Student Number: 20053722 Name: Bryan Hoang

1.

(a) **Answer:**
Using Table 1.11, the ciphertext of the plaintext message is

```
IBXFEPAQLBQAAXWQWIBXFSVAXW
```

(b) **Answer:**

Table 1: The associated decryption table of Table 1.11.

d	h	b	w	o	g	u	q	t	c	j	s	y	x	z	l	i	m	a	k	f	r	n	e	v	p
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z

(c) **Answer:**
Using Table 1 to decrypt the message yields the following plaintext message:

```
The secret password is sword fish.
```

2.

(a) **Answer:**

Proof. Let $g = \gcd(a, b)$. Then $\exists\, A, B \in \mathbb{Z}$ such that $a = gA$ and $b = gB$. Then substituting the equations into the given one yields

$$\begin{aligned} 1 &= au + bv \\ &= gAu + gBv \\ &= g(Au + Bv) \end{aligned}$$

where $Au + Bv \in Z$. Therefore, g divides 1, implying that $g = 1$. □

(b) **Answer:**
It is not necessarily true that $\gcd(a, b) = 6$. For example, take $a = 1$ and $b = 2$. Then

$$a \cdot (-6) + b \cdot 6 = 6,$$

and yet $\gcd(a, b) = 1$.
Claim. In general, all possible values of $\gcd(a, b)$ divide 6, i.e., the RHS of $au + bv = 6$.

Proof. Suppose that $au + bv = c$ has a solution. Let $g = \gcd(a, b)$ and divide c by g with remainder to get

$$c = gq + r, \quad \text{with } q, r \in \mathbb{Z},\ 0 \leq r < g.$$

Then by the extended euclidean algorithm, we can find $x, y \in \mathbb{Z}$ such that $g = ax + by$. Then

$$\begin{gathered} au + bv = c = gq + r = (ax + by)q + r \\ \Rightarrow a(u - xq) + b(v - yq) = r. \end{gathered}$$

g divides the LHS since g divides both a and b, which implies that $g \mid r$. But if $0 \leq r < g$ and $g \mid r$, then we have that $r = 0$. Therefore, $c = gq$ which means that g divides c, where $c = 6$ for the specific example. □

(c) **Answer:**

(d) **Answer:**

Proof. Let's subtract one equation from the other to get

$$\begin{aligned} au + bv - au_0 - bv_0 &= 0 \\ a(u - u_0) &= -b(v - v_0). \end{aligned}$$

Dividing both sides by g yields

$$\frac{a}{g}(u - u_0) = -\frac{b}{g}(v - v_0) \tag{1}$$

We also have that

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

which, combined with part (a), gives $\gcd(\frac{a}{g}, \frac{b}{g}) = 1$. By (1), $\frac{b}{g} \mid \frac{a}{g}(u - u_0)$. Since $\frac{b}{g}$ is relatively prime to $\frac{a}{g}$, it follows that $\frac{b}{g} \mid (u - u_0)$. Thus

$$u - u_0 = \frac{b}{g}x \quad \text{for some } x \in \mathbb{Z}.$$

Along the same lines of reasoning, we can also say that

$$v - v_0 = \frac{a}{g}y \quad \text{for some } y \in \mathbb{Z}.$$

Therefore,

$$u = u_0 + \frac{b}{g}x \quad \text{and } v = v_0 + \frac{a}{g}y.$$

Substituting it into (1) gives

$$\begin{aligned} \frac{a}{g}\frac{b}{g}x &= -\frac{b}{g}\frac{a}{g}y \\ \Rightarrow x &= -y. \end{aligned}$$

If we let $k = x$, then we have

$$u = u_0 + \frac{b}{g}k \quad \text{and } v = v_0 + \frac{a}{g}k.$$

□

3.

(a) **Answer:**

$$x \equiv 23 - 17 \equiv \boxed{6} \pmod{n}.$$

(c) **Answer:**
The squares modulo 11 are $0^2 \equiv 0, 1^2 \equiv 1, 2^2 \equiv 4, 3^2 \equiv 9, 4^2 \equiv 5, 5^2 \equiv 3, 6^2 \equiv 3, 7^2 \equiv 5, 8^2 \equiv 9, 9^2 \equiv 4$, and $10^2 \equiv 1$. Then with $5^2 \equiv 3$ and $6^2 \equiv 3$, the two solutions are $\boxed{x = 5 \text{ and } x = 6}$.

(f) **Answer:**
By substituting in $x = 0, 1, 2, \cdots, 10$ into $x^3 - x^2 + 2x - 2$ and reducing modulo 11, the three values that satisfy the equation are $\boxed{x = 1,\ x = 3, \text{ and } x = 8}$.

(g) **Answer:**

The solutions to $x \equiv 2 \mod 7$ satisfying $0 \leq x \leq 34$ are 2, 9, 16, 23, and 30. Reducing them modulo 5 respectively gives 2, 4, 1, 3, and 0. Therefore, the solution is $\boxed{x = 16}$.

4. **Answer:**

Proof.

Part 1. First, let's assume that m is prime.

Let $a \in \mathbb{Z}$ be such that $1 \leq a < m$ and let $g = \gcd(a, m)$. Then $g \mid m$, which, combined with the fact that m is prime, implies that either $g = 1$ or $g = m$. But $g \mid a$ and $1 \leq a < m$ as well, which implies that $a = 1$.

Then $\forall a \in \mathbb{Z}$ such that $1 \leq a < m$, we have that $\gcd(a, m) = 1$. Therefore,

$$\begin{aligned}\phi(m) &= \#\{1 \leq a < m : \gcd(a, m) = 1\} \\ &= \#\{1, 2, \cdots, m-1\} \\ &= m - 1\end{aligned}$$

Part 2. Now assume that $\phi(m) = m - 1$.

Then $\forall a \in \mathbb{Z}$ such that $1 \leq a < m$, we have that $\gcd(a, m) = 1$. Suppose that $a \mid m$ and that $a \neq m$. Then $1 \leq a < m$, so $\gcd(a, m) = 1$. But $a \mid m \Rightarrow \gcd(a, m) = a$. Therefore $a = 1$. Since the only dividors of m are 1 and m, we have that m is prime.

□

5.

(a) **Answer:**

$$\boxed{x = 31}$$

(b) **Answer:**

$$\boxed{x = 5764}$$

(c) **Answer:**

$$\boxed{x = 221}$$

(d) Note that the proposition to prove is a case of the Chinese remainder theorem.

Answer:

Proof. Assume that $\gcd(m, n) = 1$. Then for any $y \in \mathbb{Z}$, the solutions to the first congruence are of the form $x = +my$. Substituting in the second congruence gives

$$a + my \equiv b \pmod{n},$$

which implies that, we need to find $z \in Z$ such that

$$\begin{aligned}a + my - b &= nz \\ \Rightarrow my - nz &= b - a.\end{aligned}$$

By assumption, $\gcd(m, n) = 1$, so $\exists\, u, v \in \mathbb{Z}$ satisfying

$$\begin{gathered}mu + nv = 1 \\ \Rightarrow mu(b - a) + nv(b - a) = b - a.\end{gathered}$$

Student Number: 20053722 Name: Bryan Hoang

Now we can set $y = u(b - a)$ and $z = v(b - a)$. Thus,

$$x = a + mu(b - a) = a + (1 - nv)(b - a) = b + nv(b - a),$$

which shows that $x \equiv u \pmod{m}$ and $x \equiv v \pmod{n}$. □

6. **Answer:**

7. **Answer:**

8. **Answer:**

9. **Answer:**

10. **Answer:**

11. **Answer:**

12. **Answer:**

13. **Answer:**

14. **Answer:**

15. **Answer:**