Primality Tests and Factoring Algorithms

Joel Barnett and Nadya DeBeers

Santa Rosa Junior College

May 15, 2016

Overview

Application

- It's fun, right?

The "real" mathematics of the "real" mathematicians, the mathematics of Fermat and Euler and Gauss and Abel and Riemann, is almost wholly "useless." ...It is not possible to justify the life of any genuine professional mathematician on the ground of the "utility" of his work. - G. H. Hardy, *A Mathematicians Apology*, 1941

Application

- Encryption systems rely on these "useless" number theories developed by Fermat and Euler.
- Primes are the basis of encryption security

Primality tests

- Simple Primality Tests
- Fermat's Primality Algorithm
  - Modulo Arithmetic
  - Fermat's Little Theorem
  - The algorithm
  - Flaws
- Rabin-Miller Primality Test

Simple Primality Test

Prime or Composite?

1. 511
2. 73

Simple Primality Test

Prime or Composite?

1. 511 Composite
   $\frac{511}{2} = 2 \qquad \frac{511}{3} = 170.33 \qquad \frac{511}{5} = 102.2 \qquad \ldots \qquad \frac{511}{7} = 73$
2. 73

Simple Primality Test

Prime or Composite?

1. 511 Composite
2. 73
   $\frac{73}{2} = 36.5 \quad \frac{73}{3} = 24.33 \quad \frac{73}{5} = 18.25 \quad \frac{73}{7} = 10.43 \quad \frac{73}{8} = 9.13 \quad \frac{73}{9} = 8.11$
   Note: We stop at $\lceil\sqrt{73}\rceil = \lceil 8.544 \rceil = 9$

Simple Primality Test

This is a long process!

Simple Primality Test

This is a long process!

Testing a 400 digit number (10^{400}) requires checking approximately ($\sqrt{10^{400}} 10^{200}$) factors!

Simple Primality Test

This is a long process!

Testing a 400 digit number (10^{400}) requires checking approximately ($\sqrt{10^{400}}10^{200}$) factors!

Scientists estimate the life of the universe to be only 10^{18} seconds, rendering this process impractical.

Fermat's Method

New Strategy!

Modulo

Background

Modulo

<u>Definition</u>: Let m and n be integers and let d be a positive integer. We say that m is congruent to n modulo d if, and only if, d divides m-n and write:

$$m \equiv n \mod d \iff d|(m-n)$$

Sometimes this is written in the form:

$$m \equiv n \mod d \iff m \mod d = n \mod d$$

Example:

$15 \equiv 8 \mod 7$ because $7|(15-8)$

Or $15 \equiv 8 \mod 7$ because $15 \mod 7 = 1$ and $8 \mod 7 = 1$

Fermat's Method

Fermat's Little Theorem

If p is a prime number, then, $a^p \equiv a \mod p, \forall a \in \mathbb{Z}$.

This theorem is also often rearranged to the form:

$a^{p-1} \equiv 1 \mod p$

Fermat's Method

Shortened Proof:

Fermat's Little Theorem

If p is a prime number, then, $a^p \equiv a \mod p, \forall a \in \mathbb{Z}$.

Proof (by induction): Let p be any prime number.

Base Case: $1^p \equiv 1 \mod p \iff p | (1^p - 1)$, which is true.

Inductive Assumption: Assume $k^p \equiv k \mod p$ for some integer k.
That is, assume $p | (k^p - k)$ is true.

Fermat's Method

That is, assume $p|(k^p - k)$ is true.
[We must show the (k+1) case follows].
That is, show $(k+1)^p \equiv (k+1) \mod p$
$\iff p|(k+1)^p - (k+1)$
$\iff (k+1)^p - (k+1) = p * q, \exists q \in \mathbb{Z}$
Using the binomial theorem, the left hand side of above equation becomes:
$k^p + \binom{p}{1} k^{p-1} + \binom{p}{2} k^{p-2} + ... + \binom{p}{p-1} k + 1 - (k+1) =$
$k^p - k + [\binom{p}{1} k^{p-1} + \binom{p}{2} k^{p-2} + ... + \binom{p}{p-1} k]$
Now, $\binom{p}{j} = \frac{p!}{j!(p-j)!}$ where j is some integer. Since p is prime and $j < p$, there is a factor of p in the numerator, and no factors of p in the denominator.
Thus, $\binom{p}{1} k^{p-1} + \binom{p}{2} k^{p-2} + ... + \binom{p}{p-1} k = p * m, \exists m \in \mathbb{Z}$

Fermat's Method

Returning to what we were trying to show: $(k+1)^p - (k+1) = p * q$
$\iff k^p - k + [\binom{p}{1}k^{p-1} + \binom{p}{2}k^{p-2} + ... + \binom{p}{p-1}k] = p * q$
But, $\binom{p}{1}k^{p-1} + \binom{p}{2}k^{p-2} + ... + \binom{p}{p-1}k = p * m$, so
$k^p - k + [\binom{p}{1}k^{p-1} + \binom{p}{2}k^{p-2} + ... + \binom{p}{p-1}k] = k^p - k + p * m$
Thus, $k^p - k + [\binom{p}{1}k^{p-1} + \binom{p}{2}k^{p-2} + ... + \binom{p}{p-1}k] = p * q$
$\iff k^p - k + p * m = p * q$
$\iff k^p - k = p(q - m)$
$p|(k^p - k)$, which is true by our inductive assumption.
Thus $a^p \equiv a \mod p, \forall a > 1$. To prove this for all integers, the inductive direction

Blocks of Highlighted Text

Block 1

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Integer lectus nisl, ultricies in feugiat rutrum, porttitor sit amet augue. Aliquam ut tortor mauris. Sed volutpat ante purus, quis accumsan dolor.

Block 2

Pellentesque sed tellus purus. Class aptent taciti sociosqu ad litora torquent per conubia nostra, per inceptos himenaeos. Vestibulum quis magna at risus dictum tempor eu vitae velit.

Block 3

Suspendisse tincidunt sagittis gravida. Curabitur condimentum, enim sed venenatis rutrum, ipsum neque consectetur orci, sed blandit justo nisi ac lacus.

Multiple Columns

Heading

1. Statement
2. Explanation
3. Example

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Integer lectus nisl, ultricies in feugiat rutrum, porttitor sit amet augue. Aliquam ut tortor mauris. Sed volutpat ante purus, quis accumsan dolor.

Table

Treatments	Response 1	Response 2
Treatment 1	0.0003262	0.562
Treatment 2	0.0015681	0.910
Treatment 3	0.0009271	0.296

Table: Table caption

Theorem

Theorem (Mass–energy equivalence)

$E = mc^2$

Verbatim

Example (Theorem Slide Code)

```
\begin{frame}
\frametitle{Theorem}
\begin{theorem}[Mass--energy equivalence]
$E = mc^2$
\end{theorem}
\end{frame}
```

Figure

Uncomment the code on this slide to include your own image from the same directory as the template .TeX file.

Citation

An example of the `\cite` command to cite within the presentation:

This statement requires citation [Smith, 2012].

References

John Smith (2012)
Title of the publication
Journal Name 12(3), 45 – 678.

The End