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:
If \( ax = ay \) and \( a \neq 0 \) then \( x = y \). (Do not use division or mult. inverses.)

Proof. \( ax = ay \), given
\[ \Rightarrow ax - ay = ay - ay \] subtract \( ay \) from both sides
\[ \Rightarrow ax - ay = 0 \] additive inverses
\[ \Rightarrow a(x - y) = 0 \] distributive law
\[ \Rightarrow x - y = 0 \] since \( a \neq 0 \), by integral domain property of \( \mathbb{Z} \).
\[ \Rightarrow x = y \] basic lemma.

You may assume lemma: \( u - v = 0 \Rightarrow u = v \).

(10) 2. Use the Euclidean Algorithm to find the greatest common divisor \( d \) of 99 and 143 and find integers \( x, y \) such that \( 99x + 143y = d \). Any method.

I

\[ 143 = 1 \cdot 99 + 44 \]
\[ 99 = 2 \cdot 44 + 11 \]
\[ 44 = 4 \cdot 11 + 0 \]

\[ \gcd(143, 99) = \gcd(143 - 99, 99) = \gcd(44, 99) = \gcd(44, 11) = \gcd(0, 11) = 11 \]

II

| \( x \) | 0 | 1 | 1 | 3 | -13 |
| \( y \) | 1 | 0 | 1 | -2 | 9 |

\[ 99x + 143y = 11 \]

You can do it either way.
3. Prove by induction that for any positive integer \( n \), \( \sum_{k=1}^{n} k2^{k-1} = 2^n(n-1) + 1 \).

For \( n = 1 \), the statement is \( 0 = 2^0 = 2^1(1-1) + 1 \), which is true.

Assume the statement is true for \( n \) and consider \( n+1 \):

\[
\sum_{k=1}^{n+1} k \cdot 2^{k-1} = \sum_{k=1}^{n} k \cdot 2^{k-1} + (n+1) \cdot 2^{(n+1)-1}
\]

\[
= 2^n(n-1) + 1 + (n+1) \cdot 2^n, \text{ by induction assumption}
\]

\[
= 2^n(n+1) + 1 = 2^n(2n) + 1
\]

\[
= 2^{n+1}n + 1 = 2^{n+1}((n+1)-1) + 1, \quad Q.E.D.
\]

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

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

\[
\equiv 4 \cdot 2 - 6 \pmod{7}
\]

\[
\equiv 8 - 6 \equiv 2 \pmod{7}
\]

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

\[
\equiv (-1)^5 + 1^5 \equiv 1 + 1 \equiv 2 \pmod{7}
\]

5. Find \( 2^{123} \pmod{31} \).

Note, \( 2^5 \equiv 32 \equiv 1 \pmod{31} \). Thus

\[
2^{123} \equiv (2^5)^{24} \cdot 2^3 \equiv 1^{24} \cdot 2^3 \equiv 8 \pmod{31}
\]
6. Prove that if \( d, a, b \) are integers with \( d | a \) and \( d | b \) then \( d | (a - b) \). (Just use definition of divisibility.)

\[
\begin{align*}
    d | a & \Rightarrow d \cdot k = a \text{ for some } k \in \mathbb{Z}. \\
    d | b & \Rightarrow d \cdot l = b \text{ for some } l \in \mathbb{Z}.
\end{align*}
\]

Thus \( a - b = d \cdot k - d \cdot l = d \cdot (k - l) \).

Since \( k - l \in \mathbb{Z} \) we conclude that \( d | (a - b) \).

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

We'll use the strong form of induction, starting with \( n = 2 \), when \( n = 2 \), \( n \) is a prime, so the statement is true.

Suppose now that all positive integers less than \( n \) can be expressed as a product of primes, and consider the value \( n \). If \( n \) is a prime we are done. Otherwise \( n = ab \) for some \( a, b \in \mathbb{N} \) with \( 1 < a < n, 1 < b < n \). By assumption \( a = p_1 p_2 \cdots p_k, b = q_1 q_2 \cdots q_l \) for some primes \( p_1, p_2, \ldots, p_k \) and \( q_1, q_2, \ldots, q_l \). Thus

\[
\begin{align*}
    n &= ab \\
    &= p_1 p_2 \cdots p_k q_1 q_2 \cdots q_l, \text{ a product of primes.} \quad \text{Q.E.D.}
\end{align*}
\]

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

\[
\left[ 4 \right]_{20} = \{ x \in \mathbb{Z} : x \equiv 4 \pmod{20} \} = \{ 4 + 20k : k \in \mathbb{Z} \}
\]

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

\[
\{ 1, 3, 7, 9, 11, 13, 17, 19 \}
\]

All \( a \) with \( \gcd(a, 20) = 1 \)

c) Solve the congruence \( 3x \equiv 14 \pmod{20} \).

\[
\begin{align*}
    3x & \equiv 14 \pmod{20} \\
    \Rightarrow 7(3x) & \equiv 7 \cdot 14 \pmod{20} \\
    \Rightarrow x & \equiv 98 \pmod{20} \\
    \Rightarrow x & \equiv 18 \pmod{20}
\end{align*}
\]
9. Prove that if $\gcd(a, m) = 1$ then $a$ has a multiplicative inverse $(\mod m)$. 

Suppose $\gcd(a, m) = 1$. Then $ax + my = 1$ for some $x, y \in \mathbb{Z}$.

$$\Rightarrow ax + 0 = 1 \pmod{m}$$

$$\Rightarrow ax = 1 \pmod{m}$$

$$\Rightarrow x \text{ is the mult inverse of } a \pmod{m}.$$ 

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

$$\sqrt{3} = 1 + \frac{1}{1 + \frac{1}{\sqrt{3} - 1}} = 1 + \frac{\sqrt{3} + 1}{2}$$

$$= 1 + \frac{1}{1 + \frac{1}{\sqrt{3} - 1}} = 1 + \frac{\sqrt{3} + 1}{2}$$

$$= 1 + \frac{1}{1 + \frac{\sqrt{3} - 1}{2}} = 1 + \frac{1}{1 + \frac{2}{\sqrt{3} - 1}}$$

$$= 1 + \frac{1}{1 + \frac{1}{\sqrt{3} + 1}} = 1 + \frac{1}{1 + \frac{2 + (\sqrt{3} - 1)}{2}}$$

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

\[
\begin{array}{cccccccc}
0 & 1 & 1 & 2 & 1 & 2 & & & \\
1 & 1 & 2 & 5 & 7 & 19 & & & \\
& 1 & 1 & 3 & 4 & 11 & & & \\
\end{array}
\]

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

$$\sqrt{3} = 1 + \frac{1}{\sqrt{3} - 1} = 1 + \frac{1}{\frac{\sqrt{3} + 1}{2}}$$

$$= 1 + \frac{\sqrt{3} + 1}{2}$$

and the process repeats (goto *).