

```

1  from random import randrange
2  import numpy as np
3
4
5
6  ##### High Digit Sieve #####
7  def sieve(sieve_primes: list, l: int, u: int, t: int) -> list:
8      """
9          sieve_primes: a list of trivial primes to sieve out majority of composite numbers in high digit range
10         l: lower bound of interval
11         u: upper bound of interval
12         t: number of tests to iterate on each potential prime
13
14         t=1 conducts single Fermat test
15         t=60 for error rate of 2-128
16         """
17
18         # ensuring boundaries are odd
19         if l % 2 == 0:
20             l -= 1
21         if u % 2 == 0:
22             u += 1
23
24         shape = int((u - l) / 2)
25         bools = np.full(shape, None)
26         i = 0
27
28         # iterating through only odd numbers on interval
29         for n in range(l, u, 2):
30
31             # initially assumed to be prime
32             stat = True
33
34             # checking if any prime factors exist for n
35             # starts at smallest primes which are most probable
36             for p in sieve_primes:
37
38                 # if p is a factor of n, we know its composite and exit check
39                 if n % p == 0:
40                     stat = False
41                     break
42
43             # if all prime factor checks completed, run Miller-Rabin and store result
44             if stat:
45                 bools[i] = _mr(n, t)
46             # if prime factor checks failed, store result immediately
47             else:
48                 bools[i] = stat
49
50             # increment i
51             i += 1
52
53         # list of resulting primes
54         primes = list()
55         # iterator variable
56         j = 0
57
58         # cross checking elements in interval against boolean results
59         for n in range(l, u, 2):
60
61             if bools[j] == True:
62                 primes.append(n)
63
64             j += 1

```

```

65
66     # running each remaining prime through Fibonacci Primality
67     for p in primes:
68
69         fib = _ft(p)
70
71         if not fib:
72             primes.remove(p)
73
74     # returning result
75     return primes
76
77
78 ##### Miller-Rabin Test #####
79 # This code has been duplicated from the millerRabin.py module to avoid requiring imports when sharing
80 # with the team.
81 def _mr(n: int, t: int) -> bool:
82     """
83     n: number to be evaluated
84     t: number of test iterations
85     Function for running the Miller-Rabin primality test.
86     Will run the test t times.
87     Returns a boolean showing that n is either composite or probably prime.
88     """
89
90     if n == 2 or n == 3:
91         return True
92
93     if n > 2 and n % 2 == 0:
94         return False # n is even
95
96     # ensuring atleast 1 test iteration is run
97     if t <= 0:
98         t += 1
99
100     # we will halve m iteratively until we achieve the equality:
101     #  $n - 1 = (2^k)m$ 
102     k = 0
103     m = n - 1
104
105     # this loop halves m
106     while m % 2 == 0:
107         k += 1
108         m //= 2 # floor div
109
110     # we now have k, m such that m is an odd integer
111
112     for _ in range(t):
113
114         # determining random test value in range [2, n - 1]
115         a = randrange(2, n - 1)
116
117         # getting initial value for b
118         b = pow(a, m, n)
119
120         # initial check for primality
121         if b == 1 or b == n - 1:
122             continue
123
124         # iterate until a result is found
125         for _ in range(k - 1):
126
127             # raising b**2 and getting remainder from modulo n
128             b = pow(b, 2, n)

```

```

129     # checking value of b
130     if b == n - 1:
131         break
132
133     # if inner loop ends, check reason for ending
134     # loop was broken
135     if b == n - 1:
136         continue
137     # loop ran out
138     else:
139         return False
140
141     # if all iterations were completed without throwing False, then n is probably prime
142     return True
143
144
145 ##### Fibonacci Test #####
146 def _ft(n: int) -> bool:
147     """
148     Fibonacci test to identify if number is prime deterministically.
149     Generates Fibonacci sequence modulo p.
150     n: prime number
151     """
152
153     fib_seq = [0, 1, 1]
154     i = 3
155     while i <= n + 1:
156         next_element = (fib_seq[-1] + fib_seq[-2]) % n
157         fib_seq.append(next_element)
158         del fib_seq[0]
159         i += 1
160
161     # Then we test if the n+1th term or the n-1th of the sequence is divisible by n
162     # If yes, n is prime. Otherwise, n is composite
163     if (fib_seq[-1] == 0) or (fib_seq[0] == 0):
164         return True
165     return False
166
167

```

Combination of several algorithms to sieve for primes in the non-trivial range, returning prime numbers deterministically.

For this sieve to function, we implement a sequence of smaller algorithms to parse out primes.

First, we remove any numbers on the interval that are multiples of smaller trivial primes. Prime Number Theorem estimates that the prime numbers found up to 10000 represent approximately 80% (tbd idk what the true value is) of all possible primes. As such, removing these obvious composite numbers reduces the the number of numbers to test significantly.

We then push the remaining numbers through the Miller-Rabin test. This primality test is probabilistic, but is extremely fast and has an error rate of approximately 2^{-128} . This will effectively remove any composite numbers left.

Lastly, using the Fibonacci test, we identify deterministically which of the remaining numbers are true primes.

The High Sieve algorithm was built in order to more easily parse true prime numbers out of the non-trivial range, which is defined to be $[0, 10^{10}]$. The objective in doing so was to compare the quantities of primes found in the non-trivial range to the estimations provided by Prime Number Theorem.

The Prime Counting Function, $\pi(x)$, can be used to estimate the quantity of primes not greater than x using the formula $\frac{x}{\log x}$.

We can then alter this formula to estimate the quantity of primes on an interval $[x, x+k]$.

$$\frac{x+k}{\log(x+k)} - \frac{x}{\log(x+k)} \rightarrow \frac{k}{\log(x+k)}$$

To test the estimates of $\pi(x)$ against this sieve, we looked at increasingly high intervals outside of the trivial range and compared the true number of primes to $\pi(x)$.

During testing, we found that the difference between $\pi(x)$ and the true prime count approaches zero as the lower bound for the interval tends to infinity.