A Rapid Introduction to Analytic Number Theory

Ryan Braiden (He/Him)

$M_{\iint}$ Talk

21 March, 2025

What is analytic number theory?

- A paradox: integers are discrete, yet analysis (usually) deals with continuous phenomena.

What is analytic number theory?

- A paradox: integers are discrete, yet analysis (usually) deals with continuous phenomena.
- Elementary vs. Non-elementary (classical) approaches

What is analytic number theory?

- A paradox: integers are discrete, yet analysis (usually) deals with continuous phenomena.
- Elementary vs. Non-elementary (classical) approaches

Elementary

- Real-valued (assymptotic) estimation of arithmetic functions or sums thereof; i.e, without complex or harmonic analysis.

What is analytic number theory?

- A paradox: integers are discrete, yet analysis (usually) deals with continuous phenomena.
- Elementary vs. Non-elementary (classical) approaches

Elementary

- Real-valued (assymptotic) estimation of arithmetic functions or sums thereof; i.e, without complex or harmonic analysis.
- Sieve methods (i.e sieve of Eratosthenes, the large sieve; sieve methods important in modern An.NT)

What is analytic number theory?

- A paradox: integers are discrete, yet analysis (usually) deals with continuous phenomena.
- Elementary vs. Non-elementary (classical) approaches

Elementary

- Real-valued (assymptotic) estimation of arithmetic functions or sums thereof; i.e, without complex or harmonic analysis.
- Sieve methods (i.e sieve of Eratosthenes, the large sieve; sieve methods important in modern An.NT)

Non-elementary

- Use of transformations: e.g, Dirichlet series over $\mathbb{C}$,

$$\{n \mapsto a_n\} \longleftrightarrow D(s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s}.$$

What is analytic number theory?

- A paradox: integers are discrete, yet analysis (usually) deals with continuous phenomena.
- Elementary vs. Non-elementary (classical) approaches

Elementary

- Real-valued (assymptotic) estimation of arithmetic functions or sums thereof; i.e, without complex or harmonic analysis.
- Sieve methods (i.e sieve of Eratosthenes, the large sieve; sieve methods important in modern An.NT)

Non-elementary

- Use of transformations: e.g, Dirichlet series over $\mathbb{C}$,

$$\{n \mapsto a_n\} \longleftrightarrow D(s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s}.$$

- Riemann zeta function:

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

The squarefree integers

Definition

We say that a positive integer is squarefree if it is not divisible by the square of any prime. I.e, the squarefree integers up to 20 are

$$1, 2, 3, 5, 6, 7, 10, 11, 13, 14, 15, 17, 19$$

The squarefree integers

Definition

We say that a positive integer is squarefree if it is not divisible by the square of any prime. I.e, the squarefree integers up to 20 are

$$1, 2, 3, 5, 6, 7, 10, 11, 13, 14, 15, 17, 19$$

Let $Q(x)$ denote the number of integers less than or equal to $x \in \mathbb{R}$ that are squarefree. We have just seen that $Q(20) = 13$. Indeed, $Q(20)/20 = 0.65$.

The squarefree integers

Definition

We say that a positive integer is squarefree if it is not divisible by the square of any prime. I.e, the squarefree integers up to 20 are

$$1, 2, 3, 5, 6, 7, 10, 11, 13, 14, 15, 17, 19$$

Let $Q(x)$ denote the number of integers less than or equal to $x \in \mathbb{R}$ that are squarefree. We have just seen that $Q(20) = 13$. Indeed, $Q(20)/20 = 0.65$.

- Question: What proportion of positive integers are squarefree?

The squarefree integers

Definition

We say that a positive integer is squarefree if it is not divisible by the square of any prime. I.e, the squarefree integers up to 20 are

$$1, 2, 3, 5, 6, 7, 10, 11, 13, 14, 15, 17, 19$$

Let $Q(x)$ denote the number of integers less than or equal to $x \in \mathbb{R}$ that are squarefree. We have just seen that $Q(20) = 13$. Indeed, $Q(20)/20 = 0.65$.

- Question: What proportion of positive integers are squarefree?
- Interpretation: Does the limit

$$\lim_{x\to\infty} \frac{Q(x)}{x}$$

exist; and if so, what is its value (which we call the asymptotic density of Q).

The squarefree integers

Definition

We say that a positive integer is squarefree if it is not divisible by the square of any prime. I.e, the squarefree integers up to 20 are

$$1, 2, 3, 5, 6, 7, 10, 11, 13, 14, 15, 17, 19$$

Let $Q(x)$ denote the number of integers less than or equal to $x \in \mathbb{R}$ that are squarefree. We have just seen that $Q(20) = 13$. Indeed, $Q(20)/20 = 0.65$.

- Question: What proportion of positive integers are squarefree?
- Interpretation: Does the limit

$$\lim_{x \to \infty} \frac{Q(x)}{x}$$

exist; and if so, what is its value (which we call the asymptotic density of Q). Exercise: $P(x) := \pi(x) \log x$?

A heuristic investigation of Q

We can proceed Sieve-theoretically!

A heuristic investigation of Q

We can proceed Sieve-theoretically! For some $n \in \mathbb{Z}^+$, consider the first $4 \cdot 9 \cdot 25 \cdot n = 900n$ integers.

A heuristic investigation of Q

We can proceed Sieve-theoretically! For some $n \in \mathbb{Z}^+$, consider the first $4 \cdot 9 \cdot 25 \cdot n = 900n$ integers. Removing all multiples of 4, the proportion of integers in this range that remain are

$$\frac{(900 - 900/4)n}{900n} = 3/4.$$

A heuristic investigation of Q

We can proceed Sieve-theoretically! For some $n \in \mathbb{Z}^+$, consider the first $4 \cdot 9 \cdot 25 \cdot n = 900n$ integers. Removing all multiples of 4, the proportion of integers in this range that remain are

$$\frac{(900 - 900/4)n}{900n} = 3/4.$$

Similarly, removing multiples of 9 and 25 gives us remaining proportions of $8/9$ and $24/25$ respectively.

A heuristic investigation of Q

We can proceed Sieve-theoretically! For some $n \in \mathbb{Z}^+$, consider the first $4 \cdot 9 \cdot 25 \cdot n = 900n$ integers. Removing all multiples of 4, the proportion of integers in this range that remain are

$$\frac{(900 - 900/4)n}{900n} = 3/4.$$

Similarly, removing multiples of 9 and 25 gives us remaining proportions of $8/9$ and $24/25$ respectively.

We can assign a probability, $\mathbb{P}(p^2 \nmid n) = (p^2 - 1)/p^2 = 1 - 1/p^2$, for each p^2, where p is prime.

A heuristic investigation of Q

We can proceed Sieve-theoretically! For some $n \in \mathbb{Z}^+$, consider the first $4 \cdot 9 \cdot 25 \cdot n = 900n$ integers. Removing all multiples of 4, the proportion of integers in this range that remain are

$$\frac{(900 - 900/4)n}{900n} = 3/4.$$

Similarly, removing multiples of 9 and 25 gives us remaining proportions of $8/9$ and $24/25$ respectively.

We can assign a probability, $\mathbb{P}(p^2 \nmid n) = (p^2 - 1)/p^2 = 1 - 1/p^2$, for each p^2, where p is prime. If p and q are distinct primes, then $p^2 \nmid n$ doesn't seem to influence the "probability" that $q^2 \nmid n$; we can think about these "probabilities" as independent.

A heuristic investigation of Q

We can proceed Sieve-theoretically! For some $n \in \mathbb{Z}^+$, consider the first $4 \cdot 9 \cdot 25 \cdot n = 900n$ integers. Removing all multiples of 4, the proportion of integers in this range that remain are

$$\frac{(900 - 900/4)n}{900n} = 3/4.$$

Similarly, removing multiples of 9 and 25 gives us remaining proportions of $8/9$ and $24/25$ respectively.

We can assign a probability, $\mathbb{P}(p^2 \nmid n) = (p^2 - 1)/p^2 = 1 - 1/p^2$, for each p^2, where p is prime. If p and q are distinct primes, then $p^2 \nmid n$ doesn't seem to influence the "probability" that $q^2 \nmid n$; we can think about these "probabilities" as independent. Thus

$$\begin{aligned} \lim_{x \to \infty} \frac{Q(x)}{x} &= \lim_{k \to \infty} \mathbb{P}(\{4 \nmid n\} \cap \cdots \cap \{p_k^2 \nmid n\}) \\ &= \lim_{k \to \infty} \mathbb{P}(4 \nmid n) \cdots \mathbb{P}(p_k^2 \nmid n) = \prod_p \left(1 - \frac{1}{p^2}\right). \end{aligned}$$

The zeta function

Definition

Let $\zeta : \mathbb{R}_{>1} \to \mathbb{R}$ such that

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

We call ζ the zeta function on the real line $s > 1$.

Note: we know that ζ is defined on its domain (p-test) and uniformally convergent on any interval $[\alpha, \infty)$, $\alpha > 1$, (Weierstrass' M-test).

Euler products

The zeta function is a “suitably nice” Dirichlet series and so it has an Euler product; namely,

Zeta as a product indexed by the primes

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

Euler proved this using a simple Sieve method!

Euler products

The zeta function is a "suitably nice" Dirichlet series and so it has an Euler product; namely,

Zeta as a product indexed by the primes

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

Euler proved this using a simple Sieve method! As such, we can compute our proportion (conjectured earlier)

$\zeta(2) = \pi^2/6$

$$\prod_p \left(1 - \frac{1}{p^2}\right) = \zeta(2)^{-1} = \frac{6}{\pi^2}.$$

Euler products

The zeta function is a "suitably nice" Dirichlet series and so it has an Euler product; namely,

Zeta as a product indexed by the primes

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

Euler proved this using a simple Sieve method! As such, we can compute our proportion (conjectured earlier)

$\zeta(2) = \pi^2/6$

$$\prod_p \left(1 - \frac{1}{p^2}\right) = \zeta(2)^{-1} = \frac{6}{\pi^2}.$$

This is well-known but non-trivial. Euler did it without Dirichlet's methods!

Time to make things precise...

The Proportion of Squarefree Integers

$$\lim_{x\to\infty} \frac{Q(x)}{x} = \frac{6}{\pi^2} \approx 0.608.$$

Proof [BD]: We want to make precise the notion of independence of $\{p^2 \nmid n\}$ from $\{q^2 \nmid n\}$.

Time to make things precise...

The Proportion of Squarefree Integers

$$\lim_{x\to\infty} \frac{Q(x)}{x} = \frac{6}{\pi^2} \approx 0.608.$$

Proof [BD]: We want to make precise the notion of independence of $\{p^2 \nmid n\}$ from $\{q^2 \nmid n\}$. Define $Q^r(x)$ to be the number of positive integers less than or equal to x which are not divisible by the first r primes (under the standard ordering).

Time to make things precise...

The Proportion of Squarefree Integers

$$\lim_{x\to\infty} \frac{Q(x)}{x} = \frac{6}{\pi^2} \approx 0.608.$$

Proof [BD]: We want to make precise the notion of independence of $\{p^2 \nmid n\}$ from $\{q^2 \nmid n\}$. Define $Q^r(x)$ to be the number of positive integers less than or equal to x which are not divisible by the first r primes (under the standard ordering). A positive integer n is not divisible by the square of any of the first r primes iff n statisfies the system of congruences

$$n \equiv a_i \mod p_i^2$$

for $1 \leq i \leq r$ where $0 < a_i \leq p_i^2 - 1$.

Time to make things precise...

The Proportion of Squarefree Integers

$$\lim_{x\to\infty} \frac{Q(x)}{x} = \frac{6}{\pi^2} \approx 0.608.$$

Proof [BD]: We want to make precise the notion of independence of $\{p^2 \nmid n\}$ from $\{q^2 \nmid n\}$. Define $Q^r(x)$ to be the number of positive integers less than or equal to x which are not divisible by the first r primes (under the standard ordering). A positive integer n is not divisible by the square of any of the first r primes iff n statisfies the system of congruences

$$n \equiv a_i \mod p_i^2$$

for $1 \leq i \leq r$ where $0 < a_i \leq p_i^2 - 1$. By the Chinese Remainder Theorem, this system is solvable and has a unique solution for a given tuple $(a_1, \ldots, a_r)$, once every multiple of $2^2 3^2 \cdots p_r^2$.

Time to make things precise...

The Proportion of Squarefree Integers

$$\lim_{x\to\infty} \frac{Q(x)}{x} = \frac{6}{\pi^2} \approx 0.608.$$

Proof [BD]: We want to make precise the notion of independence of $\{p^2 \nmid n\}$ from $\{q^2 \nmid n\}$. Define $Q^r(x)$ to be the number of positive integers less than or equal to x which are not divisible by the first r primes (under the standard ordering). A positive integer n is not divisible by the square of any of the first r primes iff n statisfies the system of congruences

$$n \equiv a_i \mod p_i^2$$

for $1 \leq i \leq r$ where $0 < a_i \leq p_i^2 - 1$. By the Chinese Remainder Theorem, this system is solvable and has a unique solution for a given tuple $(a_1, \ldots, a_r)$, once every multiple of $2^2 3^2 \cdots p_r^2$.

There are $(2^2 - 1)(3^2 - 1) \cdots (p_r^2 - 1)$ such systems of congruences where $0 < a_i \leq p_i^2 - 1$.

Time to make things precise...

The Proportion of Squarefree Integers

$$\lim_{x\to\infty} \frac{Q(x)}{x} = \frac{6}{\pi^2} \approx 0.608.$$

Proof [BD]: We want to make precise the notion of independence of $\{p^2 \nmid n\}$ from $\{q^2 \nmid n\}$. Define $Q^r(x)$ to be the number of positive integers less than or equal to x which are not divisible by the first r primes (under the standard ordering). A positive integer n is not divisible by the square of any of the first r primes iff n statisfies the system of congruences

$$n \equiv a_i \mod p_i^2$$

for $1 \leq i \leq r$ where $0 < a_i \leq p_i^2 - 1$. By the Chinese Remainder Theorem, this system is solvable and has a unique solution for a given tuple $(a_1, \ldots, a_r)$, once every multiple of $2^2 3^2 \cdots p_r^2$.

There are $(2^2-1)(3^2-1)\cdots(p_r^2-1)$ such systems of congruences where $0 < a_i \leq p_i^2 - 1$. Thus, if $y = k \cdot 2^2 3^2 \cdots p_r^2$ then

$$Q^r(y) = k(2^2-1)\cdots(p_r^2-1) = y(1-2^{-2})\cdots(1-p_r^{-2}).$$

...the proof continues...

Hence

$$Q^r(y) = y(1-2^{-2})\cdots(1-p_r^{-2}) \implies \frac{Q^r(y)}{y} = (1-2^{-2})\cdots(1-p_r^{-2})$$

and it is in this sense that we can consider $\{p^2 \nmid n\}$ and $\{q^2 \nmid n\}$ "independent events".

...the proof continues...

Hence

$$Q^r(y) = y(1-2^{-2})\cdots(1-p_r^{-2}) \implies \frac{Q^r(y)}{y} = (1-2^{-2})\cdots(1-p_r^{-2})$$

and it is in this sense that we can consider $\{p^2 \nmid n\}$ and $\{q^2 \nmid n\}$ "independent events". We need a similar expression for $Q^r(x)$ where $x \in \mathbb{R}$. Letting $y = [x \cdot 2^{-2} \cdots p_r^{-2}]2^2 \cdots p_r^2$, observe that

$$0 \leq Q^r(x) - Q^r(y) \leq x - y < 2^2 \cdots p_r^2$$

and

$$0 \leq (x-y)\prod_{i=1}^{r}(1-p_i^{-2}) < x - y < 2^2 \cdots p_r^2.$$

...the proof continues...

Hence

$$Q^r(y) = y(1-2^{-2})\cdots(1-p_r^{-2}) \implies \frac{Q^r(y)}{y} = (1-2^{-2})\cdots(1-p_r^{-2})$$

and it is in this sense that we can consider $\{p^2 \nmid n\}$ and $\{q^2 \nmid n\}$ "independent events". We need a similar expression for $Q^r(x)$ where $x \in \mathbb{R}$. Letting $y = [x \cdot 2^{-2} \cdots p_r^{-2}]2^2 \cdots p_r^2$, observe that

$$0 \leq Q^r(x) - Q^r(y) \leq x - y < 2^2 \cdots p_r^2$$

and

$$0 \leq (x-y)\prod_{i=1}^{r}(1-p_i^{-2}) < x - y < 2^2 \cdots p_r^2.$$

Alas, we write

$$\begin{aligned} Q^r(x) &= x\prod_{i=1}^{r}(1-p_i^{-2}) - (x-y)\prod_{i=1}^{r}(1-p_i^{-2}) + Q^r(x) - Q^r(y) \\ &= x\prod_{i=1}^{r}(1-p_i^{-2}) + \theta \cdot 2^2 \cdots p_r^2, \qquad |\theta| \leq 1. \end{aligned}$$

...and continues...

We now wish to bound (and then squeeze) the asymptotic density of Q.

...and continues...

We now wish to bound (and then squeeze) the asymptotic density of Q. For the upper bound we have

$$\limsup_{x\to\infty} \frac{Q(x)}{x} \leq \limsup_{x\to\infty} \frac{Q^r(x)}{x} = \lim_{x\to\infty} \frac{Q^r(x)}{x} = \prod_{i=1}^{r}(1 - p_i^{-2}).$$

...and continues...

We now wish to bound (and then squeeze) the asymptotic density of Q. For the upper bound we have

$$\limsup_{x\to\infty} \frac{Q(x)}{x} \leq \limsup_{x\to\infty} \frac{Q^r(x)}{x} = \lim_{x\to\infty} \frac{Q^r(x)}{x} = \prod_{i=1}^{r}(1 - p_i^{-2}).$$

Hence

$$\limsup_{x\to\infty} \frac{Q(x)}{x} \leq \prod_{p}(1 - p^{-2}).$$

...and continues...

We now wish to bound (and then squeeze) the asymptotic density of Q. For the upper bound we have

$$\limsup_{x\to\infty}\frac{Q(x)}{x}\leq\limsup_{x\to\infty}\frac{Q^r(x)}{x}=\lim_{x\to\infty}\frac{Q^r(x)}{x}=\prod_{i=1}^{r}(1-p_i^{-2}).$$

Hence

$$\limsup_{x\to\infty}\frac{Q(x)}{x}\leq\prod_{p}(1-p^{-2}).$$

We now need to estimate from below. Observe that

$$Q^r(x)-Q(x)\leq\mathrm{card}\{n\leq x:\exists k>r,p_k^2\mid n\}\leq\sum_{k=r+1}^{\infty}\mathrm{card}\{n\leq x:p_k^2\mid n\}$$

$$=\sum_{k=r+1}^{\infty}\left[\frac{x}{p_k^2}\right]<\sum_{k=r+1}^{\infty}\frac{x}{k^2}<\int_r^{\infty}\frac{x}{t^2}\,\mathrm{d}t=\frac{x}{r}.$$

...and continues

Hence

$$\liminf_{x\to\infty} \frac{Q(x)}{x} \geq \liminf_{x\to\infty} \frac{Q^r(x)}{x} - \frac{1}{r} = \prod_{k=1}^{r}(1 - p_k^{-2}) - \frac{1}{r}.$$

...and continues

Hence

$$\liminf_{x\to\infty} \frac{Q(x)}{x} \geq \liminf_{x\to\infty} \frac{Q^r(x)}{x} - \frac{1}{r} = \prod_{k=1}^{r}(1 - p_k^{-2}) - \frac{1}{r}.$$

Letting $r \to \infty$, we obtain

$$\liminf_{x\to\infty} \frac{Q(x)}{x} \geq \prod_{p}(1 - p^{-2}).$$

...and continues

Hence

$$\liminf_{x\to\infty} \frac{Q(x)}{x} \geq \liminf_{x\to\infty} \frac{Q^r(x)}{x} - \frac{1}{r} = \prod_{k=1}^{r}(1-p_k^{-2}) - \frac{1}{r}.$$

Letting $r \to \infty$, we obtain

$$\liminf_{x\to\infty} \frac{Q(x)}{x} \geq \prod_{p}(1-p^{-2}).$$

Therefore

$$\lim_{x\to\infty} \frac{Q(x)}{x} = \prod_{p}(1-p^{-2}) = \frac{6}{\pi^2} \approx 0.608.$$

References, Recommendations and QnA

- T. Apostol, *Introduction to Analytic Number Theory*, Springer, 1976. (Classic Undergraduate Treatment)
- P. Bateman and H. Diamond, *Analytic Number Theory*, World Scientific, 2004. (Basis for this presentation; Graduate-level introductory text)
- M. Murty, *Problems in Analytic Number Theory*, Springer, 2008. (Problem-centric approach to the theory; Graduate-level)
- E. Stein and R. Shakarchi, *Fourier Analysis*, Princetom University Press, 2003. (Intro to Harmonic Analysis with loads of number theory applications; Undergraduate-level)