ALGEBRAIC SYSTEMS
Exam 1
September 26, 2007

The point value of each problem is given in the margin. You may use a calculator to check your
answers, but show all work here. Total = 80 points.

(8) 1. Prove the cancellation law for multiplication of integers, justifying each step of the proof.
If \(ax = ay\) and \(a \neq 0\) then \(x = y\).

(Do not use division or mult. inverses but you may assume the following Lemma: If \(u - v = 0\) then \(u = v\).)

Proof.

(10) 2. Use the Euclidean Algorithm to find the greatest common divisor \(d\) of 99 and 143 and
find integers \(x, y\) such that \(99x + 143y = d\). (You can use any method you like.)
(3) Prove by induction that for any positive integer $n$, 
$$\sum_{k=1}^{n} k2^{k-1} = 2^n(n - 1) + 1.$$ 

(4) Use properties of congruences to compute the following numbers modulo 7. Find the least positive values. (Make the arithmetic as easy as possible.)

(a) $711 \cdot 709 - 2106 \pmod{7}$

(b) $69^8 + 71^5 \pmod{7}$

(5) Find $2^{123} \pmod{31}$. 
6. Prove that if $d, a, b$ are integers with $d|a$ and $d|b$ then $d|(a - b)$. (Just use definition of divisibility.)

7. Prove that any positive integer $n > 1$ can be expressed as a product of primes.

8. a) Express the congruence class $[4]_{20}$ in set builder notation.

b) What integers have multiplicative inverses $\pmod{20}$. (List all such values from 1 to 20.)

c) Solve the congruence $3x \equiv 14 \pmod{20}$.
9. Prove that if \( \gcd(a, m) = 1 \) then \( a \) has a multiplicative inverse \((\mod m)\).

10. a) Find the continued fraction expansion of \( \sqrt{3} = 1.7320508... \) (Use a calculator. Go down far enough to discover a pattern.)

b) Find the first five convergents of the continued fraction for \( \sqrt{3} \). Start with \( \frac{1}{1} \). Express your answers as reduced fractions.

(3) EXTRA CREDIT: Derive the continued fraction expansion for \( \sqrt{3} \) without the use of a calculator.