MATH 301, Section A01 Name SOLUTIONS
Summer, 2011
Exam 2 Student ID number____________

PART A. (8 points each) *Carefully* define each of the following terms. Use complete sentences. Give only the definition of the defined term, not related concepts or examples.

1. $a \equiv b$ $(mod\ c)$ where $a, b \in \mathbb{Z}$ and $c \in \mathbb{Z}^+$.

   $a \equiv b\ \ (mod\ \ c)$ where $a, b \in \mathbb{Z}$ and $c \in \mathbb{Z}^+$ if and only if $c|(a-b)$.

2. An inverse of an integer a modulo m where $m \in \mathbb{Z}$, $m \geq 2$.

   An inverse of a modulo m is an integer b such that $ab \equiv 1\ \ (mod\ \ m)$.

3. The Chinese Remainder Theorem

   If $m_1, \cdots, m_k$ are pairwise relatively prime integers, then the system of congruences

$$\begin{aligned} x &\equiv a_1\ \ mod\ \ m_1 \\ &\vdots \\ x &\equiv a_k\ \ mod\ \ m_k \end{aligned}$$

   has exactly one solution $mod\ \ M = m_1 m_2 \cdots m_k$.

4. Wilson's Theorem

   If p is a prime number, then $(p-1)! \equiv -1(mod\ \ p)$.

5. Fermat's Little Theorem

   If $a \in \mathbb{Z}$ and p is a prime number which does not divide a, then $a^{p-1} \equiv 1 \pmod{p}$.

PART B. (10 points each) *Carefully* do six of the following eight problems. Mark clearly the problems which you do not want graded, and put in the box below the numbers of the problems that you do not want graded:

Problems which you don't want graded:

1. Find all solutions of the linear diophantine equation $3x + 4y = 40$ such that $x \geq 1$ and $y \geq 1$.

   Since $gcd(3,4) = 1$, the diophantine equation has a solution. We see that $x = m_0 = 12$ and $y = n_0 = 1$ is a solution. [If you don't see this by inspection, you can use the Euclidean Algorithm to find m and n such that $3m+4n = 1$ and then let $m_0 = 40m$, $n_0 = 40n$.] Then every solution of the diophantine equation $3x + 4y = 40$ has the form $x = 12 - 4k$, $y = 1 + 3k = 2k$ where $k \in \mathbb{Z}$. Since we want $x \geq 1$ and $y \geq 1$, we must have $12 - 4k \geq 1$ and $1 + 3k \geq 1$, or $0 \leq k \leq \frac{11}{4}$. Therefore, we must have $k = 0, 1,$ or 2. Hence the solutions are $x = 12, y = 1$, and $x = 8, y = 2$, and $x = 4, y = 7$.

Answer:
$x = 12, y = 1$
$x = 8, y = 4$
$x = 4, y = 7$

2. Find all (integer) solutions x with $0 \le x < 9$ of the linear congruence $6x \equiv 15(mod\ 9)$, or, if there is no solution, give a reason why there is no solution.

We must solve the linear diophantine equation $6x + 9y = 15$, or $2x + 3y = 5$. Since $2 \cdot (-1) + 3 \cdot 1 = 1$, $2 \cdot (-5) + 3 \cdot 5 = 5$. Therefore, one solution is $x = -5$. Since gcd$(9,6)$ = 3, all solutions have the form $x = -5 - (\frac{9}{3})k = -5 - 3k$. There are three solutions mod 9, namely, $-5 - 3(-2) = 1$, $-5 - 3(-3) = 4$, and $-5 - 3(-4) = 7$.

Answer:
1, 4, 7

3. (a) Use the fact that an inverse of 5 *mod* 7 is 3 to find an x between 0 and 6 such that $5x \equiv 4(mod\ 7)$. You must make clear how you are using the given information.

We multiply both sides of the congruence by 3 to get

$$x \equiv 3 \cdot 5x \equiv 3 \cdot 4 \equiv 12(mod\ \ 7).$$

Since we want x to be between 0 and 6, we take $x = 5$.

Answer:
5

(b) A seven-member band charges \$5 admission for its club act. On a particular evening, there are between 50 and 56 paying members of the audience. When the money is divided among the band members equally, there is \$2 left over. How many paying members of the audience were there?

If we let x be the number of paying audience members, then the receipts for the evening are $\$5x$. Since there is \$2 left when the money is divided among the 7 band members, $5x-2$ is divisible by 7, that is, $5x \equiv 2(mod\ 7)$. Multiplying both sides of this congruence by 3, the inverse of $5(\text{mod}\ \ 7)$, gives $x \equiv 6(\text{mod}\ \ 7)$. Since x is between 50 and 56, $x = 49+6 = 55$. Therefore, there were 55 paying customers.

Answer:
55

4. (a) Find all integers between x such that $0 \leq x \leq 11$ such that x has an inverse *mod* 12.

x has an inverse *mod* 12 if and only if x is relatively prime to 12. Therefore, the integers between 0 and 11 inclusive that have inverses *mod* 12 are $1, 5, 7, 11$.

Answer:
$1, 5, 7, 11$

(b) Find an inverse between 0 and 24 of 7 *mod* 25.

We want a solution of $7x \equiv 1(mod\ 25)$. Therefore, we solve the linear diophantine equation $7x + 25y = 1$. From the Euclidean algorithm, we get

$$\begin{aligned} 25 &= 3 \cdot 7 + 4. \\ 7 &= 1 \cdot 4 + 3. \\ 4 &= 1 \cdot 3 + 1. \end{aligned}$$

Therefore, $1 = 4 - 1 \cdot 3 = 4 - 1 \cdot (7 - 1 \cdot 4) = 2 \cdot 4 - 7 = 2 \cdot (25 - 3 \cdot 7) - 7 = (-7) \cdot 7 + 2 \cdot 25$. Therefore, -7 is an inverse of $7\ mod\ 25$, and and inverse between 0 and 24 is $-7+25 = 18$.

Answer:
18

5. Use the Chinese Remainder Theorem to find a value of x such that

$$\begin{aligned} x &\equiv 1 \; mod \, 4. \\ x &\equiv 4 \; mod \, 5. \\ x &\equiv 2 \; mod \, 3. \end{aligned}$$

Let $m_1 = 4$, $m_2 = 5$, and $m_3 = 3$. Let $M = (4)(5)(3) = 60$. Let $M_1 = \frac{M}{m_1} = (5)(3) = 15$, $M_2 = \frac{M}{m_2} = (4)(3) = 12$, and $M_3 = \frac{M}{m_3} = (4)(5) = 20$. Then an inverse of M_1 mod m_1, that is, an inverse of 15 mod 4, is $y_1 = 3$; an inverse of M_2 mod m_2, that is, an inverse of 12 mod 5, is $y_2 = 3$; and an inverse of M_3 mod m_3, that is, an inverse of 20 mod 3, is $y_2 = 2$. From the proof of the Chinese Remainder Theorem, a solution to the system of congruences is given by

$$x = 1 \cdot M_1 \cdot y_1 + 4 \cdot M_2 \cdot y_2 + 2 \cdot M_3 \cdot y_3$$

so a solution is given by

$$x = (1)(15)(3) + (4)(12)(3) + (2)(20)(2) = 269.$$

Any solution is congruent to 269 mod M, and any number congruent to 269 mod M is a solution, so the smallest non-negative solution is $x = 29$.

Answer:
29

6. Find all solutions of the following system of linear congruences. If the system has no solutions, state this fact explicitly.

$$\begin{aligned} 3x + 2y &\equiv 1\ (mod\ 7) \\ 4x + y &\equiv 2\ (mod\ 7) \end{aligned}$$

Since $\Delta = (3)(1) - (2)(4) = -5 \equiv 2$ mod 7 and 2 is relatively prime to 7, the system has a unique solution mod 7. $\Delta \equiv 2\ mod\ 7$ and an inverse of 2 mod 7 is $\overline{\Delta} = 4$. Therefore, the solution is given by $x \equiv \overline{\Delta} \cdot (1 \cdot 1 - 2 \cdot 2) \equiv 4(-3) \equiv -12 \equiv 2\ mod\ 7$ and $y \equiv \overline{\Delta} \cdot (3 \cdot 2 - 1 \cdot 4) \equiv 4(2) \equiv 8 \equiv 1\ mod\ 7$

Answer:
$x \equiv 2\ (mod\ 7)$
$y \equiv 1\ (mod\ 7)$

7. Let $n = 648743092117120512$. *Without using a calculator* determine whether n is divisible by k for each of the following values of k. If n is divisible by k, circle 'YES'. If n is not divisible by k, circle 'NO'. Your work must make clear how you are getting your answer.

(a) $k = 9$

YES. The sum of the digits of n is 63 which is divisible by 9.

YES NO

(b) $k = 16$

YES. $16 = 2^4$ and the number made up of the last four digits 20512 is divisible by 16; $0512 = (16)(32)$.

YES NO

(c) $k = 6$

YES. The sum of the digits of n is 63 which is divisible by 3. Since n is divisible by 3 and is even, it is divisible by 6.

YES NO

(d) $k = 11$

NO. $6-4+8-7+4-3+0-9+2-1+1-7+1-2+0-5+1-2 = -17$ which is not divisible by 11.

YES NO

8. (a) *Without using a calculator* find the remainder when $n = 17 \cdot 16 \cdot 15 \cdot 14 \cdot 11 \cdot 10 \cdot 9 \cdot 8 \cdot 7 \cdot 6 \cdot 5$ is divided by 13.

Since $17 \equiv 4 \ (mod\ 13)$, $16 \equiv 3 \ (mod\ 13)$, $15 \equiv 2 \ (mod\ 13)$, and $11 \equiv 1 \ (mod\ 13)$, $n \equiv 11! \ (mod\ 13)$. By Wilson's Theorem, $12! \equiv -1 \ (mod\ 13)$. Since 12 is its own inverse $(mod\ 13)$, $n = 11! \equiv -12 \ (mod\ 13)$ and since $-12 \equiv 1 \ (mod\ 13)$, the remainder is 1

Answer:
1

(b) Use Fermat's Little Theorem to find the remainder when $n = 3^{17269830416891}$ is divided by 5.

By Fermat's Little Theorem, $3^4 \equiv 1 \ (mod\ 5)$. Since the last two digits of 17269830416891 are congruent to 3 mod 4, $17269830416891 \equiv 3 \ (mod\ 4)$, so there is an integer k such that $17269830416891 = 4k+3$. Therefore, $n = 3^{4k+3} = 3^{4k}3^3 \equiv 1 \cdot 3^3 \ (mod\ 5) \equiv 27 \ (mod\ 5) \equiv 2 \ (mod\ 5)$. Therefore, the remainder is 2.

Answer:
2