Jevin Alighew #6

Hey! Notes & my work can be found on the following pages!

1) 4

2) 17, see table in notes.

3) $\phi(3200) = 1280$

4) $9^{-1} \equiv 17 \bmod 19$

5) $5^{300} \bmod 31 = 1$; $5^{300} \equiv 1 \bmod 31$

Bonus question! → see last page of this pdf!

Jevin Ali Hw #6

(228, 44)

1) Euclidean algorithm to find GCD. Euclidean alg finds greatest common divisor (GCD) of 2 #s using repeated division & reminder steps.

Step 1:

$$\begin{array}{r} 5 \\ 44\overline{)228} \\ -220 \\ \hline 8 \end{array}$$ (8 remainder)

$$\begin{array}{r} 44 \\ \times 5 \\ \hline 220 \end{array}$$

Step 2

$$\begin{array}{r} 5 \\ 8\overline{)44} \\ -40 \\ \hline 4 \end{array}$$ (4 rem)

Step 3

$8/4 = 2$ R0 Since the reminder is now 0, the last nonzero reminder is the GCD.

$$\boxed{GCD(228, 44) = 4}$$

2) Using extended Euclidean algorithm to find the multiplicative inverse of 9 mod 19.

The ex. Eud. alg. helps find #s s & t such that:

$$a \cdot s + b \cdot t = gcd(a, b)$$

where the coefficient s (mod 19) will give the multiplicative inverse of 9.

we need to find x such that:

$9x \equiv 1 \bmod 19$

↳ modular inverse

2 cont)

Remainder @ each step

i	r_i	$q_i - 1$	s_i	t_i
0	19	—	1	0
1	9	2	0	1
2	1	9	1	−2
3	0	=	−9	19

Helps express the GCD as $9s+19t=1$

The quotient from dividing the previous 2 values.

multiplicative inverse is the # that when multiplied gives 1. modular inverse is the same concept but inside modular arithmetic.

Step 1

Extended Euclidean Alg. helps $9s+19t = \gcd(9,19)$

9 & 19 are coprime. ✓

GCD = 1

we find s.

$9s \equiv 1 \bmod 19$

Step 2

Apply Euclidean alg. GCD of (9, 19)

$19/9 = 2$ R (1) $\Rightarrow$ GCD (9, 19) = 1 ✓

Step 3

Work backwards to express 1 as a combination of 9 & 19.

$1 = 19 - 2 \times 9$

$9 \cdot (-2) + 19 \cdot 1 = 1$

$9s + 19t = 1$

$s = -2$ ← inverse

$t = 1$

> expressing 1 as a linear combination of 9 & 19.

Step 4/ We need our inverse to be positive, so we take $-2 \bmod 19$.

$-2 \equiv 17 \bmod 19$

$-2 + 19 = 17$ ✓

Find $9^{-1} \bmod 19 = 17$

3) Euler's totient function (n) counts the # of integers $\leq n$ that are coprime to n.

Compute (3200)

Step 1/ Factor $3200 \Rightarrow 3200 = 2^7 \times 5^2$

Step 2/ Apply Euler's Totient Function Formula

$$(n) = n \times \left(1 - \frac{1}{p^1}\right) \times \left(1 - \frac{1}{p^2}\right)$$

$$(3200) = 3200 \times \left(1 - \frac{1}{2}\right) \times \left(1 - \frac{1}{5}\right)$$

$$(3200) = 3200 \times \frac{1}{2} \times \frac{4}{5}$$

$$3200 = 1600 \times \frac{4}{5}$$

$$(3200) = 1280$$

$\varphi(3200) = 1280$

4) Find the multiplicative inverse of (9) in GF(19) using Fermi Little Theorem.

I learn here that if p is prime & a is not divisible by p, then $a^{p-1} \equiv 1 \bmod p$

Target → find $9^{-1} \bmod 19$

$9^2 = 81 \equiv 5 \bmod 19$ (remainder) $\quad 81 - 76 = 5$

$9^4 = 5^2 = 25 \equiv 6 \bmod 19$

$9^8 = 6^2 = 36 \equiv 17 \bmod 19$

$9^{16} = 17^2 = 289 \equiv 9 \bmod 19$

$9^{17} = 4 \times 9 = 36 \equiv 17 \bmod 19$ ✓

☆ multiplicative inverse of 9 mod 19 is 17.

Step 1

$a^{p-1} \equiv 1 \bmod p$

multiply both sides by a^{-1}

$\Rightarrow a^{p-2} \equiv a^{-1} \bmod p$

means that the multiplicative inverse of a modulo p is:

Step 2

given

$a^{-1} \equiv a^{p-2} \bmod p$ ☆

↳ $9^{-1} \bmod 19$

$a = 9$

$p = 19$ (which is prime)

Step 2 Cont

$9^{-1} \equiv 9^{19-2} = 9^{17} \bmod 19$

Step 3

$9^{17} = 9^{16} \times 9 = 4 \times 9 = 36$

$36/19 = 1_{R17}$ ✓

$9^{17} \equiv 17 \bmod 19$

Final

$9^{-1} \equiv 17 \bmod 19$

or $9^{-1} \equiv 9^{17} \equiv 17 \bmod 19$

5) Confirm applicable, Never Exp. Sol in Euler rule, Conclude.

Step 1
Euler theorem states that if a & n are relatively prime (ie gcd(a,n)=1) then $a^{\varphi(n)} \equiv 1 \bmod n$, where $\varphi(n)$ is Euler totient function.

- In the question our base is 5.
  $a = 5$ and our modulo is $n = 31$.
- Since 31 is prime, $\varphi(31) = 31 - 1 = 30$ ✓
- also, $\gcd(5, 31) = 1$ ✓, so we can use the theorem. ✓

Step 2
Express Exp in term of $\varphi(31)$.

$$5^{300} \bmod 31 \Rightarrow 5^{300} = (5^{30})^{10}$$

∵ 300 = 30 × 10

Step 3
Since Euler theorem tells us that: $5^{30} \equiv 1 \bmod 31$,
we can substitute this into our expression.

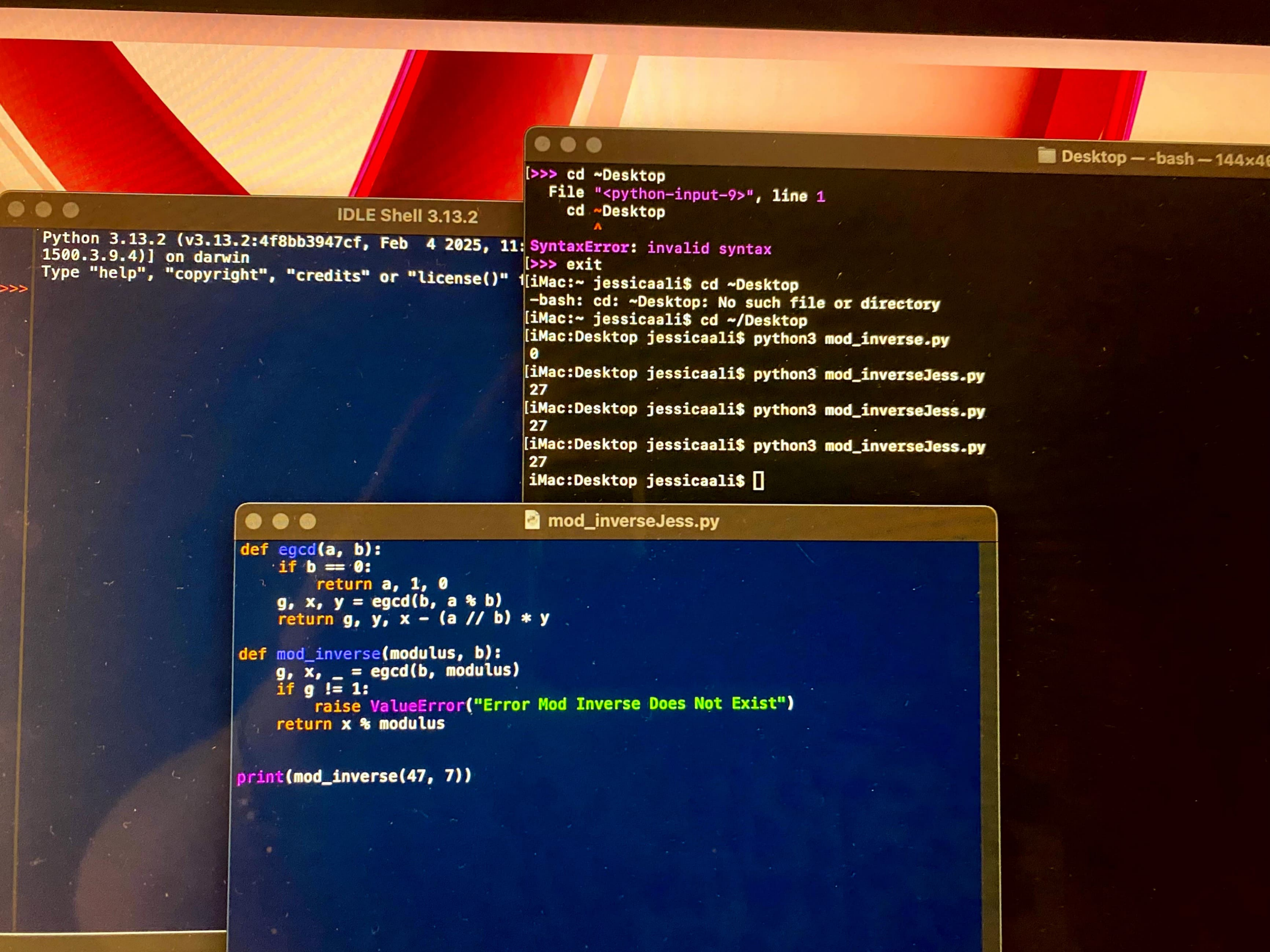
$$(5^{30})^{10} = 1^{10} \bmod 31$$

∵ $1^{10} = 1$

$$5^{300} \equiv 1 \bmod 31$$

Final

$$5^{300} \bmod 31 = 1$$


IDLE Shell 3.13.2
Python 3.13.2 (v3.13.2:4f8bb3947cf, Feb 4 2025, 11:
1500.3.9.4)] on darwin
Type "help", "copyright", "credits" or "license()"
>>>
Desktop — -bash — 144×4
[>>> cd ~Desktop
File "<python-input-9>", line 1
cd ~Desktop
^
SyntaxError: invalid syntax
[>>> exit
[iMac:~ jessicaali$ cd ~Desktop
-bash: cd: ~Desktop: No such file or directory
[iMac:~ jessicaali$ cd ~/Desktop
[iMac:Desktop jessicaali$ python3 mod_inverse.py
0
[iMac:Desktop jessicaali$ python3 mod_inverseJess.py
27
[iMac:Desktop jessicaali$ python3 mod_inverseJess.py
27
[iMac:Desktop jessicaali$ python3 mod_inverseJess.py
27
iMac:Desktop jessicaali$
mod_inverseJess.py
def egcd(a, b):
if b == 0:
return a, 1, 0
g, x, y = egcd(b, a % b)
return g, y, x - (a // b) * y
def mod_inverse(modulus, b):
g, x, _ = egcd(b, modulus)
if g != 1:
raise ValueError("Error Mod Inverse Does Not Exist")
return x % modulus
print(mod_inverse(47, 7))