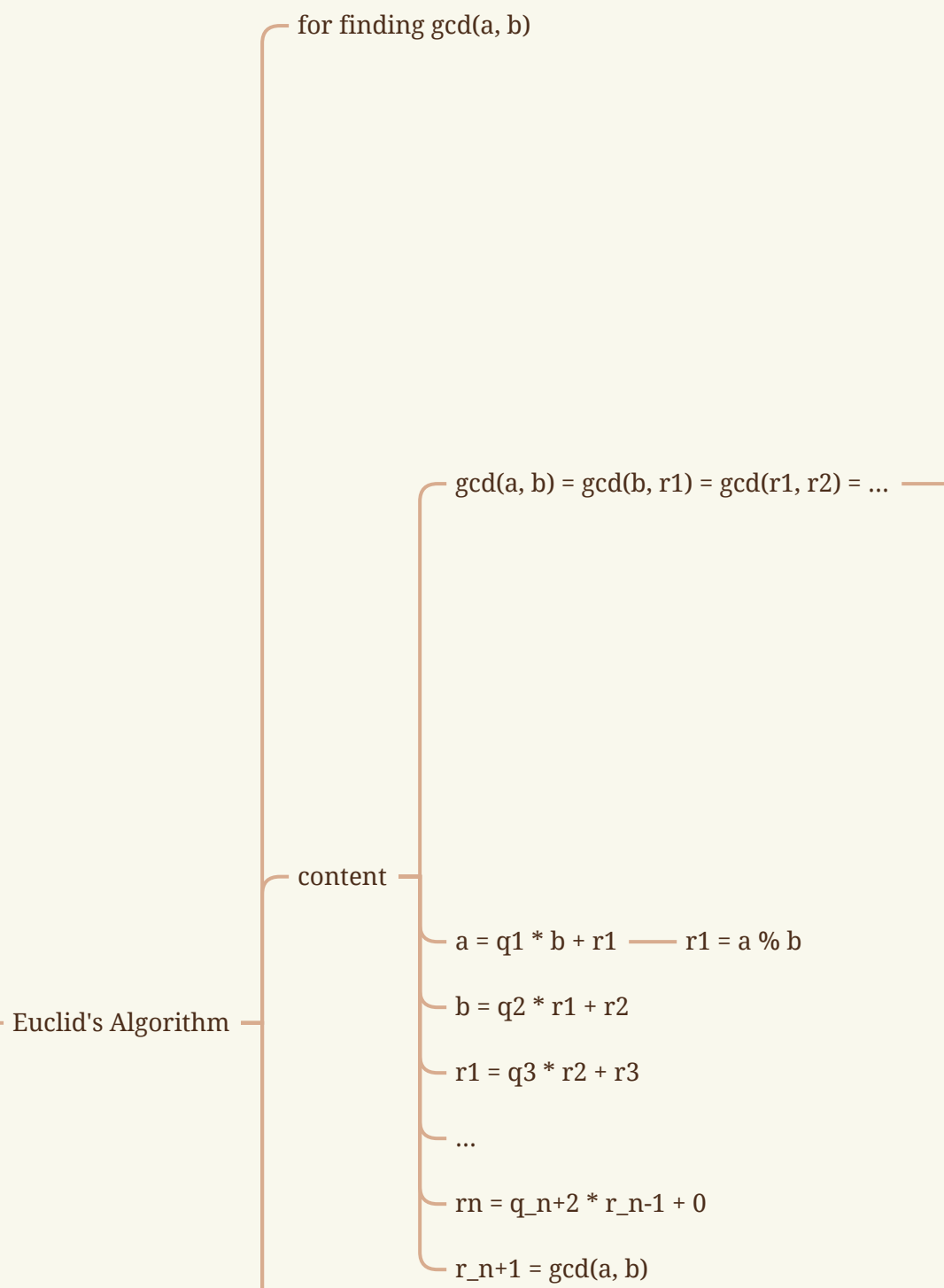
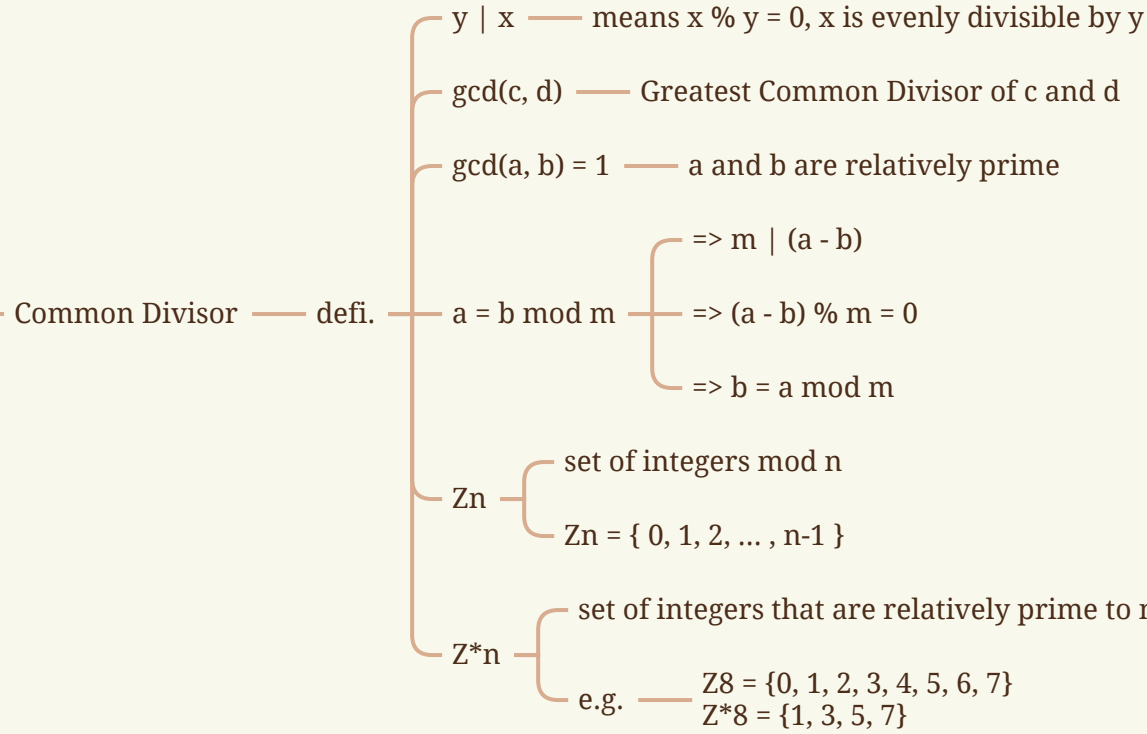


math prerequisites



Proof:

Shows that $\text{gcd}(a, b) = \text{gcd}(b, a - b)$

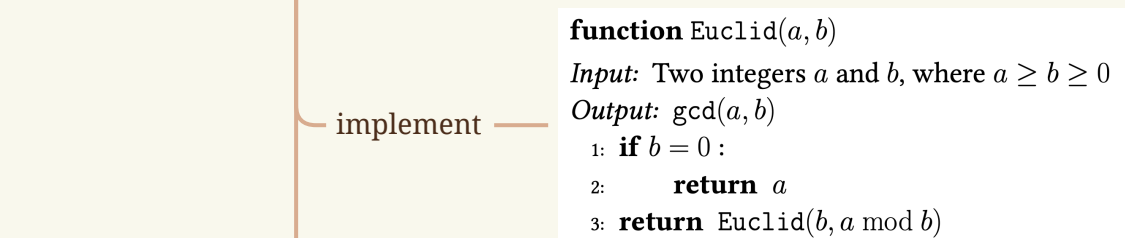
$a = x \cdot \text{gcd}(a, b)$
 $b = y \cdot \text{gcd}(a, b)$

$a - b = x \cdot \text{gcd}(a, b) - y \cdot \text{gcd}(a, b) = c$
 $= (x - y) \cdot \text{gcd}(a, b) = c$

$\text{gcd}(a, b)$ divides b and c , $\text{gcd}(a, b) \leq \text{gcd}(b, c)$
 $\text{gcd}(b, c)$ divides b and c , $\text{gcd}(b, c) \leq \text{gcd}(a, b)$ — $\text{gcd}(a, b) = \text{gcd}(b, a - b)$

$\text{gcd}(a, b) = \text{gcd}(b, a - b) = \text{gcd}(b, a - 2b) = \dots = \text{gcd}(b, a - kb)$
 $= \text{gcd}(b, R) = \text{gcd}(b, a \bmod b)$.

where $b = aR + R$.



$\text{gcd}(a, b, a \bmod b) : d = bx' + (a \bmod b)g'$
 $= bx' + (a - \lfloor \frac{a}{b} \rfloor b)g'$
 $= bx' + a(\frac{a}{b})g' - \lfloor \frac{a}{b} \rfloor b^2g'$
 $= ax + by$

where $x = g'$, $y = x' - \lfloor \frac{a}{b} \rfloor g'$

when input $a = 25, N = 11$

- On the first call, $a = 25$ and $b = 11$. Since $b \neq 0$, the function will make a recursive call with b and $a \bmod b$, which is 11 and 3 respectively.
- On the second call, $a = 11$ and $b = 3$. Again, $b \neq 0$, so the function will make another recursive call with b and $a \bmod b$, which is 3 and 2 respectively.
- On the third call, $a = 3$ and $b = 2$. The function will make yet another recursive call with 2 and 1.
- On the fourth call, $a = 2$ and $b = 1$. Now, with another recursive call, the values become $a = 1$ and $b = 0$.
- On this fifth call with $b = 0$, the function returns $(1, 0, 1)$ as $\text{gcd}(1, 0) = 1$.

calculation example:

From the fourth call:
 $(x', y', d) = (1, 0, 1)$
Returning:
 $(y', x' - \lfloor \frac{a}{b} \rfloor y') = (0, 1 - \lfloor \frac{2}{1} \rfloor 0) = (0, 1)$

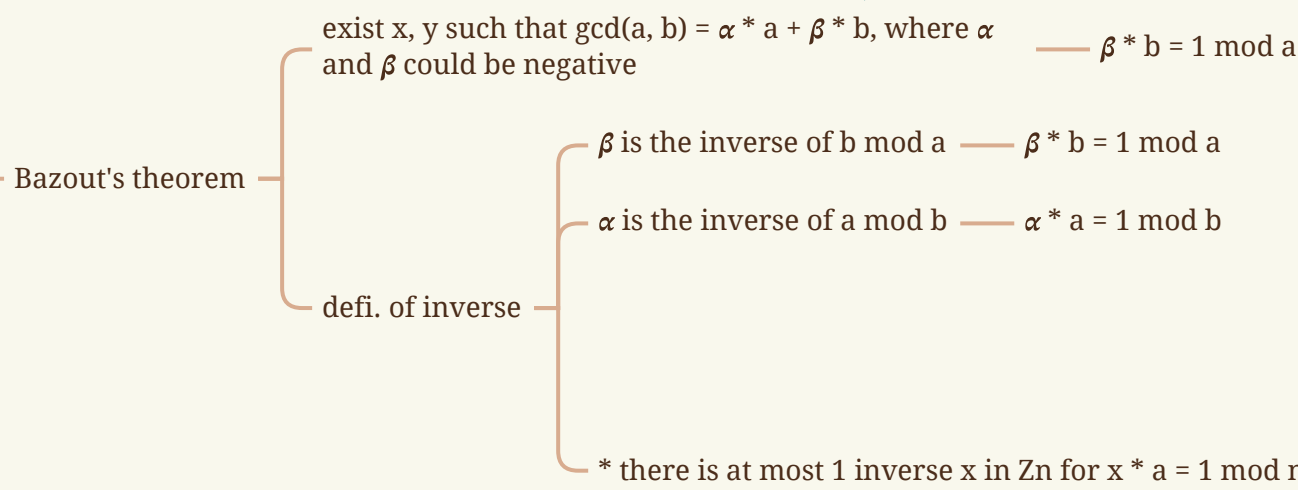
From the third call:
 $(x', y', d) = (0, 1, 1)$
Returning:
 $(y', x' - \lfloor \frac{3}{2} \rfloor y') = (1, 0 - 1) = (1, -1)$

From the second call:
 $(x', y', d) = (1, -1, 1)$
Returning:
 $(y', x' - \lfloor \frac{11}{3} \rfloor y') = (-1, 1 - (-3)) = (-1, 4)$

From the first call:
 $(x', y', d) = (-1, 4, 1)$
Returning:
 $(y', x' - \lfloor \frac{25}{11} \rfloor y') = (4, -1 - 2) = (4, -3)$

So, for $a = 25$ and $b = 11$, the values are:
 $x = 4, y = -3$, and $d = \text{gcd}(25, 11) = 1$

Thus, the result is $x = 4, y = -3$, and $d = 1$.

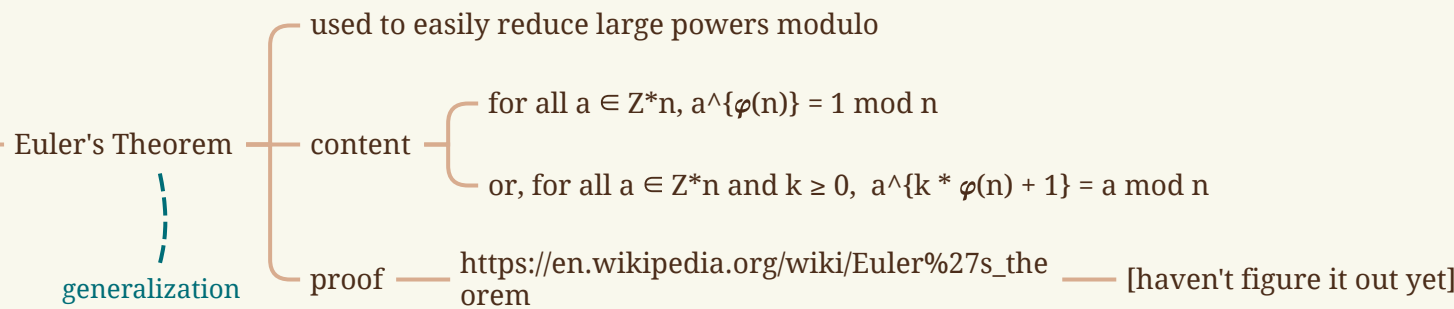
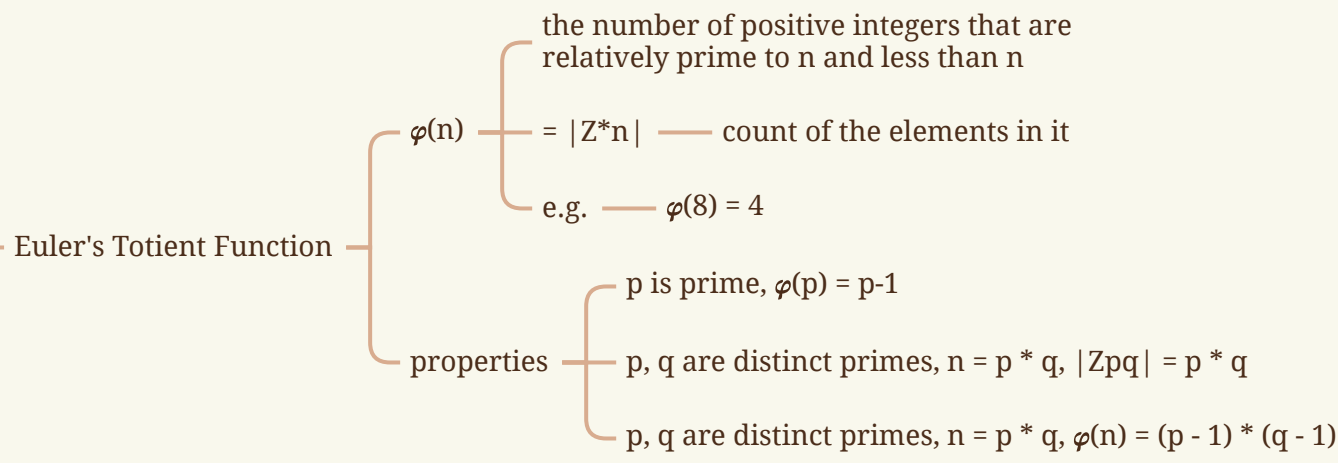


no inverse case — $2x \not\equiv 1 \pmod{4} \quad \forall x \dots$

$a = 2, n = 4$

when inverse exists? — $ax \equiv 1 \pmod{N} \Leftrightarrow N \text{ divide } ax - 1$
 $\Leftrightarrow ax - 1 = -yN \text{ for } -y \Leftrightarrow ax + Ny \equiv 1 \Leftrightarrow \text{gcd}(N, a) = 1$

that is to say, when a and N are co-prime, the inverse exists



generalization

