Math 116 HW1

Jun Ryu

1) a) b) & 2) a) b)

In [1]:
```
shift_system = ShiftCryptosystem(AlphabeticStrings())
message = "A page of history is worth a volume of logic"
plaintext = shift_system.encoding(message)
print("plaintext:", plaintext)
key = 11
encode = shift_system(key)
ciphertext = encode(plaintext)
print("ciphertext:", ciphertext)
```

```
plaintext: APAGEOFHISTORYISWORTHAVOLUMEOFLOGIC
ciphertext: LALRPZQSTDEZCJTDHZCESLGZWFXPZQWZRTN
```

In [2]:
```
shift_system = ShiftCryptosystem(AlphabeticStrings())
message = "AOLYLHYLUVZLJYLAZILAALYAOHUAOLZLJYLAZAOHALCLYFIVKFNBLZZLZ"
ciphertext = shift_system.encoding(message)
print("ciphertext:", ciphertext)
key = 7
decode = shift_system(shift_system.inverse_key(key))
print("plaintext:", decode(ciphertext))
```

```
ciphertext: AOLYLHYLUVZLJYLAZILAALYAOHUAOLZLJYLAZAOHALCLYFIVKFNBLZZLZ
plaintext: THEREARENOSECRETSBETTERTHANTHESECRETSTHATEVERYBODYGUESSES
```

In [3]:
```
shift_system = SubstitutionCryptosystem(AlphabeticStrings())
message = "The gold is hidden in the garden"
plaintext = shift_system.encoding(message)
print("plaintext:", plaintext)
key = shift_system.encoding("SCJAXUFBQKTPRWEZHVLIGYDNMO")
ciphertext = shift_system.enciphering(key, plaintext)
print("ciphertext:", ciphertext)
```

```
plaintext: THEGOLDISHIDDENINTHEGARDEN
ciphertext: IBXFEPAQLBQAAXWQWIBXFSVAXW
```

In [4]:
```
shift_system = SubstitutionCryptosystem(AlphabeticStrings())
message = "IBXLX JVXIZ SLLDE VAQLL DEVAU QLB"
ciphertext = shift_system.encoding(message)
print("ciphertext:", ciphertext)
key = shift_system.encoding("SCJAXUFBQKTPRWEZHVLIGYDNMO")
plaintext = shift_system.deciphering(key, ciphertext)
print("plaintext:", plaintext)
```

```
ciphertext: IBXLXJVXIZSLLDEVAQLLDEVAUQLB
plaintext: THESECRETPASSWORDISSWORDFISH
```

3) a) Using a calculator,

$a/b = 1498387487 / 76348$

≈ 19625.75951

$\Rightarrow q = \boxed{19625}$, $r = a - b \cdot q = \boxed{57987}$

b) $a/b = 4536782793 / 9784537$

≈ 463.6686225

Take only the decimal part and multiply it by b:

$r = 463.6686225 \cdot 9784537$

$= \boxed{6542162}$

4) $\gcd(291, 252)$

$= \gcd(39, 252) = \gcd(39, 18)$

$= \gcd(3, 18) = \boxed{3}$

$$\left(\begin{array}{l} 291 = 252 \cdot 1 + \boxed{39} \\ 252 = 39 \cdot 6 + \boxed{18} \\ 39 = 18 \cdot 2 + \boxed{3} \\ 18 = 3 \cdot 6 + \boxed{0} \end{array}\right)$$

$291u + 252v = \gcd(291, 252) = 3$

$3 = 39 - 18 \cdot 2$

$18 = 252 \cdot 1 - 39 \cdot 6$

$$39 = 291 \cdot 1 - 252 \cdot 1$$

$$3 = (291 - 252) - (252 - (291 - 252) \cdot 6) \cdot 2$$

$$= 291 \cdot 13 - 252 \cdot 15$$

$\Rightarrow u = 13, v = -15$ is a solution

```
In [5]: xgcd(291,252)
Out[5]: (3, 13, -15)
```

This confirms our answers above that $291(13) + 252(-15) = 3$ ✓

5) a) We let $d = \gcd(a, b)$. We have that $d \mid a$ and $d \mid b \Rightarrow a = d\alpha$, $b = d\beta$ for some integers α, β.

Thus, we have:

$$au + bv = d\alpha u + d\beta v = d(\alpha u + \beta v) = 1$$

Since $d \mid 1 \Rightarrow d = \gcd(a, b) = 1$ ✓

b) No, we can have

$$1 \cdot u + 3 \cdot v = 6, \text{ where } u=3 \ \& \ v=1 \text{ is a solution}$$

$$\gcd(a,b) = \gcd(1,3) = 1 \neq 6$$

By what we've shown in part a), in $au+bv=f$, $\gcd(a,b) \mid f$.

c) We have (u_1, v_1) & (u_2, v_2) are solutions

$$\Rightarrow au_1 + bv_1 = 1 \ \& \ au_2 + bv_2 = 1$$

subtract the above two:

$$a(u_1 - u_2) + b(v_1 - v_2) = 0$$

$$\Rightarrow a(u_1 - u_2) = b(v_2 - v_1)$$

from part a), we have $\gcd(a,b) = 1$

$$\Rightarrow a \mid v_2 - v_1 \ \& \ b \mid u_1 - u_2$$

$$\Rightarrow a \mid v_2 - v_1 \ \& \ b \mid u_2 - u_1 \ ✓$$

d) We let $g = \gcd(a,b)$

$$au + bv = g \Rightarrow \frac{a}{g} u + \frac{b}{g} v = 1$$

Now, we have (u_0, v_0) is one particular sol.

By part c), we have $\frac{b}{g} \mid (u - u_0)$

$\Rightarrow u - u_0 = k \cdot \frac{b}{g}$

$\Rightarrow u = u_0 + \frac{kb}{g}$ ✓

By part c) again, we have $\frac{a}{g} \mid v - v_0$

$\Rightarrow \frac{a}{g} \mid v_0 - v$

$\Rightarrow v_0 - v = k \cdot \frac{a}{g}$

$\Rightarrow v = v_0 - \frac{ka}{g}$ ✓

6) a) $347 + 513 = 860 - 763 = \boxed{97} \pmod{763}$

b) $153 \cdot 287 \equiv -200 \cdot (-66) \pmod{353}$

$= 13200 / 353 \Rightarrow q = 37$

$r = a - b \cdot q = \boxed{139} \pmod{353}$

c) $23^3 \cdot 19^5 \cdot 11^5$

$23^2 = 529 \equiv 44 \pmod{97}$

$44 \cdot 23 = 1012 \equiv 42 \pmod{97}$

$19 \cdot 19 = 361 \equiv 70 \pmod{97}$

$70 \cdot 70 \cdot 19 = 93100 \equiv 77 \pmod{97}$

$11 \cdot 11 = 121 \equiv 24 \pmod{97}$

$24 \cdot 24 \cdot 11 = 6336 \equiv 31 \pmod{97}$

$42 \cdot 77 \cdot 31 = 100254 \equiv \boxed{53} \pmod{97}$

7) a) $x \equiv 23 - 17 \equiv \boxed{6} \pmod{37}$

b) $x \equiv 19 - 42 \equiv -23 \equiv \boxed{28} \pmod{51}$

c) plugging in x from 0 to 10, we get our modulo list is

$\{0, 1, 4, 9, 5, 3, 3, 5, 9, 4, 1\}$

So, only works when $x = \boxed{5 \text{ or } 6}$

d) Our modulo list is

$\{0, 1, 4, 9, 3, 12, 10, 10, 12, 3, 9, 4, 1\}$

So, there are no solutions for $x^2 \equiv 2 \pmod{13}$

e) modulo list:

$\{0, 1, 4, 1, 0, 1, 4, 1\} \Rightarrow x = \boxed{1, 3, 5, 7}$

f) modulo list:

$\{9, 0, 6, 0, 10, 9, 3, 9, 0, 4, 5\}$

$\Rightarrow x = \boxed{1, 3, 8}$

g) $x \equiv 2 \pmod 7$ ≤ 34

$x = 2, 9, 16, 23, 30$

Now, we check if these are $\equiv 1 \pmod 5$

$2 \equiv 2 \pmod 5$ ✗
$9 \equiv 4 \pmod 5$ ✗
$16 \equiv 1 \pmod 5$ ✓
$23 \equiv 3 \pmod 5$ ✗
$30 \equiv 0 \pmod 5$ ✗

So, $x = \boxed{16}$

8) a) We have that

$2 \cdot [\text{inverse}] \equiv 1 \pmod m$

So, if the inverse is $\boxed{\frac{m+1}{2}}$ (an integer):

$2 \cdot \left(\frac{m+1}{2}\right) = m+1 \equiv 1 \pmod m$ ✓

b) $b \cdot [\text{inverse}] \equiv 1 \pmod m$

$m \equiv 1 \pmod b \rightarrow \frac{m-1}{b}$ an integer

$b \cdot \frac{1-m}{b} = 1-m \equiv 1 \pmod m$

But, $\frac{1-m}{b}$ is negative so, we add m, resulting in $\boxed{\frac{1-m}{b} + m}$