BILL START
RECORDING
Quadratic Sieve
Factoring
Notation Reminder

1) \( \text{GCD}(x, y) \) is the \textbf{Greatest Common Divisor} of \( x, y \).
Notation Reminder

1) \( \text{GCD}(x, y) \) is the Greatest Common Divisor of \( x, y \).

2) Sums and Products

\[
\sum_{i=1}^{n} a_i = a_1 + a_2 + \cdots + a_n.
\]

\[
\prod_{i=1}^{n} a_i = a_1 \times a_2 \times \cdots \times a_n.
\]
Notation Reminder

1) \( \text{GCD}(x, y) \) is the **Greatest Common Divisor** of \( x, y \).

2) **Sums and Products**

\[
\sum_{i=1}^{n} a_i = a_1 + a_2 + \cdots + a_n.
\]

\[
\prod_{i=1}^{n} a_i = a_1 \times a_2 \times \cdots \times a_n.
\]

3) **More Sums and Products** We summed or producted over \( \{1, \ldots, n\} \). Can use other sets.
Notation Reminder

1) \( \text{GCD}(x, y) \) is the \textbf{Greatest Common Divisor} of \( x, y \).

2) \textbf{Sums and Products}

\[
\sum_{i=1}^{n} a_i = a_1 + a_2 + \cdots + a_n.
\]

\[
\prod_{i=1}^{n} a_i = a_1 \times a_2 \times \cdots \times a_n.
\]

3) \textbf{More Sums and Products} We summed or producted over \( \{1, \ldots, n\} \). Can use other sets.

If \( A = \{1, 4, 9\} \) then

\[
\sum_{i \in A} a_i = a_1 + a_4 + a_9.
\]

\[
\prod_{i \in A} a_i = a_1 \times a_4 \times a_9.
\]
More Notation Reminder

4) $a_1, \ldots, a_n$ could be vectors.

$$\sum_{i \in A} \vec{a}_i = \vec{a}_1 + \vec{a}_4 + \vec{a}_9.$$ Addition is component-wise.
More Notation Reminder

4) $a_1, \ldots, a_n$ could be vectors.

$$\sum_{i \in A} \vec{a}_i = \vec{a}_1 + \vec{a}_4 + \vec{a}_9.$$ 

Addition is **component-wise**.
We will not be using any notion of a product of vectors.
4) \( a_1, \ldots, a_n \) could be \textbf{vectors}.

\[ \sum_{i \in A} \vec{a}_i = \vec{a}_1 + \vec{a}_4 + \vec{a}_9. \]

Addition is \textbf{component-wise}.

We will not be using any notion of a product of vectors.

5) We extend mod notation to vectors of integers. Example:

\[ (8, 1, 0, 9) \pmod{2} = (0, 1, 0, 1).\]
A LONG Aside on Sieving
Finding all Primes $\leq 48$, the Stupid Way

To find all primes $\leq 48$ we could do the following:

\[
\text{for } i = 2 \text{ to } 48 \text{ if isprime}(i) = \text{YES} \text{ then output } i.
\]

Is this a good idea? Discuss.
To find all primes \( \leq 48 \) we could do the following:

\[
\text{for } i = 2 \text{ to } 48 \text{ if } \text{isprime}(i) = \text{YES} \text{ then output } i.
\]

Is this a good idea? Discuss.

**No** You are testing many numbers that you could have, ahead of time, ruled out.
Finding all Primes $\leq 48$ the Smart Way

Write down the numbers $\leq 48$.

<table>
<thead>
<tr>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
<th>11</th>
<th>12</th>
<th>13</th>
<th>14</th>
<th>15</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>16</th>
<th>17</th>
<th>18</th>
<th>19</th>
<th>20</th>
<th>21</th>
<th>22</th>
<th>23</th>
<th>24</th>
<th>25</th>
<th>26</th>
<th>27</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>28</th>
<th>29</th>
<th>30</th>
<th>31</th>
<th>32</th>
<th>33</th>
<th>34</th>
<th>35</th>
<th>36</th>
<th>37</th>
<th>38</th>
<th>39</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>40</th>
<th>41</th>
<th>42</th>
<th>43</th>
<th>44</th>
<th>45</th>
<th>46</th>
<th>47</th>
<th>48</th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Write down the numbers $\leq 48$.

$$
\begin{array}{cccccccccccc}
2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 \\
\end{array}
$$

$$
\begin{array}{cccccccccccc}
16 & 17 & 18 & 19 & 20 & 21 & 22 & 23 & 24 & 25 & 26 & 27 \\
\end{array}
$$

$$
\begin{array}{cccccccccccc}
28 & 29 & 30 & 31 & 32 & 33 & 34 & 35 & 36 & 37 & 38 & 39 \\
\end{array}
$$

$$
\begin{array}{cccccccccccc}
40 & 41 & 42 & 43 & 44 & 45 & 46 & 47 & 48 \\
\end{array}
$$

Now output first unmarked—2—and MARK all multiples of 2.
We Have Marked Multiples of 2

Now Have:

<table>
<thead>
<tr>
<th></th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
<th>11</th>
<th>12</th>
<th>13</th>
<th>14</th>
<th>15</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>16</th>
<th>17</th>
<th>18</th>
<th>19</th>
<th>20</th>
<th>21</th>
<th>22</th>
<th>23</th>
<th>24</th>
<th>25</th>
<th>26</th>
<th>27</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>28</th>
<th>29</th>
<th>30</th>
<th>31</th>
<th>32</th>
<th>33</th>
<th>34</th>
<th>35</th>
<th>36</th>
<th>37</th>
<th>38</th>
<th>39</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>40</th>
<th>41</th>
<th>42</th>
<th>43</th>
<th>44</th>
<th>45</th>
<th>46</th>
<th>47</th>
<th>48</th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
We Have Marked Multiples of 2

Now Have:

<p>| | | | | | | | | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>6</td>
<td>7</td>
<td>8</td>
<td>9</td>
<td>10</td>
<td>11</td>
<td>12</td>
<td>13</td>
</tr>
<tr>
<td>X</td>
<td>X</td>
<td></td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<p>| | | | | | | | | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>16</td>
<td>17</td>
<td>18</td>
<td>19</td>
<td>20</td>
<td>21</td>
<td>22</td>
<td>23</td>
<td>24</td>
<td>25</td>
<td>26</td>
<td>27</td>
</tr>
<tr>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<p>| | | | | | | | | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>28</td>
<td>29</td>
<td>30</td>
<td>31</td>
<td>32</td>
<td>33</td>
<td>34</td>
<td>35</td>
<td>36</td>
<td>37</td>
<td>38</td>
<td>39</td>
</tr>
<tr>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<p>| | | | | | | | | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>40</td>
<td>41</td>
<td>42</td>
<td>43</td>
<td>44</td>
<td>45</td>
<td>46</td>
<td>47</td>
<td>48</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Now output first unmarked—3—and MARK all multiples of 3.
We Have Marked Multiples of 2 and 3

Now Have:

<p>| | | | | | | | | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>6</td>
<td>7</td>
<td>8</td>
<td>9</td>
<td>10</td>
<td>11</td>
<td>12</td>
<td>13</td>
</tr>
<tr>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td>X</td>
<td>X</td>
</tr>
</tbody>
</table>

<p>| | | | | | | | | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>16</td>
<td>17</td>
<td>18</td>
<td>19</td>
<td>20</td>
<td>21</td>
<td>22</td>
<td>23</td>
<td>24</td>
<td>25</td>
<td>26</td>
<td>27</td>
</tr>
<tr>
<td>X</td>
<td>X</td>
<td></td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
</tbody>
</table>

<p>| | | | | | | | | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>28</td>
<td>29</td>
<td>30</td>
<td>31</td>
<td>32</td>
<td>33</td>
<td>34</td>
<td>35</td>
<td>36</td>
<td>37</td>
<td>38</td>
<td>39</td>
</tr>
<tr>
<td>X</td>
<td>X</td>
<td></td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
</tbody>
</table>

<p>| | | | | | | | | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>40</td>
<td>41</td>
<td>42</td>
<td>43</td>
<td>44</td>
<td>45</td>
<td>46</td>
<td>47</td>
<td>48</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>X</td>
<td>X</td>
<td></td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
We Have Marked Multiples of 2 and 3

Now Have:

<table>
<thead>
<tr>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
<th>11</th>
<th>12</th>
<th>13</th>
<th>14</th>
<th>15</th>
</tr>
</thead>
<tbody>
<tr>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td>X</td>
<td>X</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td>X</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>16</th>
<th>17</th>
<th>18</th>
<th>19</th>
<th>20</th>
<th>21</th>
<th>22</th>
<th>23</th>
<th>24</th>
<th>25</th>
<th>26</th>
<th>27</th>
</tr>
</thead>
<tbody>
<tr>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
<td>X</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>28</th>
<th>29</th>
<th>30</th>
<th>31</th>
<th>32</th>
<th>33</th>
<th>34</th>
<th>35</th>
<th>36</th>
<th>37</th>
<th>38</th>
<th>39</th>
</tr>
</thead>
<tbody>
<tr>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>40</th>
<th>41</th>
<th>42</th>
<th>43</th>
<th>44</th>
<th>45</th>
<th>46</th>
<th>47</th>
<th>48</th>
</tr>
</thead>
<tbody>
<tr>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
</tbody>
</table>

Now output first unmarked—5—and MARK all multiples of 5.
We Have Marked Multiples of 2, 3 and 5

Now Have:

<p>| | | | | | | | | | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>6</td>
<td>7</td>
<td>8</td>
<td>9</td>
<td>10</td>
<td>11</td>
<td>12</td>
<td>13</td>
<td>14</td>
</tr>
<tr>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<p>| | | | | | | | | | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>16</td>
<td>17</td>
<td>18</td>
<td>19</td>
<td>20</td>
<td>21</td>
<td>22</td>
<td>23</td>
<td>24</td>
<td>25</td>
<td>26</td>
<td>27</td>
<td></td>
</tr>
<tr>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<p>| | | | | | | | | | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>28</td>
<td>29</td>
<td>30</td>
<td>31</td>
<td>32</td>
<td>33</td>
<td>34</td>
<td>35</td>
<td>36</td>
<td>37</td>
<td>38</td>
<td>39</td>
<td></td>
</tr>
<tr>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
</tbody>
</table>

<p>| | | | | | | | | | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>40</td>
<td>41</td>
<td>42</td>
<td>43</td>
<td>44</td>
<td>45</td>
<td>46</td>
<td>47</td>
<td>48</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
We Have Marked Multiples of 2, 3 and 5

Now Have:

<table>
<thead>
<tr>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
<th>11</th>
<th>12</th>
<th>13</th>
<th>14</th>
<th>15</th>
</tr>
</thead>
<tbody>
<tr>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>16</th>
<th>17</th>
<th>18</th>
<th>19</th>
<th>20</th>
<th>21</th>
<th>22</th>
<th>23</th>
<th>24</th>
<th>25</th>
<th>26</th>
<th>27</th>
</tr>
</thead>
<tbody>
<tr>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>28</th>
<th>29</th>
<th>30</th>
<th>31</th>
<th>32</th>
<th>33</th>
<th>34</th>
<th>35</th>
<th>36</th>
<th>37</th>
<th>38</th>
<th>39</th>
</tr>
</thead>
<tbody>
<tr>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>40</th>
<th>41</th>
<th>42</th>
<th>43</th>
<th>44</th>
<th>45</th>
<th>46</th>
<th>47</th>
<th>48</th>
</tr>
</thead>
<tbody>
<tr>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
</tbody>
</table>

Now output first unmarked—7—and MARK all multiples of 7. You get the idea so we stop here.
A Few Points About this Process

**Speed**

1. This process is really fast since when (say) MARKING mults of 3: We DO NOT look at (say) 23 and say no. WE DO NOT look at (say) 23 at all.
2. The KEY to many Number Theory Algorithms is not looking.
3. Good number theory algs act on a need-to-know basis.
A Few Points About this Process

Speed

1. This process is really fast since when (say) MARKING mults of 3: We DO NOT look at (say) 23 and say no. WE DO NOT look at (say) 23 at all.
2. The KEY to many Number Theory Algorithms is not looking.
3. Good number theory algs act on a need-to-know basis.

Could we make it faster?

1. When MARKING mults of 3 we skip marking \(3 + 3 \times 1\), \(3 + 3 \times 3\) since mults of 2 are already MARKED.
2. When MARKING mults of 5 we skip marking \(5 + 5 \times 1\), \(5 + 5 \times 3\), \(5 + 5 \times 5\), since mults of 2 are already MARKED. Hard to also avoid mults of 3, but could.
3. When MARKING mults of BLAH we could BLAHBLAH.
4. If our goal was to JUST get a list of primes, we might do this.
5. Our goal will be to FACTOR these numbers. As such we cannot use this shortcut. (Clear later.)
The Sieve of Eratosthenes

1. Input($N$)
2. Write down 2, 3, . . . , $N$. All are unmarked.
3. (MARK STEP) Goto the first unmarked element of the list $p$. Output($p$). Keep pointer there. (When pointer is at $N$ or beyond then stop.)
4. Mark all multiples of $p$ up to $\left\lfloor \frac{N}{p} \right\rfloor p$. (This takes $\frac{N}{p}$ steps.)
5. GOTO MARK STEP.

Time:

$$\sum_{p \leq N} \frac{N}{p} = N \sum_{p \leq N} \frac{1}{p}$$

New Question: What is $\sum_{p \leq N} \frac{1}{p}$?
An Aside on \[ \sum_{p \leq N} \frac{1}{p} \]
Notation

\[
\sum_{n \leq N} \frac{1}{n} = \frac{1}{1} + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \cdots + \frac{1}{N}
\]

\[
\sum_{n < \infty} \frac{1}{n} = \frac{1}{1} + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \cdots
\]

\[
\sum_{p \leq N} \frac{1}{p} = \frac{1}{2} + \frac{1}{3} + \frac{1}{5} + \frac{1}{7} + \cdots + \frac{1}{q}
\]

where \(q\) is the largest prime \(\leq N\).

\[
\sum_{p < \infty} \frac{1}{p} = \frac{1}{2} + \frac{1}{3} + \frac{1}{5} + \frac{1}{7} + \cdots
\]
Notation

\[
\sum_{n \leq N} \frac{1}{n} = \frac{1}{1} + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \cdots + \frac{1}{N}
\]

\[
\sum_{n < \infty} \frac{1}{n} = \frac{1}{1} + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \cdots
\]

\[
\sum_{p \leq N} \frac{1}{p} = \frac{1}{2} + \frac{1}{3} + \frac{1}{5} + \frac{1}{7} + \cdots + \frac{1}{q}
\]

where \( q \) is the largest prime \( \leq N \).

\[
\sum_{p < \infty} \frac{1}{p} = \frac{1}{2} + \frac{1}{3} + \frac{1}{5} + \frac{1}{7} + \cdots
\]

Example

\[
\sum_{p \leq 14} \frac{1}{p} = \frac{1}{2} + \frac{1}{3} + \frac{1}{5} + \frac{1}{7} + \frac{1}{11} + \frac{1}{13}
\]
What is $\sum_{p \leq N} \frac{1}{p}$ Asymptotically? History

When I looked up $\sum_{p \leq N} \frac{1}{p}$ on the web I found:

1. Proofs that $\sum \frac{1}{p} < \infty$ diverges.
2. Some of those proofs show that $\sum \frac{1}{p} \geq \ln(\ln(N)) + O(1)$.
3. Nothing on upper bounds on the sum.
4. TA Erik, when proofreading these slides, was able to find the theorem, though it was difficult. It's Merten's Second Thm.

A sequence of events:

1. In 2010 Larry Washington showed Bill G a proof that $\sum_{p \leq N} \frac{1}{p} \leq \ln(\ln(N)) + O(1)$.
2. Larry says it's a well known theorem but never written down.
3. Bill suggests they write it down. It is now on arxiv.

Moral of the Story

Google is not always enough.
What is $\sum_{p \leq N} \frac{1}{p}$ Asymptotically? History

When I looked up $\sum_{p \leq N} \frac{1}{p}$ on the web I found:

1. Proofs that $\sum_{p < \infty} \frac{1}{p}$ diverges.
What is $\sum_{p \leq N} \frac{1}{p}$ Asymptotically? History

When I looked up $\sum_{p \leq N} \frac{1}{p}$ on the web I found:

1. Proofs that $\sum_{p < \infty} \frac{1}{p}$ diverges.
2. Some of those proofs show that $\sum_{p \leq N} \frac{1}{p} \geq \ln(\ln(N)) + O(1)$.
What is $\sum_{p \leq N} \frac{1}{p}$ Asymptotically? History

When I looked up $\sum_{p \leq N} \frac{1}{p}$ on the web I found:

1. Proofs that $\sum_{p < \infty} \frac{1}{p}$ diverges.
2. Some of those proofs show that $\sum_{p \leq N} \frac{1}{p} \geq \ln(\ln(N)) + O(1)$.
3. Nothing on upper bounds on the sum.
4. TA Erik, when proofreading these slides, was able to find the theorem, though it was difficult. It’s Merten’s Second Thm.

A sequence of events:
1. In 2010 Larry Washington showed Bill G a proof that $\sum_{p \leq N} \frac{1}{p} \leq \ln(\ln(N)) + O(1)$.
2. Larry says it’s a well known theorem but never written down. Bill suggests they write it down. It is now on arXiv.

Moral of the Story
Google is not always enough.
What is $\sum_{p \leq N} \frac{1}{p}$ Asymptotically? History

When I looked up $\sum_{p \leq N} \frac{1}{p}$ on the web I found:

1. Proofs that $\sum_{p < \infty} \frac{1}{p}$ diverges.
2. Some of those proofs show that $\sum_{p \leq N} \frac{1}{p} \geq \ln(\ln(N)) + O(1)$.
3. **Nothing** on upper bounds on the sum.
4. TA Erik, when proofreading these slides, was able to find the theorem, though it was difficult. It’s Merten’s Second Thm.

A sequence of events:

1. In 2010 Larry Washington showed Bill G a proof that $\sum_{p \leq N} \frac{1}{p} \leq \ln(\ln(N)) + O(1)$.
2. Larry says it's a well known theorem but never written down. Bill suggests they write it down. It is now on arXiv.

Moral of the Story

Google is not always enough.
What is $\sum_{p \leq N} \frac{1}{p}$ Asymptotically? History

When I looked up $\sum_{p \leq N} \frac{1}{p}$ on the web I found:

1. Proofs that $\sum_{p < \infty} \frac{1}{p}$ diverges.
2. Some of those proofs show that $\sum_{p \leq N} \frac{1}{p} \geq \ln(\ln(N)) + O(1)$.
3. **Nothing** on upper bounds on the sum.
4. TA Erik, when proofreading these slides, was able to find the theorem, though it was difficult. It’s Merten’s Second Thm.

A sequence of events:

1. In 2010 Larry Washington showed Bill G a proof that

$$\sum_{p \leq N} \frac{1}{p} \leq \ln(\ln(N)) + O(1).$$
What is $\sum_{p \leq N} \frac{1}{p}$ Asymptotically? History

When I looked up $\sum_{p \leq N} \frac{1}{p}$ on the web I found:

1. Proofs that $\sum_{p < \infty} \frac{1}{p}$ diverges.
2. Some of those proofs show that $\sum_{p \leq N} \frac{1}{p} \geq \ln(\ln(N)) + O(1)$.
3. **Nothing** on upper bounds on the sum.
4. TA Erik, when proofreading these slides, was able to find the theorem, though it was difficult. It’s Merten’s Second Thm.

A sequence of events:

1. In 2010 Larry Washington showed Bill G a proof that

$$\sum_{p \leq N} \frac{1}{p} \leq \ln(\ln(N)) + O(1).$$

2. Larry says its a well known theorem but never written down. Bill suggests they write it down. It is now on arxiv.
What is $\sum_{p \leq N} \frac{1}{p}$ Asymptotically? History

When I looked up $\sum_{p \leq N} \frac{1}{p}$ on the web I found:

1. Proofs that $\sum_{p < \infty} \frac{1}{p}$ diverges.

2. Some of those proofs show that $\sum_{p \leq N} \frac{1}{p} \geq \ln(\ln(N)) + O(1)$.

3. **Nothing** on upper bounds on the sum.

4. TA Erik, when proofreading these slides, was able to find the theorem, though it was difficult. It’s Merten’s Second Thm.

A sequence of events:

1. In 2010 Larry Washington showed Bill G a proof that

   \[ \sum_{p \leq N} \frac{1}{p} \leq \ln(\ln(N)) + O(1). \]

2. Larry says it’s a well known theorem but never written down. Bill suggests they write it down. It is now on arxiv.

**Moral of the Story**  Google is not always enough.
More on $\sum_{p \leq N} \frac{1}{p}$

1. $\sum_{n \leq N} \frac{1}{n} \sim \ln(n)$.
2. $\sum_{p \leq N} \frac{1}{p} \sim \ln(\ln(N))$.

How good is this approximation?

1) When $N \geq 286$,

$$\ln(\ln N) - \frac{1}{2(\ln N)^2} + C \leq \sum_{p \leq N} \frac{1}{p} \leq \ln(\ln N) + \frac{1}{(2 \ln N)^2} + C,$$

where $C \sim 0.261497212847643$.

2) 

- $\sum_{p \leq 10} \frac{1}{p} = 1.176.$
- $\sum_{p \leq 10^9} \frac{1}{p} = 3.293.$
- $\sum_{p \leq 10^{100}} \frac{1}{p} \sim 5.7.$
- $\sum_{p \leq 10^{1000}} \frac{1}{p} \sim 7.8.$
Take Away

\[ \sum_{p \leq N} \frac{1}{p} \sim \ln(\ln N). \]

- This is a very good approximation.
- This is very small
- (Cheating to make math easier) The largest $pq$ factored is around 170-digits. We assume a limit of 1000 digits. Hence we treat $\ln(\ln(N))$ as if it was

\[ \ln(\ln(N)) \leq \ln(\ln(1000)) \sim 8. \]

(Nobody else does this.)