Name: Solutions

Directions: Show all work. No credit for answers without work.

1. **[6 points]** An adversary's sensitive plaintext message is encrypted with a substitution cipher, and the resulting ciphertext has been intercepted. You are asked to break the encryption and recover the plaintext message. What is the first thing you should do? Be specific.

   Count the number of occurences of each ciphertext symbol to begin a statistical analysis attack.

2. **[6 points]** Encrypt the message "spy found" using the shift cipher with key $k = 3$.

a	b	c	...	z
d	e	f		c

   s p y f o u n d

   v s b i r x q g $\Rightarrow$ $\boxed{\text{VSBIR XQG}}$

3. **[4 parts, 4 points each]** For the given pairs (a, b), find the quotient q and remainder r when a is divided by b.

   (a) $a = 0$, $b = 5$

   $0 = 0 \cdot 5 + 0$

   $\boxed{q = 0, \ r = 0}$

   (b) $a = 23$, $b = 8$

   $23 = (2)(8) + 7$

   $\boxed{q = 2, \ r = 7}$

   (c) $a = 35$, $b = -4$

   $35 = (-8)(-4) + 3$

   $\boxed{q = -8, \ r = 3}$

   (d) $a = -50$, $b = 7$

   $-50 = (-8)(7) + 6$

   $\boxed{q = -8, \ r = 6}$

4. **[6 points]** Suppose that a and b are integers, $a \mid b$, and $b \mid a$. What can we conclude about a and b?

We have $|a| = |b|$ or $a = \pm b$.

5. **[6 points]** Let a, b, and c be positive integers. One of the following statements is true and the other is false. Identify the **false** statement and give examples of integers a,b, and c which show the statement is false.

(a) If $ab \mid c$, then $a \mid c$ and $b \mid c$. True | (b) If $a \mid bc$, then $a \mid b$ or $a \mid c$. False

(b) is False. If $a = 6$, $b = 2$, and $c = 3$, then $a \mid bc$ (since $6 \mid 6$) but $a \nmid b$ (since $6 \nmid 2$) and $a \nmid c$ (since $6 \nmid 3$).

6. **[10 points]** Let $a = 61903$, $b = 40267$, and $d = \gcd(a, b)$. Use the extended Euclidean algorithm to find d and integers u, v such that $ua + vb = d$.

$$\begin{array}{r} 61903 \\ 40267 \\ \hline 21636 \end{array} \quad \begin{array}{r} 40267 \\ 21636 \\ \hline 18631 \end{array} \quad \begin{array}{r} 21636 \\ 18631 \\ \hline 3005 \end{array}$$

$$61903 = (1)(40267) + 21636$$
$$40267 = (1)(21636) + 18631$$
$$21636 = (1)(18631) + 3005$$
$$18631 = (6)(3005) + 601$$
$$3005 = (5)(601) + 0$$

$$\gcd(a,b) = \gcd(601, 0) = 601$$

$$\begin{aligned}
601 &= 18631 + (-6)(3005) \\
&= 18631 + (-6)[21636 - (1)(18631)] \\
&= (7)(18631) + (-6)(21636) \\
&= (7)[40267 - (1)(21636)] + (-6)(21636) \\
&= (7)(40267) + (-13)(21636) \\
&= (7)(40267) + (-13)[61903 + (-1)(40267)] \\
&= (20)(40267) + (-13)(61903)
\end{aligned}$$

So $(d, u, v) = \boxed{(601, -13, 20)}$ and

$$\boxed{601 = (-13)(61903) + (20)(40267)}$$

7. **[2 parts, 6 points each]** EEA analysis. Suppose $a \geq b$.

   (a) How many arithmetic operations does the extended Euclidean algorithm perform when called on inputs a and b?

   At most $\boxed{O(\log b)}$ operations.

   (b) In what sense does the extended Euclidean algorithm perform a linear number of arithmetic operations?

   The number of arithmetic operations is linear in the number of bits it takes to represent b, so EEA performs a linear number of operations in the size of the inputs

8. **[2 parts, ~~5~~ 6 points each]** Give the following tables.

   (a) The addition table for $\mathbb{Z}_5$.

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

   (b) The multiplication table for $\mathbb{Z}_5$.

·	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

9. **[6 points]** List all the members of the ring $\mathbb{Z}_{21}$ that **do not** have inverses.

   These are all $a \in \mathbb{Z}_{21}$ such that $\gcd(a, 21) \neq 1$, so $3|a$ or $7|a$:

   $\boxed{0, 3, 6, 7, 9, 12, 14, 15, 18}$

10. [~~6~~ 8 **points**] Suppose that $a \equiv a' \pmod{m}$ and $b \equiv b' \pmod{m}$. Prove that $a + b \equiv a' + b' \pmod{m}$.

Since $a \equiv a' \pmod m$, we know $m \mid a - a'$ and so $a - a' = km$ for some $k \in \mathbb{Z}$. Similarly, since $b \equiv b' \pmod m$, we have $b - b' = lm$ for some $l \in \mathbb{Z}$. Solving these equations for a and b gives

$$a = a' + km \qquad b = b' + lm$$

and adding these gives $a + b = a' + km + b' + lm$. Rearranging, we have $(a+b) - (a'+b') = (k+l)m$. Therefore $m \mid (a+b) - (a'+b')$ which means $a + b \equiv a' + b' \pmod m$.

$373 \times 4 = 1492$

Remove for space & Time

11. [8 **points**] Let $m = 1823$. Find the inverse of 373 in $\mathbb{Z}_m$ if it exists.

EEA(373, 1823):

$1823 - 1492 = 331$

$1823 = (4)(373) + 331$

$373 = (1)(331) + 42$

$331 - 294 = 37$

$331 = (7)(42) + 37$

$42 = (1)(37) + 5$

$37 = (7)(5) + 2$

$5 = (2)(2) + 1$

$2 = (2)(1) + 0 \Rightarrow$ GCD is 1

$1 = 5 + (-2)(2)$
$= 5 + (-2)[37 + (-7)(5)]$
$= (15)(5) + (-2)(37)$
$= (15)[42 + (-1)(37)] + (-2)(37)$
$= (15)(42) + (-17)(37)$
$= (15)(42) + (-17)(331 + (-7)(42))$
$= (134)(42) + (-17)(331)$
$= (134)[373 + (-1)(331)] + (-17)(331)$
$= (134)(373) + (-151)(331)$

$1 = (134)(373) + (-151)(331)$
$= (134)(373) + (-151)(m - 4 \cdot 373)$
$= (134 + 4 \cdot 151)(373) + (-151)m$
$= (738)(373) + (-151)(1823)$

So the inverse of 373 in $\mathbb{Z}_m$ is $\boxed{738}$.

12. [~~8~~ 12 **points**] Solve for x in $782x \equiv 32 \pmod{1125}$.

EEA(782, 1125):

$1125 = (1)(782) + 343$

$782 = (2)(343) + 96$

$343 = (3)(96) + 55$

$96 = (1)(55) + 41$

$55 = (1)(41) + 14$

$41 = (2)(14) + 13$

$14 = (1)(13) + 1$

$1 = 14 + (-1)(13)$
$= 14 + (-1)[41 + (-2)(14)]$
$= (3)(14) + (-1)(41)$
$= (3)[55 + (-1)(41)] + (-1)(41)$
$= (3)(55) + (-4)(41)$
$= (3)(55) + (-4)(96 - 55)$
$= (7)(55) + (-4)(96)$
$= (7)(343 - (3)(96)) + (-4)(96)$
$= (7)(343) + (-25)(96)$
$= (7)(343) + (-25)[782 - (2)(343)]$
$= (57)(343) + (-25)(782)$

$1 = (57)(1125 - 782) + (-25)(782)$
$= (57)(1125) + (-82)(782)$

So the inverse of 782 is -82.

We have

$782x \equiv 32 \pmod{1125}$

$(-82)(782)x \equiv (-82)(32) \pmod{1125}$

$1x \equiv -((80+2)(30+2))$
$\equiv -(2400 + 60 + 160 + 4)$
$\equiv -(2624) + 3375$
$\equiv \boxed{751}$

$3375 - 2624 = 751$