Mathematics 2513-002 Name (please print) _____

Examination III

November 14, 2005

Instructions: Give *brief,* clear answers.

I. (4) Prove that the function $f\colon \mathbb{Z}\times\mathbb{Z}\to\mathbb{Z}$ defined by $f(m,n)=m-n$ is surjective.

Let $k\in\mathbb{Z}$. Then, $(k,0)\in\mathbb{Z}\times\mathbb{Z}$ and $f(k,0)=k$.

II. (4) Using the notation $h\colon Y\to X$, define the *range* of h, the *preimage* of x for an element $x\in X$, the *image* of y for an element $y\in Y$, and the *graph* of h.

The range of h is $\{x\in X\mid \exists y\in Y, h(y)=x\}$, or $\{h(y)\mid y\in Y\}$.

The preimage of x is $\{y\in Y\mid h(y)=x\}$.

The image of y is $h(y)$.

The graph of h is the set $\{(y,h(y))\mid y\in Y\}$ (or $\{(y,x)\in Y\times X\mid x=h(y)\}$).

III. (6) Let S be the set of sequences of 0's and 1's, $S=\{a_1a_2a_3\cdots\mid a_i\in\{0,1\}\}$. A typical element of S is $001011011100011010\cdots$. Adapt Cantor's proof that $\mathbb{R}$ is uncountable to prove that S is uncountable.

Suppose for contradiction that there exists a bijective function $f\colon \mathbb{N}\to S$. List the elements $f(1)$, $f(2),\ldots$ as

$$\begin{aligned} f(1)&=a_{11}a_{12}a_{13}\cdots\\ f(2)&=a_{21}a_{22}a_{23}\cdots\\ f(3)&=a_{31}a_{32}a_{33}\cdots\\ &\vdots \end{aligned}$$

Define an element $s=b_1b_2b_3\cdots$ of S by $b_i=1$ if $a_{ii}=0$ and $b_i=0$ if $a_{ii}=1$. For all n, $b_n\neq a_{nn}$ so $s\neq f(n)$. Therefore s is an element of S which is not in the image of f, so f is not surjective. This is a contradiction, since f was a bijection.

IV. (12) Let a and b be integers, at least one of them nonzero.

1. Define the *greatest common divisor* $\gcd(a,b)$.

   $\gcd(a,b)$ is the largest integer that divides both a and b.

2. Find $\gcd(2^3\cdot3^3\cdot7^2\cdot13\cdot17, 2\cdot3^4\cdot5\cdot7\cdot17)$ and $\operatorname{lcm}(2^3\cdot3^3\cdot7^2\cdot13\cdot17, 2\cdot3^4\cdot5\cdot7\cdot17)$ (leave the results in factored form, do not multiply them out).

   For $\gcd(2^3\cdot3^3\cdot7^2\cdot13\cdot17, 2\cdot3^4\cdot5\cdot7\cdot17)$, we take the smaller power of each prime factor that appears in either a or b, obtaining $2\cdot3^3\cdot7\cdot17$. For $\operatorname{lcm}(a,b)$, we take the maximum power, obtaining $\operatorname{lcm}(2^3\cdot3^3\cdot7^2\cdot13\cdot17, 2\cdot3^4\cdot5\cdot7\cdot17)=2^3\cdot3^4\cdot5\cdot7^2\cdot13\cdot17$.

3. Assuming that both a and b are positive, describe the *Euclidean algorithm* for computing $\gcd(a,b)$.

   Take the larger of a or b and replace it by the remainder obtained when it is divided by the smaller. Repeat this process until one of the two numbers is 0, and then the greatest common divisor is the other one.

V. (3) Which positive integers less than 10 are relatively prime to 10?

Since the prime divisors of 10 are 2 and 5, they are the integers from 1 to 9 that are not even, eliminating 2, 4, 6, and 8, and not divisible by 5, eliminating 5. The remaining ones are 1, 3, 7, and 9.

VI. (4) Use the fact that $7 \cdot 8 \equiv 1 \mod 55$ to find an integer m for which $8m \equiv 11 \mod 55$.

We will "solve" the equation $8m \equiv 11 \mod 55$, using properties of congruence. Multiplying both sides of it by 7, we would have $7 \cdot 8 \cdot m \equiv 7 \cdot 11 \mod 55$, and $7 \cdot 8 \equiv 1 \mod 55$ so this becomes just $m \equiv 77 \mod 55$. That is, m can be anything of the form $55k + 77$. (This set can also be described as all numbers of the form $55k + 22$.)

VII. (6) Use induction to prove that $1 \cdot 1! + 2 \cdot 2! + \cdots + n \cdot n! = (n+1)! - 1$ whenever n is a positive integer.

For $n = 1$, we have $1 \cdot 1! = 1 \cdot 1 = 1$ and $(1+1)! - 1 = 2 - 1 = 1$, so the assertion is true for $n = 1$. Inductively, assume that $1 \cdot 1! + 2 \cdot 2! + \cdots + k \cdot k! = (k+1)! - 1$. Then, $1 \cdot 1! + 2 \cdot 2! + \cdots + k \cdot k! + (k+1) \cdot (k+1)! = (k+1)! - 1 + (k+1) \cdot (k+1)! = (1 + (k+1)) \cdot (k+1)! - 1 = (k+2) \cdot (k+1)! - 1 = (k+2)! - 1$.

VIII. (6) Prove that if there exists d so that $cd \equiv 1 \mod m$, then $\gcd(c, m) = 1$. Hint: use the theorem that says $\gcd(a, b)$ is the least positive sum of multiples of a and b.

Assume that $cd \equiv 1 \mod m$. This says that $m | cd - 1$, so there exists s so that $sm = cd - 1$ or $1 = dc + (-s)m$. By the theorem, this says that $\gcd(c, m) = 1$.

IX. (6) Adapt the argument of Cantor's proof that $\mathbb{Q}$ is countable to prove that $\mathbb{N} \times \mathbb{N}$ is countable.

Arrange the pairs (m, n) with $m, n \in \mathbb{N}$ is an infinite array:

$$\begin{array}{cccccc} (1,1) & (1,2) & (1,3) & (1,4) & \cdots \\ (2,1) & (2,2) & (2,3) & (2,4) & \cdots \\ (3,1) & (3,2) & (3,3) & (3,4) & \cdots \\ (4,1) & (4,2) & (4,3) & (4,4) & \cdots \\ \vdots & & & & \end{array}$$

The Cantor method of going up and down the diagonals allows us to turn this into a single list: $(1,1), (1,2), (2,1), (3,1), (2,2), (1,3), (1,4), (2,3), (3,2), (4,1), \ldots$. Then, we define a bijection from $\mathbb{N}$ to $\mathbb{N} \times \mathbb{N}$ by sending n to the n^{th} pair in this list.

X. (6) Use congruence to prove that 3 divides $n^3 + 2n$ for any integer n.

If $n \equiv 0 \mod 3$, then $n^3 + 2n \equiv 0^3 + 2 \cdot 0 \equiv 0 \mod 3$.
If $n \equiv 1 \mod 3$, then $n^3 + 2n \equiv 1^3 + 2 \cdot 1 \equiv 1 + 2 \equiv 0 \mod 3$.
If $n \equiv 2 \mod 3$, then $n^3 + 2n \equiv 2^3 + 2 \cdot 2 \equiv 8 + 4 \equiv 12 \equiv 0 \mod 3$.
In any case, $n^3 + 2n \equiv 0 \mod 3$, so $n^3 + 2n$ is divisible by 3.