COT4115.001S15 - HOMEWORK 01
DUE JANUARY 22, 2015

Show all work (including any computer code) for full credit.

Question 1 (30 pts)**.** Use the *extended Euclidean algorithm* to find **all** $x, y \in \mathbb{Z}$ such that:

(1) $71x + 113y = 1$

Answer:

$$\begin{array}{rcl} 113 = 1 \cdot 71 + 42 & & 1 = 22\,(113 - 1 \cdot 71) - 13 \cdot 71 = \mathbf{22} \cdot 113 - \mathbf{35} \cdot 71 \\ 71 = 1 \cdot 42 + 29 & & 1 = 9 \cdot 42 - 13\,(71 - 1 \cdot 42) = 22 \cdot 42 - 13 \cdot 71 \\ 42 = 1 \cdot 29 + 13 & & 1 = 9\,(42 - 1 \cdot 29) - 4 \cdot 29 = 9 \cdot 42 - 13 \cdot 29 \\ 29 = 2 \cdot 13 + 3 & & 1 = 1 \cdot 13 - 4\,(29 - 2 \cdot 13) = 9 \cdot 13 - 4 \cdot 29 \\ 13 = 4 \cdot 3 + 1 & \Longrightarrow & 1 = 13 - 4 \cdot 3 \\ 3 = 3 \cdot \mathbf{1} + 0 & & \end{array}$$

Check: $\gcd(71, 113) = 1$ and $1 \mid 1$, so an infinite number of solutions exist. Initial solutions are $x_0 = 22$ and $y_0 = 35$, and all solutions are give by:

$$x = 22 + 113k \quad \text{and} \quad y = 35 - 71k \quad \text{for all } k \in \mathbb{Z}.$$

(2) $3x - 5y = 7$

Answer:

$$\begin{array}{rcl} 5 = 1 \cdot 3 + 2 & & 1 = 1 \cdot 3 - 1\,(5 - 1 \cdot 3) = \mathbf{2} \cdot 3 - \mathbf{1} \cdot 5 \\ 3 = 1 \cdot 2 + 1 & \Longrightarrow & 1 = 3 - 1 \cdot 2 \\ 2 = 2 \cdot \mathbf{1} + 0 & & \end{array}$$

Check: $\gcd(3, 5) = 1$ and $1 \mid 7$, so an infinite number of solutions exist. First solve

$$3x - 5y = \gcd(3, 5) = 1,$$

then multiply both sides of the equation by 7. By the extended Euclidean algorithm above, a particular solution to $3X - 5Y = 1$ is $X_0 = 2$ and $Y_0 = 1$. Multiplying both sides of $3X_0 - 5Y_0 = 1$ by 7 gives $3\,(7X_0) - 5\,(7Y_0) = 1(7)$ which means $x_0 = 7X_0 = 14$ and $y_0 = 7Y_0 = 7$ is a particular solution to the original equation $3x_0 - 5y_0 = 7$ and the general solution is

$$x = 14 + 5k \quad \text{and} \quad y = 7 - (-3)k \quad \text{for all } k \in \mathbb{Z}.$$

(3) $119x + 221y = 1$

Answer:

$$\begin{aligned} 221 &= 1 \cdot 119 + 102 \\ 119 &= 1 \cdot 102 + 17 \\ 102 &= 6 \cdot \mathbf{17} + 0 \end{aligned}$$

Check: $\gcd(119, 221) = 17$ but $17 \nmid 1$, so there are no solutions.

Question 2 (30 pts)**.** Find **all** $x \in \mathbb{Z}$ such that:

(1) $11x + 4 \equiv 0 \pmod{37}$

Answer: Note that the $\gcd(11, 37) = 1$ so $11^{-1} \pmod{37}$ exists. To find this value, we must solve

$$11k \equiv 1 \pmod{37}$$

which is to say, $11k - 1 = 37j$ for some $j \in \mathbb{Z}$, i.e., $11k - 37j = 1$. A particular solution to this equation is $k = 27$ and $j = 8$, however we are only concerned with the value of k which gives:

$$11^{-1} \equiv 27 \pmod{37}.$$

Thus

$$\begin{aligned} 11x &\equiv -4 \equiv 33 \pmod{37} \\ x &\equiv 11^{-1} \cdot 33 \pmod{37} \\ &\equiv 27 \cdot 33 \pmod{37} \\ &= 726 \pmod{37} \\ &\equiv 23 \pmod{37}. \end{aligned}$$

(2) $6x + 3 \equiv 9 \pmod{12}$

Answer: Initially we investigate

$$6x \equiv 6 \pmod{12}$$

and note that $6 \mid 6$ and $6 \mid 12$, so the solution also satifies $(6x)/6 \equiv 6/6 \pmod{12/6}$ which is $x \equiv 1 \pmod{2}$. As an equality, this says that $x = 2k + 1$ for some $k \in \mathbb{Z}$. Considering this solution modulo 12,

$$x \equiv 1, 3, 5, 7, 9, 11 \pmod{12}$$

are all solutions to the original equation.

(3) $5x + 10 \equiv 4 \pmod{15}$

Answer: Subtracting 10 from both sides, $5x \equiv -6 \equiv 9 \pmod{15}$. Checking that $\gcd(5, 15) = 5$ but $5 \nmid 9$, so there are no solutions to the equation.

Question 3 (10 pts)**.** Decode the following Caesar shift cipher:

`ZWOZGDSMYZKDSKLVAVFLYWLAL`

Answer:

A bruteforce attack of all the shifts reveils the plaintext:

0:	ZWOZGDSMYZKDSKLVAVFLYWLAL	13:	MJBMTQFZLMXQFXYINISYLJYNY
1:	AXPAHETNZALETLMWBWGMZXMBM	14:	NKCNURGAMNYRGYZJOJTZMKZOZ
2:	BYQBIFUOABMFUMNXCXHNAYNCN	15:	OLDOVSHBNOZSHZAKPKUANLAPA
3:	CZRCJGVPBCNGVNOYDYIOBZODO	16:	PMEPWTICOPATIABLQLVBOMBQB
4:	DASDKHWQCDOHWOPZEZJPCAPEP	17:	QNFQXUJDPQBUJBCMRMWCPNCRC
5:	EBTELIXRDEPIXPQAFAKQDBQFQ	18:	ROGRYVKEQRCVKCDNSNXDQODSD
6:	FCUFMJYSEFQJYQRBGBLRECRGR	19:	SPHSZWLFRSDWLDEOTOYERPETE
7:	GDVGNKZTFGRKZRSCHCMSFDSHS	20:	TQITAXMGSTEXMEFPUPZFSQFUF
8:	HEWHOLAUGHSLASTDIDNTGETIT	21:	URJUBYNHTUFYNFGQVQAGTRGVG
9:	IFXIPMBVHITMBTUEJEOUHFUJU	22:	VSKVCZOIUVGZOGHRWRBHUSHWH
10:	JGYJQNCWIJUNCUVFKFPVIGVKV	23:	WTLWDAPJVWHAPHISXSCIVTIXI
11:	KHZKRODXJKVODVWGLGQWJHWLW	24:	XUMXEBQKWXIBQIJTYTDJWUJYJ
12:	LIALSPEYKLWPEWXHMHRXKIXMX	25:	YVNYFCRLXYJCRJKUZUEKXVKZK

Question 4 (20 pts)**.** Knowing that `c` $\mapsto$ `L` and `m` $\mapsto$ `H`, what is the encryption key, decryption key, and plaintext for the following affine ciphertext:

`RORKRELFIITFMHFREPRLJYLRNFTEFRLWWREI`

Answer: An affine cipher has an encryption key (α, β) which maps some plaintext x into the ciphertext X according to the rule $X \equiv \alpha x + \beta \pmod{26}$. Since we know how two of the plaintext letters are decrypted, we get the following system of equations:

$$11 \equiv \alpha \cdot 2 + \beta \pmod{26} \quad \text{and} \quad 7 \equiv \alpha \cdot 12 + \beta \pmod{26}.$$

Subtracting the first equation from the second gives

$$(11) - (7) \equiv (2\alpha + \beta) - (12\alpha + \beta) \pmod{26}$$
$$4 \equiv -10\,\alpha \equiv 16\,\alpha \pmod{26}$$

Check: $\gcd(16, 26) = 2$ and $2 \nmid 4$, so we solve

$$4/2 \equiv 16/2\alpha \pmod{26/2}$$
$$2 \equiv 8\,\alpha \pmod{13}$$

Check: $\gcd(8, 13) = 1$, so we know that $8^{-1} \pmod{13}$ exists. It can easily be shown that $8^{-1} \equiv 5 \pmod{13}$, so

$$\alpha \equiv 2 \cdot 5 \equiv 10 \pmod{13}$$

which corresponds to the solutions $x \equiv 10 \pmod{26}$ and $x \equiv 23 \pmod{26}$. Substituting the first solution back into the original equation, we get

$$\beta \equiv 11 - 2 \cdot 10 = -9 \equiv 17 \pmod{26}.$$

Similarly, the second solution gives

$$\beta \equiv 11 - 2 \cdot 23 = -35 \equiv 17 \pmod{26}.$$

Thus, there are two valid encryption keys, $(10, 17)$ and $(23, 17)$, which assign . To find their corresponding decryption keys, solve for x in each of the equations

$$X \equiv 10x + 17 \pmod{26} \quad \text{and} \quad X \equiv 23x + 17 \pmod{26}.$$

Starting with the first equation, we get $10x \equiv X - 17 \pmod{26}$. Since $\gcd(10, 26) = 2$, either $2 \mid X - 17$ or there are no solutions to the congruence. Since X can represent any letter of the alphabet, $2 \nmid X - 17$ for all $X \in \mathbb{Z}$.

We now check for a decryption key using the equation corresponding to the encryption key $(23, 17)$. Since $\gcd(23, 26) = 1$, the inverse $23^{-1} \pmod{26}$ exists, and it can be shown that $23^{-1} \equiv 17 \pmod{26}$. Hence

$$x \equiv 23^{-1}(X - 17) \equiv 17(X - 17) \equiv 17X - 289 \equiv 17X + 23 \pmod{26}$$

so $(17, 23)$ is a decryption key, and the plaintext message is:

`abalanceddietmeansacupcakeineachhand`

TLDR; There are two encryption keys, $(10, 17)$ and $(23, 17)$, which map `c` $\mapsto$ `L` and `m` $\mapsto$ `H`, but only $(23, 17)$ has a decryption key, $(17, 23)$, that ciphers all the alphabet letters distinctly.

Question 5 (10 pts)**.** Use a Vigenére cipher with the key "`hungry`" to encode the message:

`iwantahippopotamusforchristmas`

Answer:

Add the plaintext letters to the key letters. For example: $\mathtt{i}(8) + \mathtt{h}(7) \equiv \mathtt{P}(15) \pmod{26}$.

plain:	i	w	a	n	t	a	h	i	p	p	o	p	o	t	a	m	u	s	f	o	r	c	h	r	i	s	t	m	a	s
key:	h	u	n	g	r	y	h	u	n	g	r	y	h	u	n	g	r	y	h	u	n	g	r	y	h	u	n	g	r	y
cipher:	P	Q	N	T	K	Y	O	C	C	V	F	N	V	N	N	S	L	Q	M	I	E	I	Y	P	P	M	G	S	R	Q