Math 55 Second Midterm 7 Nov 2007

NAME (1 pt): _____

TA (1 pt): _____

Name of Neighbor to your left (1 pt): _____

Name of Neighbor to your right (1 pt): _____

Instructions: This is a closed book, closed calculator, closed computer, closed network, open brain exam. You are allowed one page of notes (double sided) that can be read without a magnifying glass.

You get one point each for filling in the 4 lines at the top of this page. The values of the other questions are indicated on each page.

Write all your answers on this exam. If you need scratch paper, ask for it, write your name on each sheet, and attach it when you turn it in (we have a stapler).

1	
2	
3	
Total	

Question 1 (20 points)

1.1) (7 points) Use the Euclidean Algorithm to find an integer x such that $71x \equiv 1 \pmod{100}$.

Answer: Running the Euclidean algorithm:

$$\begin{aligned}
100 &= 1(71) + 29 \\
71 &= 2(29) + 13 \\
29 &= 2(13) + 3 \\
13 &= 4(3) + 1
\end{aligned}$$

Finding s and t such that $1 = 71s + 100t$:

$$\begin{aligned}
1 &= 13 - 4(3) \\
&= 13 - 4(29 - 2(13)) \\
&= 9(13) - 4(29) \\
&= 9(71 - 2(29)) - 4(29) \\
&= 9(71) - 22(29) \\
&= 9(71) - 22(100 - 1(71)) \\
&= 31(71) - 22(100)
\end{aligned}$$

So $x = 31$ is an inverse of 71 modulo 100.

1.2) (7 points) Find an integer x such that $3^{11}x \equiv 1 \pmod{19}$.

Answer: By Fermat's little theorem, $3^{18} \equiv 1 \pmod{19}$. Thus, $3^{11}3^7 \equiv 1 \pmod{19}$, and so $x = 3^7$ is a solution.

Another way of solving the problem is to compute $3^{11} \bmod 19$ using the algorithm for fast modular exponentiation. $3^{11} \bmod 19 = 10$, and so an inverse is $x = 2$.

1.3) (6 points) How many integers x, where $0 \leq x < 1900$, are there such that $71x \equiv 1 \pmod{100}$ and $3^{11}x \equiv 1 \pmod{19}$. Justify your answer.

Answer: By uniqueness of inverses, any x such that $71x \equiv 1 \pmod{100}$, must satisfy $x \equiv 31 \pmod{100}$. Similarly, any x such that $3^{11}x \equiv 1 \pmod{19}$ must satisfy $x \equiv 3^7 \pmod{19}$. By the Chinese remainder theorem, the system:

$$\begin{aligned}
x &\equiv 31 \pmod{100} \\
x &\equiv 3^7 \pmod{19}
\end{aligned}$$

has a unique solution modulo $19 \cdot 100 = 1900$. Thus, there is one integer $0 \leq x < 1900$ satisfying the two congruences.

Question 1 (20 points)

1.1) (7 points) Use the Euclidean Algorithm to find an integer x such that $53x \equiv 1 \pmod{100}$.

Answer: Running the Euclidean algorithm:

$$\begin{aligned}
100 &= 1(53) + 47 \\
53 &= 1(47) + 6 \\
47 &= 7(6) + 5 \\
6 &= 1(5) + 1
\end{aligned}$$

Finding s and t such that $1 = 53s + 100t$:

$$\begin{aligned}
1 &= 6 - 1(5) \\
&= 6 - 1(47 - 7(6)) \\
&= 8(6) - 1(47) \\
&= 8(53 - 1(47)) - 1(47) \\
&= 8(53) - 9(47) \\
&= 8(53) - 9(100 - 1(53)) \\
&= 17(53) - 9(100)
\end{aligned}$$

So $x = 17$ is an inverse of 53 modulo 100.

1.2) (7 points) Find an integer x such that $7^{14}x \equiv 1 \pmod{23}$.

Answer: By Fermat's little theorem, $7^{22} \equiv 1 \pmod{23}$. Thus, $7^{14}7^8 \equiv 1 \pmod{23}$, and so $x = 7^8$ is a solution.

Another way of solving the problem is to compute $7^{14} \bmod 23$ using the algorithm for fast modular exponentiation. $7^{14} \bmod 23 = 2$, and so an inverse is $x = 12$.

1.3) (6 points) How many integers x, where $0 \leq x < 2300$, are there such that $53x \equiv 1 \pmod{100}$ and $7^{14}x \equiv 1 \pmod{23}$. Justify your answer.

Answer: By uniqueness of inverses, any x such that $53x \equiv 1 \pmod{100}$, must satisfy $x \equiv 17 \pmod{100}$. Similarly, any x such that $7^{14}x \equiv 1 \pmod{23}$ must satisfy $x \equiv 7^8 \pmod{23}$. By the Chinese remainder theorem, the system:

$$\begin{aligned}
x &\equiv 17 \pmod{100} \\
x &\equiv 7^8 \pmod{23}
\end{aligned}$$

has a unique solution modulo $23 \cdot 100 = 2300$. Thus, there is one integer $0 \leq x < 2300$ satisfying the two congruences.

Question 2 (15 points) Let $a(n)$ be defined by $a(0) = 0$, $a(1) = 1$, and $a(n+1) = a(n)+a(n-1)$ for $n \geq 1$. Prove by induction that every nonnegative integer m can be written as the sum of distinct $a(i)$.

Answer: The result is clearly true for $m = 0 = a(0)$ and $m = 1 = a(1)$. Suppose it is true for $m \leq a(n)$; we will use induction to show it is true for $m \leq a(n+1)$. If $m = a(n+1)$ we are done, so assume $a(n) < m < a(n+1)$, and write $m = a(n)+(m-a(n))$. Now $m < a(n+1) = a(n)+a(n-1)$ so $0 < m - a(n) < a(n-1)$, and by induction we can write $m - a(n)$ as the sum of distinct $a(i)$ for $i < n-1$, and so $m = a(n)$ plus this sum.

Question 2 (15 points) Let $c(m)$ be defined by $c(0) = 0$, $c(1) = 1$, and $c(m+1) = c(m)+c(m-1)$ for $m \geq 1$. Prove by induction that every nonnegative integer n can be written as the sum of distinct $c(i)$.

Answer: The result is clearly true for $n = 0 = c(0)$ and $n = 1 = c(1)$. Suppose it is true for $n \leq c(m)$; we will use induction to show it is true for $n \leq c(m+1)$. If $n = c(m+1)$ we are done, so assume $c(m) < n < c(m+1)$, and write $n = c(m)+(n-c(m))$. Now $n < c(m+1) = c(m)+c(m-1)$ so $0 < n - c(m) < c(m-1)$, and by induction we can write $n - c(m)$ as the sum of distinct $c(i)$ for $i < m - 1$, and so $n = c(m)$ plus this sum.

Question 3 (20 points) You are organizing a dance with students attending from 4 classes: there are 4 freshman, 4 sophomores, 4 juniors, and 6 seniors. For one of the dances, you need to arrange 10 students to stand in a circle, all facing the center and holding hands.

3.1) (10 points) How many different circles of students can you arrange? (Two circles are the same if and only if everyone is holding hands with the same neighbors using the same hands.) You do not need to simplify your expression (eg you can leave in factorials, etc.).

Answer: There are 18 students altogether. There are P(18,10) = 18!/8! ways to arrange 10 of them in different orders standing in a row (not a circle). These orders may be grouped into groups of 10, corresponding to the same circle, depending on where you say the first person in the circle is, and going clockwise. So the answer is P(18,10)/10 = 15878903040 circles.

3.2) (10 points) How many different circles of students can you arrange if there must be exactly 1 sophomore and 1 junior, with the sophomore to the right of the junior?

*Answer: Going clockwise around the circle, one must encounter the sophomore and junior in the order SJ. The number of ways to assign the S and J is 4*4=16. The number of spaces continuing clockwise from J around to S is 8. There are P(10,8) ways to order 8 of the remaining 4 freshman and 6 seniors to fit in these spaces. Thus there are 16*P(10,8) = 16*10!/2! = 29030400 circles.*

Question 3 (20 points) You are organizing a tournament with players attending from 4 universities: there are 3 Bruins, 3 Cardinals, 3 Trojans, and 5 Bears. For one of the cheers, you need to arrange 8 players to stand in a circle, all facing the center and holding hands.

3.1) (10 points) How many different circles of players can you arrange? (Two circles are the same if and only if everyone is holding hands with the same neighbors using the same hands.) You do not need to simplify your expression (eg you can leave in factorials, etc.).

Answer: There are 14 players altogether. There are P(14,8) = 14!/6! ways to arrange 8 of them in different orders standing in a row (not a circle). These orders may be grouped into groups of 8, corresponding to the same circle, depending on where you say the first person in the circle is, and going clockwise. So the answer is P(14,8)/8 = 15135120 circles.

3.2) (10 points) How many different circles of players can you arrange if there must be exactly 1 Bruin and 1 Cardinal, with the Bruin to the right of the Cardinal?

*Answer: Going clockwise around the circle, one must encounter the Bruin and Cardinal in the order BC. The number of ways to assign the B and C is 3*3=9. The number of spaces continuing clockwise from C around to B is 6. There are P(8,6) ways to order 6 of the remaining 3 Bruins and 5 Bears to fit in these spaces. Thus there are 9*P(8,6) = 181440 circles.*