

2

(1) 次の a, b の組に対し、その最大公約数 $d = \gcd(a, b)$ を Euclid の互除法で求めよ。
 また、拡張互除法により $ax + by = d$ となる整数 x, y の組を一組見付けよ。

(a) $(a, b) = (156, 91)$

i	$r_{i-2} = r_{i-1} \times q_i + r_i$	q_i	r_i	x_i	y_i	$ax_i + by_i$
-1	---	-	156	1	0	
0	---	-	91	0	1	
1	$156 = 91 \times \quad +$					
2	$91 = \quad \times \quad +$					
3	$\quad = \quad \times \quad +$					

(b) $(a, b) = (34, 21)$

i	$r_{i-2} = r_{i-1} \times q_i + r_i$	q_i	r_i	x_i	y_i	$ax_i + by_i$
-1	---	-	34	1	0	
0	---	-	21	0	1	
1	$34 = 21 \times \quad +$					
2	$21 = \quad \times \quad +$					
3	$\quad = \quad \times \quad +$					

(2) $a, b \in \mathbb{Z}$ に対し、連立合同式

$$(*) \quad \begin{cases} x \equiv a \pmod{27} \\ x \equiv b \pmod{19} \end{cases}$$

の解 x を一つ求めたい。

(a) Euclid の互除法により $\gcd(27, 19) = 1$ であることを示し、 $27s + 19t = 1$ となる整数 s, t の組を一組見付けよ。

(b) 上の解を観察して、

(i) 連立合同式 $\begin{cases} x \equiv 1 \pmod{27} \\ x \equiv 0 \pmod{19} \end{cases}$ の解 x を一つ見出せ。

(ii) 連立合同式 $\begin{cases} x \equiv 0 \pmod{27} \\ x \equiv 1 \pmod{19} \end{cases}$ の解 x を一つ見出せ。

(c) $a, b \in \mathbb{Z}$ に対し、連立合同式 $(*)$ の解 x を (一つ) 求めよ。