```
isMember(set, elem)

add(set, elem)
```

```
prompt user
read string
set = empty
```

```
for each char c in string:
    if !isMember(set, c):
        add(set, c)
```

Union(A, B)

```
set = A
for each c in B
    if !isMember(set, c):
        add(set, c)
```

---

int(A, B)

```
set = empty
for each c in A:
    if isMember(B, c):
        add(set, c)
```

Modular Arithmetic

"a is congruent to b, modulo m"

$a \equiv b \pmod{m}$

means $m \mid (a-b)$

---

ex: $3 \equiv 18 \pmod{5}$ — 3

$7 \equiv 29 \pmod{11}$

$115 \equiv 90 \pmod{5}$ — 0

$a \equiv b \pmod{m}$ iff a & b give the same remainder when divided by m.

$a = xm + r \qquad b = ym + r$

$a - b = (xm + r) - (ym + r) = xm + r - ym - r$

$= xm - ym$

$= m(x - y)$

$m \mid (a - b)$

$a = xm + r \qquad b = ym + r$

$a - b = (xm + r) - (ym + r) = xm + r - ym - r$

$= xm - ym$

$= m(x - y)$

$m \mid (a - b)$

---

if $m \mid (a - b)$ then $m \mid (b - a)$

So if $a \equiv b$ then $b \equiv a$

Modular Arithmetic

"a is congruent to b, modulo m"

$a \equiv b \pmod{m}$

means $m \mid (a-b)$

ex: $3 \equiv 18 \pmod{5}$

$7 \equiv 29 \pmod{11}$

$115 \equiv 90 \pmod{5}$

3

0

$\frac{7}{11} = 0 \text{ R } 7$

$\frac{29}{11} = 2 \text{ R } 7$

$a \equiv b \pmod{m}$ iff

a & b give the same

remainder when divid

if $a \equiv b \pmod{m}$ then $b \equiv a \pmod{m}$

$c \cdot a \equiv c \cdot b \pmod{m}$ for any int c

if $c \equiv d \pmod{m}$

then $a + c \equiv b + d \pmod{m}$

$a \cdot c \equiv b \cdot d \pmod{m}$

mod 5

$13 \equiv 28$ (3) $\equiv 28$

(2) $\equiv 7$

$13 \cdot 2 \equiv 28 \cdot 7$

$26 \equiv 196$

$(1256)^{17000} \pmod 5$

$1256 \equiv 1 \pmod 5$

$196 - 26 = 170$

$1256 \times 1256 \times 1256 \times \ldots$

$\equiv 1 \times 1 \times 1 \ldots \times 1$

$\equiv 1$

mod 5

$13 \equiv 28$ ③ $\equiv 28$

② $\equiv 7$

$13 \cdot 2 \equiv 28 \cdot 7$

$26 \equiv 196$

$(1256)^{17000}$ (mod 5)

$1256 \equiv 1$ (mod 5)

2^{17000} (mod 5)

$2^1 \equiv 2$

$2^2 \equiv 4$

$2^3 \equiv 8 \equiv 3$

$2^4 \equiv 6 \equiv 1$

$2^5 \equiv 2$

$2^6 \equiv 4$

$\vdots$

196
−26
170

1256 × 1256 × 1256 × ...

$\equiv 1 \times 1 \times 1 \times \cdots \times 1$

$\equiv 1$

Multiplication Mod 5

	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Mod 4

	1	2	3
1	1	2	3
2	2	0	2
3	3	2	1

$a = \frac{1}{b}$

$ab = 1$

A prime number is an int >1 that is divisible only by itself & 1.

A ~~not~~ number that is not prime is called "composite"

if $\frac{n}{a} = b$ then $\frac{n}{b} = a$

if $n = ab$ then $a \leq \sqrt{n}$ or $b \leq \sqrt{n}$

Sieve of Eratosthenes

~~1~~ ~~X~~ (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~~

A prime number is an int >1 that is divisible only by itself & 1.

A ~~not~~ number that is not prime is called "composite"

if $\frac{n}{a} = b$ then $\frac{n}{b} = a$

if $n = ab$ then $a \leq \sqrt{n}$ or $b \leq \sqrt{n}$

Sieve of Eratosthenes

~~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~~

FUNDAMENTAL THEOREM OF ARITHMETIC

any int > 1 can be written uniquely* as a product of primes.

$100 = 2 \cdot 2 \cdot 5 \cdot 5$

* other than re-arranging the primes

How many prime numbers are there?

Theorem: There is no largest prime.

Proof: Let B be the largest prime.

Let $X = 2 \cdot 3 \cdot 4 \cdot 5 \cdots (B-3)(B-2)(B-1)B + 1$

$X > B$ so X is not prime.

Mersenne Primes

$2^p - 1$

$2^{2} - 1 = 3$ ✓

$2^{3} - 1 = 7$ ✓

$2^{4} - 1 = 15$

$2^{5} - 1 = 31$ ✓

$2^{6} - 1 = 63$

$2^{7} - 1 = 127$ ✓

$2^{8} - 1 = 255$

$2^{9} - 1 = 511$

$2^{10} - 1 = 1023$

$2^{11} - 1 = 2047$

Contents hide
(Top)
Notes
References
External links

50	77,232,917	467333...179071	23,249,425	109200...301056	46,498,850	Dec 26, 2017	GIMPS / Jonathan Pace	LLT / Prime95 on PC with Intel Core i5-6600 processor	[65][66]
*	79,156,177	*Lowest unverified milestone*[f]							
51[g]	82,589,933	148894...902591	24,862,048	110847...207936	49,724,095	Dec 7, 2018	GIMPS / Patrick Laroche	LLT / Prime95 on PC with Intel Core i5-4590T processor	[67][68]
52[g]	136,279,841	881694...871551	41,024,320	388692...008576	82,048,640	Oct 12, 2024	GIMPS / Luke Durant	LLT / PRPLL on Nvidia H100 GPU[h]	[69]
*	138,512,911	*Lowest untested milestone*[f]							

Notes [edit]

a. ^ The first four perfect numbers were documented by Nicomachus circa 100, and the concept was known (along with

Mersenne Primes

$2^p - 1$

$2^{2} - 1 = 3$ ✓

$2^{3} - 1 = 7$ ✓

$2^{4} - 1 = 15$

$2^{5} - 1 = 31$ ✓

$2^{6} - 1 = 63$

$2^{7} - 1 = 127$ ✓

$2^{8} - 1 = 255$

$2^{9} - 1 = 511$

$2^{10} - 1 = 1023$

$2^{11} - 1 = 2047$

If n & $n+2$ are prime,

they are called "twin primes."

Is there a largest pair of twin primes?

Unknown

The Prime Number Theorem

Let $p(n) = \#$ of primes $\leq n$

as $n \to \infty$, $p(n)$ gets close to $\log_e(n)$

$$\lim_{n \to \infty} \frac{p(n)}{\log_e(n)} = 1$$

If n & $n+2$ are prime,

they are called "twin primes."

Is there a largest pair of twin primes?

Unknown

The Prime Number Theorem

Let $p(n) = \#$ of primes $\leq n$

as $n \to \infty$, $p(n)$ gets close to $\log_e(n)$

$\lim_{n \to \infty} \frac{p(n)}{\log_e(n)} = 1$

(Zeta function
Riemann Hypothesis)