MATH 115, SUMMER 2012
MIDTERM EXAM
WEDNESDAY, JULY 18TH

JAMES MCIVOR

The exam is out of 180 points. You have the full class time (1 hour, fifty minutes) to complete it. No calculators or cheat sheets are allowed, and do not use your cellphone, etc... You must explain your work clearly in complete English sentences for full credit. The letter p always stands for a prime number.

Problem 1 (40 pts)	
Problem 2 (15 pts)	
Problem 3 (10 pts)	
Problem 4 (10 pts)	
Problem 5 (20 pts)	
Problem 6 (15 pts)	
Problem 7 (5 pts)	
Problem 8 (15 pts)	
Problem 9 (20 pts)	
Problem 10 (15 pts)	
Problem 11 (15 pts)	

(1) (5 points each) True or False. Give very brief reasons for your answers.
(a) Let $m, c > 0$. If $a \equiv b \mod mc$ then $a \equiv b \mod m$.

(b) Let $m, c > 0$. If $a \equiv b \mod m$ then $a \equiv b \mod mc$.

(c) If $m = pq$, with p, q distinct primes, then $\phi(m) \equiv 1 - p - q \mod m$.

(d) If the ring $\mathbb{Z}/m$ contains zerodivisors, then m is composite.

(e) If $a|c$ and $b|c$, then $ab|c$.

(f) If $p \equiv 1 \mod 4$, then the congruence $x^2 \equiv -1 \mod p$ has a solution.

(g) If $(ab, p) = 1$, then

$$\frac{(ab)^{p-1} - 1}{p} \equiv \frac{a^{p-1} - 1}{p} + \frac{b^{p-1} - 1}{p} \mod p$$

(h) 4 is a primitive root mod 5.

(2) (15 points) Find the smallest positive integer a such that $3^{52} \equiv a \mod 40$.

(3) (10 points) Find the gcd of 234 and 108 and express it as a $\mathbb{Z}$-linear combination of 234 and 108.

(4) (10 points) Explain why the equation

$$72x - 42y = 112$$

has no solutions in integers x, y.

(5) (20 points) Solve the following system of congruences for x:

$$\begin{aligned} x &\equiv 1 \quad \bmod 4 \\ x &\equiv 3 \quad \bmod 5 \\ x &\equiv 5 \quad \bmod 7 \end{aligned}$$

Be sure to describe *all* solutions.

(6) (15 points) Find *all* solutions, if any, to the congruence

$$12x \equiv 18 \quad \bmod 30$$

(7) (5 points) Compute $\phi(140)$.

(8) (15 points) Solve the congruence

$$x^2 + x \equiv 0 \mod 27$$

(9) (20 points) Determine whether the following congruences have a solution. Justify your answer carefully.
  (a) $x^2 \equiv 101 \mod 61$
  (b) $x^2 + 90 \equiv 0 \mod 19$

(10) (15 points) Prove that the congruence

$$(x^2 - 2)(x^2 - 17)(x^2 - 34) \equiv 0 \mod p$$

has a solution for every odd prime p.

(11) (15 points) Let p be a odd prime, and q a prime factor of $2^p - 1$. Prove that the order of 2 mod q is p, and that therefore $p|(q-1)$.