

Prime Number Test: Trial Division

- •Division of n by a sequence of number greater than 1 and less than n.
- Helps eliminate unwanted numbers

Example, 47

47 can only be divided by {1, 47}

Example, 49

49 Can be divided by {1, 7, 49}

Prime Number Test: Fermat Test

- • a^{n-1} mod n = 1
- •If the number passes the test then it might be a prime, but if it does not, then it is not a prime.
- •Example:

$$n = 4$$

$$a = 3$$

$$27 \mod 4 = 3$$

Failed

$$n = 5$$

$$a = 3$$

$$81 \mod 5 = 1$$

Passed

Prime Number Test: Lucas Test •Find prime factors of n. •Run a sequence of test (almost similar to the Fermat equation) on them. •Example: n = 47n - 1 = 46Factors: {2, 23}



 $\pi(n)$ -# of primes up to n

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

1 digit numbers: 4 are prime

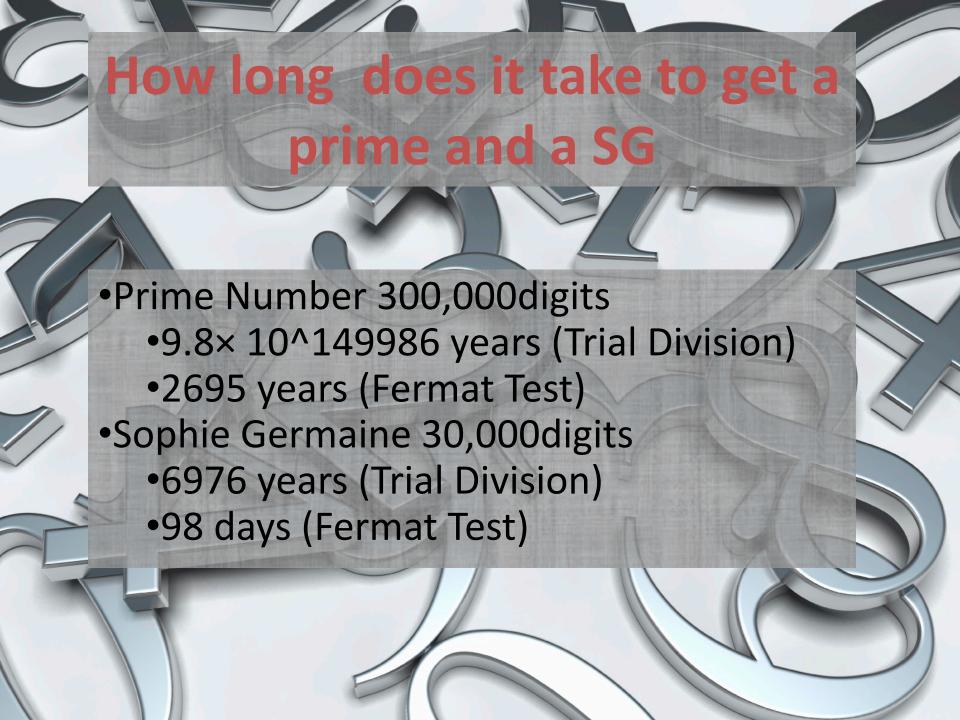
2 digit numbers: 21 are prime

30,000 digit numbers: about 1/70,000 are prime

300,000 digit numbers: about 1/700,000 are prime

Sohpie Germain Primes

- n and 2n + 1 are both prime
- 30,000 digit numbers
 - $\sim (\frac{1}{70,000})^2$ are Sophie Germain primes



Method used

```
Is n prime?
Loop()
1- Trial division try n/2
                 n/3
                 n/5.... n/9973
2- Fermat's test : a^{n-1} \mod n = 1
3- Lucas theorem
```