\infty} B_n \frac{t^n}{n!} = \frac{t}{e^t - 1} + \frac{t}{2} = \frac{t}{2} \cdot \frac{e^t + 1}{e^t - 1}. \tag{4.1}$$

Now we note that

$$S(-1) = \frac{-t}{2} \cdot \frac{e^{-t} + 1}{e^{-t} - 1} = \frac{-t}{2} \cdot \frac{1 + e^t}{1 - e^t} = \frac{t}{2} \cdot \frac{e^t + 1}{e^t - 1} = S(t).$$

Hence $S(t)$ is an even function, and the Taylor coefficients of the odd powers of t in (4.1) must be 0. This proves the theorem. □

Much more could be said about Bernoulli numbers; at this point I will mention only that the denominators of the numbers B_n, for odd n, can be completely determined by the *Theorem of von Staudt and Clausen*. Also, closely related to the Bernoulli numbers are the *Bernoulli polynomials*. Many intermediate and advanced number theory books have sections on Bernoulli numbers and polynomials; see, e.g., [2].

4.3. **Euler's formula.** In this section we will establish a well-known connection between the Riemann zeta function and Bernoulli numbers. The following is known as *Euler's formula*.

Theorem 4.12. *For all $k \geq 1$ we have*

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

Before proving this, we derive a few immediate consequences. Using the values obtained in the example following Theorem 4.10, we find the following specific evaluations.

Corollary 4.13. *The first positive even integer values of the Riemann zeta function are*

$$\zeta(2) = \sum_{n=1}^{\infty} \frac{1}{n^2} = \frac{\pi^2}{6}, \qquad \zeta(4) = \sum_{n=1}^{\infty} \frac{1}{n^4} = \frac{\pi^4}{90}, \qquad \zeta(6) = \sum_{n=1}^{\infty} \frac{1}{n^6} = \frac{\pi^6}{945}.$$

Corollary 4.14. (*a*) *The even-index Bernoulli numbers have alternating signs. More specifically, for $k \geq 1$ we have*

$$(-1)^{k+1} B_{2k} > 0.$$

(*b*) *We have asymptotically*

$$(-1)^{k+1} B_{2k} \sim \frac{2(2k)!}{(2\pi)^{2k}} \quad \text{as} \quad k \to \infty.$$

Proof. Since $\zeta(2k) > 0$, part (a) follows immediately from Theorem 4.12. Furthermore, by Definition 4.1 we have $\zeta(2k) \to 1$ as $k \to \infty$. This proves part (b), again with Theorem 4.12. □

For the proof of Euler's formula we require two lemmas. As is the case with much of analytic number theory, concepts and results from complex analysis are required. The first lemma could be considered an "infinite partial fraction decomposition" of the function on the left.

Lemma 4.15. *For any $z \in \mathbb{C}$ with $|z| < 1$ we have*

$$\pi \cot(\pi z) = \frac{1}{z} + \sum_{n=1}^{\infty} \frac{2z}{z^2 - n^2}.$$

This is a standard result from classical complex analysis. For some hints about possible different proofs, see [2, p. 231].

Lemma 4.16. *For any $z \in \mathbb{C}$ with $|z| < \pi$ we have*

$$\cot z = \frac{1}{z} + \sum_{k=1}^{\infty} \frac{\zeta(2k)}{\pi^{2k}} z^{2k-1}.$$

Proof. In Lemma 4.15 we replace z by z/π, obtaining

$$\cot z = \frac{1}{z} - 2z \sum_{n=1}^{\infty} \frac{1}{n^2\pi^2 - z^2} \quad (|z| < \pi).$$

Now, with

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

we get

$$\cot z = \frac{1}{z} - 2z \sum_{n=1}^{\infty} \sum_{k=0}^{\infty} \frac{z^{2k}}{(n\pi)^{2k+2}}.$$

Now note that this double series converges absolutely for $|z| < \pi$, therefore we may interchange the order of summation:

$$\cot z = \frac{1}{z} - 2z \sum_{k=0}^{\infty} \frac{z^{2k}}{\pi^{2k+2}} \sum_{n=1}^{\infty} \frac{1}{n^{2k+2}} = \frac{1}{z} - 2 \sum_{k=1}^{\infty} \frac{z^{2k-1}}{\pi^{2k}} \zeta(2k),$$

where we have shifted the summation in the second line and then used the definition of the zeta function. This proves the lemma. □

We are now ready to prove Euler's formula.

Proof of Theorem 4.12. Using $\cos z = \frac{1}{2}(e^{iz} + e^{-iz})$ and $\sin z = \frac{1}{2i}(e^{iz} - e^{-iz})$, we obtain

$$\cot z = i \, \frac{e^{iz} + e^{-iz}}{e^{iz} - e^{-iz}} = \frac{i(e^{2iz} - 1) + 2i}{e^{2iz} - 1} = i + \frac{1}{z} \cdot \frac{2iz}{e^{2iz} - 1}. \tag{4.2}$$

On the other hand, by the definition of Bernoulli numbers we have

$$\frac{2iz}{e^{2iz} - 1} = \sum_{k=0}^{\infty} \frac{B_k}{k!} (2iz)^k = 1 - iz + \sum_{k=1}^{\infty} \frac{B_{2k}}{(2k)!} 2^{2k} (-1)^k z^{2k},$$

where we have used the fact that $B_{2k+1} = 0$ for $k \geq 1$. Comparing this last equation with (4.2) we then get

$$\cot z = \frac{1}{z} + \sum_{k=1}^{\infty} (-1)^k \frac{B_{2k} 2^{2k}}{(2k)!} z^{2k-1}.$$

Finally, equating coefficients of z^{2k-1} in this last equation and in Lemma 4.16, we get

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

which immediately gives Euler's formula. □

A great deal more could be said about the Riemann zeta function and its connections with the Bernoulli numbers. For instance, $\zeta(s)$ can be analytically continued to all of $\mathbb{C}$, with a simple pole at 0 as its only singularity. It can then be shown that

$$\zeta(-n) = -\frac{B_{n+1}}{n+1}, \qquad n = 1, 2, 3, \ldots,$$

which in particular means that by Theorem 4.11 we have $\zeta(-2n) = 0$ for $n = 1, 2, 3, \ldots$. These zeros are known as the *trivial zeros* of the Riemann zeta function, as opposed to the nontrivial zeros which, according to the famous *Riemann hypothesis*, are conjectured to all lie on the *critical line* $\mathrm{Re}(s) = \frac{1}{2}$.

We also note that Euler's formula implies that all values $\zeta(2k)$, $k = 1, 2, 3, \ldots$, are transcendental. No such formula exists for $\zeta(2k+1)$; it is only known that $\zeta(3)$ is irrational.

Some bibliographic notes

Most of the material in these four lectures was taken from the two excellent textbooks [2] and [4], where the former is more advanced than the latter. The other references below a referred to in the lectures. The handbook [6] is a very authoritative resource on special functions, with Chapters 24 and 25 relevant to these lectures.

References

[1] C. K. Caldwell, *The prime pages. Prime number research, records, and resources*, `http://www.utm.edu/research/primes/`
[2] K. Ireland and M. Rosen, *A classical introduction to modern number theory*, Second Edition, Springer-Verlag, New York, 1990.
[3] A. Ya. Khinchin, *Continued fractions*, Third Edition, University of Chicago Press, 1964.
[4] I. Niven, H. S. Zuckerman and H. L. Montgomery, *An introduction to the theory of numbers*, Fifth Edition, Wiley, New York, 1991.
[5] C. D. Olds, *Continued fractions*, Random House, New York, 1963.
[6] F. W. J. Olver et al. (eds.), *NIST Handbook of Mathematical Functions*, Cambridge Univ. Press, New York, 2010. Online companion: `http://dlmf.nist.gov/`.
[7] H. S. Wall, *Analytic theory of continued fractions*, Van Nostrand, New York, 1948.

Department of Mathematics and Statistics, Dalhousie University, Halifax, Nova Scotia, B3H 4R2, Canada
E-mail address: `dilcher@mathstat.dal.ca`