Prime Numbers and Sophie Germain

What are prime numbers? Most students will answer, “A prime number is a number that is divisible only by itself and 1.” This describes what they are like, but why are they important?

Prime numbers are, for numbers, what the elements (like Hydrogen, Oxygen and Carbon) are for molecules. Prime numbers are the basic building blocks of numbers, when you use multiplication to build. Remember doing “factor trees” in elementary school? This process was really something called “prime factorization” and in fact was a search for the prime building blocks of a number.

Take 60, for example. Though there are many ways to form the tree, the leaves will always be the same prime numbers.

So, $60 = 2^2 \cdot 3 \cdot 5$. This is called the prime factorization of 60. And every number has a unique prime factorization. So every number is the product of some prime numbers. Thus, in a sense, knowing things about prime numbers means you know something about all numbers.

Questions to be investigated further in this activity package:
1) Is there a way to find all prime numbers?
2) How many prime numbers are there?
3) What are Sophie Germain Primes?

Assignment: Find the prime factorizations for 45, 70, 88, 124.
1) **Sieve of Eratosthenes**

Eratosthenes (~200 BC) was a Greek mathematician who devised this simple and effective strategy for eliminating the composite numbers and leaving behind the primes. For small primes, it may be the most efficient way to find them. Are there better methods for finding large primes?

<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>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<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>
</tr>
<tr>
<td>11</td>
<td>12</td>
<td>13</td>
<td>14</td>
<td>15</td>
<td>16</td>
<td>17</td>
<td>18</td>
<td>19</td>
<td>20</td>
</tr>
<tr>
<td>21</td>
<td>22</td>
<td>23</td>
<td>24</td>
<td>25</td>
<td>26</td>
<td>27</td>
<td>28</td>
<td>29</td>
<td>30</td>
</tr>
<tr>
<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>40</td>
</tr>
<tr>
<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>49</td>
<td>50</td>
</tr>
<tr>
<td>51</td>
<td>52</td>
<td>53</td>
<td>54</td>
<td>55</td>
<td>56</td>
<td>57</td>
<td>58</td>
<td>59</td>
<td>60</td>
</tr>
<tr>
<td>61</td>
<td>62</td>
<td>63</td>
<td>64</td>
<td>65</td>
<td>66</td>
<td>67</td>
<td>68</td>
<td>69</td>
<td>70</td>
</tr>
<tr>
<td>71</td>
<td>72</td>
<td>73</td>
<td>74</td>
<td>75</td>
<td>76</td>
<td>77</td>
<td>78</td>
<td>79</td>
<td>80</td>
</tr>
<tr>
<td>81</td>
<td>82</td>
<td>83</td>
<td>84</td>
<td>85</td>
<td>86</td>
<td>87</td>
<td>88</td>
<td>89</td>
<td>90</td>
</tr>
<tr>
<td>91</td>
<td>92</td>
<td>93</td>
<td>94</td>
<td>95</td>
<td>96</td>
<td>97</td>
<td>98</td>
<td>99</td>
<td>100</td>
</tr>
</tbody>
</table>

1. Cross out 1 … it is called “unity” and is not prime.
2. Circle 2 and cross out (or colour) all multiples of 2.
3. Circle 3 and cross out (or colour) all multiples of 3.
4. Circle the next available number, and then cross out (or colour) all multiples of that number. Repeat until no numbers are left.
5. List the circled numbers in order below …

All circled numbers are ____________________________.

All crossed out (or coloured) numbers are called ____________________________.

**Assignments:**

1) Write a computer program (or TI-83) to print the prime numbers from 1 to $n$; or to test whether a number is prime. What strategy would you use? (see p.3)

2) Write a computer program (or TI-83) to find the prime factorization of any positive integer.
Prime Numbers Less than 2100

2    3    5    7    11   13    17   19    23   29    31    37    41    43    47    53    59    61    67    71
73   79   83   89   97  101  103  107  109  113  127  131  137  139  149  151  157  163
167  173  179  181  191  193  197  199  211  223  227  229  233  239  241  251  257
263  269  271  277  281  283  293  307  311  313  317  331  337  347  349  353  359
367  373  379  383  389  397  401  409  419  421  431  433  439  443  449  457  461
463  467  479  487  491  499  503  509  521  523  541  547  557  563  569  571  577
587  593  599  601  607  613  617  619  631  641  643  647  653  659  661  673  677
683  691  701  709  719  727  733  739  743  751  757  761  769  773  787  797  809
811  821  823  827  829  839  853  857  859  863  877  881  883  887  907  911  919
929  937  941  947  953  967  971  977  983  991  997  1009  1013  1019  1021  1031  1033
1039 1049 1051 1053 1061 1063 1069 1087 1091 1093 1097 1103 1109 1117 1123 1129 1151
1153 1163 1171 1181 1187 1193 1201 1213 1217 1223 1229 1231 1237 1249 1259 1277
1279 1283 1289 1291 1297 1301 1303 1307 1319 1321 1327 1361 1367 1373 1381 1399
1409 1423 1427 1429 1433 1439 1447 1451 1453 1459 1471 1481 1483 1487 1489 1493
1499 1511 1523 1531 1543 1549 1553 1559 1567 1571 1579 1583 1597 1601 1607 1609
1613 1619 1621 1627 1637 1657 1663 1667 1669 1693 1697 1699 1709 1721 1723 1733
1741 1747 1753 1759 1777 1783 1787 1789 1801 1811 1823 1831 1847 1861 1867 1871
1999 2003 2011 2017 2027 2029 2039 2053 2063 2069 2081 2083 2087 2089 2099

Sample: The following is a sample program for the TI-83 that tests whether a number is prime. Several modifications and/or improvements could be made. What changes could you make?

TI-83 Program: ISPRIME

ClrHome
Input N
1→P

For (J,2,√(N))
N/J→D
int(D)→E
If D=E:0→P
End

If P=1:Output(2,1,”PRIME”) If P=0:Output(2,1,”NOT PRIME”)

Clears the screen; allows the user to enter a number (N) to check primality; assigns the variable P the value 1, which will mean N is prime; so we assume N is prime to start.

The For command lets variable J take on all values from 2 to the integer part of the square root of N. If any of these numbers divides into N without remainder, then the value of variable P is changed from 1 to 0.

If P still has value 1, then no numbers divided into N without remainder, and N is Prime. If P has a value of 0, it must not be Prime.
2) **Euclid**

Euclid (~300 BC) was a Greek mathematician who was most famous for his work in geometry, but who also made wonderful discoveries about numbers. One such discovery concerned the number of prime numbers.

Euclid imagined that perhaps there was only a finite set of prime numbers, say $N$ of them. Then we could list them all out, naming them $P_1, P_2, P_3, \ldots, P_N$.

Now Euclid imagined a new, very large number that was one more than the product of all the prime numbers. We could call this number $Q = P_1 \cdot P_2 \cdot P_3 \cdot \ldots \cdot P_N + 1$.

Either $Q$ is prime, or not prime. If it is prime, then we missed it in our first list of primes, $P_1, P_2, P_3, \ldots, P_N$, since it is larger than all of these numbers. But this cannot be, since our list comprised all primes. So $Q$ must not be prime; it must be composite.

If $Q$ is composite, then like the number 60 we saw before, it must have a prime factorization. At least, it must be divisible by some smaller prime number. But we know $P_1, P_2, P_3, \ldots, P_N$ is the list of all prime numbers, and dividing $Q$ by any of them always leaves a remainder of 1. So there must be a prime we are missing from our list that divides into the composite $Q$. But again, our list was assumed to be complete.

Something is wrong here, and if we follow Euclid’s argument back, it seems that we must point our finger at the assumption that there is only a finite set of prime numbers.

The truth must be that there are unlimited (or infinite) prime number. This remarkable argument by Euclid is one of the first times that a mathematical proof was made indirectly: that is, we make an assumption, then find a contradiction or an impossibility, then conclude that the assumption is wrong, and its converse is true.

**Assignment:** Find a proof that $\sqrt{2}$ is not a rational number. It will be an indirect proof.
3) **Sophie Germain** – a model for math fans and all women (fill in the blanks)

Sophie Germain was born in a time of great turmoil, in the country of ______________________ during the Revolution. As a young girl, she became interested in mathematics when she read a story about the great Greek mathematician ______________________________. Legend states that he was killed because a mathematics problem so captured his attention that he ignored an enemy soldier, who angrily ended his life. Sophie thought that if mathematics could be that interesting to a Greek genius, it must surely be something worth studying.

Her parents discouraged Sophie’s interest in mathematics, because her culture thought it was unbecoming for a girl to study math. They even resorted to hiding her books, and even her clothes and candles, so that she would be confined to her room and unable to study math. Nothing ultimately deterred her, and they eventually relented. However, she didn’t think her society would be as easily conquered.

Sophie wanted to study math at ______________________________ in Paris, but only boys were allowed. So Sophie submitted papers and assignments using a fake male name, ________________________________________. One teacher, Joseph-Louis Lagrange, thought her papers were brilliant, and came to her home. When he discovered her true identity, he encouraged her, and arranged to tutor her privately.

Sophie became interested in solving Fermat’s Last Theorem. She made some discoveries about numbers, and wanted to check them with the greatest mathematician in the world, the German professor named ______________________________. However, she chose to correspond with him using her fake male name, rather than risk rejection from him because she was a woman. She shouldn’t have worried. Many years later, when the German professor found out that Sophie was a woman, he declared how much more he now admired her, not just for her brilliance, but also for her courage to overcome prejudice and other obstacles that men of the time did not face. In fact, he succeeded in getting Sophie an honorary degree from the University of Gottingen, but unfortunately Sophie died of ____________________________ before she received the degree.

Sophie’s work on Fermat’s Last Theorem led her to discover something about prime numbers of a certain form. They are now known as Sophie Germain Primes.

**Assignment:** What is Fermat’s Last Theorem? Who eventually solved it?
Sophie Germain Primes

A Sophie Germain prime is an odd number $p$ that is itself prime, and that makes $2p + 1$ also prime. (Sophie Germain suggested that Fermat’s Last Theorem is true for exponents that have Sophie Germain Primes as factors.)

Let’s test the first few (10) possible Sophie Germain primes.

<table>
<thead>
<tr>
<th>$p$ (odd primes)</th>
<th>$2p + 1$</th>
<th>Is $2p + 1$ Prime?</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td></td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>$2(11) + 1 = 23$</td>
<td>Yes</td>
</tr>
<tr>
<td>13</td>
<td></td>
<td></td>
</tr>
<tr>
<td>17</td>
<td></td>
<td></td>
</tr>
<tr>
<td>19</td>
<td>$2(19) + 1 = 39$</td>
<td>No; 39 = 3(13)</td>
</tr>
<tr>
<td>23</td>
<td></td>
<td></td>
</tr>
<tr>
<td>29</td>
<td></td>
<td></td>
</tr>
<tr>
<td>31</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Assignment:

1) What is the first Sophie Germain Prime, $p$, greater than 100? Greater than 1000? Use your list of primes on p.3.

2) The largest Sophie Germain Prime was found just this year, 2007. It is 51910 digits long, and is $p = 48047305725 \cdot 2^{172403} - 1$, since $2p + 1 = 48047305725 \cdot 2^{172404} - 1$ is also prime. (From http://primes.utm.edu/largest.html) Another group of famous primes (some very large) are called Mersenne primes. Who are they named after, and what is their formula? What is the largest Mersenne prime?