

1.9) Sum:

$$\underline{x} \equiv x' \pmod{N}, \quad \underline{y} \equiv y' \pmod{N} \Rightarrow x+y \equiv x'+y' \pmod{N}$$

This means they will have  
the same remainder when  
divided by N

$$23 \equiv 9 \pmod{7} \rightarrow 23-9 = 14 = \frac{2}{2}N$$

Always goes back to a  
multiple of N.

$$x+y \equiv x'+y' \pmod{N} \rightarrow (x-y) - (x'-y') = cN$$

$$y \equiv y' \pmod{N} \rightarrow y-y' = aN \quad (a \text{ is a constant } \in \mathbb{Z})$$

$$x \equiv x' \pmod{N} \rightarrow x-x' = bN \quad (b \text{ is a constant } \in \mathbb{Z})$$

$$(y-y') + (x-x') = aN + bN$$

$$(y+x) - (y'+x') = (a+b)N \quad (a+b \text{ is constant } \in \mathbb{Z})$$

$$x+y \equiv x'+y' \pmod{N}$$

since  $(a+b)N$  means that the difference will be a multiple of N, then we can conclude that the remainders of the additions will be the same, and thus holds.

Multiplication:  $x \equiv x' \pmod{N}, \quad y \equiv y' \pmod{N} \Rightarrow xy \equiv x'y' \pmod{N}$

$$\left. \begin{array}{l} x-x' = aN \\ y-y' = bN \end{array} \right\} \rightarrow (x-x')(y-y') = abN^2 \rightarrow \text{need to get } xy - x'y'$$

$$(x-x')(y-y') = abN^2$$

$$\begin{aligned} x &= x' + aN \\ y &= y' + bN \end{aligned}$$

$$xy - xy' - x'y + x'y' = abN^2$$

$$xy - (xy' + x'y) + x'y' = abN^2$$

$$xy - (y'(x' + aN) + x'(y' + bN)) + x'y' = abN^2$$

Need to get rid of all the remaining x and y because we already have the xy term.

$$xy - (y'x' + y'aN + x'y' + x'bN) + x'y' = abN^2$$

$$xy - x'y' - (aNy' + bNx') = abN^2$$

$$xy - x'y' = abN^2 + (ay' + bx')N$$

$$xy - x'y' = \underbrace{(abN + ay' + bx')}_{N}$$

This shows us that the difference will be a multiple of N, so the two remainders must be the same.

$$\Rightarrow xy \equiv x'y' \pmod{N}$$

1.1) Is  $4^{1536} - 9^{4824}$  divisible by 35?

Try to find a simpler number for N than 35.

$\begin{array}{c} 35 \\ \swarrow \quad \nwarrow \\ 7 \quad 5 \end{array}$  5, 7 are both prime, so they will be the smallest factors of 35 to help simplify the problem.  
IF  $4^{1536}$  and  $9^{4824}$  are both multiples of 5 and 7, then their difference will be a multiple of 35 (as shown by previous problem)

Divisible by 7:

$$4^{1536} \mod 7$$

$$4^2 = 16 \rightarrow 1 \mod 7$$

$$\frac{4^3 = 64}{r_1} \rightarrow 1^{512}$$

$$4^{1536} = 1 \mod 7$$

$$9^{4824} \mod 7$$

$$7 \times 9 = 63 \quad 9^2 = 81 = 4 \mod 7$$

$$7 \times 10 = 70$$

$$\begin{aligned} &7 \times 11 = 77 \\ &\text{If we use this one, then} \\ &\text{we can reuse the work} \\ &\text{for checking } 4^{1536} \end{aligned}$$

$$\begin{aligned} &7 \times 12 = 84 \\ &= (4^3)^{804} \mod 7 \\ &= 1^{804} = 1 \mod 7 \end{aligned}$$

$$\begin{aligned} 4^{1536} - 9^{4824} &= (1 \mod 7) - (1 \mod 7) = 1-1 \mod 7 \\ &= 0 \mod 7 \end{aligned}$$

So difference is divisible by 7

Divisible by 5:

$$4 \times 3 = 12$$

$$4 \times 4 = 16$$

$$4 \times 5 = 20$$

Cannot be 5 b/c  
exponents not div  
by 5 evenly

$$\begin{aligned} 4^{1536} &\\ \Rightarrow (4^4)^{384} \mod 5 &\\ = 1^{384} \mod 5 &= 1 \end{aligned}$$

$$9^{4824} \mod 5$$

$$\begin{aligned} 9 \times 9 = 81 \quad 9^{4824} &= (9^2)^{2412} = (81)^{2412} \\ 81 \mod 5 = 1 & \quad |^{2412} \mod 5 = 1 \end{aligned}$$

$$\begin{aligned} 4^{1536} - 9^{4824} \mod 5 &= 1 \mod 5 - 1 \mod 5 \\ &= 1-1 \mod 5 = 0 \mod 5 \end{aligned}$$

So the difference is divisible  
by 5

Since the difference is divisible by both 5 and 7, it must also be divisible by 35.

1.12) What is  $2^{2006} \bmod 3$

$$\begin{array}{l} 4 \times 5 = 20 \\ 3 \times 7 = 21 \end{array} \quad \left\{ \begin{array}{l} \text{Want work} \\ 2006 \% 5 = 0 \end{array} \right.$$

$$2^{2006} = 4^{1003} \bmod 3$$
$$4^{2006} = (4^2)^{1003} = 16^{1003}$$
$$(16 \bmod 3)^{1003} = 1^{1003} = 1$$

$$4^2 = 16$$
$$16 \bmod 3 = 1$$

(Tinkering)

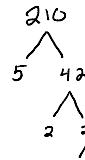
$$2^{2006} \bmod 3 = 4^{1003} \bmod 3 = (4^2 \bmod 3)^{1003}$$
$$= 1^{1003} \bmod 3 = \boxed{1}$$

1. 18) Compute  $\gcd(210, 588)$

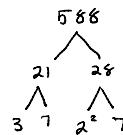
Factorization:

Factors of 210: 2, 3, 5, 6, 7, 10, 14, 15, 21, 30, 35, 42, 70, 105

Factors of 588: 2, 3, 4, 6, 7, 12, 14, 21, 28, 42, 49, 84, 98, 147, 196, 294



$$210 = 5 \times 2 \times 3 \times 7$$

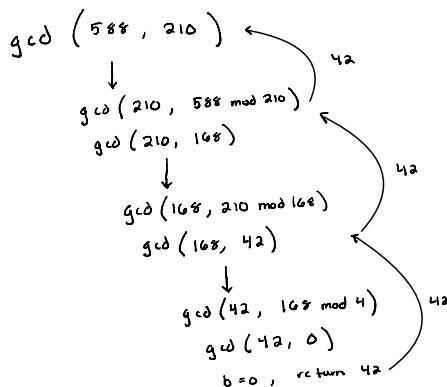


$$588 = 3 \times 7^2 \times 2^2$$

$$7 \times 3 \times 2 = 42$$

$$\gcd(210, 588) = 42$$

Euler's Algorithm:



$$\boxed{\gcd(588, 210) = 42}$$

1.31) Consider  $N! = 1 \cdot 2 \cdot 3 \cdots N$

a) how many bits long is  $N!$  in  $\Theta(n)$  form

From Stirling's Approximation, we know that the bit length of a factorial is  $O(\log_2(\text{Factorial}))$

$$\Rightarrow \log_2(N!) = \log_2(N \cdot (n-1) \cdot (n-2) \cdots 2 \cdot 1) = \underbrace{\log_2(N) + \log_2(n-1) + \dots + \log_2(2) + \log_2(1)}$$

Magnitude of all the terms is relatively close to  $\log_2(n)$ .  
So for our approximation we will treat them like they are all the same magnitude of  $\log_2(n)$

$$\Rightarrow \Theta(\log_2 n!) = \boxed{\Theta(n \log_2 n)}$$

b) Algorithm for computing  $N!$  with runtime analysis.

$$N! = n(n-1)(n-2)\dots(1) \rightarrow \begin{array}{l} \text{Because multiplication is commutative, we can use a for loop to multiply} \\ \text{from 1 to } N \end{array}$$
$$N! = (1)(2)\dots(n-1)(N)$$

NFactorial(N)

result = 1

for i in range(1, N+1):

    result = result \* i

return result

will go through  $n$ -iterations  
Multiplication of 2  $n$ -bit numbers will take  $O(n^2)$   
Bit length  $O(n) \times$  Bit length  $O(n)$

# of iterations  $\Theta(n) \times$  time for multiplication  $O(n^2)$

$$\boxed{\Theta(n^3) \text{ time}}$$

## Lab 2 Results:

- 3 trials of 100, 1000, 10000 digit numbers

Results:		
	Regular	Div and Conq
100	4.29E-06	8.30E-05
	2.62E-06	2.72E-05
	2.86E-06	3.81E-05
Avg	3.26E-06	4.94E-05
1000	3.10E-06	4.60E-05
	2.15E-06	2.88E-05
	2.15E-06	4.10E-05
Avg	2.46E-06	3.86E-05
10000	4.29E-06	4.60E-05
	2.86E-06	4.51E-05
	3.81E-06	4.60E-05
Avg	3.66E-06	4.57E-05