Fermat Primality Test
Lecture 11a: 2022-03-28

MAT A02 – Winter 2022 – UTSC

Prof. Yun William Yu

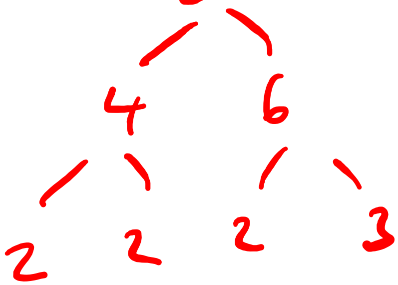
What's a prime number

- A prime number p is any natural number greater than 1 than is divisible by only 1 and itself.

  Ex. 7 is prime because it's not divisible by 2, 3, 4, 5, 6.

- Prime factors form the multiplicative building blocks of the natural numbers.

  $24 = 2^3 \cdot 3$



How to find a large prime

- Suppose I want a prime number that's between 10^{210} and 10^{211}. How can I find one?

A: Euclidean algorithm — finding gcd
B: Sieve of Eratosthenes — finding primes
C: Pythagorean theorem — sides of a right triangle
D: Euler's Phi function — finding numbers of relative primes
E: None of the above

Sieve of Eratosthenes

- Method for computing list of primes by filtering out all multiples of a number.
- Repeatedly filter out all multiples of the smallest remaining number in a list.
- Start with filter out multiples of 2.
- Then multiples of 3.
- Then multiples of 5, because 4 is filtered, etc.

Eratosthenes of Cyrene
276 BCE – 194 BCE

Sieve of Eratosthenes in action

1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

- How quickly do we get all the primes between 1 and 100?

How fast is the sieve?

- If n is not prime, then it must be divisible by a prime $p \leq \sqrt{n}$.

Let p be the smallest prime that divides n.

Then $n = p \cdot k$, where $k \geq p$

Thus $n = p \cdot k \geq p^2$

$\Rightarrow n \geq p^2 \Rightarrow p \leq \sqrt{n}$

- To figure out if a number n is prime, you only have to run the Sieve of Eratosthenes up to a prime $p \leq \sqrt{n}$.

Ex. Is 97 prime? YES

Need to check: 2, 3, 5, 7.

$2\overline{)97}$ = 48 r1 $\quad 3\overline{)97}$ = 32 r1 $\quad 5\overline{)97}$ = 19 r2 $\quad 7\overline{)97}$ = 13 r6

Is the following number prime?

- $\underbrace{128394182491824983485276927645694578483457}_{x,\ 42 \text{ digits}}$

$x \approx 10^{42}$

- How long would it take to determine if it's prime using the Sieve of Eratosthenes if it takes one second to remove multiples of each prime? Choose the best approximation.

Need to check up to $\sqrt{x}$

$\sqrt{x} \approx \sqrt{10^{42}} \approx 10^{21}$

Need to check all primes up to 10^{21}

A: 21 seconds
B: 42 seconds
C: 10^{21} seconds = $3 \cdot 10^{13}$ years
D: 10^{42} seconds = $3 \cdot 10^{34}$ years
E: None of the above

Prime Number Theorem

- [Hadamard, 1895, Poussin, 1896]
- There are approximately $\frac{n}{\ln n}$ prime numbers between 2 and n.

between 2 and 10^{21},

approximately $\frac{10^{21}}{\ln 10^{21}} \approx 2 \cdot 10^{19}$ primes

- So in the sieve on the previous slide, we can check fewer numbers, since we only check primes.

Still $2 \cdot 10^{19}$ primes to check.

At one per sec., still $6 \cdot 10^{11}$ years

At one billion a sec, still $6 \cdot 10^{2}$ years

$=$ 600 years,

6 centuries.

Chances of guessing a prime

- 128394182491824983485276927645694578483457

$\approx 10^{42}$

- What if we just said that this was a prime. What's the chance we are right?
  - Recall the Prime Number Theorem says that approximately $\frac{n}{\ln n}$ numbers are prime from 1 to n.

$n \approx 1.2839 \cdot 10^{42}$

$\ln n \approx 97$

$\Rightarrow$ about $\frac{1}{97}$ chance of it being prime

A: $\frac{1}{21}$ chance
B: $\frac{1}{42}$ chance
C: $\frac{1}{97}$ chance
D: $\frac{1}{10^{21}}$ chance
E: None of the above

Fermat Primality Test

- Fermat's Little Theorem: If n is a prime number, and a is any number between 1 and $n - 1$, then
$$a^{n-1} \equiv 1 \pmod n$$

Ex. $n = 11$, $2^{10} \equiv 1 \mod 11$, $3^{10} \equiv 1 \mod 11$, ...

- Conversely: If a is any number between 1 and $n - 1$, and
$$a^{n-1} \not\equiv 1 \pmod n$$
then n is not prime.

Ex. $n = 10$ $a = 2$.

$2 \equiv 2$

$2^2 \equiv 4$

$2^4 \equiv 16 \equiv 6$

$2^8 \equiv 36 \equiv 6$

$2^9 \equiv 2^8 \cdot 2 \equiv 6 \cdot 2 \equiv 2 \mod 10$

$\Rightarrow$ 10 is not prime

Fermat Liars and Witnesses

- If $a^{n-1} \not\equiv 1 \pmod{n}$, then a is a witness to the fact that n is not prime, because it tells us that n is not prime.

Ex. $2^9 \equiv 2 \mod 10$, so 2 is a witness that 10 is not prime.

- If $a^{n-1} \equiv 1 \pmod{n}$, but n is not prime, then a is a Fermat liar, since it looks like n is prime, but it isn't.

Ex. $8^8 \equiv 1 \mod 9$

$8^1 \equiv 8$

$8^2 \equiv 64 \equiv 1$

$8^4 \equiv 1$

$8^8 \equiv 1$

$\Rightarrow$ 8 is a liar claiming 9 might be prime when it isn't

Example

- Claim: 129 is not prime.
- Witness: let $a = 2$.

$2^{128} \bmod 129 \equiv 4 \bmod 129$

$\Rightarrow$ 129 is not prime

$2^1 \equiv 2$

$2^2 \equiv 4$

$2^4 \equiv 16$

$2^8 \equiv 256 \equiv 127 \equiv -2$

$2^{16} \equiv 4$

$2^{32} \equiv 16$

$2^{64} \equiv 256 \equiv -2$

$2^{128} \equiv 4$

Try it out

- Which of the following numbers is a witness to the fact that 33 is not a prime number?

possible a's

A: 1
B: 10
C: 23
D: 31
E: None of the above

$1^{32} \bmod 33 \equiv 1$ not a witness $\Rightarrow$ liar

$10^{32} \bmod 33 \equiv 1$ not a witness $\Rightarrow$ liar

10
$10^2 \equiv 100 \equiv 1$
$10^4 \equiv 1$
$10^8 \equiv 1$
$10^{16} \equiv 1$
$10^{32} \equiv 1$

$23^{32} \bmod 33 \equiv 1$
$23^2 \equiv 529 \equiv 1$
$23^4 \equiv 1$
$23^8 \equiv 1$
$23^{16} \equiv 1$
$23^{32} \equiv 1$

not a witness $\Rightarrow$ liar

$31^{32} \bmod 33$
$31 \equiv -2$
$31^2 \equiv 4$
$31^4 \equiv 16$
$31^8 \equiv 256 \equiv 25 \equiv -8$
$31^{16} \equiv 64 \equiv -2$
$31^{32} \equiv 4$

witness

Fermat Primality Test

- We want to know if n is prime.

$n = 33$

1. Pick a random number a between $\cancel{1}\ 2$ and $n - \cancel{1}\ 2$

$a = 10$ $a = 31$

2. Compute $a^{n-1} \pmod{n}$

$10^{32} \equiv 1 \mod 33$ $31^{32} \equiv 4 \mod 33$

3. If $a^{n-1} \not\equiv 1 \pmod{n}$, then n is not prime and a is a witness to this fact. Otherwise, n passes the test, and you don't know for certain.

Don't know $\Rightarrow$ 33 is not prime

- If you repeat this process enough times, and it passes the test each time, then maybe it's prime, but you can't prove it for sure.

Going back

$n =$

- 128394182491824983485276927645694578483457
- Claim $a = 2$ is a witness because we can compute
  $$2^{128394182491824983485276927645694578483456}$$ $\leftarrow n-1$
  in mod 128394182491824983485276927645694578483457 $\nwarrow n$
  arithmetic.

- Using a computer, we get an answer of 173110836615146533060996179225822896577728, which is not equal to 1.

- Therefore, the original number was not prime.

Fermat's test and finding large primes

- Fermat's test strictly speaking only tells you when a number is not prime.
- However, except for a very special class of exceptions (called Carmichael numbers), each time a number passes the test with a different number a, you decrease the chance of being composite by 50% each time.

Not a Carmichael numbers

Ex. $n = 563$

$$\left.\begin{array}{l} 231^{562} \bmod 563 \equiv 1 \\ 108^{562} \bmod 563 \equiv 1 \\ 7^{562} \bmod 563 \equiv 1 \\ 499^{562} \bmod 563 \equiv 1 \end{array}\right\}$$

probability that 563 is composite $\leq \frac{1}{16}$.

$\Rightarrow$ Probability 563 is prime $\geq \frac{15}{16} \approx 93\%$

Miller-Rabin and other tests

- Except for a certain class of hard numbers, Fermat's test tells us that a number is probably prime.
- Other modifications guarantee it, and don't have any hard numbers. The Miller-Rabin test (see Section 23.9) always works to show that a number is probably prime.
- This lets us just guess a bunch of large numbers, and quickly filter out the non-primes, to get a large prime number.
- These large prime numbers are essential in cryptography.