

Theorem: There are infinitely many primes.

Proof: Suppose there are only finitely many primes:

$$p_1, p_2, p_3, \dots, p_k$$

Multiply the primes and add 1:

$$\text{let } N = p_1 \cdot p_2 \cdot p_3 \cdots p_k + 1$$

Which primes divide  $N$ ?

$p_1$  cannot divide  $N$ , since  $N$  is one more than a multiple of  $p_1$ .

$p_2$  cannot divide  $N$  for the same reason.

Similarly,  $p_3, \dots, p_k$  cannot divide  $N$ .

So  $N$  is not divisible by any prime.

Thus: either  $N$  is prime, or  $N$  has a prime factor that wasn't in our list.

Either option contradicts our assumption.

Therefore, there are infinitely many primes. ▣

# Sieve of Eratosthenes

<del>1</del>	2	3	<del>4</del>	5	<del>6</del>	7	<del>8</del>	<del>9</del>	<del>10</del>
11	<del>12</del>	13	<del>14</del>	<del>15</del>	<del>16</del>	17	<del>18</del>	19	<del>20</del>
<del>21</del>	<del>22</del>	23	<del>24</del>	<del>25</del>	<del>26</del>	<del>27</del>	<del>28</del>	29	<del>30</del>
31	<del>32</del>	<del>33</del>	<del>34</del>	<del>35</del>	<del>36</del>	37	<del>38</del>	<del>39</del>	<del>40</del>
41	<del>42</del>	43	<del>44</del>	<del>45</del>	<del>46</del>	47	<del>48</del>	<del>49</del>	<del>50</del>
<del>51</del>	<del>52</del>	53	<del>54</del>	<del>55</del>	<del>56</del>	<del>57</del>	<del>58</del>	59	<del>60</del>
61	<del>62</del>	<del>63</del>	<del>64</del>	<del>65</del>	<del>66</del>	67	<del>68</del>	<del>69</del>	<del>70</del>
71	<del>72</del>	73	<del>74</del>	<del>75</del>	<del>76</del>	<del>77</del>	<del>78</del>	79	<del>80</del>
<del>81</del>	<del>82</del>	83	<del>84</del>	<del>85</del>	<del>86</del>	<del>87</del>	<del>88</del>	89	<del>90</del>
<del>91</del>	<del>92</del>	<del>93</del>	<del>94</del>	<del>95</del>	<del>96</del>	97	<del>98</del>	<del>99</del>	<del>100</del> ← 100 = N

Implementing the sieve in Python

- Start with a list of integers
- Deleting from lists is computationally expensive
- Instead of deleting, simply mark composite numbers as not prime.

If I want to find primes up to  $N$ , I only have to consider factors up to  $\sqrt{N}$ .

Why? Suppose  $N = a \cdot b$

If  $a > \sqrt{N}$  and  $b > \sqrt{N}$ , then  $a \cdot b > \sqrt{N} \cdot \sqrt{N} = N$ , which is not possible since  $N = a \cdot b$ .

So if  $N = a \cdot b$ , then either  $a$  or  $b$  has to be  $\leq \sqrt{N}$ .