Exercises to turn in:

- 1. In each case determine whether the statement is true or false. (A calculator will be useful for the larger numbers.)
 - (a) $40 \equiv 13 \pmod{9}$ (b) $-29 \equiv 1 \pmod{7}$ (c) $8 \equiv 48 \pmod{14}$ (d) $-8 \equiv 48 \pmod{14}$
 - (e) $7754 \equiv 357482 \pmod{3643}$ (f) $4015 \equiv 33303 \pmod{1295}$
- 2. In each case find all integers k making the statement true.
 - (a) $4 \equiv 2k \pmod{7}$ (b) $12 \equiv 3k \pmod{10}$ (c) $3k \equiv k \pmod{9}$ (d) $5k \equiv k \pmod{15}$
- 3. Find all incongruent solutions to each of the following congruences.

(a)	$7x \equiv 3 \pmod{15}$	(b)	$6x \equiv 5 \pmod{15}$
(c)	$3x \equiv 1 \pmod{12}$	(d)	$3x \equiv 1 \pmod{11}$
(e)	$15x \equiv 5 \pmod{17}$	(f)	$5x \equiv 5 \pmod{18}$
(g)	$x^2 \equiv 1 \pmod{8}$	(h)	$x^2 \equiv 3 \pmod{7}$

- 4. Determine the number of incongruent solutions for each of the following congruences. You need not write down the actual solutions.
 - (a) $72x \equiv 47 \pmod{200}$
 - (b) $1537x \equiv 2862 \pmod{6731}$
- 5. If $a \in \mathbb{Z}$ and n > 1 then a *multiplicative inverse of a mod* n is a solution of the congruence $ax \equiv 1 \pmod{n}$.
 - (a) Explain how Theorem 8.1 (Page 57) of the handout shows that a has a multiplicative inverse mod n if and only if the greatest common divisor (a, n) = 1. Note that this theorem also shows you explicitly how to *find* the multiplicative inverse of $a \mod n$, when it exists.
 - (b) Find the inverse of 13 mod 35.
 - (c) Find the inverse of 9 mod 16.
- 6. Let $n = d_k d_{k-1} \cdots d_2 d_1 d_0$ be the decimal representation of n. Recall that this means that

 $n = d_k 10^k + d_{k-1} 10^{k-1} + \dots + d_2 10^2 + d_1 10 + d_0,$

and each d_j is an integer between 0 and 9.

- (a) Show that 3|n if and only if $3|(d_0 + d_1 + \cdots + d_k)$.
- (b) Show that 11|n if and only if $11|(d_0 d_1 + d_2 d_3 + \cdots \pm d_k)$.

Hint: Use the congruences $10 \equiv 1 \pmod{3}$ and $10 \equiv -1 \pmod{11}$ and the rules of congruence arithmetic on Page 53 of the handout.