- Extended Euclidean Algorithm -

$gcd(a, b) = t.a + s.b$ or $ax + by$ $\qquad a = b.q + r$

$gcd(252, 198) = 18$

$252 = 198.1 + 54$
$198 = 54.3 + 36$
$54 = 36.1 + 18$
$36 = 18.2 + 0$
$18 = 0 \dots$

r	a	b	q
$54 = 252 - 198.1$			
$36 = 198 - 54.3$			
$18 = 54 - 36.1$			
~~$0 = 36 - 18.2$~~			

$18 = 54 - 1.36$
$18 = 54 - 1.(198 - 54.3)$
$18 = 4.54 - 198.1$
$(252 - 198.1)$
$18 = 4.252 - 5.198$

$gcd(252, 198)$	①	$18 = 252x + 198y$
$gcd(198, 54)$	②	$18 = 198x + 54y$
$gcd(54, 36)$		$18 = 54x + 36y$
$gcd(36, 18)$		$18 = 36x + 18y$
$gcd(18, 0)$	$\Longrightarrow$	$18 = 18x + 0y$

base solution: $(1, 0)$

✱ When we know the answer of ② How to solve ① $\longrightarrow g = ax + by$

② $g = a x_1 + b_1 y_1$ $\qquad 252 = 198.1 + 54$, $a = b.q + r$, $54 = b_1$

$g = b x_1 + b_1 y_1$ $\qquad b_1 = a \bmod b$ $\qquad 252 \bmod 198$

$g = b x_1 + (a \bmod b) y_1$ $\qquad a \bmod b = a - \lfloor \frac{a}{b} \rfloor * b$

$g = b x_1 + \left(a - \lfloor \frac{a}{b} \rfloor . b\right) y_1$

$g = b x_1 + a y_1 - b y_1 \lfloor \frac{a}{b} \rfloor$

$g = a \underbrace{y_1}_{x} + b \underbrace{\left(x_1 - y_1 \lfloor \frac{a}{b} \rfloor\right)}_{y}$

$\begin{cases} x = y_1 & \checkmark \\ y = x_1 - y_1 \lfloor \frac{a}{b} \rfloor & \checkmark \end{cases}$

```
int extendedEuclidean(int a, int b, int &x, int &y)
{
    if (b == 0) {
        x = 1;
        y = 0;
        return a;
    }
    int x1, y1;
    int d = extendedEuclidean(b, a%b, x1, y1);
    x = y1;
    y = x1 - y1 * (a/b);
    return d;
}
```