By: Ali Salman Soutcho Toure

SEARCHING FOR UNBERS

INDIANA STATE UNIVERSITY

Professors: Jeff Kinne **Geoffrey Exoo**



Example : 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47 ...



SOPHIE GERMAIN PRIMES

Sophie Germain primes : *n* and 2*n*+1 Are primes

2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47 ...





RECORDS

* Largest known prime: 17,425,170 digits

* Our largest prime yet: 712,748 digits (187th largest known)

* Largest known SG prime: 200,701 digits

* Our largest SG prime: 31,112 digits (16th largest known SG)

HOW RARE ARE PRIMES ?

 $\pi(n) = \# \, primes \le n$ $\pi(10) = 4$ $\pi(20) = 8$

$$\pi(n) \sim \frac{1}{ln(n)}$$

10 digit number $\rightarrow 4 \%$ 100 digit number $\rightarrow 0.4 \%$ 100,00 digit number $\rightarrow 0.00004 \%$ 20,000,000 digit number -> 0.000,000,000,2%



TRIAL DIVISION

Example, 2013 2013 / 2 ? 2013 / 3 ? Example, 2011 2011 / 2 ? 2011 / 3 ?

2013 can only be divided by { 1, 3, 671, 2013 }

2011 can only be divided by { 1, 2001 }

4,363,477,260,190,362

FERMAT'S TEST

 $a^{n-1} \bmod n = 1$

If the number **passes** this equation then **it might be a prime**, if the number **doesn't pass** the test, then it is **not a prime**.

n = 5	n = 4
a = 3	a = 3
$3^{4} \mod 5$	3° <i>mod</i> 4
$81 \mod 5 = 1$	$27 \mod 4 = 3$
passed	Failed

LUCAS THEOREM

Another test similar to Fermat's test. However, if the number **passes**, then it is **guaranteed** to be **prime**.

METHOD USED

- Is n prime?
- 1- Trial division
 2- Fermat's test
 2- Lucce theorem
- 3- Lucas theorem

ACKNOWLEDGEMENTS

ISU SURE program

ISU Center for Student Research and Creativity

Professors

- Jeff Kinne
- Geoffrey Exoo

Students

- Ali Salman
- Soutcho Toure
- Po-Ching Liu
- Troy Schotter
- Karthik Tottempudi



LUCAS THEOREM

n = 47 n - 1 = 46 *Factors of* 46 {2,23} $5^{46} \mod 47 = 1$

$$5^{46/2} \mod 47 \neq 1$$

$$5^{46/23} \mod 47 \neq 1$$

 $a^{n-1} \equiv 1 \mod n$ $a^{n-1/q} \not\equiv 1 \mod n$

n = 4,363,477,260,190,361

Factors of *n*-1 = { 2, 5, 13, 34781, 241261103 }

$3^{4,363,477,260,190,360} \mod 4,363,477,260,190,361 = 1$

$3^{4,363,477,260,190,360/q} \ mod \ 4, 363, 477, 260, 190, 361 \neq 1$

HOW LONG DOES IT TAKE TO GET A PRIME

Prime Number Theorem : $n * \ln(10)$ numbers before finding a prime.

