Deterministic Polynomial-Time Primality Testing

The AKS Primality Testing Algorithm

Kumar Sannidhya Shukla
kshukla5@uwo.ca

Department of Mathematics

Wednesday 28$^{\text{th}}$ June, 2023

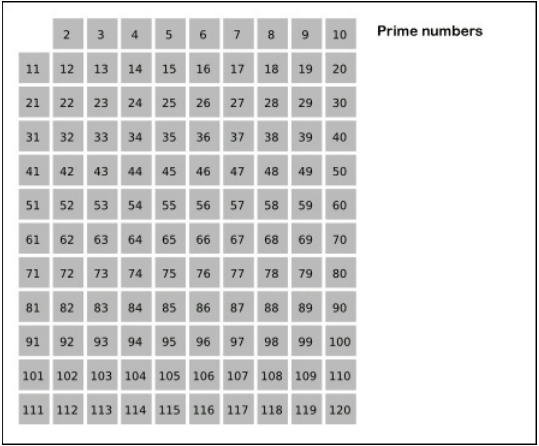
Math 9171L - Mathematical Computation

Outline

Sieve of Eratosthenes

An algorithm to generate all primes up to n.

- Start with a list of numbers $\{2, \dots, n\}$



Sieve of Eratosthenes

- Add 2 to the list of primes.

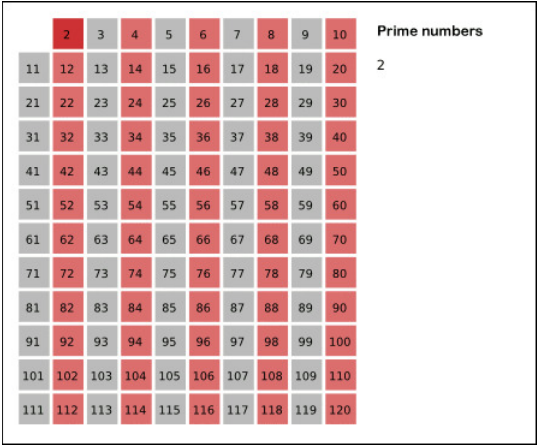
	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100
101	102	103	104	105	106	107	108	109	110
111	112	113	114	115	116	117	118	119	120

Prime numbers

2

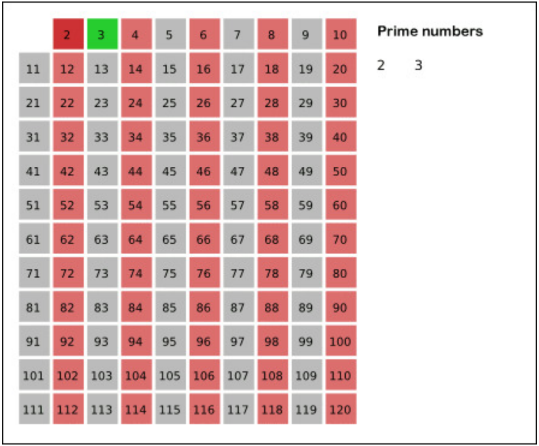
Sieve of Eratosthenes

- Drop all multiples of 2.



Sieve of Eratosthenes

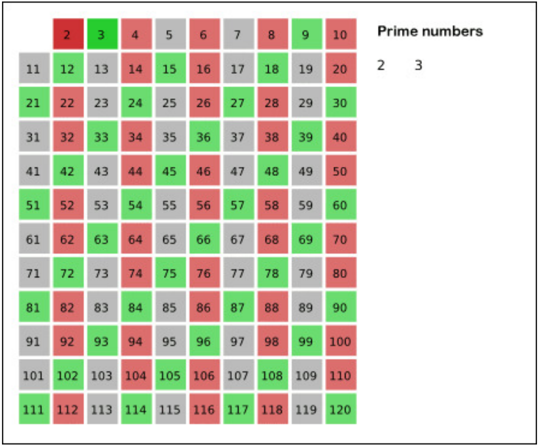
- Add 3 to the list of primes.



Western

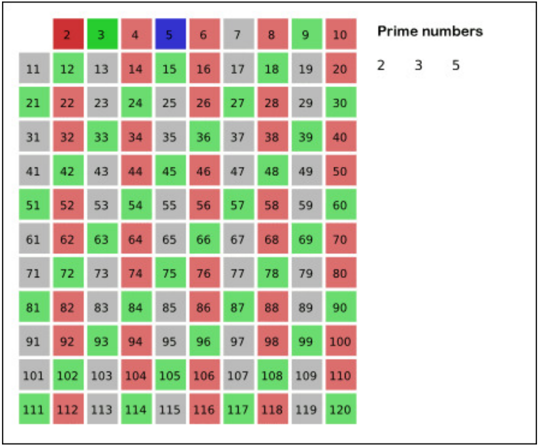
Sieve of Eratosthenes

- Drop all multiples of 3.



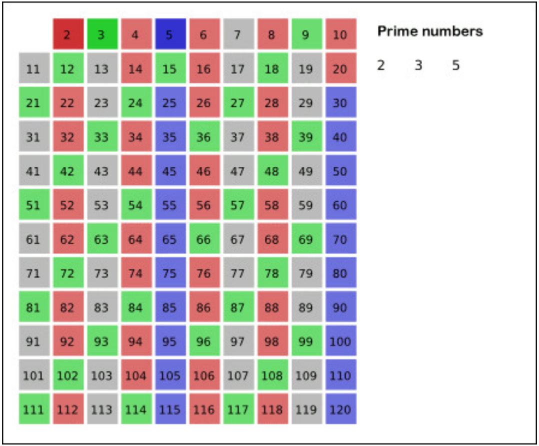
Sieve of Eratosthenes

- Add 5 to the list of primes.



Sieve of Eratosthenes

- Drop all multiples of 5.



Sieve of Eratosthenes

- ...

Sieve of Eratosthenes

An algorithm to generate all primes up to n.

Algorithm 1 Seive of Eratosthenes

```
Input. n
L = [1, n]
i = 1
while i < len(L) do
    for j = 2 → ⌊n/i⌋ do
        Delete L[i]*j from L
    end for
end while
return L
```

Runtime: $\mathcal{O}(2^{\log n})$

Fermat's Primality Test

Theorem (Fermat's little theorem)

Let p be a prime then $a^p \equiv a \mod p$

This can theorem can be used to devise a primality test as follows:

- Given a number n
- Pick a random $a, 1 < a < n$
- Test whether $a^n \equiv a \mod n$
- If false, return `Composite`
- Otherwise, return `Prime`

Fermat's Primality Test

Theorem (Fermat's little theorem)

Let p be a prime then $a^p \equiv a \mod p$

This can theorem can be used to devise a primality test as follows:

1. Given a number n
2. Pick a random $a, 1 < a < n$
3. Test whether $a^n \equiv a \mod n$
4. Run the above steps multiple times
5. If the congruence in step 3 is false even once, return `Composite`
6. Otherwise, return `Prime`

Fermat's Primality Test

Algorithm 2 Fermat's Primality Test

```
Input. n
for i = 1 → 10 do
    Generate random a, 1 < a < n.
    if a^n ≢ a mod n then
        return Composite
    end if
end for
return Prime
```

Fermat's Primality Test

Definition (Carmichael numbers)

A Carmichael number is a composite number n, such that $a^n \equiv a \mod n$ for all $1 < a < n$.

Example. 561, 1729, 2465, etc.

Fermat's Primality Test

Definition (Carmichael numbers)

A Carmichael number is a composite number n, such that $a^n \equiv a \mod n$ for all $1 < a < n$.

Example. 561, 1729, 2465, etc.
Carmichael numbers will fool Fermat's test 100% of the times!

Fermat's Primality Test

Definition (Carmichael numbers)

A Carmichael number is a composite number n, such that $a^n \equiv a \mod n$ for all $1 < a < n$.

Example. 561, 1729, 2465, etc.

Carmichael numbers will fool Fermat's test 100% of the times!

There are infinitely many Carmichael numbers!!

Western

Generalized Fermat's Theorem

Theorem

Let $n > 1$ and $a \in \mathbb{Z}_n^*$. Then n is a prime if and only if

$$(x + a)^n = x^n + a$$

in $\mathbb{Z}_n[x]$.

Generalized Fermat's Theorem

Theorem

Let $n > 1$ and $a \in \mathbb{Z}_n^*$. Then n is a prime if and only if

$$(x+a)^n = x^n + a$$

in $\mathbb{Z}_n[x]$.

Proof.

If n is a prime, then $n \Big| \binom{n}{k}$ for all k.

Generalized Fermat's Theorem

Theorem

Let $n > 1$ and $a \in \mathbb{Z}_n^*$. Then n is a prime if and only if

$$(x+a)^n = x^n + a$$

in $\mathbb{Z}_n[x]$.

Proof.

If n is a prime, then $n \Big| \binom{n}{k}$ for all k.
If n is a composite, suppose $n = p^k.m$, $p \not| m$. Then, $p^k \not| \binom{n}{p} a^{n-p}$. □

Examples

Example

The number 5 is a prime. So,

$$(x+1)^5 = x^5 + 5x^4 + 10x^3 + 10x^2 + 5x + 1 = x^5 + 1 \text{ in } \mathbb{Z}_5[x].$$

Examples

Example

The number 5 is a prime. So,

$$(x+1)^5 = x^5 + 5x^4 + 10x^3 + 10x^2 + 5x + 1 = x^5 + 1 \text{ in } \mathbb{Z}_5[x].$$

Example

The number 4 is not a prime. So,

$$\begin{aligned}(x+1)^4 &= x^4 + 4x^3 + 6x^2 + 4x + 1\\ &= x^4 + 2x^2 + 1\\ &\neq x^4 + 1 \text{ in } \mathbb{Z}_4[x].\end{aligned}$$

Reduction mod $x^r - 1$

- If we naively try to turn the generalized Fermat's little theorem into a primality test, then we get exponential runtime.
- The idea is to reduce the number of coefficients by modding out by $x^r - 1$.
- The ring to consider: $\mathbb{Z}_n[x]/(x^r - 1)$.
- $x^n + a = x^{n \bmod r} + a$

How to choose r?

- r should be small so that enough coefficients of $(x+a)^n$ get killed but not so small that composite numbers don't satisfy the congruence.

Theorem

There exist an r, $3 \leq r \leq \lceil \log^5 n \rceil$, such that $o_r(n) > \lfloor \log^2 n \rfloor$.

Proof.

Suppose for all $r \leq R$, we have $o_r(n) \leq \lfloor \log^2 n \rfloor$. Then,
$r | (n-1)(n^2-1)\ldots(n^{\lfloor \log^2 n \rfloor} - 1) = P$.
So, $\mathrm{LCM}\{r : 1 \leq r \leq R\} | P$. By LCM bound, $2^R \leq P$. Thus,
$R < \log^5 n$. $\square$

The AKS Algorithm

Algorithm 3 AKS Primality Test

Input. n
if $n = a^b$, $a, b > 1$ **then**
    return `Composite`
end if
Find r, such that $o_r(n) > \log^2 n$
if $\exists a \in [r], 1 < (a, n) < n$ **then**
    return `Composite`
end if
for $a = 1 \to \lceil 2\sqrt{r} \log n \rceil$ **do**
    if $(x + a)^n \neq x^n + a$ in $\mathbb{Z}_n[x]/(x^r - 1)$ **then**
        return `Composite`
    end if
end for
return `Prime`

Proof of Correctness

Theorem

The AKS test returns `Prime` *if and only if then input n is prime.*

Proof.

$(\Longleftarrow)$ Obvious.
$(\Longrightarrow)$ Suppose conversely that the algorithm returns `Prime`. In particular this means, that all congruences in line 10 hold true. Suppose the n has a prime factor p. We will show that $n = p$.
Define a group,

$$I := \langle p, n \mod r \rangle$$

$$t := |I| \geq o_r(n) > \log^2 n$$

□

Proof of Correctness

Proof.

(Continued.) Let $h(x)$ be an irreducible factor of $(x^r - 1)/(x - 1)$. Then, $\mathbb{Z}_p[x]/(h(x))$ is a field. Define another group,

$$J := \langle x + 1, x + 2, \dots, x + r \mod (p, h)\rangle$$

$$|J| > n^{2\sqrt{t}}$$

J is a cyclic group, let f be a generator of J. $\square$

Proof of Correctness

Proof.

(Continued.) There exist $(i,j) \neq (i',j')$, $0 \leq i,j,i',j' \leq \sqrt{t}$ such that $n^i p^j = n^{i'} p^{j'}$. Then,

$$f(x^{n^i p^j}) = f(x^{n^{i'} p^{j'}}) \text{ in } \mathbb{Z}_p[x]/(h(x))$$

$$f(x)^{n^i p^j} = f(x)^{n^{i'} p^{j'}} \text{ in } \mathbb{Z}_p[x]/(h(x))$$

$$n^i p^j = n^{i'} p^{j'} \mod |J|$$

So n is a prime power, but we already rejected all higher powers, so n must be a prime. □

Western

Arithmetic in $\mathbb{Z}_p$ and $\mathbb{Z}_p[x]/(q(x))$

- **Notation.** $\widetilde{\mathcal{O}}(f(n)) = \mathcal{O}(f(n) \cdot \texttt{poly}(\log f(n)))$
- Multiplication in $\mathbb{Z}_p$: $\mathcal{O}(\log p \cdot (\log \log p)^2) = \widetilde{\mathcal{O}}(\log p)$
- Multiplication in $\mathbb{Z}_p[x]/(q(x))$: $\widetilde{\mathcal{O}}(r \log r \log p)$ where $r = \deg q(x)$.

Western

Time Complexity

- Perfect power test: $\widetilde{\mathcal{O}}(\log^3 n)$
- Finding appropriate value of r: $\widetilde{\mathcal{O}}(R \log^2 n) = \widetilde{\mathcal{O}}(\log^7 n)$.
- GCD step: $\widetilde{\mathcal{O}}(r \log n) = \widetilde{\mathcal{O}}(\log^6 n)$
- Generalized FLT step: $(\sqrt{r} \log n)\widetilde{\mathcal{O}}(r \log^2 n) = \widetilde{\mathcal{O}}(\log^{21/2} n)$
- Total complexity: $\widetilde{\mathcal{O}}(\log^{21/2} n)$

Epilogue

- Recall the language PRIMES of all prime numbers.

$$\mathtt{PRIMES} = \{p \in \mathbb{N} : p \text{ is a prime}\}$$

- Then the existence of a deterministic polynomial time algorithm proves that

Theorem (Agrawal-Kayal-Saxena, 2002)

PRIMES is in P.

Source code available on `https://github.com/feynhat/math9171`.

References

Ivan Niven, Herbert Zuckerman, Hugh Montgomery
An Introduction to the Theory of Numbers.
John Wiley & Sons, 1991.

Manindra Agrawal, Neeraj Kayal, Nitin Saxena
PRIMES is in P.
Annals of Mathematics, 2004.

Western