Prime Nos :   2, 3, 5, 7, 13, - - - - -

~~1~~, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, ~~13~~

```
for( i = 2;  i < N;  i++ ) {
        if ( N % i ) {
                Not Prime;
        }
}
Prime
```

Another Example:

1	×	36
2	×	18
3	×	12
4	×	9
6	×	6
9	×	4
12	×	3
18	×	2
36	×	1

This is repeated, hence ignore.

3 × 12

12 × 3

Hence, only make checks for numbers ≤ sqrt(n)

$$c \le \mathrm{sqrt}(N)$$

$$c * c \le N$$

Q: $N = 40$

2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37

	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~~

O → F

X → T

Time complexity:

$$\frac{n}{2} + \frac{n}{3} + \frac{n}{5} + \frac{n}{7} + \dots$$

$$\underbrace{n\left(\frac{1}{2} + \frac{1}{3} + \frac{1}{5} + \frac{1}{7} + \dots\right)}_{\text{Harmonic progression for primes.}}$$

$$= \log(\log N)$$

Total time complexity: $O(N * \log(\log N))$

Finding square root of a number

0 18 36

if (m * m > n)

e = m - 1

else

s = m + 1

Sqrt(40) = 6.32

above way

?

0.1

root = 6.1

= 6.2

= 6.3 this

= 6.4

same thing for 0.01

Newton Raphson method

$$root = \frac{\left(X + \frac{N}{X} \right)}{2}$$

actual sq root $= \sqrt{N}$

Sqrt you have assumed

$error = |root - X|$

You will find your ans when error < 1

1. Assign X to N
2.
3. Update the value of X = root

Complexity: $O((\log N)\, F(N))$

$F(N)$ = cost of calculating $\frac{f(n)}{f'(n)}$

with n-digit precision.

Why the formula works?

$$\sqrt{N} = \frac{\left(X + \frac{N}{X}\right)}{2}$$

$$\sqrt{N} = \frac{\sqrt{N} + \frac{\sqrt{N}}{\cancel{\sqrt{N}}}}{2} \Rightarrow \sqrt{N} = \frac{2\sqrt{N}}{2}$$

$$\sqrt{N} = \sqrt{N}$$

Factor of a number:

$n = 20 \Rightarrow 1, 2, 4, 5, 10, 20$

20, 10, 5

$20 \% 1$ ✓ $\Rightarrow 20 * 1 = 20$

$20 \% 2$ ✓ $\Rightarrow 10 * 2 = 20$

$20 \% 4$ ✓ $\Rightarrow 5 * 4 = 20.$

$20 \% 5$ ✓ $= 4 * 5 = 20$

$20 \% 10 = 2 * 10 = 20$

Repeated

Properties of modulo (%)

- $(a+b)\%m = ((a\%m)+(b\%m))\%m$
- $(a-b)\%m = ((a\%m)-(b\%m)+m)\%m$
- $(a*b)\%m = ((a\%m)*(b\%m))\%m$
- $\left(\frac{a}{b}\right)\%m = ((a\%m)*(b^{-1}\%m))\%m$

$b^{-1}\%m \Rightarrow$ multiplicative modulo inverse (mmi)

Ex:

$$(6 * y) \% 7 = 1$$

y = mmi for 6 & $y = 6$

$$(6 * 6) \% 7 = 36 \% 7 = 1$$

mmi = $b^{-1} \% m$ means that

b & m are co-primes.

* $(a \% m) \% m = a \% m$

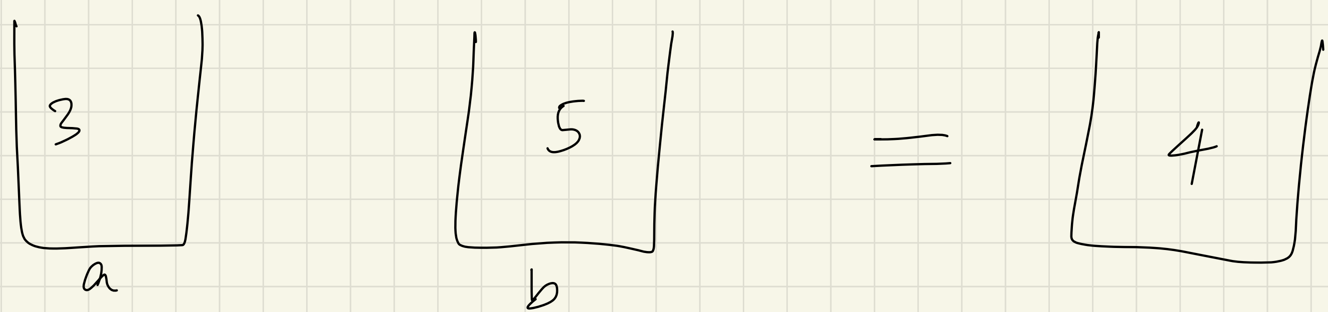
* $m^x \% m = 0 \quad \forall x \in$ the integers.

Extra:

If p is prime no. which is not a divisor of b, then $ab^{p-1} \% p = a \% p$ due to Fermat's Little theorem.

How? will be covered in advance DS course :)

Die-hard Example:



$$\begin{array}{lcccc}
 & (a,\ b) & & & \\
1^{st} \rightarrow & (0,0) & \rightarrow (3,0) & \rightarrow (0,3) & \\
2^{nd} \rightarrow & (0,3) & \rightarrow (3,3) & \rightarrow (1,5) & \\
 & & (0,1) & \leftarrow (1,0) & \\
3^{rd} \rightarrow & (0,1) & \rightarrow (3,1) & \rightarrow (0,4) & \\
 & & & \text{Ans} &
\end{array}$$

jug a → 2^{1} times

jug b → 2^{2} times

$$\begin{cases} r = as^1 - bs^2 \\ r = as^1 + (-bs^2) \end{cases}$$

$$L = s'a + t'b$$

$$s'a = L - t'b$$

$$r = s'a + t'b - t'b - bs^2$$

$$r = L - (t' + u)b$$

If $t' + u \neq 0 \Rightarrow [r < 0 \text{ or } r > b]$

which is not true

$$t' + u = 0 \Rightarrow u = -t'$$

$$r = s'a + t'b = L$$

aka $\rightarrow$ $r = ax + by$

$$3x + 5y = 4$$?

Put x & y as integers, what is the minimum +ve value you can have of eq^n.

$x = -3$, $y = 2$

$3x + 5y = 1$ → minimum +ve value that I can form

★ This is called HCF!

HCF/ of a & b = min +ve value of eqn $ax + yb$

GCD

when x & y are ints.

$HCF(4, 18) = 2$

4: $1, 2, 4$

18: $1, 2, 3, 6, 9, 18$

Ans

$HCF(3, 9) = 3$

3: $1, 3$

9: $1, 3, 9$

$$\min(3x + 9y) = 3$$

$$3x + 1y$$

$$3(x + 3y)$$

$$= 3(-2 + 3) = 3$$

$a \quad , \quad b$

$$ax + by = L$$

$$2x + 4y = 5$$

$$2(x + 2y) = 5$$

$$x + 2y = 2.5$$

note :

Whatever it is you will get, that will come out as common.

$$3x + 6y = 9$$

$$3(x + 6y) = 1$$

$$x + 2y = 3$$

$$\underbrace{3x + 5y} = 17$$

$$1(3x + 1y) = 17$$

Euclid's Algorithm:

$$\gcd(a, b) = \gcd(\mathrm{rem}(b, a), a)$$

$$\gcd(105, 224) = \gcd(\mathrm{rem}(224, 105), 105)$$

$$= \gcd(14, 105)$$

Why?

$$105x + 224y$$

why subtract?

$14x + 105y$

i.e. because the gcd of $(105, 224)$ also divides a linear combination of 105 & 224.

Ex: $224 - 2 * 105 = 14$ (rem)

LCM:

$$\text{lcm}(a, b) = \text{min. no. divisible by both } a \,\&$$

$$\text{lcm}(2, 4) = 4$$

$$(3, 7) = 21$$

Note:

Say we have a, b

$$d = \gcd(a, b)$$

$$f = \frac{a}{d}, \quad g = \frac{b}{d}$$

$$\Rightarrow a = fd, \quad b = gd$$

lcm = c

$\star$ $\operatorname{lcm}(a, b) = \operatorname{lcm}(fd, gd)$

$\star$ We know that f & g will have no other common factor.

$a = 9$, $b = 18$ $d = 9$

$f = 1$, $g = 2$

Say, $h \cdot y = \cancel{2} * 3 = 9$

$\downarrow$ bigger

$j = \cancel{9}\ \cancel{3}\ 3$ $\quad g = \cancel{18}\ \cancel{3}\ 6$

wrong?

$a = jd \qquad b = gd$

$lcm = j * g * d$ $\Rightarrow$ This is how above conditions are satisfied.

more info:

$= a * b$

$= jd * g * d$ $\rightarrow$ d is repeating, hence remove

17, 19

$$lm = f * g * d$$

☆ $$a * b = fd * gd$$

$$= d * dfg$$

$$= hy * lm$$

$$hy * lm = a \times b$$

Formula!

$$\boxed{\mathrm{Lim}(a,b) = \frac{a \times b}{\mathrm{HCF}(a,b)}}$$