Primes and Primality Testing

A Technological/Historical Perspective

Jennifer Ellis
Department of Mathematics and Computer Science
What is a prime number?

- A number $p$ greater than one is prime if and only if the only divisors of $p$ are 1 and $p$.

Examples:

2, 3, 5, and 7
A few larger examples:

71887
524287
65537
$2^{127} - 1$
Primality Testing: Origins

- **Eratosthenes:**
  - Developed “sieve” method
  - 276-194 B.C.
  - Nicknamed *Beta* – “second place” in many different academic disciplines
  - Also made contributions to geometry, approximation of the Earth’s circumference

[www-history.mcs.st-andrews.ac.uk/PictDisplay/Eratosthenes.html](http://www-history.mcs.st-andrews.ac.uk/PictDisplay/Eratosthenes.html)
### Sieve of Eratosthenes

<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>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></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>
We only need to “sieve” the multiples of numbers less than 10. Why?

\[(10)(10)=100\]
\[(p)(q)\leq100\]

Consider \(pq\) where \(p>10\).

Then for \(pq \leq 100\), \(q\) must be less than 10.

By sieving all the multiples of numbers less than 10 (here, multiples of \(q\)), we have removed all composite numbers less than 100.
Primes less than 100:

Sieve of Eratosthenes

Analysis:
The sieving method is still used today in the discovery of new large primes, over two millennia after the time of Eratosthenes!
Three Major Primality Tests

- Pepin’s Test
- Test for Mersenne numbers
- Lucas Test
Why should we keep looking?

- The list of primes is infinite!
- Proofs given by Euclid, Washington (not George), Schorn, Euler, and Kummer.
- Proof by Contradiction: $p \rightarrow q$

Assume $q$ to be false. Then show that this logically leads to a contradiction. Then our original assumption was not valid, and $q$ must be true.
Infinitude of primes:

- Kummer’s proof:
- Suppose there exist only a finite number of primes where $p_1 < p_2 < \ldots < p_r$.
  Let $N$ be the product $p_1 \cdot p_2 \cdot \ldots \cdot p_r$. Then the integer $N-1$, being the product of primes, will have as a factor at least one prime; this prime must be a factor of $N$ as well, since $N$ is the product of all possible primes. Since this same prime divides both $N$ and $N-1$, it divides their difference as well, so it divides $N-(N-1) = 1$. This is clearly impossible!
- Thus the number of primes is infinite.
Before we begin:

- A note on modular congruence:
  We say that \( a \) is congruent to \( b \) modulo \( m \), if and only if \( a - b = km \) for some integer \( k \).

- Ex: \( 7 \equiv 2 \pmod{5} \)
  \[ 7 - 2 = 1 \cdot 5 \]
More Preliminaries:

- Mathematica and modular congruence: \( \text{Mod}[a\_, n\_] \) gives a solution \( 0 \leq x < n \) such that \( x \equiv a \pmod{n} \)

- Note: \( \text{PowerMod}[a\_, k\_, n\_] \) works better for powers of \( a \); it solves \( x \equiv a^k \pmod{n} \)
At last... Pepin’s Test

- Used to determine the primality of Fermat numbers:

\[ F_n = 2^{2^n} + 1 \]

- Some examples of Fermat numbers: 5, 17, 257, and 65537

- In 1877, Pepin proved a method for testing the primality of Fermat numbers
Historical Context: Fermat Numbers

- Pierre de Fermat
  - 1601-1665

- Fermat’s Last Theorem:
  \[x^n + y^n = z^n, \quad n \geq 2\]
  has no integer solutions for \(x, y, z\) when \(n > 2\)

- Believed that all Fermat numbers were prime

http://turnbull.mcs.st-and.ac.uk/~history/PictDisplay/Fermat.html
Pepin’s Test:

Let $F_n$ be a Fermat number where $n$ is greater than or equal to two. Then the following are equivalent:

i) $F_n$ is prime and $L(k,F_n) = -1$, and

ii) $k^{(F_n-1)/2} \equiv -1 \pmod{F_n}$, where

$L(k,F_n)$ is equivalent to the Legendre symbol $\left(\frac{k}{F_n}\right)$; that is

$L(a,b) = 1$, if $a$ is a quadratic residue modulo $b$
-1, otherwise

What is a quadratic residue?

We say that $a$ is a quadratic residue modulo $b$ if there exists some $t$ such that $a \equiv t^2 \pmod{b}$. 
Pepin’s Test

Let’s use Pepin’s Test (by hand) to see if \( F_2 = 17 \) is prime. Try using \( k = 3 \). Then

\[
3^{(17-1)/2} = 3^{16/2} = 3^8
\]

\[
3^8 = 3^2 \cdot (3^3)^2
\]

\[
3^2 = 9 \equiv 9 \pmod{17}
\]

\[
3^3 = 27 \equiv 10 \pmod{17}
\]

\[
(3^3)^2 \equiv 10^2 = 100 \equiv 100 - 6 \cdot 17 = 100 - 102 \equiv -2 \pmod{17}
\]
Pepin’s Test

- Finally,
  \[ 3^8 = 3^2 \cdot (3^3)^2 = 9 \cdot (-2) = -18 \equiv -1 \pmod{17} \]
  so \( F_2 = 17 \) is prime.

- The Largest known prime Fermat number: \( F_4 = 65537 \)

- *Mathematica* and Pepin’s test:
Enter *Mathematica*:

- Show $F_4 = 65537$ is prime (taking $k = 3$):

  \[
  \text{Fer}[n_] := (2^{2^n}) + 1 \\
  \text{PowerMod}[3, (\text{Fer}[4]-1)/2, \text{Fer}[4]] == \text{Fer}[4]-1
  \]

  *Mathematica*'s response:
  True

- How far can we go?
Analysis: Pepin’s Test

Challenges:
- Finding $k$
- Only able to test up to $F_{19}$
- Time limitations
Primality Test for Mersenne Numbers

- What is a Mersenne number?

\[ M_n = 2^n - 1 \]

where \( n \) is a known prime. Mersenne numbers that are prime are called \textit{Mersenne primes}.

Some examples of Mersenne numbers:

3, 7, 31, 127, 2047, 8191, 131071, 524287
History of Mersenne numbers

- Marin Mersenne
  - 1588-1648
  - Claimed that $M_n$ is prime when $n = 2, 3, 5, 7, 13, 17, 19, 31, 67, 127, 257$ and composite for any other prime less than 257
  - Wrong! Mersenne missed 3 primes less than 257 that give Mersenne primes and included 2 choices of $n$ that do not generate Mersenne primes

http://turnbull.mcs.st-and.ac.uk/~history/PictDisplay/Mersenne.html
Mersenne Test

- A primality test for Mersenne numbers was given by Lucas and modified by Lehmer and others.

\[ M_n \text{ is prime if and only if } M_n \text{ divides } S_{n-2^r} \text{ where } s \text{ is defined by} \]

\[ s_0 = 4 \]

\[ s_r = (s_{r-1})^2 - 2 \]
Mersenne Test

- Examine \( M_5 = 31 \)
- We need to know \( S_3 \):

\[
\begin{align*}
s_0 &= 4 \\
s_1 &= 4^2 - 2 = 14 \\
s_2 &= 14^2 - 2 = 194 \\
s_3 &= 194^2 - 2 = 37634
\end{align*}
\]

We know that if 31 divides 37634, 31 is prime. Since 37634 = 1214(31), 31 must be prime.
Mathematica and Mersennes

- The test for Mersenne numbers in Mathematica form:
  
  ```mathematica
  s[0] := 4;
  s[n_] := (s[n-1])^2 - 2
  m[k_] := (2^k) - 1
  MerTest[n_] := Mod[s[n-2], m[n]] == 0
  ```

- Test for $M_5 = 31$:
  
  ```mathematica
  k = 5;
  MerTest[5]
  ```

  Mathematica gives True
Mersenne Test

- How high can we go?
- Modified Mersenne Test:
  \[ m[k_] = (2^k) - 1; \]
  \[ s[0] = 4 \]
  \[ s[n_] := \text{Mod}[(s[n-1])^2 - 2, m[k]] \]
  \[ k = ____; \]
  \[ s[k-2] == 0 \]
- And the real limit of our test is...

  \[ s[18366] \]

- Why?
  memory
What is the largest known Mersenne prime?

- Discovered May 15, 2004
- 41st known Mersenne prime
- $M_{224036583} = 2^{224036583} - 1$
- This is currently the largest known prime number!
- Discovered through Project GIMPS
What is Project GIMPS?

- The Great Internet Mersenne Prime Search
- Uses both a modified sieve of Eratosthenes and the test given here for Mersenne numbers, along with a test to find potential factors of Mersenne numbers (see www.mersenne.org for more information)
- Just to make sure: each primality test is run again to double-check for errors
Analysis: Mersenne Test

- Shortcomings:
  - Only works on Mersenne numbers!
  - Can only be evaluated for $M_n$ when $n < 18368$

- Great way to find (relatively) large primes
  - True implies $M_n$ is prime; False implies $M_n$ is composite – it’s that easy!
Lucas’ Test

- Can test primality of any kind of number (not just Fermat or just Mersenne)

- Follows from Fermat’s Little Theorem:
  
  If $p$ is prime and $a$ is an integer, then $a^p$ is congruent to $a \pmod{p}$.

- Developed by Lucas in 1891
Historical Background: Lucas’ Test

- 1842-1891
- Lucas sequence named after him
- Gave a formula for the Fibonacci numbers: 1, 2, 3, 5, 8, 13, ...
- Major contributor to Mersenne test and developed Lucas’ Test for primality

http://turnbull.mcs.st-and.ac.uk/~history/PictDisplay/Lucas.html
Lucas’ Test

- A number $n$ is prime if there exists an integer $a$ such that
  
i) $a^{n-1} \equiv 1 \pmod{n}$,
  
  and
  
ii) $a^{(n-1)/q} \pmod{1}$ is not congruent to $1 \pmod{n}$ for any prime $q$ that divides $n - 1$. 

Lucas’ Test

- Show that \( n = 7 \) is prime (using \( a = 3 \)):

\[
3^{7-1} = 729 \equiv 729 - 7 \cdot 100 = 29 \equiv 1 \pmod{7}
\]

Thus we have satisfied i). Now, for ii), we must test all primes that divide 6, namely 2 and 3.

\[
3^{(7-1)/2} = 3^3 = 27 \equiv -1 \pmod{7}
\]
\[
3^{(7-1)/3} = 3^2 = 9 \equiv 2 \pmod{7}
\]

We have just shown that 7 is prime.
Mathematica and Lucas’ Test

- \( \text{LTTest3}[a_-, c_-, n_-] := \text{PowerMod}[a, c, n] == 1 \)
- Lucas’ Test for 71887, \( M_{127} \)
  and a few Fermat numbers
Analysis of Lucas’ Test

- Fewer restrictions than Pepin’s Test or the test for Mersenne numbers
- Facilitated by the \texttt{PowerMod} command

Problems:
- Knowing all of the prime factors of $n-1$
- Finding an appropriate choice of $a$
Parting Comments:

- Although all of these tests have positive and negative aspects, one test stands out far above the others in finding new large primes. And the winner is...
- the Test for Mersenne numbers!


Thank-You’s

Dr. Bryan Dawson, project advisor

Dr. Matt Lunsford, mathematics seminar instructor