Euclidean Algorithm

$a = bq + r$, $a, b, q, r \in \mathbb{Z}$ $\Rightarrow$ $\gcd(a,b) = \gcd(b,r)$

proof. If $d \mid a$ and $d \mid b$, then $d \mid a - bq = r$

If $d \mid b$ and $d \mid r = a - bq$, then $d \mid a = r + bq$

q_1	$a \geq$	b	
	bq		
	r_1	b	q_2
		$r_1 q_2$	
q_3	r_1	r_3	
	$r_3 q_3$		
	r_4	$\vdots$	
	r_n	0	

$\gcd(a,b)$
$\|$
$\gcd(r_1,b)$
$\|$
$\gcd(r_1,r_3)$
$\|$
$\vdots$
$\gcd(r_n, 0) = r_n$.

The number of divisions required is $O(\log b)$

EX.

1	662	414	
	414		
	248	414	1
		248	
1	248	166	
	166		
	82	166	2
		164	
41	82	2	
	82		
	0	2	

$\gcd(662, 414)$
$\|$
$\gcd(248, 414)$
$\|$
$\gcd(248, 166)$
$\|$
$\gcd(82, 166)$
$\|$
$\gcd(82, 2)$
$\|$
$\gcd(0, 2) = 2$.

Extended Euclidean Algorithm : finds $\gcd(b,n)$ and x_0, y_0 such that $b x_0 + n y_0 = \gcd(b,n)$

```
def xgcd(b, n):
    x0, x1, y0, y1 = 1, 0, 0, 1
    while n:
        q, b, n = b//n, n, b%n
        x0, x1 = x1, x0 - q * x1
        y0, y1 = y1, y0 - q * y1
    return b, x0, y0
```

EX. $B = 662$ $N = 414$

q	b	n	x_0	x_1	y_0	y_1
	662	414	1	0	0	1
1	414	248	0	1	1	-1
1	248	166	1	-1	-1	2
1	166	82	-1	2	2	-3
2	82	2	2	-5	-3	8
41	2	0	-5	207	8	-331

returns $(2, -5, 8)$

Remark) if $\begin{cases} b = x_0 B + y_0 N \\ n = x_1 B + y_1 N \end{cases}$ in a loop, then $\begin{cases} b = x_0 B + y_0 N \\ n = x_1 B + y_1 N \end{cases}$ also holds in the next iteration. This is true initially, so is true all the way.

Application : Modular inverse.

Assumption : $\gcd(b,n)=1$.

Objective : Find b^{-1} so that $b \cdot b^{-1} \equiv 1 \pmod{n}$

Method: Run $xgcd(b,n)$ then x_0 is the modular inverse of b mod n.

proof. If $\gcd(b,n)=1$, then $xgcd(b,n)$ returns $1, x_0, y_0$ such that $b x_0 + n y_0 = 1$

Thus $b x_0 \equiv 1 \pmod{n}$

Ex. From $\gcd(662, 414)=2$, we find that $\gcd\left(\frac{662}{2}, \frac{414}{2}\right)=1$, that is, $\gcd(331, 207)=1$.

$xgcd(331, 207)$ returns $(1, -5, 8)$

(Notice that $-5, 8$ are also obtained from $xgcd(662, 414)$)

$x_0 = -5$. Thus, the modular inverse of 331 mod 207 is -5 mod 207. ($= 202$ mod 207)

The number of operations in the xgcd is also $O(\log \min(b,n))$

Mathematical Induction

To prove that $P(n)$ is true for all positive integers n,

Basis Step $P(1)$ is true

Inductive step $P(k) \to P(k+1)$ is true for all positive integers k.

$$\left(P(1) \wedge \forall k\left(P(k) \to P(k+1)\right)\right) \to \forall n P(n)$$

Ex6. $2^n < n!$ for every integer $n \geq 4$

$P(4)$: $2^4 < 4!$ is true.

if $P(k)$ is true for some positive integer, $k \geq 4$

$2^k < k!$

Then $2^k \cdot 2 < k! \cdot 2 < k!(k+1) = (k+1)!$

So $2^{k+1} < (k+1)!$ and $P(k+1)$ is true.

Hence, by mathematical induction, $2^n < n!$ is true for all positive integers $n \geq 4$.

Strong Induction

Basis step $P(1)$ is true

Inductive step $P(1) \wedge \cdots \wedge P(k) \to P(k+1)$ for all $k \geq 1$

$$\left(P(1) \wedge \forall k\left(\bigwedge_{1 \leq i \leq k} P(i) \to P(k+1)\right)\right) \to \forall n P(n)$$