[1]

```python
from prime import *
```

[3]

```python
A = [166,984,1124,1281,1338,2021,202103,20210301,1301,1601]
B = [332,1038,1213,2019,2018,313,1601,1231,1373,1681]
i = 1
for a,b in zip(A,B):
    ans = bezout(a,b)
    print(f'({i})   a = {a} , b = {b} , s = {ans[0]} , t = {ans[1]}')
    i += 1
```

```
(1)   a = 166 , b = 332 , s = 1 , t = 0
(2)   a = 984 , b = 1038 , s = -77 , t = 73
(3)   a = 1124 , b = 1213 , s = -368 , t = 341
(4)   a = 1281 , b = 2019 , s = -145 , t = 92
(5)   a = 1338 , b = 2018 , s = -92 , t = 61
(6)   a = 2021 , b = 313 , s = -116 , t = 749
(7)   a = 202103 , b = 1601 , s = -637 , t = 80412
(8)   a = 20210301 , b = 1231 , s = -570 , t = 9358141
(9)   a = 1301 , b = 1373 , s = 553 , t = -524
(10)   a = 1601 , b = 1681 , s = 21 , t = -20
```

20210308 数基

519021910025 钟裔哲

定理1.3.12 设$a_1,\dots,a_n$，c为整数，若$(a_i,c)=1$，$1\le i\le n$，则 ~~$(a_1,\dots,a$~~ $(a_1\cdots a_n,c)=1$.

当$n=2$，设$(a_1,c)=1$，$(a_2,c)=1$ $\Rightarrow \begin{cases} s_1a_1+t_1c=1 \\ s_2a_2+t_2c=1. \end{cases}$

$\Rightarrow (s_1s_2)(a_1a_2)=(1-t_1c)(1-t_2c)=1-(t_1+t_2-t_1t_2c)\cdot c$

$\Rightarrow (s_1s_2)\cdot(a_1a_2)+(t_1+t_2-t_1t_2c)\cdot c=1$.

$\Rightarrow (a_1a_2,c)=1$.

设$n-1$时，命题成立.

当n时，$(a_1a_2\cdots a_{n-1},c)=1$. 由$(a_n,c)=1$.

$\Rightarrow (a_1a_2\cdots a_n,c)=((a_1\cdots a_{n-1})a_n,c)=1$. 证毕.

定理1.3.14

设$a_1,\dots,a_n$为整数，$a_1\ne0$，$(a_1,a_2)=d_2$，$(d_2,a_3)=d_3$，…

$(d_{n-1},a_n)=d_n$.

则$(a_1,\dots,a_n)=d_n$ 则$\exists s_1,\dots,s_n$，使$\sum_{i=1}^{n}a_is_i=d_n$.

当$n=2$时，$(a_1,a_2)=2$，且$\exists s_1,s_2$，$s_1a_1+s_2a_2=d_2$.

设当$n-1$时成立，则$(a_1,\dots,a_{n-1})=d_{n-1}$，$s_1a_1+\dots+s_{n-1}a_{n-1}=d_{n-1}$

对于n，令$e=(a_1,\dots,a_n)$，则$e|a_1,\dots,e|a_n \Rightarrow e|d_{n-1}, e|a_n \Rightarrow e|(a_n,d_{n-1})=d_n$

$\Rightarrow e|d_n \Rightarrow e\le d_n$.

由$(d_{n-1},a_n)=d_n \Rightarrow d_n|d_{n-1}, d_n|a_n \Rightarrow d_n|a_1,\dots,d_n|a_n$

$\Rightarrow d_n$是公因数 $\Rightarrow d_n|e \Rightarrow d_n=e$. 证毕.

定理1.3.15 最大公因数的充要条件:

(1) $d|a_1, \dots, d|a_n$

(2) 若 e 是公因数，则 $e|d$ (1) 显然成立.

必要性：设 d 为最大公因数，则：$s_1a_1+\dots+s_na_n=d$

若 e 为公因数，则 $e|a_i \Rightarrow e|\sum_{i=1}^{n} s_ia_i \Rightarrow e|d$.

充分性：由(1)知，d 为公因数.

由(2)知，$\forall e$ 且 e 为公因数，$e\le d \Rightarrow d$ 为 gcd.

证：$(a,b)=1 \iff ax+by=1$ 有解.

"$\Longrightarrow$" 当 $(a,b)=1$，由 Bezout 等式，$sa+tb=1$. 令 $x=s$，$y=t$，得证.

"$\Longleftarrow$" 当 $ax+by=1$ 有解，设 $x=s$，$y=t$，则 $sa+tb=1$

设 $d=(a,b) \Rightarrow d|a, d|b \Rightarrow d|(sa+tb)=1 \Rightarrow d|1 \Rightarrow d=1$

$\Rightarrow a,b$ 互素.