GCD

Euclid's Algorithm

- `gcd( a , b ) = gcd( b , a%b )`

  ### Lemma

  If a > 0 and b > 0 :

  - `gcd( a , b ) = gcd( a - b , b )` [a > b]
  - `gcd( a , b ) = gcd( a , b - a )` [b > a]

Properties

- `gcd( a , b ) * lcm( a, b ) = a * b`

- The smallest positive integer `d` which can be written in the form

  `d = a*p + b*q`

  where `p` and `q` are integers is `gcd( a, b )`

  The expression is called **Bézout's identity**

- If `m` is a *non-negative* integer

  `gcd( m*a , m*b ) = m * gcd( a , b )`

- If `m` is *any* integer

  `gcd( a+m*b , b ) = gcd( a , b )`

- If `m` is a positive common divisor of `a` and `b`

  `gcd( a/m , b/m ) = gcd( a , b ) / m`

  $\frac{a}{m}$

  ```
  $\frac{a}{m}$
  ```

  $\frac{a/m}{b/m}$

  $\sum_{d|n} i^2$

  $\sum_{d|n} i^2$