HW3 - GCD and Extended GCD

(정수론)

18013195

정보보호학과

이풍원

1) gcd(a, b): it returns the gcd value d of a and b.

```
1  def gcd(a,b):
2
3      if b==0:
4          return a
5      else:
6          return gcd(b,a%b)
7
```

그림 1) gcd(a,b) 함수

3~4 행: if 문으로 b 가 0 이되면 a 를 리턴한다.

5~6 행: 위의 조건문이 만족하지 않으면 실행하는데 gcd 를 호출하고 첫번째 인자에는 b 가 들어가고 두번째 인자에는 a%b 가 들어가게 되는데 a>b 를 가정하고 a 에 b 로 나눠 나머지 값이 항상 b 값 보다 낮아 두 번째 인자에 들어가게 되고 원래 b 값이 첫번째 인자에 들어가게 되는데 입력 값이 a<b 로 들어와도 a%b 나머지 연산을 하여 굳이 a,b 값을 swap 하지 않아도 된다.

이렇게 반복하게 되면 b 값이 0 이되고 3~4 행 이 만족하게 되며 gcd(a,0)=a 로 a 값을 리턴한다.

2) extended_gcd(a, b): it returns the gcd value d, two costants s and t which satisfy d = s*a + t*b.

```
8   def extended_gcd(a,b):
9       if b==0:
10          st=[[1,0],[0,1]]
11          for i in range(len(q)):
12              st.append([st[i][0]-st[i+1][0]*q[i], st[i][1]-st[i+1][1]*q[i]] )
13          return st[-2][0],st[-2][1]
14      else:
15          q.append(a//b)
16          return extended_gcd(b,a%b)
```

그림 2) extended_gcd(a,b) 함수

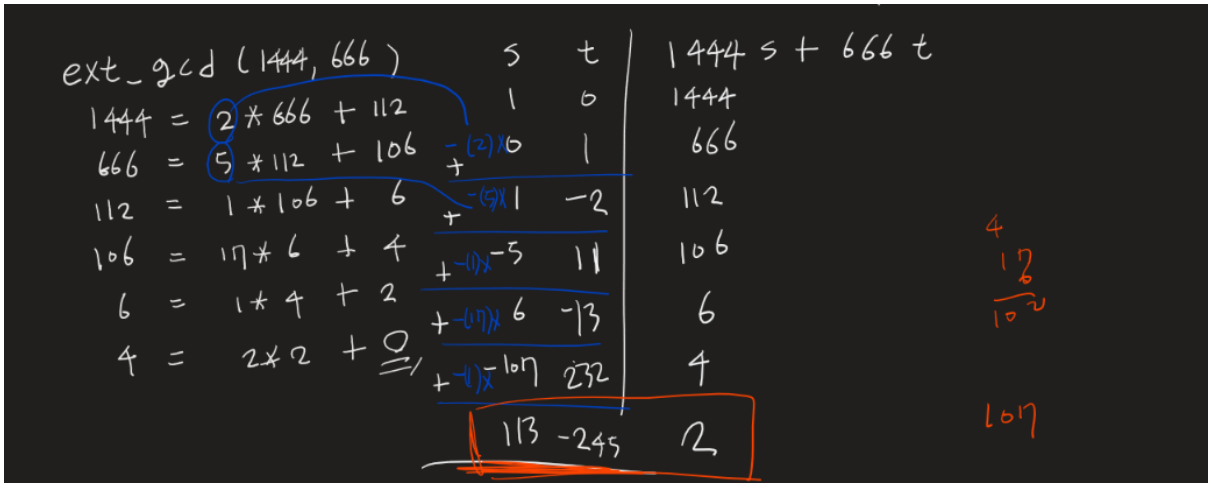
위의 gcd 함수와 똑 같은 로직으로 반복된다.

9 행: b 가 0 이면 실행한다.

10 행: st 를 list 로 선언해 초기값 [1,0],[0,1]으로 설정한다.

11 행: q 는 리스트인데 q 의 길이만큼 반복한다.

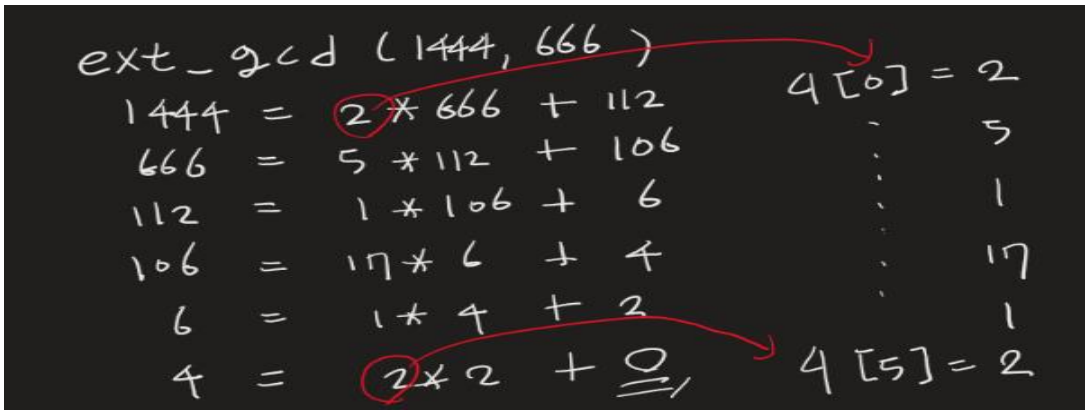
12 행: st 리스트의 원소를 추가하면서 유클리드 확장 공식을 적용하여 연산해 값을 저장한다.



위의 그림은 15 행에서 구한 몫들을 이용해 만든 s,t 값을 구하는 방법이고 11~12 행의 로직과 같다.

13 행: a 값은 자동으로 gcd 값이 저장되고, s,t 값 마지막에서 2 번째 값을 각각 리턴 한다.

14~16 행: 위의 조건이 만족하지 않으면 실행되고 q 에 append 하여 a 에 b 를 나눈 몫을 넣어 추가한다 그리고 extended_gcd 를 호출하며 위의 gcd 함수와 같이 동작한다.



위에서 설명한 a 에 b 를 나눈 몫을 q 리스트에 담은것이다

3) main 및 출력

```python
g=[[45,75],[666,1414],[102,222],[2**101+16,2**202+8]]
for i in g:
    print("gcd(%d,%d)= %d "%(i[0],i[1],gcd(i[0],i[1])))


q=[]
a_e=[[45,75],[666,1414],[102,222],[2**101+16,2**202+8]]
for i in a_e:
    s,t=extended_gcd(i[0],i[1])
    print("extended_gcd(%d,%d)= %d s= %d t= %d"%(i[0],i[1],s*i[0]+i[1]*t,s,t))
    q=[]

```

```
PS C:\Users\vnddn\OneDrive\바탕 화면\js> & C:/Users/vnddn/AppData/Local/Programs/Python/Python39/python.exe "c:/Users/vnddn/OneDrive/바탕 화면/js/asd.py"
gcd(45,75)= 15
gcd(666,1414)= 2
gcd(102,222)= 6
gcd(2535301200456458802993406410768,642775217703596110216784836936465041008881197513117134120551 2)= 24
extended_gcd(45,75)= 15 s= 2 t= -1
extended_gcd(666,1414)= 2 s= -138 t= 65
extended_gcd(102,222)= 6 s= -13 t= 6
extended_gcd(2535301200456458802993406410768,642775217703596110216784836936465041008881197513117134120551 2)= 24 s= 12173773062568108148045167366197880614254963637818238455189
t= -4801706819046323490517815 1719
```

그림 3) main 및 실행 결과

과제에 예시로 나온 값을 넣어 확인한 값이다.

4) 소스 코드(main 제외 함수)

```
def gcd(a,b):

    if b==0:
        return a
    else:
        return gcd(b,a%b)

def extended_gcd(a,b):
    if b==0:
        st=[[1,0],[0,1]]
        for i in range(len(q)):
            st.append([st[i][0]-st[i+1][0]*q[i], st[i][1]-st[i+1][1]*q[i]] )
        return st[-2][0],st[-2][1]
    else:
        q.append(a//b)
        return extended_gcd(b,a%b)
```