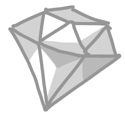
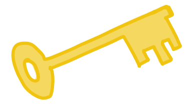
Large Primes

Diamonds, Keys,
& a One Million Dollar Question





?

① Math in the news

2, 3, 5, 7, 11, ...

Dec 2018: largest known prime,
Patrick Laroch, FL

$$2^{\boxed{82,589,933}} - 1$$

- almost 25 million digits
- 7000 pages ... 14 reams
- 4.7 months to write (2 digits/sec.)

Mersenne prime: $M_p = 2^p - 1$ (51 known)

- **Euclid** (c 350 BC), perfect numbers

sum of proper divisors
is itself
$6 = 1 + 2 + 3$

even perfect numbers $\longleftrightarrow$ $2^{p-1}\underbrace{(2^p - 1)}_{\text{prime}}$

(odd perfect numbers?)

- Mersenne (c 1600)

  conj. @ which primes $p \Rightarrow$ prime $2^p - 1$

- GIMPS: Great Internet Mersenne Prime Search (1996 – present)

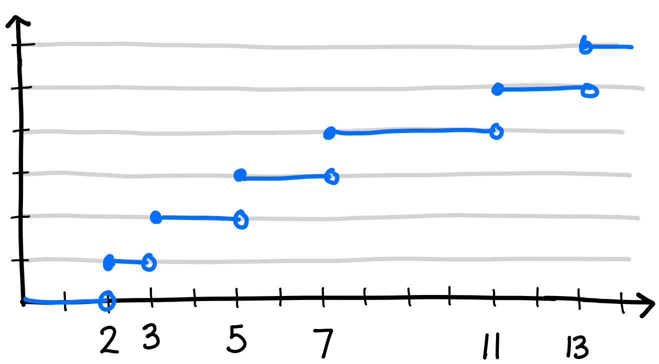
  - individual volunteers download software & run on computer
  - 17 most recent Mersenne primes found in this way

② Large Primes

How many primes are there? ∞'ly many

How are they distributed among the integers?

- Intuitively: less & less frequent
- $\pi(X)$ = # primes $\leq X$ ("staircase")



Legendre (1798)

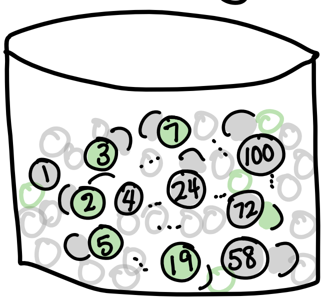
$$\pi(X) \sim \frac{\boxed{X}}{\boxed{\ln X}}$$

Pf : Hadamard & de la Valée Poussin (1896)

... " Prime Number Theorem "

↑ uses cx. analysis & Riemann ζ-fcn.

Probability that a large number N is prime

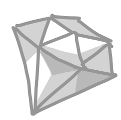


How many prime? $N/\ln N$

How many numbers? N

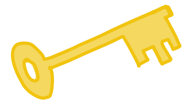
probability : about $1/\ln N$

digits of N	prob. that N is prime
10	4.34%
100	0.434 %
1000	0.0434 %
⋮	⋮
25 million	1.7 millionths of a percent



Applications (despite Hardy ...)

Cryptology : the math of making & breaking codes

- encryption (RSA, El Gamal) 

  practically impossible to factor product of 2 large primes

- pseudo-random number generators → OTP

  2 3 1 1 1 5 9 6 4 7 $\boxed{?}$

  BBS : randomness ⟷

OTP (one time pad), "perfectly secure"

③ Primality Testing

- Fast, probabalistic
- Isolate a feature common to all primes; Call any number w/ that feature a "pseudo-prime"; it's "probably" prime.

- Analogy : hair color, outfits

Clock arithmetic

Mod 12 : 10:00 + 3:00 = 1:00

$10 + 3 \equiv 1 \mod 12$

A way of making the infinite finite!

$\mathbb{Z}/12 = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12\}$

usu. prefer 0 instead of 12

Powers

In $\mathbb{Z}/6$:

$0, 0, 0, \ldots$

$1, 1, 1, \ldots$

$2, 4, \boxed{1}, \boxed{2}, \ldots$ $\qquad 2^3 = 8 = 6 + 1$

$3, \boxed{3}, \boxed{3}, \ldots$ $\qquad 3^2 = 9 = 6 + 3$

$4, \boxed{4}, \boxed{4}, \boxed{4}, \ldots$ $\qquad 4^2 = 16 = 12 + 4$

$5, \boxed{1}, \boxed{5}, \boxed{1}, \ldots$ $\qquad 5^2 = 25 = 24 + 1$

$-1, 1, -1, -1, \ldots$

In $\mathbb{Z}/7$:

$0, 0, 0, \ldots, 0, \ldots$
$1, 1, 1, \ldots, 1, \ldots$
$2, 4, 1, 2, 4, 1, \ldots$
$3, 9, 6, 4, 5, 1, 3, 9, \ldots$
$4, 2, 1, 4, 2, 1, 4, \ldots$
$5, 4, 6, 2, 3, 1, 5, \ldots$
$6, 1, 6, 1, 6, 1, 6, \ldots$

For $b \neq 0$ in $\mathbb{Z}/7$,

$$b^{\boxed{6}} = 1. \qquad (\boxed{6} = 7 \boxed{-1})$$

In general (FℓT), for $b \neq 0$ in $\mathbb{Z}/p$ (p prime), $b^{p-1} = 1$.

Contrast : In $\mathbb{Z}/6$, $2^5 = 2 \neq 1$.

<u>Def</u> A Fermat pseudo-prime base b is a number n s.t. $b^{n-1} \equiv 1 \mod n$.

<u>Ex</u> $n = 341$, $b = 2$:

$$2^{\boxed{340}} \equiv \boxed{1} \mod \boxed{341}$$

So 341 is a F. ps. prime base 2

But $341 = 11 \cdot 13$, so 341 is not prime

Note There is a fast algorithm for exponentiation mod n.

Square Roots of One

In $\mathbb{Z}/7$:

0, 0, 0, ..., 0, ...
1, 1, 1, ..., 1, ...
2, 4, 1, 2, 4, 1, ...
3, 9, 6, 4, 5, 1, 3, 9, ...
4, 2, 1, 4, 2, 1, 4, ...
5, 4, 6, 2, 3, 1, 5, ...
6, 1, 6, 1, 6, 1, 6, ...

Only square roots of one are: 1 & 6

$\boxed{-1}$

However in $\mathbb{Z}/12$,

$5^2 = 25 = 1$ & $7^2 = 49 = 1$

$\Rightarrow$ sq. roots of one are ± 1 & ± 5

(1, 11) (5, 7)

In general: In $\mathbb{Z}/p$ (p prime),

$$x^2 = 1 \Rightarrow x = \boxed{\pm 1}$$

Putting this together w/ FℓT we get another feature of primes.

Ex $p = 13$

For all $b \neq 0$ in $\mathbb{Z}/p$,

$$\underbrace{b^{12}}_{(b^6)^2} = 1 \qquad \text{(FℓT)}$$

$$\Rightarrow b^{\boxed{6}} = -1 \quad \text{or} \quad \underbrace{b^{\boxed{6}}}_{(b^3)^2} = 1$$

in which case

$$b^{\boxed{3}} = -1 \quad \text{or} \quad b^{\boxed{3}} = 1$$

Summarize:

For all $b \neq 0$,

either $b^3 \equiv \pm 1 \mod 13$

or $b^6 \equiv -1 \mod 13$

Generalize.

exponent

$$b^{12} = 1 \quad \longleftarrow \quad p-1 \quad \text{even}$$

$$b^{6} = -1 \quad \text{or} \quad b^{6} = 1 \quad \longleftarrow \quad \boxed{\frac{p-1}{2}} \quad \text{even}$$

$$b^{3} = -1 \quad \text{or} \quad b^{3} = 1 \quad \longleftarrow \quad \boxed{\frac{p-1}{4}} \quad \text{odd}$$

- Given a prime p
- Subtract 1 & factor out 2's :

$$p-1 \to (p-1)/2 \to (p-1)/4 \to \dots$$

$$\dots \to (p-1)/2^{s} = m \quad \text{odd}$$

$$\Rightarrow \quad p-1 = 2^{s} \cdot m$$

- For any $b \neq 0$,

either $b^{m} \equiv \pm 1 \mod p$

or $b^{2^{r} m} \equiv -1 \mod p$ for some $r \leq s$

Def For an odd number n, with s & m

given by $n-1 = 2^s \cdot m$ (m odd), the number n is a strong pseudoprime base b if either $b^m \equiv \pm 1 \mod n$
or $b^{2^r m} \equiv -1 \mod n$ for some $r \leq s$.

Moreover : If n is composite, about 3/4 of the bases will be witnesses to this fact!

Miller-Rabin Test

Given an odd integer N, choose k random integers in the range $1 < b < N-1$; if N is a strong pseudoprime for each chosen base b, then N is probably prime, with probability $1-(1/4)^k$.

Note : $k = 2$, > 90% certain
$k = 4$, > 99 % certain
$k = 5$, > 99.9 % certain

... very certain, very fast!

④ Proving Primality

For large N, do not attempt unless already quite certain that N is prime.

Lucas-Lehmer Test (for Mersenne primes)

$M_p = 2^p - 1$, p prime

Define sequence $s_0, s_1, \ldots$ recursively:

$$s_0 = 4 \; ; \qquad s_n = s_{n-1}^2 \underset{\text{mod}}{\text{red.}} M_p \qquad (n \geq 1)$$

Look at $(p-2)^{th}$ term:

$$M_p \text{ prime} \iff s_{p-2} \equiv \underline{\;0\;} \mod M_p$$

Lucas-Pocklington-Lehmer Test

N large, odd

$$N - 1 = K \cdot U$$

Known factorization (divide out small primes from N-1)

unknown factz'n

Want $\underline{K > \sqrt{N}}$

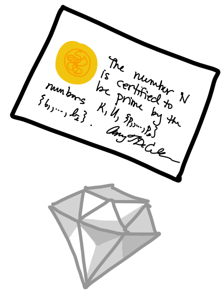
Let $\underline{p_1, p_2, \ldots, p_\ell}$ be the primes dividing K.

Suppose that for each index i w/ $1 \leq i \leq \ell$, there is a base b_i s.t.

$$b_i^{N-1} \equiv 1 \mod N \quad \text{but} \quad \gcd(b_i^{(N-1)/p_i} - 1, N) = 1$$

Then N is prime.

↳ **Primality Certificate**



$$K, \ U, \ \{p_1, \dots, p_\ell\}, \ \{b_1, \dots, b_\ell\}$$

Constructing Large Primes

Given 2 large primes (attempt) to construct a larger one.

- M, N large primes
- Look among

  $$2MN+1, \ 4MN+1, \ 6MN+1, \ \dots$$

  until one passes MRT

  $$\downarrow$$

  $n = 2kMN+1$ HUGE & "probably prime"

- LPL Test : $n-1 = 2kMN$

  HUGE

  easy to factor into primes!

Find bases for each prime dividing $n-1$ ...

⑤ The Riemann Hypothesis

Riemann (1858)

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}, \quad \text{for } s \text{ a complex number}$$

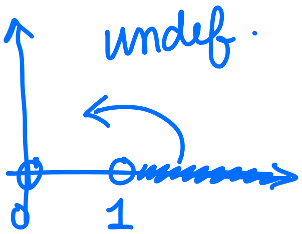
ex $\zeta(2) = \sum_{n=1}^{\infty} \frac{1}{n^2} = \frac{\pi^2}{6}$ (Euler)

$$\zeta(3) = \sum_{n=1}^{\infty} \frac{1}{n^3} < \boxed{\infty}$$

irrational
Apéry's number
quantum electrodynamics

but $\zeta(1)$ would be $\sum_{n=1}^{\infty} \frac{1}{n}$

undef.



harmonic series;
diverges

Euler : $\zeta(s) = \prod_{p \text{ prime}} \frac{1}{1-p^{-s}}$

Fund. Thm. of Arithmetic

Hadamard Product :

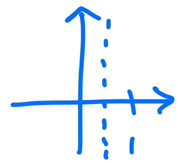
$\rho : \zeta(\rho) = 0$

$\zeta(s) = \ldots$ product of $(s-\rho)$'s ...

Riemann : explicit formula making connection

primes $\longleftrightarrow$ zeros of ζ

RH Probably... $\rho = \frac{1}{2} + it \quad t \in \mathbb{R}$



Note PNT was proven using zeros of ζ

RH $\Leftrightarrow$ optimal error term in PNT

But No proof of RH yet...

one of math's most imp. ?'s.