Number theory

Luka Horjak (luka1.horjak@gmail.com)

March 8, 2024

Contents

Introduction

These are my lecture notes on the course Number theory in the year 2023/24. The lecturer that year was gost. izr. prof. dr. rer. nat. Daniel Smertnig.

The notes are not perfect. I did not write down most of the examples that help with understanding the course material. I also did not formally prove every theorem and may have labeled some as trivial or only wrote down the main ideas.

I have most likely made some mistakes when writing these notes – feel free to correct them.

1 Distribution of prime numbers

1.1 Riemann zeta function

February 23, 2024

Definition 1.1.1. The *prime counting function* is defined as

$$\pi(x) = \left|\{p \in \mathbb{P} \mid p \leq x\}\right|.$$

Definition 1.1.2. Let $(a_n)_n \subseteq \mathbb{C}$ be a sequence. The infinite product

$$\prod_{n=1}^{\infty} a_n$$

converges *absolutely* if it converges normally as a product of constant functions.

Theorem 1.1.3. Let $\sigma > 1$ be a real number. For $s \in \mathbb{C}$ with $\mathrm{Re}(s) \geq \sigma$, we have

$$\sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_{p \in \mathbb{P}} (1 - p^{-s})^{-1},$$

with both the product and sum converging uniformly and absolutely.[1]

Proof. Note that

$$\sum_{n=1}^{\infty} \left|\frac{1}{n^s}\right| = \sum_{n=1}^{\infty} \frac{1}{n^{\mathrm{Re}(s)}} \leq \sum_{n=1}^{\infty} \frac{1}{n^\sigma}$$

is convergent, hence the given series converges as well. To prove the convergence of the product, first note that

$$\prod_{p \in \mathbb{P}} (1 - p^{-s})^{-1} = \prod_{p \in \mathbb{P}} \left(\sum_{k=0}^{\infty} p^{-sk}\right).$$

As

$$\sum_{p \in \mathbb{P}} \left|\sum_{k=1}^{\infty} p^{-sk}\right| \leq \sum_{p \in \mathbb{P}} \left(\sum_{k=1}^{\infty} (p^k)^{-\sigma}\right) \leq \sum_{n=1}^{\infty} n^{-\sigma}$$

converges normally, so does the product. To prove equality, we can bound

$$\left|\prod_{\substack{p \in \mathbb{P} \\ p \leq x}} \frac{1}{1 - p^{-s}} - \sum_{n=1}^{x} \frac{1}{n^s}\right| \leq \sum_{n=x+1}^{\infty} \left|\frac{1}{n^s}\right| \leq \sum_{n=x+1}^{\infty} \frac{1}{n^\sigma},$$

which converges to 0 as $x \to \infty$. $\square$

Definition 1.1.4. The *Riemann zeta function* is defined as

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

for $\mathrm{Re}(s) > 1$.

Lemma 1.1.5. If $\mathrm{Re}(s) > 1$, then $\zeta(s) \neq 0$.

[1] See Complex analysis, section 3 for definition and properties of convergence for products.

Proof. No term in the infinite product is equal to 0. $\square$

Proposition 1.1.6. The function $\zeta(s)-\frac{1}{s-1}$ has a holomorphic continuation to $\mathrm{Re}(s)>0$.

Proof. We can write

$$\begin{aligned}\zeta(s)-\frac{1}{s-1} &= \sum_{n=1}^{\infty} n^{-s} - \int_1^\infty x^{-s}\,dx \\ &= \sum_{n=1}^{\infty}\left(n^{-s}-\int_n^{n+1} x^{-s}\,dx\right) \\ &= \sum_{n=1}^{\infty}\int_n^{n+1}\left(n^{-s}-x^{-s}\right)\,dx\end{aligned}$$

as long as $\mathrm{Re}(s)>1$. Now, for $n\le x\le n+1$, we can bound

$$\left|n^{-s}-x^{-s}\right| = \left|\int_n^x su^{-s-1}\,du\right| \le \frac{|s|}{n^{\mathrm{Re}(s)+1}}.$$

Let $L\subseteq\{z\in\mathbb{C}\mid \mathrm{Re}(z)>0\}$ be a compact set. As

$$\left|\sum_{n=1}^{\infty}\int_n^{n+1}\left(n^{-s}-x^{-s}\right)\,dx\right| \le \sum_{n=1}^{\infty}\frac{|s|}{n^{\mathrm{Re}(s)+1}} \le \|\mathrm{id}\|_L\cdot\sum_{n=1}^{\infty}\frac{1}{n^{\sigma+1}}$$

for all $s\in L$, where $\sigma=\min_L|z|$, the series converges uniformly on compact sets. $\square$

Remark 1.1.6.1. The ζ function can be analytically extended to $\mathbb{C}\setminus\{1\}$ by

$$\zeta(1-s) = 2\cdot(2\pi)^{-s}\cos\left(\frac{\pi}{2}s\right)\Gamma(s)\zeta(s).$$

It has a simple pole with residue 1 at 1.

Lemma 1.1.7. The equation $\overline{\zeta(\overline{s})}=\zeta(s)$ holds for all $s\in\mathbb{C}\setminus\{1\}$.

Proof. The function $\overline{\zeta(\overline{s})}$ is holomorphic. As it coincides with $\zeta(s)$ for $s\ge 1$, the functions are equal. $\square$

1.2 Prime number theorem

Proposition 1.2.1. The series
$$\sum_{p\in\mathbb{P}} \frac{\log(p)}{p^s}$$
converges uniformly and absolutely for $\mathrm{Re}(s) \geq \sigma > 1$.

Proof. We can bound
$$\sum_{p\in\mathbb{P}} \left|\frac{\log(p)}{p^s}\right| \leq \sum_{p\in\mathbb{P}} \frac{\log(p)}{p^\sigma} \leq \sum_{n=1}^{\infty} \frac{\log(p)}{n^\varepsilon} \cdot \frac{1}{n^{\sigma-\varepsilon}},$$
which clearly converges for $0 < \varepsilon < \sigma - 1$. □

Definition 1.2.2. We define functions
$$\theta(x) = \sum_{\substack{p\in\mathbb{P}\\ p\leq x}} \log(p)$$
and
$$\phi(s) = \sum_{p\in\mathbb{P}} \frac{\log(p)}{p^s}.$$

Remark 1.2.2.1. The function ϕ is holomorphic for $\mathrm{Re}(s) > 1$.

Proposition 1.2.3. The function ϕ has a meromorphic continuation to $\mathrm{Re}(s) > \frac{1}{2}$. It has simple poles at points $s = 1$ and zeros of $\zeta(s)$.

Proof. Calculate the logarithmic derivative of ζ as
$$\begin{aligned}
-\frac{\zeta'(s)}{\zeta(s)} &= -\sum_{p\in\mathbb{P}} \frac{\left((1-p^{-s})^{-1}\right)'}{(1-p^{-s})^{-1}} \\
&= -\sum_{p\in\mathbb{P}} \frac{-(1-p^{-s})^{-2}\cdot p^{-s}\log(p)}{(1-p^{-s})^{-1}} \\
&= \sum_{p\in\mathbb{P}} \frac{\log(p)}{p^s - 1} \\
&= \phi(s) + \sum_{p\in\mathbb{P}} \frac{\log(p)}{p^s(p^s-1)}.
\end{aligned}$$
Similarly as in the proof of proposition 1.2.1, we can show that the above series converges locally uniformly and absolutely for $\mathrm{Re}(s) > \frac{1}{2}$. □

Theorem 1.2.4. If $\mathrm{Re}(s) = 1$, then $\zeta(s) \neq 0$.

Proof. Let $\mu = \mathrm{ord}_{1+ib}\,\zeta \geq 0$. As $\zeta(\overline{z}) = \overline{\zeta(z)}$, we also have $\mu = \mathrm{ord}_{1-ib}\,\zeta$. $\theta = \mathrm{ord}_{1+2ib}\,\zeta = \mathrm{ord}_{1-2ib}\,\zeta$. As ϕ has a simple pole at 1, we have
$$\lim_{\varepsilon\to 0} \varepsilon\phi(1+\varepsilon) = 1.$$

Similarly,

$$\lim_{\varepsilon\to 0} \varepsilon\phi(1+\varepsilon \pm ib) = -\mu,$$

as the logarithmic derivative of ζ at b has residue $-\mu$, and

$$\lim_{\varepsilon\to 0} \varepsilon\phi(1+\varepsilon \pm 2ib) = -\theta.$$

Now compute

$$f(\varepsilon) = \sum_{r=-2}^{2} \binom{4}{2+r} \phi(1+\varepsilon+rib) = \sum_{p\in\mathbb{P}} \frac{\log(p)}{p^{1+\varepsilon}} \cdot \left(p^{\frac{ib}{2}} - p^{-\frac{ib}{2}}\right)^4 = \sum_{p\in\mathbb{P}} \frac{\log(p)}{p^{1+\varepsilon}} \cdot \left(2\operatorname{Re}\left(p^{\frac{ib}{2}}\right)\right)^4.$$

It follows that

$$0 \le \lim_{\varepsilon\to 0} \varepsilon \cdot f(\varepsilon) = 6 - 8\mu - 2\theta.$$

As $\theta \ge 0$, we have $\mu = 0$. □

Corollary 1.2.4.1. The function ϕ is holomorphic for $\operatorname{Re}(s) = 1$, except for a simple pole with residue 1 at 1. In particular, the function

$$g(z) = \frac{\phi(z+1)}{z+1} - \frac{1}{z}$$

is holomorphic for $\operatorname{Re}(z) \ge 0$.

Proof. The proof is obvious and need not be mentioned. □

Lemma 1.2.5. Let $x \ge 0$. Then $\theta(x) \le 4x$.

Proof. First let $n \in \mathbb{N}$ be an integer. Then

$$e^{\theta(2n)-\theta(n)} = \prod_{n<p\le 2n} p \le \binom{2n}{n} \le 2^{2n},$$

therefore $\theta(2n) - \theta(n) \le 2n\log(2)$. Now let $n = \left\lceil \frac{x}{2} \right\rceil$. Then

$$\theta(x) - \theta\left(\frac{x}{2}\right) \le \theta(2n) - \theta(n-1) \le \log(n) + 2n\log(2) \le 3n \le 2x$$

for all $x \ge 6$, but we can manually check that it holds for $x < 6$ as well. But then

$$\theta(x) = \sum_{n=0}^{\infty} \left(\theta\left(\frac{x}{2^n}\right) - \theta\left(\frac{x}{2^{n+1}}\right)\right) \le \sum_{n=0}^{\infty} \frac{2x}{2^n} = 4x.$$ □

Lemma 1.2.6. Let $h\colon \mathbb{R}_{\ge 0} \to \mathbb{C}$ be bounded and locally integrable. Then the following statements are true:

i) The Laplace transform

$$H(z) = \int_0^\infty h(t)e^{-zt}\,dt$$

of h is holomorphic for $\operatorname{Re}(z) > 0$.

March 1, 2024

ii) The function

$$\int_0^T h(t)e^{-zt}\,dt$$

is holomorphic for all $z \in \mathbb{C}$.

Proof.

i) Analysis 2b, proposition 4.1.4.

ii) Evident. □

Theorem 1.2.7. Let $h\colon \mathbb{R}_{\geq 0} \to \mathbb{C}$ be bounded and locally integrable. Suppose that its Laplace transform

$$H(z) = \int_0^\infty h(t)e^{-zt}\,dt$$

extends to a holomorphic function on $\operatorname{Re}(z) \geq 0$. Then

$$H(0) = \int_0^\infty h(t)\,dt.$$

Proof. Define

$$H_T(z) = \int_0^T h(t)e^{-zt}\,dt$$

for $T > 0$. Fix some $R > 0$ and consider the region

$$\Omega = \left\{z \in \mathbb{\Delta}(R) \mid \operatorname{Re}(z) \geq -\delta\right\}.$$

By compactness of $i[-R, R]$, we can pick a δ such that H is holomorphic on Ω. Now partition $\partial\Omega$ into sets $C_1 = \{z \in \partial\Omega \mid \operatorname{Re}(z) \geq 0\}$, $C_2 = \{z \in \partial\Omega \mid -\delta < \operatorname{Re}(z) < 0\}$ and $C_3 = \{z \in \partial\Omega \mid \operatorname{Re}(z) = -\delta\}$. Taking

$$I(z) = \frac{H(z) - H_T(z)}{z} e^{zT}\left(1 + \frac{z^2}{R^2}\right),$$

we can write

$$H(0) - H_T(0) = \frac{1}{2\pi i}\oint\limits_{\partial\Omega} I(z)\,dz$$

using the Cauchy integral formula. Setting $B = \max\left\{|h(t)| \mid t \in \mathbb{R}_{\geq 0}\right\}$, we can bound

$$|H(z) - H_T(z)| \leq \int_T^\infty |h(t)| \cdot \left|e^{-zt}\right|\,dt \leq B\frac{e^{-\operatorname{Re}(z)T}}{\operatorname{Re}(z)},$$

hence

$$|I(z)| \leq \frac{B}{\operatorname{Re}(z)} \cdot \left|1 + \frac{z^2}{R^2}\right| \cdot \left|\frac{1}{z}\right| = \frac{B}{R\operatorname{Re}(z)} \cdot \left|\frac{z}{R} + \frac{R}{z}\right| = \frac{B}{R\operatorname{Re}(z)} \cdot 2\operatorname{Re}\left(\frac{z}{R}\right) = \frac{2B}{R^2}$$

for $z \in C_1$. Integrating, we find that

$$\frac{1}{2\pi} \cdot \int\limits_{C_1} |I(z)|\,dz \leq \frac{B}{R}.$$

Next, we bound the integral of H_T over $C_2 \cup C_3$. As H_T is holomorphic, we can write

$$\int_{C_2 \cup C_3} H_T(z)\, dz = \int_{-C_1} H_T(z)\, dz,$$

but as

$$|H_T(z)| \leq \int_0^T \left|h(z)e^{-zt}\right| \, dt \leq B \int_0^T e^{-\operatorname{Re}(z)t} \, dt = \frac{B}{\operatorname{Re}(z)} \cdot \left(1 - e^{-\operatorname{Re}(z)T}\right) \leq B \frac{e^{-\operatorname{Re}(z)T}}{|\operatorname{Re}(z)|},$$

which is the same bound as above. As

$$\left| H(z) \cdot \left(1 + \frac{z^2}{R^2}\right) \cdot \frac{1}{z} \right| \leq M$$

on $C_2 \cup C_3$ for some $M > 0$, we see that

$$\left| H(z) \cdot \left(1 + \frac{z^2}{R^2}\right) \cdot \frac{1}{z} \right| \cdot \left|e^{zT}\right|$$

converges to 0 as $T \to \infty$. By the dominated convergence theorem, the integral

$$\frac{1}{2\pi} \cdot \int_{C_2 \cup C_3} \left| H(z) \left(1 + \frac{z^2}{R^2}\right) \cdot \frac{1}{z} \right| \cdot \left|e^{zT}\right| \, dz$$

converges to 0 as well. Then

$$\limsup_{T \to \infty} |H(0) - H_T(0)| \leq \frac{2B}{R},$$

which, by taking $R \to \infty$, implies

$$\lim_{T \to \infty} H_T(0) = H(0). \qquad \square$$

Lemma 1.2.8. For $\operatorname{Re}(z) > 0$, we have

$$g(z) = \int_0^\infty \left(\theta\left(e^t\right) e^{-t} - 1\right) e^{-zt} \, dt,$$

where g is defined as in corollary 1.2.4.1.

Proof. Note that $\theta\left(e^t\right) e^{-t} - 1$ is bounded, hence the given Laplace transform exists. Let

$(p_n)_n$ be the ascending sequence of prime numbers. Setting $p_0 = 1$, we have

$$\begin{aligned}
\phi(s) &= \sum_{p\in\mathbb{P}} \frac{\log(p)}{p^s} \\
&= \sum_{j=1}^{\infty} \frac{\theta(p_j) - \theta(p_{j-1})}{p_j^s} \\
&= \sum_{j=0}^{\infty} \theta(p_j) \cdot \left(\frac{1}{p_j^s} - \frac{1}{p_{j+1}^s}\right) \\
&= \sum_{j=0}^{\infty} \theta(p_j) s \int_{p_j}^{p_{j+1}} \frac{1}{x^{s+1}}\, dx \\
&= \sum_{j=0}^{\infty} s \int_{p_j}^{p_{j+1}} \frac{\theta(x)}{x^{s+1}}\, dx \\
&= s \int_1^{\infty} \frac{\theta(x)}{x^{s+1}}\, dx \\
&= s \int_0^{\infty} \theta(e^t) e^{-st}\, dt
\end{aligned}$$

for all $\mathrm{Re}(s) > 1$. Hence

$$g(z) = \int_0^{\infty} \theta(e^t) e^{-(z+1)t}\, dt - \int_0^{\infty} e^{-zt}\, dt = \int_0^{\infty} \left(\theta\left(e^t\right) e^{-t} - 1\right) e^{-zt}\, dt. \qquad \square$$

Theorem 1.2.9. The integral

$$\int_1^{\infty} \frac{\theta(x) - x}{x^2}\, dx$$

exists.

Proof. We compute

$$\int_1^{e^T} \frac{\theta(x) - x}{x^2}\, dx = \int_0^T \left(\theta\left(e^t\right) e^{-t} - 1\right) dt.$$

Applying theorem 1.2.7, the claim follows. □

Theorem 1.2.10. We have $\theta(x) \sim x$, that is

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

Proof. Suppose otherwise. We split two cases:

i) For some $\lambda > 1$, there exist arbitrarily large x such that $\theta(x) \geq \lambda x$. We can compute

$$\int_x^{\lambda x} \frac{\theta(t) - t}{t^2}\, dt \geq \int_x^{\lambda x} \frac{\lambda x - t}{t^2}\, dt = \int_1^{\lambda} \frac{\lambda x - xy}{x^2 y^2} x\, dy = \int_1^{\lambda} \frac{\lambda - y}{y^2}\, dy = c > 0.$$

This contradicts the previous theorem.

ii) For some $\lambda < 1$, there exist arbitrarily large x such that $\theta(x) \leq \lambda x$. As above, we can compute

$$\int_{\lambda x}^{x} \frac{\theta(t) - t}{t^2}\, dt \leq \int_{\lambda x}^{x} \frac{\lambda x - t}{t^2}\, dt = \int_{\lambda}^{1} \frac{\lambda - y}{y^2}\, dy = c < 0.$$

This again contradicts the previous theorem. □

Theorem 1.2.11 (Prime number theorem)**.** The prime counting function is asymptotically equivalent to $\frac{x}{\log(x)}$.

Proof. Note that

$$\theta(x) \leq \log(x) \cdot \pi(x)$$

and

$$\theta(x) \geq \sum_{\substack{p \in \mathbb{P} \\ x^{1-\varepsilon} \leq p \leq x}} \log(p) \geq (1 - \varepsilon) \log(x) \cdot \left(\pi(x) - x^{1-\varepsilon}\right),$$

therefore

$$\frac{\theta(x)}{x} \leq \frac{\pi(x) \log(x)}{x} \leq \frac{\theta(x)}{(1-\varepsilon)x} + \frac{\log(x)}{x^{\varepsilon}}.$$

This implies

$$1 \leq \limsup_{x \to \infty} \frac{\pi(x) \log(x)}{x} \leq \frac{1}{1 - \varepsilon}$$

and

$$1 \leq \liminf_{x \to \infty} \frac{\pi(x) \log(x)}{x} \leq \frac{1}{1 - \varepsilon}.$$

□

2 Algebraic integers

2.1 Gaussian integers

Definition 2.1.1. A domain R is *Euclidean* if there is a $\delta \colon \mathbb{R} \setminus \{0\} \to \mathbb{N}_0$, such that for all $a \in R$ and $b \in R \setminus \{0\}$ we can write $a = bq + r$ for $q, r \in R$, such that $r = 0$ or $\delta(r) < \delta(b)$.

Proposition 2.1.2. The Gaussian integers are an Euclidean domain.

Proof. Algebra 2, theorem 6.3.4. □

Definition 2.1.3. A domain R is a *unique factorisation domain* if every $\alpha \in R$ is of the form

$$\alpha = \prod_{i=1}^{n} p_i$$

for irreducible elements in a unique way up to permutation and multiplication of factors by a unit element.

Remark 2.1.3.1. Principal ideal domains (and therefore $\mathbb{Z}[i]$) are unique factorisation domains.

Lemma 2.1.4. The function $N \colon \mathbb{Z}[i] \to \mathbb{N}_0$, given by $N(a+bi) = a^2+b^2$, has the following properties:

i) The equality $N(\alpha) = 0$ is equivalent to $\alpha = 0$.

ii) For all $\alpha, \beta \in \mathbb{Z}[i]$ we have $N(\alpha\beta) = N(\alpha) \cdot N(\beta)$.

iii) An element $\alpha \in \mathbb{Z}[i]$ is invertible if and only if $N(\alpha) = 1$.

Proof. The proof is obvious and need not be mentioned. □

Lemma 2.1.5. Let $p \in \mathbb{P}$ be a prime. Then -1 is a quadratic residue modulo p if and only if $p = 2$ or $p \equiv 1 \pmod{4}$.

Proof. If $p \equiv 1 \pmod{4}$, we can write $-1 \equiv \left(e^{\frac{p-1}{4}}\right)^2 \pmod{p}$. If $p \equiv 3 \pmod{4}$ and $p \mid c^2 + 1$, then

$$1 \equiv \left(c^2\right)^{\frac{p-1}{2}} \equiv (-1)^{\frac{p-1}{2}} = -1,$$

a clear contradiction. □

Theorem 2.1.6 (Fermat)**.** Let p be an odd prime. Then p can be written as a sum of two squares if and only if $p \equiv 1 \pmod{4}$.

Proof. It is clear that primes $p \equiv 3 \pmod{4}$ cannot be written in such a way. Now suppose that $p \equiv 1 \pmod{4}$ and take $b \in \mathbb{N}$ such that $b^2 \equiv -1 \pmod{p}$. Now note that $p \mid (b-i)(b+i)$, but p clearly can't divide either factor. It follows that p is not a prime element, hence we can factor it as $p = \alpha\beta$.

Now, write $p^2 = N(p) = N(\alpha) \cdot N(\beta)$, therefore $N(\alpha) = p$, which gives us a representation of p as a sum of two squares. □

Proposition 2.1.7. Up to associativity, the prime elements of $\mathbb{Z}[i]$ are the following:

i) $1+i$,

ii) $a+bi$ with $a^2+b^2=p\in\mathbb{P}$ with $p\equiv 1 \pmod 4$ and $0<|b|<a$,

iii) $p\in\mathbb{P}$ with $p\equiv 3 \pmod 4$.

Proof. It is clear that $1+i$ is a prime element. Elements of the second form are prime by the proof of the previous theorem. For the last one, if $p=\alpha\beta$ for non-invertible α and β, then $N(\alpha)=N(\beta)=p$, which is of course impossible. Clearly, they are not associated.

Suppose now that $p\in\mathbb{Z}[i]$ is a prime element. Then $N(p)=p\overline{p}$, which can be factored in integers. But then p divides some prime element $q\in\mathbb{P}$. It follows that $N(p)\mid q^2$, but as q^2 can be factored by the above prime elements, p is of such form. □

Theorem 2.1.8. Let $n\in\mathbb{N}$. Then there exist integers a and b such that $n=a^2+b^2$ if and only if $2\mid \nu_p(n)$ for all prime numbers $p\equiv 3 \pmod 4$.

Proof. It is clear that all such numbers can be written as a sum of two squares, as the property is multiplicative. For the converse, suppose that $n=a^2+b^2$ and take any prime number $p\in\mathbb{P}$ such that $p\equiv 3 \pmod 4$ and $p\mid n$. Then, if b is invertible in $\mathbb{Z}_p$, we can write

$$p \;\middle|\; \left(\frac{a}{b}\right)^2+1\,,$$

which is impossible. It follows that $p\mid a,b$. The theorem is now proven by infinite descent. □

Remark 2.1.8.1. This theorem can also be proven by factoring $\alpha=a+bi$.

Remark 2.1.8.2. A positive integer n can be written as a sum of 3 squares if and only if it is not of the form $n=4^a\cdot(8k+7)$.

Proposition 2.1.9. Let $\alpha\in\mathbb{Q}(i)$. Then $\alpha\in\mathbb{Z}[i]$ if and only if there exist some $c,d\in\mathbb{Z}$ such that α is a root of the polynomial $P(x)=x^2+cx+d$.

Proof. We see that $P(\alpha)=0$ and $\alpha\notin\mathbb{Q}$ is equivalent to $P(x)=(x-\alpha)\,(x-\overline{\alpha})$. Of course, if $\alpha\in\mathbb{Q}$, we must have $\alpha\in\mathbb{Z}$ by characterisation of rational roots of integer polynomials. Otherwise, for $\alpha=a+bi$, the condition is equivalent to $2a\in\mathbb{Z}$ and $a^2+b^2\in\mathbb{Z}$, which is only possible if both $a\in\mathbb{Z}$ and $b\in\mathbb{Z}$. □

Index