Problem 2- Repeated Squaring Method

March 26, 2020

[89]:
```
# Class example
a = 5
k = 596
k = str(bin(k))  # put it in binary
k_vals = k.split('b')
k_vals = k_vals[1]
print(k_vals)

n = 1234
```

```
1001010100
```

[90]:
```
# Use the repeated squaring method to calculate 652^853 mod 4847
```

[91]:
```
a = 652
k = 853
k = str(bin(k))  # put it in binary
k_vals = k.split('b')
k_vals = k_vals[1]
print(k_vals)
n = 4847
```

```
1101010101
```

[92]:
```
# ModExp(a,k,n)
def ModExp(a,k,n):
    b = 1
    A = a
    t = len(k_vals)
    if k_vals[-1]=='1':
        b = a
    i = 1
    while i < t:
        A = A**2 % n
        if k[-1-i] == '1':
            b = (A*b) % n
        print("i= " +str(i)+", a= " +str(A)+ ", b= " +str(b))
        i += 1
```

```
    return b
```

[93]:
```
print("\n652^853 mod 4847 = " + str(ModExp(a,k,n)))
```

```
i= 1, a= 3415, b= 652
i= 2, a= 343, b= 674
i= 3, a= 1321, b= 674
i= 4, a= 121, b= 4002
i= 5, a= 100, b= 4002
i= 6, a= 306, b= 3168
i= 7, a= 1543, b= 3168
i= 8, a= 972, b= 1451
i= 9, a= 4466, b= 4574

652^853 mod 4847 = 4574
```