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.

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

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
B: Sieve of Eratosthenes
C: Pythagorean theorem
D: Euler's Phi function
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 $p \leq \sqrt{n}$.

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

Is the following number prime?

- 1283941824918249834852769276456945784834 57

- 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.

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.

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

Chances of guessing a prime

- 128394182491824983485276927645694578483457

- 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.

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

$$a^{n-1} \equiv 1 \pmod{n}$$

- 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.

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.

- 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.

Example

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

Try it out

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

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

Fermat Primality Test

- We want to know if n is prime.

1. Pick a random number a between 1 and $n-1$
2. Compute $a^{n-1} \pmod{n}$
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.

- 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

- 1283941824918249834852769276456945784834 57
- Claim $a = 2$ is a witness because we can compute $2^{1283941824918249834852769276456945784834 56}$ in mod 1283941824918249834852769276456945784834 57 arithmetic.

- Using a computer, we get an answer of 1731108366151465330609961792258228965772 8, 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.

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.