Primality Testing

Prime?

$N > 1$

divisors

$N \to 1, N \to$

a b

$18 = 1 \times 18$ $\Delta = 17$

2×9 $\Delta = 7$

3×6 $\Delta = 3$

$\vdots$

$\Delta = 0$

$a \leq \sqrt{N}$

$N = 16$

a	b
1	✓
2	✓
3	✗
4	✓

$N = a \times a$ $\Delta = 0$

$\therefore a = \sqrt{N}$

```
bool isPrime(int N) {
    if(N ≤ 1) return false;
    for(int i=2; i<N; i++) {
        if(N % i==0)
            return false;
    }
    return true;
}
```

lower half	upper half
a	b

$N = ab$

$i \,!= \frac{n}{i}$

$\Rightarrow i \times i \,!= n$

$\boxed{\log_2(N)}$

$\boxed{y = \sqrt{x}}$

Newton-Raphson

$f(x) = N - x^2$

$\gcd(a,b) = \gcd(b,a)$ $\boxed{f(x) = 0}$ Hence, $x = \sqrt{N}$

GCD

$gcd(a,b) = gcd(b,a)$ $\boxed{f(x) = 0}$ Hence, $x =$

$gcd(a,0) = a$

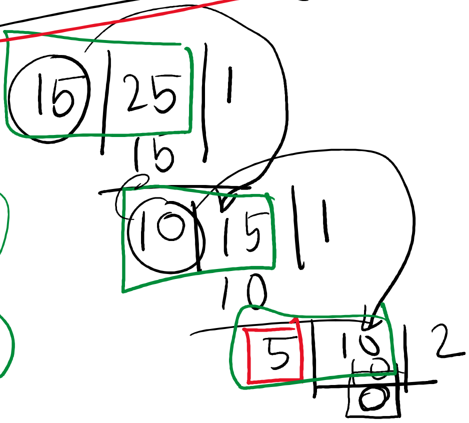
$\boxed{gcd(a,b) = gcd(b, a\%b)}$ $\boxed{gcd(a,b) = gcd(b, a-b)}$

$O(\log_2(max(a,b)))$

$(15,25) = (10,15)$

$(10,15) = (5,10)$

$(5,10) = (0,5)$



```
int getHCD(a, b) {
  if(b==0) return a;
  return getHCD(b, a%b);
}
```