Mathematics 2513-001 Name (please print) ______________________

Examination III Form A

April 27, 2006

Instructions: Give brief, clear answers. “Prove” means “give an argument”.

I. (4) Let $f\colon X \to Y$ and $g\colon Y \to Z$. Prove that if f and g are injective, then the composition $g \circ f$ is injective.

Assume that f and g are injective. Let $x_1, x_2 \in X$ and assume that $g \circ f(x_1) = g \circ f(x_2)$. This says that $g(f(x_1)) = g(f(x_2))$. Since g is injective, this implies that $f(x_1) = f(x_2)$. Since f is injective, this implies that $x_1 = x_2$.

II. (4) Prove that if $a \equiv b \mod m$ and $b \equiv c \mod m$, then $a \equiv c \mod m$.

Assume that $a \equiv b \mod m$ and $b \equiv c \mod m$. Then, $m|a-b$ and $m|b-c$, so $m|(a-b)+(b-c)$. Since this says that $m|a-c$, we have $a \equiv c \mod m$.

III. (4) Give Euclid's proof that there are infinitely many primes.

Suppose for contradiction that there are only finitely many primes, say $p_1, p_2, \ldots, p_k$. Put $N = p_1 p_2 \cdots p_k + 1$. Notice that no p_i divides N.

If N is prime, then it is a prime different from any of the p_i, a contradiction. If N is composite, the Fundamental Theorem of Arithmetic ensures that we can write it as $N = q_1 q_2 \cdots q_m$. But then, q_1 is a prime which divides N, so q_1 is a prime which is not equal to any of the p_i, again contradicting the fact that $p_1, p_2, \ldots, p_k$ are the only primes.

[Of course, as seen in class there are several other reasonable ways to write this proof.]

IV. (4) State the Fundamental Theorem of Arithmetic.

Any integer greater than 1 can be written as a product of prime factors. If the factors are written in nondecreasing order, then this factorization is unique.

V. (4) (a) Show that $ac \equiv bc \mod m$ and $c \not\equiv 0 \mod m$ does not always imply that $a \equiv b \mod m$.

$1 \cdot 2 \equiv 3 \cdot 2 \mod 4$ and $2 \not\equiv 0 \mod 4$, but $1 \not\equiv 3 \mod 4$.

(b) Tell without proof a condition (which always holds when m is prime and $c \not\equiv 0 \mod m$) that ensures that $ac \equiv bc \mod m$ does imply that $a \equiv b \mod m$.

$\gcd(c, m) = 1$.

VI. (5) 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, $1\cdot 1! + 2\cdot 2! + \cdots + k\cdot k! + (k+1)\cdot(k+1)! = (k+1)! - 1 + (k+1)\cdot(k+1)! = (1 + (k+1))\cdot(k+1)! - 1 = (k+2)\cdot(k+1)! - 1 = (k+2)! - 1$.

VII. (5) Let X be the set of all infinite sequences in which each term is one of the letters a, b, or c. Some elements of X are bbbbbbbbbbb$\cdots$, aabbccaabbccaabbcc$\cdots$, and abbabccbbaccbcbacbacbabcabaacbbbbaccbc$\cdots$. Using Cantor's idea, prove that there does not exist any surjective function from $\mathbb{N}$ to X.

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

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

Define a sequence $x = x_1x_2x_3\cdots$ in X by $x_i = a$ if $x_{ii} = b$ or $x_{ii} = c$, and $x_i = b$ if $x_{ii} = a$. For all n, $x_n \neq x_{nn}$ so $x \neq f(n)$. Therefore x is an element of X which is not in the range of f, contradicting the fact that f is surjective.

VIII. (4) Let Y be the set of all positive fractions (not rational numbers, so $\frac{1}{2}$ and $\frac{2}{4}$ are different fractions). Using Cantor's idea, prove that Y is countable.

Arrange the fractions m/n with $m, n \in \mathbb{N}$ is an infinite array:

$$\begin{array}{ccccc} 1/1 & 1/2 & 1/3 & 1/4 & \cdots \\ 2/1 & 2/2 & 2/3 & 2/4 & \cdots \\ 3/1 & 3/2 & 3/3 & 3/4 & \cdots \\ 4/1 & 4/2 & 4/3 & 4/4 & \cdots \\ & & \vdots & & \end{array}$$

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 the set of positive fractions by sending n to the n^{th} fraction in this list.

IX. (4) Let B be a nonempty set, so that we can choose an element b_0 of B. Prove that there exists a surjective function from $\mathcal{P}(B)$ to B.

Define $f\colon \mathcal{P}(B) \to B$ by the rule that $f(S) = b$ if S is of the form $\{b\}$, and $f(S) = b_0$ if S does not have cardinality 1. This is surjective, since if b is any element of B, then $f(\{b\}) = b$, so b is in the range of f.

X. (4) Let a, b, and c be integers. Using the definition of "divides", prove that if $a|b$ and $b|c$, then $a|c$.

Assume that $a|b$ and $b|c$. Then there exists some n such that $b = na$, and there exists some m so that $c = mb$. Therefore $c = mb = (mn)a$, so $a|c$.

XI. Let Z be an infinite set.

(5) (a) Informally, saying that Z is countable means that it is possible to list the elements of Z. This is not a real definition, since the word "list" is not precise. Give the formal definition of "Z is countable."

Z is *countable* when there exists a bijective function from $\mathbb{N}$ to Z.

(b) Now suppose that Z is set of all infinite sequences in which each term is one of the letters a, or b, and *exactly one* of the terms is b. Some elements of Y are baaaaaaa$\cdots$, aaaaaaaaabaaaaaa$\cdots$, and aaaaaaa$\cdots$aaaabaaaa$\cdots$, where in the last sequence the b appears after exactly $35,014,227$ a's have appeared. Prove that Z is countable.

Define $f\colon \mathbb{N} \to Z$ by $f(n) =$ aaaaaaa$\cdots$aaaabaaaa$\cdots$, where the b is in the n^{th} place. This is injective, since if $f(m) = f(n)$ then the b appears in the m^{th} position and the n^{th} position, and as there is only one b we must have $m = n$. Also, it is surjective, since if aaaaaaa$\cdots$aaaabaaaa$\cdots$ is any sequence in Z, then putting n equal to the place in which the b occurs, this sequence is $f(n)$.

XII. Let m and n be two positive integers. Show that if $mn = 360$ and the least common multiple of m and n

(4) is 10 times their greatest common divisor, then both m and n are divisible by 6.

In general, $mn = \mathrm{lcm}(m,n)\ \gcd(m,n)$, and in this case we have $\mathrm{lcm}(m,n) = 10\gcd(m,n)$, so $mn = 10\gcd(m,n)^2$. Since $mn = 360$, this says that $\gcd(m,n)^2 = 36$, so $\gcd(m,n) = 6$. Therefore 6 divides both m and n. [Possibilities for $\{m,n\}$ are $\{6,60\}$ and $\{12,30\}$.]