4.1

- Division Algorithm: $a = dq + r$
- Training problems, sets 1, 2, 3
- Congruency
- Addition Modulo

$$a +_m b = (a+b) \bmod m$$
$$a \cdot_m b = (a \cdot b) \bmod m$$

4.2

- Base conversions: decimal to non-decimal, vice versa,
  non-decimal to non-decimal
- octal: 0-7
  hex: 0-9 A-F
- Addition and multiplication of various bases.
- Must indicate base of your final answer.
- Modular Exponentiation

Python

- Comprehensions: as mentioned in the coding the matrix book (chapter 0).
- lists, sets
- intersections, unions, etc

4.3

- Prime factorization
- lcm
- gcd ← know both Euclidean and finding min of components (from prime factorization)
- relatively prime, pairwise relatively prime
- primes, composites
- Euclidean Algorithm
- Linear combinations
  - Backward pass
  - Extended Euclidean Algorithm
- Bezout's Theorem

ex: Express gcd(126, 34) as a linear combination of 126 and 34

Solution:

Euclidean Algorithm:

Larger number is a and smaller is b.

$a = 126$

$b = 34$

$\gcd(a,b) = \gcd(b,r)$

$126 = 34 \cdot 3 + 24$

$34 = 24 \cdot 1 + 10$

$24 = 10 \cdot 2 + 4$

$10 = 4 \cdot 2 + 2$

$4 = 2 \cdot 2 + 0$

gcd(126, 34)

Backward pass

$2 = 10 - 4 \cdot 2$ ✓

$4 = 24 - 10 \cdot 2$ ✓

$10 = 34 - 24$

$24 = 126 - 34 \cdot 3$

linear combinations for gcd(a, b) of a and b means we need it to be in this format:

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

$2 = s \cdot 126 + t \cdot 34$

$2 = 10 - 4 \cdot 2 = 10 - (24 - 10 \cdot 2) \cdot 2 = 10 - 2 \cdot 24 + 4 \cdot 10$

$= 5 \cdot 10 - 2 \cdot 24 = 5 \cdot (34 - 24) - 2 \cdot 24$

$= 5 \cdot 34 - 5 \cdot 24 - 2 \cdot 24 = 5 \cdot 34 - 7 \cdot 24$

$= 5 \cdot 34 - 7 \cdot (126 - 34 \cdot 3) = 5 \cdot 34 - 7 \cdot 126 + 21 \cdot 34$

$=26\cdot 34-7\cdot 126$

$$\boxed{2=-7\cdot 126+26\cdot 34}$$

Extended Euclidean Algorithm:

$s_j = s_{j-2} - q_{j-1}\, s_{j-1}$

$t_j = t_{j-2} - q_{j-1}\, t_{j-1}$

$s_0 = 1$
$s_1 = 0$
$t_0 = 0$
$t_1 = 1$

$126 = 34\cdot 3 + 24$
$34 = 24\cdot 1 + 10$
$24 = 10\cdot 2 + 4$
$10 = 4\cdot 2 + 2$
$4 = 2\cdot 2 + 0$

Start s_2 and t_2
You have five equations,
so you'll need s_5 and t_5

$q_1 = 3$
$q_2 = 1$
$q_3 = 2$
$q_4 = 2$

$s_2 = s_0 - q_1 s_1 = 1 - 3\cdot 0 = 1$

$t_2 = t_0 - q_1 t_1 = 0 - 3\cdot 1 = -3$

$s_3 = s_1 - q_2 s_2 = 0 - 1\cdot 1 = -1$

$t_3 = t_1 - q_2 t_2 = 1 - 1\cdot(-3) = 1+3 = 4$

$s_4 = s_2 - q_3 s_3 = 1 - 2\cdot(-1) = 1+2 = 3$

$t_4 = t_2 - q_3 t_3 = -3 - 2\cdot(4) = -3 - 8 = -11$

$s_5 = s_3 - q_4 s_4 = -1 - 2 \cdot 3 = -1 - 6 = -7$

$t_5 = t_3 - q_4 t_4 = 4 - 2 \cdot (-11) = 4 + 22 = 26$

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

$$\boxed{2 = -7 \cdot 126 + 26 \cdot 34}$$

octal addition:

$$\begin{array}{r} \overset{1}{7}\,\overset{1}{1}\,5 \\ +\,2\,5\,6 \\ \hline 1\,1\,7\,3 \end{array}$$

$(715)_8 + (256)_8 = (1173)_8$

$$\begin{array}{r} 5 \\ +6 \\ \hline 11 \end{array} \quad \begin{array}{r} 11 \\ -8 \\ \hline 3 \end{array} \qquad \begin{array}{r} 7 \\ +2 \\ \hline 9 \end{array} \quad \begin{array}{r} 9 \\ -8 \\ \hline 1 \end{array}$$

ex: $4^{601} \bmod 21 = ?$

Solution:

convert 601 to binary

$2 \overline{)601}$ 300 R1

$2 \overline{)300}$ 150 R1

$2 \overline{)150}$ 75 R0

$2 \overline{)75}$ 37 R1

$2 \overline{)37}$ 18 R1

$2 \overline{)18}$ 9 R0

$2 \overline{)9}$ 4 R1

$2 \overline{)4}$ 2 R0

$2 \overline{)2}$ 1 R0

$2 \overline{)1}$ 0 R1

$(601)_{10} = \overset{10\,9\,8\,7\,6\,5\,4\,3\,2\,1}{1001011001}$

10 bits = 10 modular exponentiation steps

Step	
1	$4^1 \bmod 21 = 4$
2	$4^2 \bmod 21 = 16$
3	$4^4 \bmod 21 = 4^2 \cdot 4^2 = 16 \cdot 16 \bmod 21 = 4$

step

4 $4^{8} \bmod 21 \equiv 4^{4} \cdot 4^{4} = 4 \cdot 4 \bmod 21 = 16$

5 $4^{16} \bmod 21 \equiv 4^{8} \cdot 4^{8} = 16 \cdot 16 \bmod 21 = 4$

$$\left.\begin{array}{ll} 6 & 4^{32} \bmod 21 = 16 \\ 7 & 4^{64} \bmod 21 = 4 \\ 8 & 4^{128} \bmod 21 = 16 \\ 9 & 4^{256} \bmod 21 = 4 \\ 10 & 4^{512} \bmod 21 = 16 \end{array}\right\} \text{Because of pattern}$$

$$(601)_{10} = \overset{10\,9\,8\,7\,6\,5\,4\,3\,2\,1}{1001011001}$$

(we only care when the bit has a 1 value.)

$4^{601} \bmod 21 = (4 \cdot 16 \cdot 4 \cdot 4 \cdot 16) \bmod 21 = \boxed{4}$ ← ANS

$(4 \cdot 16 \cdot 4 \cdot 4 \cdot 16) \bmod 21 = ((4 \cdot 16 \bmod 21)(4 \cdot 4 \cdot 16 \bmod 21)) \bmod 21$

Is 77 prime?

Solution:
check if any prime up to $\sqrt{77}$ divides 77.

$\sqrt{77} \approx 8.77$
check up to 8. (upto the floor of the number)

2, 3, 5, 7
$7 \mid 77$ so 77 is not prime