Intro to Algorithms: Homework #1

Due on February 18 2021

Prof. Zaki

Jared Gridley

Problem 1

Problem 1.17:

```
Iterative (x, y):
    res = x
    For i in range(0, y-1):
        res = res * x
    return res
```

Repeats y-1 times → For

$O(N)$ ↑ # of multiplication

$\leftarrow O(mn)$ If x is an n-bit #, then res will be a m-bit # because $m \geq n$ (in bit length)

Total time = # of mult x mult time

$$= O(N) \times O(mn)$$

$$= O(Nmn) \cong O(n^3)$$

```
Recursive (x, y):
    if y == 0:
        return 1
    z = Recursive(x, y//2)
    if y % 2 == 0:
        return z*z
    else:
        return x·z·z
```

# of recursive calls = $O(n)$

$O(n)$ to do multiplication with large numbers

Size of z returned will increase exponentially

$$\text{Total time} = \underbrace{O(n^2)}_{\text{multiplication}} \times \underbrace{O(\log_2 n)}_{\text{recursive calls}} = O(n^2 \log_2 n)$$

Figure 1: Problem 1.17

Problem 2

Problem 1.19:

Base Case: $n=1$: $\gcd(F_2, F_1) = 1$

$\gcd(1, 1) = 1$ (because that is the only factor)

Prove true for $n \to n+1$

Assume $\gcd(F_{n+1}, F_n) = 1$

Prove $\gcd(F_{n+2}, F_{n+1}) = 1$

F_{n+2}

$F_{n+2} = F_n + F_{n+1}$

$F_{n+2} - F_{n+1} = F_n$

So then $\gcd(F_{n+2}, F_{n+1})$ becomes $\gcd(F_{n+1}, F_{n+2} - F_{n+1})$ since the larger number must come first. This makes sense because the smaller Fibonacci num in gcd will always be greater than ½ of F_{n+1} and when the gcd is carried out, this will hold for all recursive calls until 1 is hit. So therefore the $\gcd(F_{n+1}, F_n) = 1$ always.

Tinkering

$n=1$ $\gcd(1, 1) = 1$

$n=2$ $\gcd(2, 1) = 1$

$n=3$ $\gcd(3, 2) = 1$

$n=4$ $\gcd(5, 3) = 1$

$n=5$ $\gcd(8, 5) = 1$

$n=6$ $\gcd(13, 8) = 1$

Figure 2: Problem 1.19

Problem 3

Problem 1.23) Assuming that there exists a multiplicative inverse for a (modulo N.

Uniqueness

Proof by contradiction:

We will assume that the inverse is not unique, so there must exist 2 numbers that are both the multiplicative inverse. (call these i_1 and i_2)

$a i_1 \equiv 1 \mod N$ $\quad a i_2 \equiv 1 \mod N$ $\quad$ (num x inv. $\equiv 1 \mod N$)

So, if this assumption is true, then $\exists x, y \in \mathbb{Z}$

$a i_1 + Nx = 1$ $\quad a i_2 + Ny = 1$

$$a i_1 + Nx = a i_2 + Ny$$

$$a i_1 - a i_2 \equiv Ny - Nx$$

$$a i_1 - a i_2 \equiv 0 \mod N$$

$$a(i_1 - i_2) = 0 \mod N$$

We know that $a \neq 0$, so that means that:

$$i_1 \equiv i_2 \mod N$$

Therefore, they are the same value, so our assumption is incorrect, and the multiplicative inverse is unique.

Figure 3: Caption

Problem 4

Given that $x^{86} \equiv 6 \bmod 29$

$$x^{86} \equiv 6 \mod 29$$

Fermat's Little Theorum: $x^{28} \equiv 1 \mod 29$

$86 \equiv 2 \mod 29$

$28 \times 3 = 84$

$3 \text{ r } 2$

$x^{86} \equiv x^2 \mod 29$

Simpler to solve for x^2,

$x^2 \equiv 6 \mod 29$

$x^2 \equiv 6 \mod 29$

$x^2 \equiv 64 \mod 29$

29×2

$58 + 6 = 64$

$\downarrow$

$x = 8, \cancel{-8}$

So $\boxed{x = 8}$

Figure 4: Problem 4

Since negative numbers become positive when passed through a mod, we can just use the positive value.