Suggested reading: Trappe-Washington Ch 3.3-3.4

1. Let $a, n \in \mathbb{Z}$, $n > 0$.
   (a) Suppose that a is a unit modulo n. Show that the multiplicative inverse of the congruence class $[a]$ is unique. This justifies referring to "the" multiplicative inverse of $[a]$ and using the notation $[a]^{-1}$. *Hint:* Suppose that the congruence classes $[b]$ and $[c]$ are both multiplicative inverses of $[a]$ modulo n; the goal is to show they are equal. Consider the product $[b][a][c]$.
   (b) If $\gcd(a, n) = 1$, show that the equation $ax \equiv d \pmod{n}$ has exactly one solution $[x]$ in $\mathbb{Z}/n\mathbb{Z}$. Conclude that there is a unique integer solution $x = t \in \mathbb{Z}$ with $0 \leq t < n$.

2. To receive credit for this question, submit your solution to Problem 3 typeset in Latex, using `Template.tex`. Use the "theorem" environment to state the result, and the "proof" environment to type your proof.

   Some useful commands (used in math environments):

`\equiv`	outputs	$\equiv$	
`2 \pmod{3}`	outputs	$2 \pmod 3$	
`\mathbb{Z}`	outputs	$\mathbb{Z}$	("bb" stands for "blackboard bold")
`a \; \vert \; b`	outputs	$a \mid b$	(The `\;` commands create small spaces)

3. If $a, b \in \mathbb{Z}$ and $3 \mid (a^2 + b^2)$, prove that $3 \mid a$ or $3 \mid b$.
   Hint: Consider the possibilities for the congruence classes of a, b, and $a^2 + b^2 \pmod 3$.

4. In this question we will verify the textbook's procedure for finding solutions for $ax \equiv b \pmod{n}$ when $\gcd(a, n) = d$ (page 74).
   (a) As a warm-up, verify what happens to the 12 congruence classes modulo 12 when they are reduced modulo 4. Verify that each class modulo 4 (considered as a set of integers) is a union of congruence classes modulo 12.
   (b) Suppose that n is a positive integer with divisor k. Show that if a congruence class modulo n reduces to the class $[c]$ modulo k, it must have been one of the $\frac{n}{k}$ classes
   $$[c], \quad [c+k], \quad [c+2k], \quad \ldots, \quad [c+\left(\frac{n}{k}-1\right)k] \qquad \text{modulo } n.$$
   (c) Suppose that $ax \equiv b \pmod{n}$ with $\gcd(a, n) = d$. Show that if $[x_0]$ modulo $\frac{n}{d}$ is a solution to
   $$\left(\frac{a}{d}\right)x \equiv \left(\frac{b}{d}\right) \pmod{\frac{n}{d}},$$
   then the solutions to $ax \equiv b \pmod{n}$ are exactly the congruence classes
   $$[x_0], \quad [x_0 + \frac{n}{d}], \quad [x_0 + 2\left(\frac{n}{d}\right)], \quad \ldots, \quad [x_0 + (d-1)\left(\frac{n}{d}\right)] \qquad \text{modulo } n.$$

5. Find all solutions to each of the following equations. Show your work.
   (a) $5x + 3 \equiv 7 \pmod 8$
   (b) $4x \equiv 12 \pmod{20}$
   (c) $10x \equiv 8 \pmod{25}$

6. In this question, we will let the letters of the alphabet represent congruence classes modulo 26 as follows:

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
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

To facilitate encoding and decoding, you may wish to use an online program such as: `http://rumkin.com/tools/cipher/affine.php`. They denote α by a and β by b.

(a) Read Chapter 2 of the textbook up to the end of Section 2.2 (ie, pages 12-16). State the definition of an *affine cipher*.

(b) Show that the affine function

$$x \longmapsto \alpha x + \beta \pmod{26}$$

is invertible if and only if $\gcd(\alpha, 26) = 1$. In the case that it is invertible, write down its inverse (in terms of α^{-1}).

(c) The following text was encoded using an invertible affine function $x \longmapsto \alpha x + \beta \pmod{26}$.

G CGRVWCGRMOMGT MA G FWZMOW NKJ RIJTMTE OKNNWW MTRK RVWKJWCA - GLNJWF JWTYM KT BGIL WJFKA

Suppose that you correctly guess that "MA G" encodes the words " is a". Find the affine function used to encode this message. Show your work.

(d) Find the inverse of the affine function in part (c). Show your work.

(e) Decode the message from part (c).

7. (a) State the general form of the Chinese Remainder Theorem.

(b) Find the unique solution $[x]$ modulo $(4)(3)(5) = 60$ to the system of simultaneous congruences

$$x \equiv 2 \pmod 4 \qquad x \equiv 1 \pmod 3 \qquad x \equiv 3 \pmod 5.$$

(c) Find an example of integers m, n, a, b where $\gcd(m, n) \neq 1$ so that

$$x \equiv a \pmod m \qquad x \equiv b \pmod n$$

has no solutions, and an example of m, n, a, b as above where the system has more than one solution.

8. Find all solutions x to the equation $x^2 \equiv 1 \pmod{77}$, using a method other than simply squaring all 77 congruence classes. (Note that $77 = (7)(11)$ is a product of distinct primes). Explain how you know that your method finds every solution.