HW 2 Double Spend Problem

Assume result of attcking between different time intervals are independent, we can view the attacking process as a Markov Process. We model the expected gain (expected reward - cost) as $E_{m,n}$, where m is the length of the main (being attacked) chain, and n is the length of the attacker's chain.

We define the following expected gains:

1. If $m = k$, $E_{m,n} = 0$, the transaction is confirmed, failed attack leads to no gains.
2. If $n = k$, $E_{m,n} = 100$, the attacker's chain first get confirmed with k lengths.
3. For other cases, we have $E_{m,n} = 0.49 \times E_{m+1,n} + 0.51 \times E_{m,n+1} - 1$, indicating the attacks fails for 49% probability, where the main chain grows by one and succeeds for 51% probability, where the attacker's chain grows by one. -1 indicates the cost of an extra unit of time using the computation power.

Our goal is to find a k where $E_{1,0} > 0$, i.e. starting from the initial state, the expected gain of attacks is larger than the costs.

We write a program to calculate the whole $E_{m,n}$ table. We find that $k = 29$ gives the first negative result in $E_{1,0}$

```
K = 29
E_table = []
for i in range(K+1):
    E_table.append([0 for j in range(K+1)])

for i in range(K+1):
    E_table[i][K] = 100

for i in range(K-1,-1,-1):
    for j in range(K-1,-1,-1):
        E_table[i][j] = - 1 + 0.51 * E_table[i][j+1] +\
                                    0.49 * E_table[i+1][j]

for i in range(K):
    print(29-i, E_table[1+i][i])
```

The expected gain for every $K = 29$ is $-0.3282W$