Math 220 (*Intro. to Pure Math.*) — Final Exam — Dec. 11, 2007

$(\frac{10}{100})$ 1. Prove (by induction) that $n! > 2^n$ for all $n \geq 4$.

Solution: *Base case* $(n = 4)$: $4! = 24 > 16 = 2^4$.

Induction: Let $n \geq 4$ and suppose $n! > 2^n$. Then

$$(n+1)! \ = \ (n+1) \cdot n! \ \underset{(*)}{>} \ (n+1) \cdot 2^n \ \underset{(\dagger)}{>} \ 2 \cdot 2^n \ = \ 2^{n+1},$$

as desired. Here, $(*)$ is by induction hypothesis, and $(\dagger)$ is because $n \geq 4 > 2$. □

$(\frac{10}{100})$ 2. Let $\mathbf{A}$, $\mathbf{B}$, and $\mathbf{C}$ be sets. Prove that $\mathbf{A} \setminus (\mathbf{B} \cap \mathbf{C}) \ = \ (\mathbf{A} \setminus \mathbf{B}) \cup (\mathbf{A} \setminus \mathbf{C})$, by showing that $\Big(x \in \mathbf{A} \setminus (\mathbf{B} \cap \mathbf{C})\Big) \iff \Big(x \in (\mathbf{A} \setminus \mathbf{B}) \cup (\mathbf{A} \setminus \mathbf{C})\Big)$.

Solution: Let $x \in \mathbf{A}$. Then

$$\begin{aligned}
\Big(x \in \mathbf{A} \setminus (\mathbf{B} \cap \mathbf{C})\Big) \quad &\iff \quad \Big(x \notin \mathbf{B} \cap \mathbf{C}\Big) \iff \text{not}\Big(x \in \mathbf{B} \cap \mathbf{C}\Big) \\
&\iff \quad \text{not}\Big(x \in \mathbf{B} \text{ and } x \in \mathbf{C}\Big) \iff \Big(x \notin \mathbf{B}\Big) \text{ or } \Big(x \notin \mathbf{C}\Big) \\
&\iff \quad \Big(x \in \mathbf{A} \setminus \mathbf{B}\Big) \text{ or } \Big(x \in \mathbf{A} \setminus \mathbf{C}\Big) \iff \Big(x \in (\mathbf{A} \setminus \mathbf{B}) \cup (\mathbf{A} \setminus \mathbf{C})\Big).
\end{aligned}$$

□

$(\frac{20}{100})$ 3. Let $\mathbf{A}$, $\mathbf{B}$, and $\mathbf{C}$ be sets. Let ${}^{\mathbf{B}}\mathbf{C}$ be the set of functions from $\mathbf{B}$ into $\mathbf{C}$. Let ${}^{\mathbf{A}\times\mathbf{B}}\mathbf{C}$ be the set of functions from $\mathbf{A} \times \mathbf{B}$ into $\mathbf{C}$. Finally, let ${}^{\mathbf{A}}({}^{\mathbf{B}}\mathbf{C})$ be the set of functions from $\mathbf{A}$ into ${}^{\mathbf{B}}\mathbf{C}$.

Prove that ${}^{\mathbf{A}\times\mathbf{B}}\mathbf{C}$ is equipotent to ${}^{\mathbf{A}}({}^{\mathbf{B}}\mathbf{C})$.

Solution: Define $\Phi : {}^{\mathbf{A}}({}^{\mathbf{B}}\mathbf{C}) \longrightarrow {}^{\mathbf{A}\times\mathbf{B}}\mathbf{C}$ as follows: for any $f \in {}^{\mathbf{A}}({}^{\mathbf{B}}\mathbf{C})$ (that is, any function $f : \mathbf{A} \longrightarrow {}^{\mathbf{B}}\mathbf{C}$), let $\Phi(f)$ be the function from $\mathbf{A} \times \mathbf{B}$ into $\mathbf{C}$ defined by $\Phi(f)(a,b) := f(a)(b)$.

Φ *is injective:* Let $f, g \in {}^{\mathbf{A}}({}^{\mathbf{B}}\mathbf{C})$.

$$\begin{aligned}
\Big(\Phi(f) = \Phi(g)\Big) \quad &\iff \quad \Big(\text{For any } (a,b) \in \mathbf{A} \times \mathbf{B}, \text{ we have } \Phi(f)(a,b) = \Phi(g)(a,b)\Big) \\
&\iff \quad \Big(\text{For any } (a,b) \in \mathbf{A} \times \mathbf{B}, \text{ we have } f(a)(b) = g(a)(b)\Big) \\
&\iff \quad \Big(\text{For any } a \in \mathbf{A}, \text{ we have: } f(a)(b) = g(a)(b) \text{ for all } b \in \mathbf{B}\Big) \\
&\iff \quad \Big(\text{For any } a \in \mathbf{A}, \text{ we have: } f(a) = g(a) \text{ (as functions from } \mathbf{B} \text{ to } \mathbf{C})\Big). \\
&\iff \quad \Big(f = g \text{ (as functions from } \mathbf{A} \text{ to } {}^{\mathbf{B}}\mathbf{C})\Big).
\end{aligned}$$

Φ *is surjective:* Let $g \in {}^{\mathbf{A}\times\mathbf{B}}\mathbf{C}$; that is, let g be a function from $\mathbf{A} \times \mathbf{B}$ into $\mathbf{C}$. Define $f : \mathbf{A} \longrightarrow {}^{\mathbf{B}}\mathbf{C}$ by $f(a)(b) = g(a,b)$ for all $a \in \mathbf{A}$ and $b \in \mathbf{B}$. It follows that $\Phi(f) = g$; thus, Φ is surjective.

Thus, Φ is injective and surjective, hence bijective; thus, ${}^{\mathbf{A}\times\mathbf{B}}\mathbf{C}$ is equipotent to ${}^{\mathbf{A}}({}^{\mathbf{B}}\mathbf{C})$. □

$\left(\frac{20}{100}\right)$ 4. Let $\mathbf{X}$ and $\mathbf{Y}$ be sets and let $f : \mathbf{X} \longrightarrow \mathbf{Y}$. Recall that $\overleftarrow{f} : \mathcal{P}(\mathbf{Y}) \longrightarrow \mathcal{P}(\mathbf{X})$ is defined

$$\overleftarrow{f}(\mathbf{B}) \quad := \quad \{x \in \mathbf{X} \ ; \ f(x) \in \mathbf{B}\}, \qquad \forall \ \mathbf{B} \subseteq \mathbf{Y}.$$

Suppose f is surjective. Show that $\overleftarrow{f}$ is injective.

Solution: Suppose f is surjective. We must show that $\overleftarrow{f}$ is injective. Let $\mathbf{A}, \mathbf{B} \subseteq \mathbf{Y}$, and suppose $\overleftarrow{f}(\mathbf{A}) = \overleftarrow{f}(\mathbf{B})$; we will show that $\mathbf{A} = \mathbf{B}$.

"$\mathbf{A} \subseteq \mathbf{B}$": Let $a \in \mathbf{A}$. We want to show that $a \in \mathbf{B}$.

Now, there exists $x \in \mathbf{X}$ such that $f(x) = a$ (because f is surjective by hypothesis). Thus, $x \in \vec{f}(\mathbf{A})$. But $\vec{f}(\mathbf{A}) = \vec{f}(\mathbf{B})$, so $x \in \vec{f}(\mathbf{B})$ as well. But that means that $f(x) \in \mathbf{B}$. But that means that $a \in \mathbf{B}$. Thus, we have shown:

$$\Big(b \in \mathbf{A}\Big) \Longrightarrow \Big(b \in \mathbf{B}\Big).$$

This means $\mathbf{A} \subseteq \mathbf{B}$.

"$\mathbf{B} \subseteq \mathbf{A}$": Exact same proof; just switch $\mathbf{A}$ and $\mathbf{B}$.

It follows that $\mathbf{A} = \mathbf{B}$. This works for any $\mathbf{A}$ and $\mathbf{B}$. Thus, $\overleftarrow{f}$ is injective. □

5. Recall that a number N is a *perfect square* if $N = M^2$ for some $M \in \mathbb{N}$.

$\left(\frac{10}{100}\right)$ (a) Suppose $N = p_1^{n_1} p_2^{n_2} \cdots p_k^{n_k}$. where $p_1, \ldots, p_k$ are distinct primes, and $n_1, \ldots, n_k \in \mathbb{N}$. Show that

$$\Big(N \text{ is a perfect square}\Big) \iff \Big(n_1, \ldots, n_k \text{ are all even.}\Big)$$

Solution: "$\Longrightarrow$" Suppose $N = M^2$. If $M = p_1^{m_1} p_2^{m_2} \cdots p_k^{m_k}$, for some $m_1, \ldots, m_k \in \mathbb{N}$. then $N = M^2 = p_1^{2m_1} p_2^{2m_2} \cdots p_k^{2m_k}$. Thus, by the 'uniqueness' part of the Fundamental Theorem of Arithmetic, we must have $n_1 = 2m_1, \ldots, n_k = 2m_k$, so $n_1, \ldots, n_k$ are all even.

"$\Longleftarrow$" Suppose $n_1, \ldots, n_k$ are all even. Then $n_1 = 2m_1, \ldots, n_k = 2m_k$ for some $m_1, \ldots, m_k \in \mathbb{N}$. Let $M := p_1^{m_1} p_2^{m_2} \cdots p_k^{m_k}$; then $N = M^2$, so N is a perfect square. □

$\left(\frac{10}{100}\right)$ (b) Let $A, B \in \mathbb{N}$, and suppose A and B are coprime. Show that

$$\Big(AB \text{ is a perfect square}\Big) \iff \Big(A \text{ and } B \text{ are both perfect squares}\Big).$$

Solution: Let $A = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$ and $B = q_1^{b_1} q_2^{b_2} \cdots q_j^{b_j}$ where $p_1, \ldots, p_k$ and $q_1, \ldots, q_j$ are distinct primes, and where $a_1, \ldots, a_k \in \mathbb{N}$ and $b_1, \ldots, b_j \in \mathbb{N}$. Corollary 23.4.3 implies that the sets $\{p_1, \ldots, p_k\}$ and $\{q_1, \ldots, q_j\}$ must be *disjoint*, because A is coprime to B.

Thus $A \cdot B = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k} q_1^{b_1} q_2^{b_2} \cdots q_j^{b_j}$. Thus,

$$\begin{aligned} \Big(AB \text{ is a perfect square}\Big) &\iff \Big(a_1, \ldots, a_k \in \mathbb{N} \text{ and } b_1, \ldots, b_j \text{ are all even.}\Big) \\ &\iff \Big(A \text{ is a perfect square and } B \text{ is a perfect square}\Big). \end{aligned}$$

Here, both "$\iff$" are by part (a). □

$(\frac{10}{100})$ 6. What is the last digit of 3^{1000}? (**Hint:** *First compute the first few powers of* 3*, mod* 10.)

Solution: $3^2 = 9$, $3^3 = 27$ and $3^4 = 81 \underset{10}{\equiv} 1$. But $1000 = 4 \times 250$. Thus,

$$3^{1000} = 3^{4\times 250} = (3^4)^{250} \underset{10}{\equiv} 1^{250} = 1.$$

Thus, $3^{1000} \underset{10}{\equiv} 1$, which means the last digit of 3^{1000} is $\boxed{1.}$ □

$(\frac{10}{100})$ 7. Recall that x is the *multiplicative inverse* for y modulo 17 if $xy \underset{17}{\equiv} 1$.

Find the multiplicative inverse of 5, mod 17.

Solution: We must solve the equation $5x \underset{17}{\equiv} 1$. This is equivalent to the linear Diophantine equation $5x + 17n = 1$. First we compute $1 = \gcd(5, 17)$ using the Euclidean algorithm:

$$\begin{aligned} 17 &= 3\times 5 + 2 \implies 2 = 17 - 3\times 5 \\ 5 &= 2\times 2 + 1 \implies 1 = 5 - 2\times 2 = 5 - 2\times(17 - 3\times 5) \\ &\qquad\qquad\qquad\quad = 5 - 2\times 17 + 6\times 5 = 7\times 5 - 2\times 17 \end{aligned}$$

Thus, we get the Bezout identity: $1 = 7\times 5 - 2\times 17$. It follows that $7\times 5 = 1 + 2\times 17 \underset{17}{\equiv} 1$. Thus, the inverse of 5 is $\boxed{7}$. □