tests

November 20, 2020

[76]:
```
import os
from datetime import datetime
import random
from math import gcd
```

[77]:
```
class TimeMachineCore:

        n = 3
        m = 2
        c = 1


        def __init__(self, seed):
                self.year = seed

        def next(self):
                self.year = (self.year * self.m + self.c) % self.n
                return self.year
```

[78]:
```
a = datetime.now()
a
```

[78]:
```
datetime.datetime(2020, 11, 20, 20, 6, 26, 982748)
```

[79]:
```
date_str = a.strftime('%Y%m%d')
date_str
```

[79]:
```
'20201120'
```

[80]:
```
rand = random.getrandbits(128)
rand
```

[80]:
```
217082759444782165305237964512445010129
```

[81]:
```
seed = int(date_str) <<1337
seed
```

[81]:
```
606009805389553370009939258064625118151880128663196435957885090768431361879203507897873616848501659526834297496887984387968083492228443811042357426136588145698323903255057440412659639497160666751453529971240671742923851670720115306000550380714039828098359806220183523127212516860483148439611591941335463736426973863988707535902170024623185015543250408959937601749347853389042274422507156692591863816998250086 40
```

[82]:
```
seed = seed % rand
seed
```

[82]:
```
140761934669708764024237938189656479 30
```

[83]:
```
gen = TimeMachineCore(seed)
gen
```

[83]:
```
<__main__.TimeMachineCore at 0x7f57c036b1f0>
```

[84]:
```
gen.next()
```

[84]:
```
0
```

[85]:
```
gen.next()
```

[85]:
```
1
```

[14]:
```
import requests
```

[42]:
```
CONTAINER = "http://docker.hackthebox.eu:32122"
```

[39]:
```
#CONTAINER = "http://127.0.0.1:8080"
```

[46]:
```
def predict_year(year: int):
    payload = {'year': year}
    r = requests.post(CONTAINER + "/predict_year", json=payload)
    return r.json()
```

[47]:
```
predict_year(123)
```

[47]:
```
{'fail': 'wrong year'}
```

[48]:
```
def next_year():
    r = requests.get(CONTAINER + "/next_year")
    return r.json()['year']
```

[49]:
```
next_year()
```

[49]:
```
'2044452719'
```

[50]:
```
def jump_to_2020(seed: int):
    payload = {'seed': seed}
    r = requests.post(CONTAINER + "/travelTo2020", json=payload)
    return r.json()
```

[86]:
```
jump_to_2020(0)
```

[86]:
```
{'error': 'What?? This is not 2020. It\\s 0!'}
```

[54]:
```
%%timeit
next_year()
```

```
73.2 ms ± 896 µs per loop (mean ± std. dev. of 7 runs, 10 loops each)
```

[55]:
```
%%timeit
jump_to_2020(0)
```

```
1 s ± 62.4 ms per loop (mean ± std. dev. of 7 runs, 1 loop each)
```

average ping (round-trip time) is 27.5ms

–> execution takes around 50 ms

–> hops is at least 20

[90]:
```
jump_to_2020(1)
```

[90]:
```
{'error': 'What?? This is not 2020. It\\s 430046689!'}
```

jump_to_2020 seems deterministic... at least

[95]:
```
def seed_to_year(seed: int):
    error = jump_to_2020(seed)['error']
    year = error.split(' ')[-1][:-1]
    return int(year)
```

[96]:
```
seed_to_year(1)
```

[96]:
```
430046689
```

[104]:
```
for seed in range(20):
    print("seed=%d year=%d" % (seed, seed_to_year(seed)))
```

```
seed=0 year=0
seed=1 year=430046689
seed=2 year=860093378
seed=3 year=1290140067
seed=4 year=1720186756
seed=5 year=2749798
seed=6 year=432796487
```

```
seed=7 year=862843176
seed=8 year=1292889865
seed=9 year=1722936554
seed=10 year=5499596
seed=11 year=435546285
seed=12 year=865592974
seed=13 year=1295639663
seed=14 year=1725686352
seed=15 year=8249394
seed=16 year=438296083
seed=17 year=868342772
seed=18 year=1298389461
seed=19 year=1728436150
```

[105]:
```
seeds = []
years = []

for seed in range(100):
    year = seed_to_year(seed)
    print("seed=%d year=%d" % (seed, year))
    seeds.append(seed)
    years.append(year)
```

```
seed=0 year=0
seed=1 year=430046689
seed=2 year=860093378
seed=3 year=1290140067
seed=4 year=1720186756
seed=5 year=2749798
seed=6 year=432796487
seed=7 year=862843176
seed=8 year=1292889865
seed=9 year=1722936554
seed=10 year=5499596
seed=11 year=435546285
seed=12 year=865592974
seed=13 year=1295639663
seed=14 year=1725686352
seed=15 year=8249394
seed=16 year=438296083
seed=17 year=868342772
seed=18 year=1298389461
seed=19 year=1728436150
seed=20 year=10999192
seed=21 year=441045881
seed=22 year=871092570
seed=23 year=1301139259
seed=24 year=1731185948
```

```
seed=25 year=13748990
seed=26 year=443795679
seed=27 year=873842368
seed=28 year=1303889057
seed=29 year=1733935746
seed=30 year=16498788
seed=31 year=446545477
seed=32 year=876592166
seed=33 year=1306638855
seed=34 year=1736685544
seed=35 year=19248586
seed=36 year=449295275
seed=37 year=879341964
seed=38 year=1309388653
seed=39 year=1739435342
seed=40 year=21998384
seed=41 year=452045073
seed=42 year=882091762
seed=43 year=1312138451
seed=44 year=1742185140
seed=45 year=24748182
seed=46 year=454794871
seed=47 year=884841560
seed=48 year=1314888249
seed=49 year=1744934938
seed=50 year=27497980
seed=51 year=457544669
seed=52 year=887591358
seed=53 year=1317638047
seed=54 year=1747684736
seed=55 year=30247778
seed=56 year=460294467
seed=57 year=890341156
seed=58 year=1320387845
seed=59 year=1750434534
seed=60 year=32997576
seed=61 year=463044265
seed=62 year=893090954
seed=63 year=1323137643
seed=64 year=1753184332
seed=65 year=35747374
seed=66 year=465794063
seed=67 year=895840752
seed=68 year=1325887441
seed=69 year=1755934130
seed=70 year=38497172
seed=71 year=468543861
seed=72 year=898590550
```

```
seed=73 year=1328637239
seed=74 year=1758683928
seed=75 year=41246970
seed=76 year=471293659
seed=77 year=901340348
seed=78 year=1331387037
seed=79 year=1761433726
seed=80 year=43996768
seed=81 year=474043457
seed=82 year=904090146
seed=83 year=1334136835
seed=84 year=1764183524
seed=85 year=46746566
seed=86 year=476793255
seed=87 year=906839944
seed=88 year=1336886633
seed=89 year=1766933322
seed=90 year=49496364
seed=91 year=479543053
seed=92 year=909589742
seed=93 year=1339636431
seed=94 year=1769683120
seed=95 year=52246162
seed=96 year=482292851
seed=97 year=912339540
seed=98 year=1342386229
seed=99 year=1772432918
```

[99]:
```
base_year = 430046689
```

[101]:
```
modulo_n = seeds[5] * base_year - years[5]
modulo_n
```

[101]: 2147483647

[102]:
```
seeds[5] * base_year % modulo_n == years[5]
```

[102]: True

[106]:
```
for seed, year in zip(seeds, years):
    print(seed * base_year % modulo_n == year)
```

```
True
True
True
True
True
True
```

```
True
True
True
True
True
True
True
True
True
True
True
True
True
True
True
True
True
True
True
True
True
True
True
True
True
True
True
True
True
True
True
True
True
True
True
True
True
True
True
True
True
True
True
True
True
True
True
True
```

```
True
True
True
True
True
True
True
True
True
True
True
True
True
True
True
True
True
True
True
True
True
True
True
True
True
True
True
True
True
True
True
True
True
True
True
True
True
True
True
True
True
True
True
True
True
True
```

year should be 2020, so:

`seed * 430046689 % 2147483647 == 2020`

`2147483647 = 2^31 - 1` (until 1867 it was the largest known prime number)

solved the equation using wolframalpha.com :

`solve x * 430046689 mod 2147483647 = 2020`

[107]:
```
4260992388* 430046689 % 2147483647 == 2020
```

[107]:
```
True
```

[108]:
```
jump_to_2020(4260992388)
```

[108]:
```
{'flag': 'HTB{l1n34r_c0n9ru3nc35_4nd_prn91Zz}'}
```