6.3

Full transparency, I don't know how to do this the proper way, but I did write a code at the beginning of the semester that would find all invertible elements and their inverses given a proper modulus, so I did that. The top row shows the invertible elements, and the bottom row is their respective inverse:

a. 6

```
Modulo: 101

  1   2   3   4   5   6   7   8   9  10  11  12  13  14  15  16  17  18  19  20  2
  1  51  34  76  81  17  29  38  45  91  46  59  70  65  27  19   6  73  16  96  7
```

b. 1075

```
345  347  349  351  353  355  357  359  361  363  365  367  369  371  373  375
 93  601 1135 1009  825   73 1075   55  523   17   71  501  719 1081  397  283
```

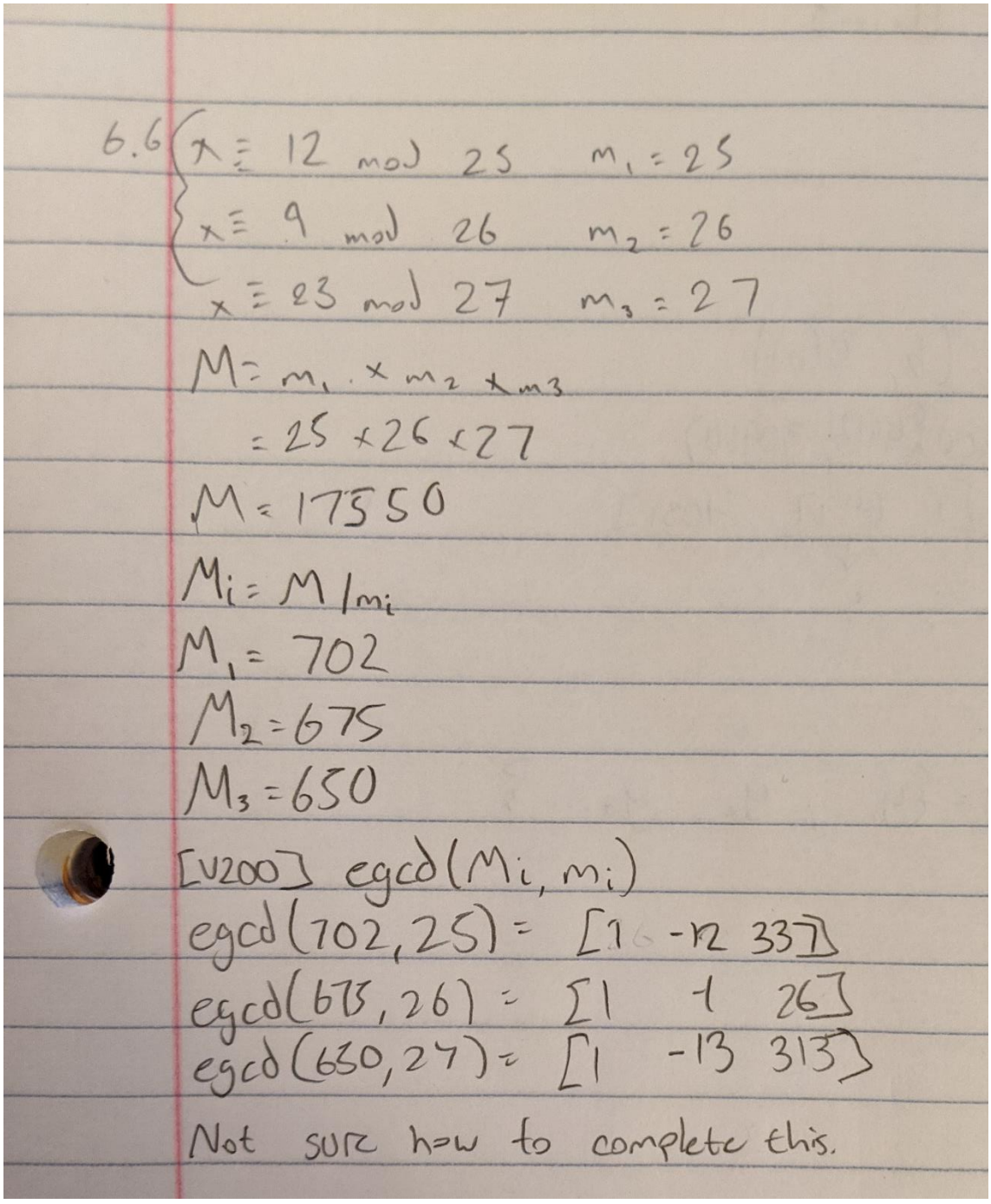
c. 3125

```
4 1835 1837 1838 1840 1841 1843 1844 1846 1847 1849 1850 1852 1853 1855 1856 1858
7 1562 4072  614 4543 5300 4075 3125 9235 9230 4159 9323 1882 2393 5260  113 4972
```

The file on *c* cut off before reaching 3125 on the invertible elements, but if I remember correctly, the elements are inverses of each other, as seen in part a.

```
      # Find all invertible elements and their inverses
# given a modulo.

import math
mod = 26

invertibleAndInverses = {'Invertible': [], 'Inverse': []}
for i in range(mod):
    if math.gcd(i, mod) == 1:
        #A number is invertible if the gcd of the number and the modulo is 1.
        invertibleAndInverses['Invertible'].append(i)
        for j in range(mod):
            if (i * j) % mod == 1:
                #A number's inverse occurs when the number is multiplied by a
number
                #, % 26, and it equals 1.
                invertibleAndInverses['Inverse'].append(j)
                break

print(f'Invertibles: {invertibleAndInverses["Invertible"]}')
print(f'Inverses:    {invertibleAndInverses["Inverse"]}')
print(f'Number n:    {len(invertibleAndInverses["Invertible"])}')

#Uncomment to write to a file if output is too long.
fileout = open('./output.txt', 'w')
fileout.write(f'Modulo: {mod}\n\n')
for i in invertibleAndInverses['Invertible']:
    fileout.write('%5d' % i)
fileout.write('\n')
for i in invertibleAndInverses['Inverse']:
    fileout.write('%5d' % i)
```

6.6


6.6
x ≡ 12 mod 25 m1 = 25
x ≡ 9 mod 26 m2 = 26
x ≡ 23 mod 27 m3 = 27
M = m1 x m2 x m3
= 25 x 26 x 27
M = 17550
Mi = M / mi
M1 = 702
M2 = 675
M3 = 650
[U200] egcd(Mi, mi)
egcd(702, 25) = [1 -12 337]
egcd(675, 26) = [1 -1 26]
egcd(650, 27) = [1 -13 313]
Not sure how to complete this.

6.13

Interestingly, this was surprisingly easy because of the function already written in V200. I took the logic from SAM and nttbook, and I was able to throw this together in about 10 minutes. I will include codes and the work I did to find the input variables.

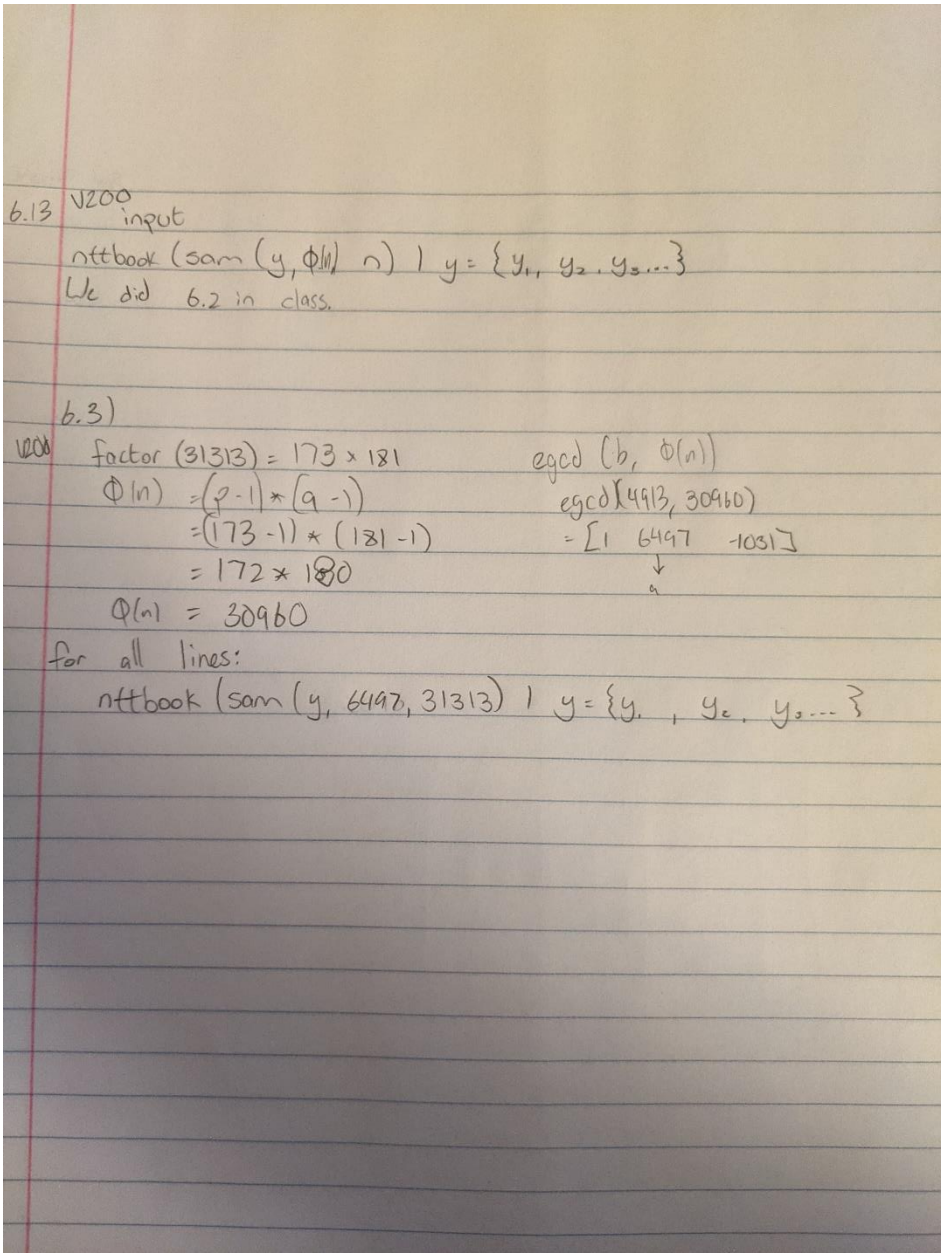
6.2 Output

I became involved in an argument about modern painting, a subject upon which i am spectacularly ill informed. However, many of my friends can become heated and even violent on the subject and I enjoy their wrangles in a modest way. I am an artist myself and I have some sympathy with the abstractionists. Although I have gone beyond them in my own approach to art, I am a lumpist. Two or three decades ago it was quite fashionable to be a cubist and to draw everything in cubes. Then, there was a revolt by the vorticists, who drew everything in whirls wenowhve*(I can't figure this out)* the abstractionists who paint everything in a very abstracted manner, but my own small works done on my telephone pad are composed of carefully shaded, strangely shaped lumps with traces of cubism, vorticism, and abstraction is min them for those who possess the seeing eyes. A lumpist, I stand alone.

6.3 Output

Lake Wobegon is mostly poor, sandy soil, and every spring the earth heaves up a new crop of rocks. Piles of rocks, ten feet high in the corners of fields, picked by generations of us, monuments to our industry. Our ancestors chose the place, tired from their long journey, sad for having left the motherland behind, and this place reminded them of the reso*(?)* they settled here, forgetting that they had left there because the land wasn't so good. So, the new life turned out to be a lot like the old, except the winters are worse. z

Work


6.13 V200 input
nttbook (sam (y, ϕ(n) n) | y = {y1, y2, y3...}
We did 6.2 in class.
6.3)
V200 factor (31313) = 173 x 181
ϕ(n) = (p-1) * (q-1)
= (173-1) * (181-1)
= 172 * 180
ϕ(n) = 30960
egcd (b, ϕ(n))
egcd(4913, 30960)
= [1 6497 -1031]
a
for all lines:
nttbook (sam (y, 6497, 31313) | y = {y1, y2, y3...}

Code

```
import math
def nttbook(x):
    t = ''
    lst = x
    bt = ''

    n = x
    while n > 0:
        c = math.floor(n % 26)
        bt += chr(c + 97)
        n = (n - c)/26

    t += bt
    return t
```

[11] ✓ 0.4s

```
def sam(x, n, m):
  z = 1
  while n > 0:
    if n % 2 == 1:
      z = x*z % m
      n -= 1
    else:
      x = x**2 % m
      n /= 2
  return z
```

[6] ✓ 0.2s

```
filein = open('./input.txt', 'r')
x = []
for row in filein:
  arr = row.split(' ')
  for y in arr:
    x.append(int(y.strip()))
```

[30] ✓ 0.2s

```
for i in range(len(x)):
  print(nttbook(sam(x[i], 5797, 18923))[::-1], end='')
  #For some reason it prints backwards, so reverse it and I'll fix it later.
```

[31] ✓ 0.3s

Output:


for i in range(len(x)):
print(nttbook(sam[x[i], 5797, 18923))[::-1], end='')
0.3s
Python
ibecameinvolvedinanargumentboutmodernpintingasubjectuponwhichiamspectaculrlyilllinformedhowevermanyofmyfriendscanbecomeheteedandevenviolentonthesubjectndienjoytheirwranglesinmodestwayiamanrtistmyselfndihavesomesympathywiththebstractionistsltheughihavegonebeyondthemInmyownapprochtoartimalumpisttw
oorthreedecadesgoltwsquitefashionabletobeacubistandtodrweverythingincubesthentherewasarevoltbythevorticistswhodreweverythinginwhirlswenowhvethebstractionistswhopainteverythinginaveryabstrctedmnnerbutmyownsmllworksdoneonmytelephonepadarecomposedofcrefullyshadedstrangelyshapedlumpswithtracesofcu
bismvorticismandabstrctionisminthemforthosewhopossesstheseeingeyesalumpististandalone