ANALYTIC NUMBER THEORY (MASTERMATH)

PART II: SIEVE METHODS

Fall 2024

Lola Thompson &
Sebastián Carrillo Santana
Universiteit Utrecht

e-mail: l.thompson@uu.nl

address: Hans Freudenthalgebouw, Budapestlaan 6, 3584 CD
Utrecht, office 406
URL: https://www.lolathompson.com

Literature

Below is a list of recommended additional literature. Much of the material in part II of this course has been taken from the books of Pollack, Cojocaru-Murty, and Davenport.

A. Cojocaru and M. R. Murty, *An Introduction to Sieve Methods and Their Applications*, Cambridge University Press; 1st edition, January 30, 2006.

H. Davenport, *Multiplicative Number Theory (2nd ed.)*, Springer Verlag, Graduate Texts in Mathematics 74, 1980.

J. Friedlander, H. Iwaniec, *Opera de Cribo,* American Mathematical Society Colloquium Publications 57, American Mathematical Society, 2010.

A. Granville *Primes in intervals of bounded length,* Bulletin of the American Mathematical Society 52, Number 2, April 2015, Pages 171–222.

P. Pollack, *Not Always Buried Deep,* American Mathematical Society; New ed. edition (October 14, 2009).

Acknowledgements

We would like to express our gratitude to the following people for offering feedback and correcting errors in earlier versions of this manuscript: Harald Andrés Helfgott, Jan-Hendrik Evertse, Samuel Tiersma, Greg Martin.

Chapter 7

Introduction to Sieves

7.1 Motivation: Counting Primes

One of the most important questions in number theory is:

Fundamental Question. Given a set $\mathscr{A} \subseteq \mathbb{Z}^+$, how many primes are in $\mathscr{A}$?

Many results and open problems in number theory can be formulated in this way. For example:

(i) Let $\mathscr{A} = \mathbb{Z}^+$. Then,

- Euclid showed that $\mathscr{A}$ contains infinitely many primes.
- The Prime Number Theorem states that

$$\pi(x) = \#\{p \in \mathscr{A} \cap (1, x]\} \sim \frac{x}{\log x} \text{ as } x \to \infty.$$

- The Riemann Hypothesis is equivalent to the statement

$$\pi(x) = \int_2^x \frac{\mathrm{d}t}{\log t} + O(x^{1/2+\varepsilon}).$$

(ii) The Twin Prime Conjecture states that the set $\mathscr{A} := \{p + 2 : p \text{ is prime}\}$ contains infinitely many primes.

(iii) The $n^2 + 1$ problem asks whether the set $\mathscr{A} := \{n^2 + 1 : n \in \mathbb{Z}^+\}$ contains infinitely many primes.

One way to tackle this fundamental question is via multiplicative number theory, which uses the following property of the primes:

Property 1. Primes generate the positive integers via multiplication.

Property 1 allows us to reformulate the fundamental theorem of arithmetic as

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

Let's look again at the example $\mathscr{A} = \mathbb{Z}^+$:

- The fact that $\mathscr{A}$ contains infinitely many primes follows from the fact that $\zeta(s)$ has a pole at $s = 1$;
- The Prime Number Theorem is equivalent to the fact that $\zeta(1 + it) \neq 0$;
- The Riemann Hypothesis states that all non-trivial zeros of $\zeta(s)$ lie on the line $\mathfrak{Re}(s) = 1/2$.

In particular, we can see that there is an interesting connection between the zeros of the zeta function and the primes! The limitation of studying the Riemann zeta function is that we (still) have a rather limited understanding of its zeros.

The purpose of the second half of this course is to examine another set of methods for tackling our fundamental question. We refer to these methods as *sieve methods.* These new methods take a different approach using another important property of the prime numbers:

Property 2. Primes are integers n which have no divisor smaller than $\sqrt{n}$ other than 1.

Property 2 shows that primes are examples of integers with no small divisors, so it is natural to look at the more general quantity

$$S(\mathscr{A}, z) := \sum_{\substack{n \in \mathscr{A} \\ p|n \Rightarrow p > z}} 1.$$

Observe that, if $\mathscr{A} \subseteq (1, x]$, the quantity $S(\mathscr{A}, \sqrt{x})$ essentially counts primes in $\mathscr{A} \cap (\sqrt{x}, x]$ by Property 2. We will see in the next section that, in order to deal with the condition of having no small divisors, it is possible to use sieve methods to show that

$$S(\mathscr{A}, z) = \sum_{\substack{d \\ p|d \Rightarrow p \leqslant z}} \mu(d) \sum_{\substack{n \in \mathscr{A} \\ d|n}} 1.$$

Thus, knowing how $\mathscr{A}$ is distributed in arithmetic progressions, i.e., understanding the set

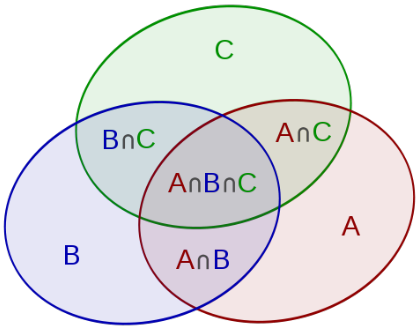
$$\mathscr{A}_d := \{a \in \mathscr{A} \ : \ d|a\}$$

will gives us some information about the primes in $\mathscr{A}$.

But first, what do we mean when we refer to *sieve methods*? Broadly speaking, sieves are used to bound the size of a set after elements with certain "undesirable" properties have been removed. A basic example of a sieve is the method of inclusion-exclusion, which gives an exact count for the number of elements in a set. In this chapter, we will focus on inclusion-exclusion and its relationship to the Sieve of Eratosthenes. We will also examine some variants of the Sieve of Eratosthenes.

7.2 Inclusion-Exclusion

As mentioned in the introduction, sieve methods are useful for counting elements with certain desirable properties. Sometimes this amounts to counting the elements in the union of several sets. But what happens if those sets have some overlap?



If we want to count all of the elements in the above diagram exactly once, we would use the following formula:

$$\begin{aligned}\#(A \cup B \cup C) = \#A &+ \#B + \#C \\ &- \#(A \cap B) - \#(B \cap C) - \#(C \cap A) \\ &+ \#(A \cap B \cap C)\end{aligned}$$

Example 1. How many integers in $[1, 100]$ are not divisible by $2, 3$ or 5?

Let $A = \{n \in \mathbb{Z} : 2 \mid n\}, \quad B = \{n \in \mathbb{Z} : 3 \mid n\}, \quad C = \{n \in \mathbb{Z} : 5 \mid n\}$. Observe that

$$\begin{aligned}\#A &= \lfloor 100/2 \rfloor = 50, \\ \#B &= \lfloor 100/3 \rfloor = 33, \\ \#C &= \lfloor 100/5 \rfloor = 20, \\ \#(A \cap B) &= \lfloor 100/6 \rfloor = 16, \\ \#(B \cap C) &= \lfloor 100/15 \rfloor = 6, \\ \#(C \cap A) &= \lfloor 100/10 \rfloor = 10, \\ \#(A \cap B \cap C) &= \lfloor 100/30 \rfloor = 3.\end{aligned}$$

Then, the number of integers that are not divisible by $2, 3$ or 5 is

$$100 - (50 + 33 + 20 - 16 - 6 - 10 + 3) = 26.$$

We can give a general statement of the principle of inclusion-exclusion using the Möbius function, μ. Let $m = p_1 \cdots p_k$. Then, we have

$$\sum_{d \mid m} \mu(d) \left\lfloor \frac{x}{d} \right\rfloor = \lfloor x \rfloor - \sum_{i=1}^{k} \left\lfloor \frac{x}{p_i} \right\rfloor + \sum_{1 \leqslant i < j \leqslant k} \left\lfloor \frac{x}{p_i p_j} \right\rfloor \pm \cdots . \tag{7.2.1}$$

In the example above, $x = 100$ and $m = 2 \cdot 3 \cdot 5 = 30$. Finding the number of integers in $[1, 100]$ that are not divisible by $2, 3,$ or 5 amounts to asking how many numbers in that range are relatively prime to 30.

Let's prove that $\sum_{d \mid m} \mu(d) \left\lfloor \frac{x}{d} \right\rfloor$ yields the correct answer. Since

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

it follows that

$$\begin{aligned}
\sum_{\substack{n\leqslant x\\ \gcd(n,m)=1}} 1 &= \sum_{n\leqslant x}\ \sum_{d\mid\gcd(n,m)} \mu(d)\\
&= \sum_{n\leqslant x}\sum_{\substack{d\mid n\\ d\mid m}} \mu(d)\\
&= \sum_{d\mid m}\mu(d)\sum_{\substack{n\leqslant x\\ d\mid n}} 1\\
&= \sum_{d\mid m}\mu(d)\left\lfloor \frac{x}{d}\right\rfloor .
\end{aligned}$$

Most sieves are not as exact, nor as user-friendly, as inclusion-exclusion. However, they are powerful tools for giving (approximate) answers to the question "How many numbers are there with a given property?"

7.3 Sieve of Eratosthenes

Sieves have been used for thousands of years, dating back to Eratosthenes. The Sieve of Eratosthenes is used to generate a table of prime numbers by systematically removing all integers with "small" primes as proper divisors.

1	$\textcircled{2}$	$\textcircled{3}$	$\cancel{4}$	$\textcircled{5}$	$\cancel{6}$	7	$\cancel{8}$	$\cancel{9}$	$\cancel{10}$
11	$\cancel{12}$	13	$\cancel{14}$	$\cancel{15}$	$\cancel{16}$	17	$\cancel{18}$	19	$\cancel{20}$
$\cancel{21}$	$\cancel{22}$	23	$\cancel{24}$	$\cancel{25}$	$\cancel{26}$	$\cancel{27}$	$\cancel{28}$	29	$\cancel{30}$

In a table with N integers, one begins by circling the prime 2, and then crossing out all multiples of 2. Next, one circles the prime 3 and crosses out all multiples of 3. This continues until all of the primes up to $\sqrt{N}$ have been circled, and their corresponding multiples have been crossed out. At that point, the remaining entries in the table must be prime since it is impossible for a composite number that is less than N to have two prime factors greater than $\sqrt{N}$.

One might wonder how many numbers are left uncrossed and uncircled after performing the sieve of Eratosthenes (i.e., how many primes p are there with $\sqrt{N} < p \leqslant N$)? We will consider this question more carefully in Chapter 8.

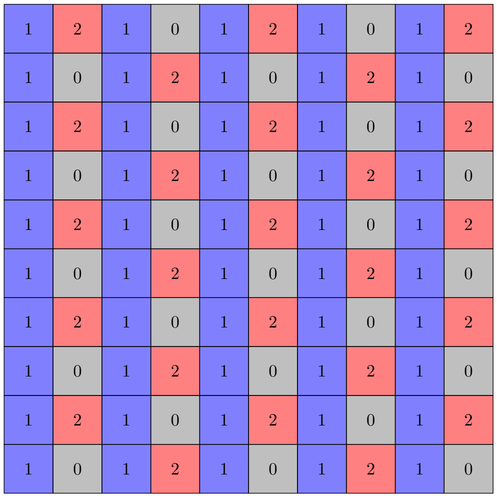
There is a nice generalization of the Sieve of Eratosthenes for detecting "almost primes." Namely, rather than sieving multiples of primes up to $N^{1/2}$, one could instead go up to N^{α} for any $\alpha \in (0, 1/2)$. Then, the numbers that remain have no prime factors less than N^{α}. But this also means that these remaining numbers have at most $\lfloor \alpha^{-1} \rfloor$ prime factors. Such numbers are "almost prime" in the sense that they have a restricted number of prime factors. One could ask, for example, how many numbers there are between 1 and N with at most k prime factors, where k is a positive integer that is small relative to N.

7.3.1 Sieving for values of $\mu(n)$

We can also use the Sieve of Eratosthenes to find values of the Möbius function. In this case, we start with a table that has all 1's as entries:

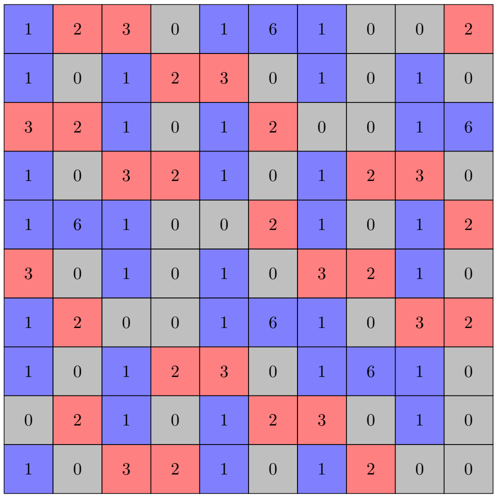
1	1	1	1	1	1	1	1	1	1
1	1	1	1	1	1	1	1	1	1
1	1	1	1	1	1	1	1	1	1
1	1	1	1	1	1	1	1	1	1
1	1	1	1	1	1	1	1	1	1
1	1	1	1	1	1	1	1	1	1
1	1	1	1	1	1	1	1	1	1
1	1	1	1	1	1	1	1	1	1
1	1	1	1	1	1	1	1	1	1
1	1	1	1	1	1	1	1	1	1

First, we flip the sign on every even entry, replacing every second even entry with a zero to account for the fact that these integers are divisible by 4, and $\mu(4 \cdot m) = 0$ for all positive integers m. Here, red represents -1, blue represents $+1$, and grey represents 0. The entries in the table that are not in the set $\{0, 1\}$ correspond to the primes that have already been checked at this stage (for reasons that will later become clear, whenever we flip an even number to red, we also multiply all of the numbers in the boxes that we flip by two).



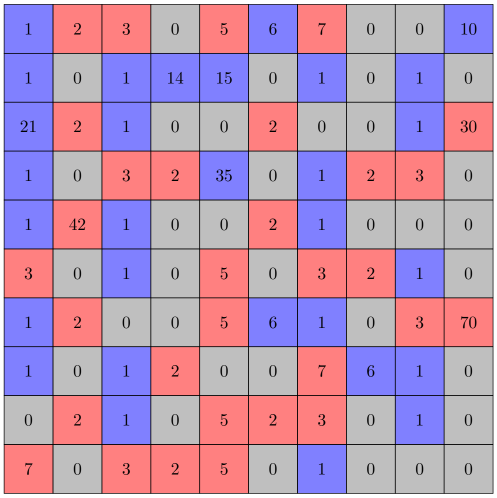
1	2	1	0	1	2	1	0	1	2
1	0	1	2	1	0	1	2	1	0
1	2	1	0	1	2	1	0	1	2
1	0	1	2	1	0	1	2	1	0
1	2	1	0	1	2	1	0	1	2
1	0	1	2	1	0	1	2	1	0
1	2	1	0	1	2	1	0	1	2
1	0	1	2	1	0	1	2	1	0
1	2	1	0	1	2	1	0	1	2
1	0	1	2	1	0	1	2	1	0

Next, we flip the sign on every multiple of three, replacing every third multiple of three with a zero. Again, we multiply the nonzero entries by three when we flip the signs.



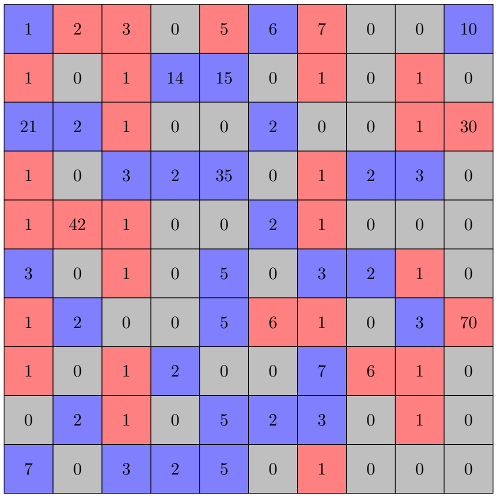
1	2	3	0	1	6	1	0	0	2
1	0	1	2	3	0	1	0	1	0
3	2	1	0	1	2	0	0	1	6
1	0	3	2	1	0	1	2	3	0
1	6	1	0	0	2	1	0	1	2
3	0	1	0	1	0	3	2	1	0
1	2	0	0	1	6	1	0	3	2
1	0	1	2	3	0	1	6	1	0
0	2	1	0	1	2	3	0	1	0
1	0	3	2	1	0	1	2	0	0

We repeat the same process for multiples of five and seven.



1	2	3	0	5	6	7	0	0	10
1	0	1	14	15	0	1	0	1	0
21	2	1	0	0	2	0	0	1	30
1	0	3	2	35	0	1	2	3	0
1	42	1	0	0	2	1	0	0	0
3	0	1	0	5	0	3	2	1	0
1	2	0	0	5	6	1	0	3	70
1	0	1	2	0	0	7	6	1	0
0	2	1	0	5	2	3	0	1	0
7	0	3	2	5	0	1	0	0	0

At this point, we would appear to be finished, since we have handled all of the primes up to $\sqrt{N}$ in a table of size N. However, upon closer inspection, we see that the last table contains some errors. For example, $\mu(11)$ should be -1 since 11 is prime. However, the 11^{th} entry in the table is 1. The same problem holds for all numbers containing a prime factor larger than $\sqrt{N}$. The good news is that each entry in the table contains at most one prime factor larger than $\sqrt{N}$, so we simply need to store the product of primes that have already been used in each entry in the table, and then look for entries that are "too small" relative to their positions in the table. Every nonzero entry that is "too small" relative to its location is thus missing a large prime factor, so we flip the signs on those entries and obtain a table with correct values of $\mu(n)$.



1	2	3	0	5	6	7	0	0	10
1	0	1	14	15	0	1	0	1	0
21	2	1	0	0	2	0	0	1	30
1	0	3	2	35	0	1	2	3	0
1	42	1	0	0	2	1	0	0	0
3	0	1	0	5	0	3	2	1	0
1	2	0	0	5	6	1	0	3	70
1	0	1	2	0	0	7	6	1	0
0	2	1	0	5	2	3	0	1	0
7	0	3	2	5	0	1	0	0	0

7.3.2 Sieving for primes of the form n^2+1

To use the Sieve of Eratosthenes to find integers n for which n^2+1 is prime, we first find the congruence conditions that prohibit such numbers from being prime, and then we eliminate the arithmetic progressions of values of n that satisfy those congruence conditions.

For example, notice that $1^2+1=2$ is prime, so 1 is an integer n for which n^2+1 is prime. Now, $n^2+1 \equiv 0 \pmod{2}$ if and only if $n \equiv 1 \pmod{2}$. So, we can cross out all $n \equiv 1 \pmod{2}$ in our table.

①	2	~~3~~	4	~~5~~	6	~~7~~	8	~~9~~	10
~~11~~	12	~~13~~	14	~~15~~	16	~~17~~	18	~~19~~	20
~~21~~	22	~~23~~	24	~~25~~	26	~~27~~	28	~~29~~	30

Observe that $n^2+1 \equiv 0 \pmod{3}$ has no solutions, so there are no arithmetic progressions (mod 3) that need to be eliminated.

We see that $2^2+1=5$, so 2 is an integer that gives rise to a prime of the form n^2+1. Moreover, $n^2+1 \equiv 0 \pmod{5}$ if and only if $n \equiv 2, 3 \pmod{5}$. Thus, we eliminate all integers $n \equiv 2, 3 \pmod{5}$ with $n > 2$.

①	②	~~3~~	4	~~5~~	6	~~7~~	~~8~~	~~9~~	10
~~11~~	~~12~~	~~13~~	14	~~15~~	16	~~17~~	~~18~~	~~19~~	20
~~21~~	~~22~~	~~23~~	24	~~25~~	26	~~27~~	~~28~~	~~29~~	30

There are no solutions to $n^2+1 \equiv 0 \pmod{7}$ or $\pmod{11}$. However, there are solutions (mod 13). We have $n^2+1 \equiv 0 \pmod{13}$ if and only if $n \equiv \pm 5 \pmod{13}$. Thus, we can eliminate these congruence classes (mod 13).

Observe that $4^2+1=17$, so we circle 4. On the other hand, $n^2+1 \equiv 0 \pmod{17}$ if and only if $n \equiv \pm 4 \pmod{17}$, hence we need to eliminate all $n > 4$ with $n \equiv \pm 4 \pmod{17}$.

Continuing in this fashion (stopping the sieving process once we have $p = N$, the size of the table), we obtain the following table of integers n for which n^2+1 is prime:

$\enclose{circle}{1}$	$\enclose{circle}{2}$	$\cancel{3}$	$\enclose{circle}{4}$	$\cancel{5}$	$\enclose{circle}{6}$	$\cancel{7}$	$\cancel{8}$	$\cancel{9}$	$\enclose{circle}{10}$
$\cancel{11}$	$\cancel{12}$	$\cancel{13}$	$\enclose{circle}{14}$	$\cancel{15}$	$\enclose{circle}{16}$	$\cancel{17}$	$\cancel{18}$	$\cancel{19}$	$\enclose{circle}{20}$
$\cancel{21}$	$\cancel{22}$	$\cancel{23}$	$\enclose{circle}{24}$	$\cancel{25}$	$\enclose{circle}{26}$	$\cancel{27}$	$\cancel{28}$	$\cancel{29}$	$\cancel{30}$

It is not known whether there are infinitely many primes of the form n^2+1. The strongest result that is known is that there are infinitely many n for which n^2+1 has at most 2 prime factors. There are also a number of important papers investigating the size of the largest prime factor of n^2+1, including a stunning 2024 paper of Hector Pasten [1] which shows that it must be at least of size about $(\log\log n)^2$. In Chapter 8, we will use sieve methods to obtain an upper bound on the number of primes of the form n^2+1. The work of Pasten uses deep results about Shimura curves, which fall outside the purview of this course.

7.4 Modern Sieves

In modern times, more-sophisticated sieves have been developed (by Brun, Selberg, Linnik, and others) to attack famous problems in number theory, such as the Twin Primes Conjecture and the Goldbach Conjecture. While these problems are still unsolved, we will see how sieves can shed some light on them. First, we will see how we can use Brun's sieve to obtain upper bounds for the number of twin prime pairs, or to show that the set of positive integers n such that n^2+1 is prime has asymptotic density zero. Later in the course, we will see how the work of Selberg led to an improvement on Brun's sieve (this is often referred to as "Selberg's sieve"). Both Brun's sieve and Selberg's sieve are examples of combinatorial sieves, which are proven using combinatorial arguments. We will also encounter the Large Sieve, which is proven using analytic methods. The Large Sieve is used to prove deep results about the distribution of primes in arithmetic progressions.

In the last decade, sieves have played a key role in the two proofs that there are bounded gaps between primes infinitely often (due to Zhang and Maynard) and in the proof that all odd numbers greater than 5 can be written as a sum of three primes (the so-called Ternary Goldbach Theorem, due to Helfgott). In particular, a variant of the Selberg sieve (due to Barban and Vehov; adapted to this context by Goldston, Pintz, and Yıldırım) was a key ingredient in Zhang's proof. Maynard created his own improvement to the Selberg sieve in his proof of bounded gaps between primes.

Helfgott's proof uses the Large Sieve as well as a variant of the Selberg sieve studied by Barban-Vehov et al. While the proofs of bounded gaps between primes and the Ternary Goldbach Theorem go beyond the scope of this course, you will become familiar with some of the main ingredients that arise from sieve theory.

7.5 Exercises

Exercise 7.1. *An integer n is called y-smooth (or y-friable) if all of its prime factors are less than or equal to y. Let $\psi(x,y) := \#\{n \leqslant x : \text{if } p \mid n \text{ then } p \leqslant y\}$. In other words, $\psi(x,y)$ counts the number of y-smooth integers in the interval $[1,x]$. In this exercise, we will obtain an estimate for the count given by the Sieve of Eratosthenes using some facts about smooth numbers.*

(a) Let $P_y := \prod_{p\leqslant y} p$. Using the notation introduced in this chapter, let

$$S(\mathbb{N},y) := \#\{n \leqslant x : n \textit{ is not divisible by any prime} \leqslant y\}.$$

Explain why

$$\begin{aligned} S(\mathbb{N},y) &= \sum_{\substack{d\mid P_y\\ d\leqslant x}} \mu(d)\left\lfloor \frac{x}{d}\right\rfloor \\ &= x\sum_{\substack{d\mid P_y\\ d\leqslant x}} \frac{\mu(d)}{d} + O(\psi(x,y)). \end{aligned}$$

(b) Next we will use a trick of Rankin to estimate $\psi(x,y)$. Rankin observed that, for any $\delta > 1/2$,

$$\psi(x,y) = \sum_{\substack{n\leqslant x\\ p\mid n\Rightarrow p\leqslant y}} 1 \leqslant \sum_{\substack{n\leqslant x\\ p\mid n\Rightarrow p\leqslant y}} \left(\frac{x}{n}\right)^{\delta} \leqslant x^{\delta}\prod_{p\leqslant y}\left(1-\frac{1}{p^{\delta}}\right)^{-1}.$$

Use Rankin's trick to argue that

$$\psi(x,y) \ll x^{\delta}\prod_{p\leqslant y}\left(1+\frac{1}{p^{\delta}}\right).$$

(c) *Use the fact that* $1+x \leqslant e^x$ *to show that*

$$\psi(x,y) \ll \exp\left(\delta \log x + \sum_{p \leqslant y} \frac{1}{p^\delta}\right).$$

(d) *Take* $\delta := 1-\eta$ *with* $\eta \to 0$ *as* $y \to \infty$. *Deduce that*

$$\sum_{p \leqslant y} \frac{1}{p^\delta} \leqslant \sum_{p \leqslant y} \frac{1}{p}(1 + (\eta \log p) y^\eta).$$

(e) *Take* $\eta := \frac{1}{\log y}$. *Conclude that*

$$\psi(x,y) \ll x(\log y) \exp\left(-\frac{\log x}{\log y}\right)$$

as $x \to \infty$. *Here, you may use (without proof) the facts that* $\sum_{p \leqslant x} \frac{1}{p} \sim \log\log x$ *and* $\sum_{p \leqslant x} \frac{\log p}{p} \sim \log x$ *as* $x \to \infty$.

(f) *Show that*

$$\sum_{\substack{d \mid P_y \\ d \leqslant x}} \frac{\mu(d)}{d} = \prod_{p \leqslant y}\left(1 - \frac{1}{p}\right) + O\left((\log y)^2 \exp\left(-\frac{\log x}{\log y}\right)\right).$$

(Hint: Start by showing that

$$\sum_{\substack{d \mid P_y \\ d \leqslant x}} \frac{\mu(d)}{d} = \prod_{p \leqslant y}\left(1 - \frac{1}{p}\right) - \sum_{\substack{d \mid P_y \\ d > x}} \frac{\mu(d)}{d}$$

and apply partial summation to the subtracted sum.)

(g) *Use the previous parts to conclude that*

$$\sum_{\substack{d \mid P_y \\ d \leqslant x}} \mu(d) \left\lfloor \frac{x}{d} \right\rfloor = x \prod_{p \leqslant y}\left(1 - \frac{1}{p}\right) + O\left(x(\log y)^2 \exp\left(-\frac{\log x}{\log y}\right)\right)$$

as $x, y \to \infty$.

(h) *As a corollary, deduce that*

$$\pi(x) \ll \frac{x}{\log x}(\log\log x).$$

Your proof should NOT use Chebyshev's inequality! Hint: Begin by proving that $\pi(x) \leqslant S(\mathbb{N}, y) + \pi(y)$ *and then use the inequality* $1 - u \leqslant e^{-u}$ *for* $u > 0$. *Again you will need the estimate for the sum of* $1/p$ *and you must choose* y *appropriately.*