Name: Chad Mullikin

Test 2

Spring 2003

CS/MATH 2610

March 4, 2003

Directions : You have 75 minutes to complete all 7 problems on this exam. There are a possible 100 points to be earned. You may not use your book or any notes. Please be sure to show all pertinent work. *An answer with no work will receive very little credit!* If any portion of the exam is unclear please come to me and I will elaborate provided I can do so without giving away the problem.

(1) (20 points)

Let A be a set and let $a, b, m \in \mathbb{Z}$ with $m > 0$. Answer each of the following questions.

(a) Define what it means for A to be countably infinite.

(b) Define the statement $a \mid b$.

(c) Define $\gcd(a, b)$.

(d) What does it mean to say the integers $a_1, a_2, \ldots, a_n$ are pairwise prime?

(e) Define the statement $a \equiv b$ (mod m).

Solution :

(a) The set A is countably infinite iff there exists a bijection $f : A \longrightarrow \mathbb{N}$.

(b) $a|b$ iff there exists $s \in \mathbb{Z}$ so that $b = sa$.

(c) The $\gcd(a, b)$ is the largest integer dividing a and b.

(d) It means $\gcd(a_i, a_j) = 1$ whenever $i \neq j$.

(e) $a \equiv b$ (mod m) iff $m|(a - b)$.

(2) (10 points)

(a) Convert the number 123 from decimal into binary.

(b) Convert the number $(237)_8$ from octal into decimal.

Solution :

(a)

$$\begin{aligned} 123 &= 2(61) + 1 \\ 61 &= 2(30) + 1 \\ 30 &= 2(15) + 0 \\ 15 &= 2(7) + 1 \\ 7 &= 2(3) + 1 \\ 3 &= 2(1) + 1 \\ 1 &= 2(0) + 1. \end{aligned}$$

So, $(1111011)_2 = 123$.

(b)

$$\begin{aligned} (237)_8 &= 2 \cdot 8^2 + 3 \cdot 8^1 + 7 \cdot 8^0 \\ &= 2 \cdot 64 + 3 \cdot 8 + 7 \cdot 1 \\ &= 128 + 24 + 7 \\ &= 159. \end{aligned}$$

(3) (10 points)

Recall that Caesar's cipher is obtained by enumerating the letters as $A = 0$, $B = 1$, ..., $Z = 25$ and encoding messages by encoding the corresponding numbers by $f(p) = (p+3)$ (mod 26). Suppose that the message "BRY ZLQ" has been encoded with this cipher. Decode the message.

Solution : Recall that to undo this cipher we hit the number corresponding to each letter with the function $f(p) = (p - 3)$ (mod 26). Note that if we list the letters of the alphabet by $A = 0, B = 1, C = 2, \ldots, Y = 24, Z = 25$ we see that $BRXZLQ$ corresponds to the numbers 1, 17, 23, 25, 11, and 16. So,

$$f(1) = 1 - 3 \text{ (mod 26)} = -2 \text{ (mod 26)} = 24$$
$$f(17) = 17 - 3 \text{ (mod 26)} = 14 \text{ (mod 26)} = 14$$
$$f(23) = 23 - 3 \text{ (mod 26)} = 20 \text{ (mod 26)} = 20$$
$$f(25) = 25 - 3 \text{ (mod 26)} = 22 \text{ (mod 26)} = 22$$
$$f(11) = 11 - 3 \text{ (mod 26)} = 8 \text{ (mod 26)} = 8$$
$$f(16) = 16 - 3 \text{ (mod 26)} = 13 \text{ (mod 26)} = 13$$

Which after exchanging these numbers for letters we obtain the phrase "YOUWIN."

(4) (15 points)
Use the Euclidean Algorithm to compute $\gcd(135, 532)$. (You will receive very few points if you do not use the Euclidean Algorithm).

Solution : As is instructed, we will use the Euclidean Algorithm.

$$
\begin{aligned}
532 &= 135(3) + 127 \\
135 &= 127(1) + 8 \\
127 &= 8(15) + 7 \\
8 &= 7(1) + 1 \\
7 &= 1(7) + 0.
\end{aligned}
$$

It follows that $\gcd(135, 532) = 1$ since this is the last nonzero remainder.

(5) (10 points)

Solve the following linear congruence.

$$135x \equiv 17 \pmod{532}$$

Solution : We need to find an inverse of 135 modulo 532. So, we reverse engineer the Euclidean Algorithm using the data from the last problem.

$$\begin{aligned} 1 &= 8 - 7 \\ &= 8 - (127 - 8(15)) \\ &= 8(16) - 127 \\ &= (135 - 127)(16) - 127 \\ &= (135)(16) - (127)(17) \\ &= 135(16) - (532 - 135(3))(17) \\ &= 135(67) - 532(17). \end{aligned}$$

So, 67 is the inverse of 135 modulo 532. Hence,

$$\begin{aligned} 67(135)x &\equiv 67(17) \pmod{532} \\ \Rightarrow x &\equiv 1139 \pmod{532} \\ &\equiv 75 \pmod{532}. \end{aligned}$$

So, all solutions are of the form,

$$x = 75 + 532k, \text{ where } k \in \mathbb{Z}.$$

(6) (15 points)

Prove that if $a, b, c \in \mathbb{Z}$ so that $a \mid b$ and $a \mid (b + c)$, then $a \mid c$.

Solution : We will prove this directly.

Proof. Assume $a|b$ and $a|(b + c)$. Then, by definition of divide, we know that there exist $s, t \in \mathbb{Z}$ so that $b = as$ and $(b + c) = at$. We would like to show that $a|c$, that is we would like to show that there exists $k \in \mathbb{Z}$ so that $c = ak$. But, we know $b + c = at$, so $c = at + b$. Furthermore, we know $b = as$, so combining this we obtain the equation $c = at + as = a(t + s)$. Let $k = t + s$ (notice that this is an integer) and we have shown that $c = ak$ as desired. $\square$

(7) (20 points)

Is there an integer x that leaves a remainder of 1 when divided by 3, leaves a remainder of 3 when divided by 4, and also leaves a remainder of 5 when divided by 7? If so why? (You can cite a theorem.) If there is more than one such number, what are they?

Solution : This question is asking whether or not there is a solution to the system of linear congruences:

$$x \equiv 1 \text{ (mod 3)}$$
$$x \equiv 3 \text{ (mod 4)}$$
$$x \equiv 5 \text{ (mod 7)}.$$

Since $\{3, 4, 7\}$ is a set of relatively prime numbers the Chinese Remainder Theorem guarantees that there is a unique solution modulo $3 \cdot 4 \cdot 7 = 84$. Moreover, the proof of the theorem tells us how to construct the solution. Indeed,

$$x = 1(4 \cdot 7)\overline{(4 \cdot 7)}_3 + 3(3 \cdot 7)\overline{(3 \cdot 7)}_4 + 5(3 \cdot 4)\overline{(3 \cdot 4)}_7$$

is the solution generated by the proof. Note that $\overline{(4 \cdot 7)}_3 = 1$, $\overline{(3 \cdot 7)}_4 = 1$, and $\overline{(3 \cdot 4)}_7 = 3$ (you should check this). So, using these values in the above equation we find that,

$$x = 1(4 \cdot 7)(1) + 3(3 \cdot 7)(1) + 5(3 \cdot 4)(3) = 271.$$

Indeed, $271 = 3(90) + 1$, $271 = 4(67) + 3$, and $271 = 7(38) + 7$. That is x does satisfy the system of linear congruences.

All solutions to this system will be of the form

$$x = 271 + 84k, \text{ where } k \in \mathbb{Z}$$

and $x = 19$ is the unique solution modulo 84 guaranteed by the Chinese Remainder Theorem.