# Math 220 — Final Exam —December 15, 2006.

$(\frac{10}{200})$ 1. Let $f : \mathcal{X} \longrightarrow \mathcal{Y}$ be a function. Recall that $\vec{f} : \mathcal{P}(\mathcal{X}) \longrightarrow \mathcal{P}(\mathcal{Y})$ is defined by $\vec{f}(\mathcal{A}) := \{f(a) \; ; \; a \in \mathcal{A}\}$, for any $\mathcal{A} \subseteq \mathcal{X}$.

If $\mathcal{A}, \mathcal{B} \subseteq \mathcal{Y}$, show that $\vec{f}(\mathcal{A} \cup \mathcal{B}) \;=\; \vec{f}(\mathcal{A}) \cup \vec{f}(\mathcal{B})$.

**Solution:**

$$\begin{aligned}\vec{f}(\mathcal{A} \cup \mathcal{B}) &= \{f(x) \; ; \; x \in \mathcal{A} \cup \mathcal{B}\} \quad = \quad \{f(x) \; ; \; x \in \mathcal{A} \text{ or } x \in \mathcal{B}\} \\ &= \{f(x) \; ; \; x \in \mathcal{A}\} \cup \{f(x) \; ; \; x \in \mathcal{B}\} \quad = \quad \vec{f}(\mathcal{A}) \cup \vec{f}(\mathcal{B})\end{aligned}$$

□

$(\frac{15}{200})$ 2. Let $f : \mathcal{X} \longrightarrow \mathcal{Y}$ be a function. Recall that $\overleftarrow{f} : \mathcal{P}(\mathcal{Y}) \longrightarrow \mathcal{P}(\mathcal{X})$ is defined by $\overleftarrow{f}(\mathcal{B}) := \{x \in \mathcal{X} \; ; \; f(x) \in \mathcal{B}\}$, for any $\mathcal{B} \subseteq \mathcal{Y}$.

If $\mathcal{A}, \mathcal{B} \subseteq \mathcal{Y}$, show that $\overleftarrow{f}(\mathcal{A} \cap \mathcal{B}) \;=\; \overleftarrow{f}(\mathcal{A}) \cap \overleftarrow{f}(\mathcal{B})$.

**Solution:** Let $x \in \mathcal{X}$. Then

$$\begin{aligned}\Big(x \in \overleftarrow{f}(\mathcal{A} \cap \mathcal{B})\Big) &\iff \Big(f(x) \in \mathcal{A} \cap \mathcal{B}\Big) \iff \Big(f(x) \in \mathcal{A} \text{ and } f(x) \in \mathcal{B}\Big) \\ &\iff \Big(x \in \overleftarrow{f}(\mathcal{A}) \text{ and } x \in \overleftarrow{f}(\mathcal{B})\Big) \iff \Big(x \in \overleftarrow{f}(\mathcal{A}) \cap \overleftarrow{f}(\mathcal{B})\Big).\end{aligned}$$

In short, $x \in \overleftarrow{f}(\mathcal{A} \cap \mathcal{B})$ if or only if $x \in \overleftarrow{f}(\mathcal{A}) \cap \overleftarrow{f}(\mathcal{B})$. Thus, $\overleftarrow{f}(\mathcal{A} \cap \mathcal{B}) \;=\; \overleftarrow{f}(\mathcal{A}) \cap \overleftarrow{f}(\mathcal{B})$. □

$(\frac{15}{200})$ 3. Let $f : \mathcal{X} \longrightarrow \mathcal{Y}$ and $g : \mathcal{Y} \longrightarrow \mathcal{Z}$ be two *injective* functions. Consider the composition $g \circ f : \mathcal{X} \longrightarrow \mathcal{Z}$. Show that $g \circ f$ is also injective.

**Solution:** We must show that

$$\forall \; x_1, x_2 \in \mathcal{X}, \qquad \Big(x_1 \neq x_2\Big) \Longrightarrow \Big(g \circ f(x_1) \neq g \circ f(x_1)\Big).$$

Let $x_1, x_2 \in \mathcal{X}$. Suppose $x_1 \neq x_2$. Then $f(x_1) \neq f(x_2)$, because $f$ is injective. Thus, $g[f(x_1)] \neq g[f(x_2)]$, because $g$ is injective. But $g[f(x_1)] = g \circ f(x_1)$, and $g[f(x_2)] = g \circ f(x_2)$, so this shows that $g \circ f(x_1) \neq g \circ f(x_1)$, as desired. □

4. We define a relation "$\prec$" between sets as follows: For any two sets $\mathcal{X}$ and $\mathcal{Y}$, we say "$\mathcal{X} \prec \mathcal{Y}$" if there is an injective function $f : \mathcal{X} \longrightarrow \mathcal{Y}$.

$(\frac{5}{200})$ (a) Is the relation "$\prec$" *reflexive*? Why or why not?

**Solution:** Yes. For any set $\mathcal{X}$, the identity function $\mathbf{Id}_{\mathcal{X}} : \mathcal{X} \longrightarrow \mathcal{X}$ is an injection. Thus, $\mathcal{X} \prec \mathcal{X}$. □

$(\frac{5}{200})$ (b) Is the relation "$\prec$" *symmetric*? Why or why not?

**Solution:** No. For example, $\{1,2\} \prec \{1,2,3\}$, but $\{1,2,3\} \not\prec \{1,2\}$ (by the Pigeonhole principle). □

$(\frac{5}{200})$ (c) Is the relation "$\prec$" *transitive*? Why or why not?

**Solution:** Yes. If $\mathcal{X} \prec \mathcal{Y}$ and $\mathcal{Y} \prec \mathcal{Z}$, then there are injections $f : \mathcal{X} \longrightarrow \mathcal{Y}$ and $g : \mathcal{Y} \longrightarrow \mathcal{Z}$. But then $g \circ f : \mathcal{X} \longrightarrow \mathcal{Z}$ is also injective (by Question #3). Thus, $\mathcal{X} \prec \mathcal{Z}$. □

$(\frac{5}{200})$ (d) Is "$\prec$" an *equivalence relation*? Why or why not?

**Solution:** No, because it is not symmetric. □

$(\frac{20}{200})$ 5. If $\mathbf{A} \subseteq \mathbf{X}$, recall that the *characteristic function* of $\mathbf{A}$ is the function $\chi_{\mathbf{A}} : \mathbf{X} \longrightarrow \{0, 1\}$ defined

$$\forall\, x \in \mathbf{X}, \quad \chi_{\mathbf{A}}(x) \quad := \quad \begin{cases} 1 & \text{if} \quad x \in \mathbf{A}; \\ 0 & \text{if} \quad x \notin \mathbf{A}. \end{cases}$$

Suppose $\mathbf{A} \subseteq \mathbf{X}$ and $\mathbf{B} \subseteq \mathbf{Y}$. Find a set $\mathbf{D} \subseteq \mathbf{X} \times \mathbf{Y}$ such that $\chi_{\mathbf{D}}(x, y) = \chi_{\mathbf{A}}(x) \cdot \chi_{\mathbf{B}}(y)$ for all $(x, y) \in \mathbf{X} \times \mathbf{Y}$. Justify your answer.

**Solution:** Let $\mathbf{D} = \mathbf{A} \times \mathbf{B}$. Then for all $x \in \mathbf{X}$ and $y \in \mathbf{Y}$,

$$\begin{aligned}\Big(\chi_{\mathbf{D}}(x,y) = 1\Big) \quad &\Longleftrightarrow \quad \Big((x,y) \in \mathbf{D} = \mathbf{A} \times \mathbf{B}\Big) \Longleftrightarrow \Big(x \in \mathbf{A} \text{ and } y \in \mathbf{B}\Big) \\ &\Longleftrightarrow \quad \Big(\chi_{\mathbf{A}}(x) = 1 \text{ and } \chi_{\mathbf{B}}(y) = 1\Big) \Longleftrightarrow \Big(\chi_{\mathbf{A}}(x) \cdot \chi_{\mathbf{B}}(y) = 1\Big).\end{aligned}$$

Thus, $\chi_{\mathbf{D}}(x, y) = \chi_{\mathbf{A}}(x) \cdot \chi_{\mathbf{B}}(y)$ for all $(x, y) \in \mathbf{X} \times \mathbf{Y}$. □

$(\frac{10}{200})$ 6. (a) Compute the least residue of $2^{11}$ mod 13.

**Solution:** $2^4 = 16 \underset{13}{\equiv} 3$. Thus, $2^8 = (2^4)^2 \underset{13}{\equiv} 3^2 = 9$

Also, $2^3 = 8 \underset{13}{\equiv} -5$. Thus, $2^{11} = 2^3 \cdot 2^8 \underset{13}{\equiv} -5 \cdot 9 = -45 \underset{13}{\equiv} -6 \underset{13}{\equiv} 7$. □

$(\frac{10}{200})$ (b) Does the number 2 have a *multiplicative inverse* modulo 13? If so, what is it? If not, why not?

**Solution:** The inverse of 2 is 7, because

$$7 \cdot 2 \quad \overset{(*)}{\underset{13}{\equiv}} \quad 2^{11} \cdot 2 \quad = \quad 2^{12} \quad \overset{(\dagger)}{\underset{13}{\equiv}} \quad 1.$$

Here, $(*)$ is by part (a), and $(\dagger)$ is by Fermat's theorem. Alternately, $2 \cdot 7 = 14 \underset{13}{\equiv} 1$. □

$(\frac{10}{200})$ 7. Let $\alpha, \beta \in \mathbb{R}$. Show that $\alpha + \beta \;=\; \min\{\alpha, \beta\} + \max\{\alpha, \beta\}$.

**Solution:** Suppose without loss of generality that $\alpha \leq \beta$. Then $\alpha = \min\{\alpha, \beta\}$ and $\beta = \max\{\alpha, \beta\}$. Thus, $\alpha + \beta \;=\; \min\{\alpha, \beta\} + \max\{\alpha, \beta\}$, as desired. □

$(\frac{20}{200})$ 8. Let $a, b \in \mathbb{N}$. Using prime factorizations, show that $\gcd(a, b) \cdot \operatorname{lcm}(a, b) = a \cdot b$. (**Hint:** *You may use any result from the text*)

**Solution:** Suppose $a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$ and $b = p_1^{\beta_1} p_2^{\beta_2} \cdots p_r^{\beta_r}$ where $p_1, \ldots, p_k$ are distinct primes, and where $\alpha_i, \beta_i \in \mathbb{N}$ (possibly zero). Then Corollary 23.4.3 says that $\gcd(a, b) \;=\; p_1^{\gamma_1} p_2^{\gamma_2} \cdots p_r^{\gamma_r}$, where $\gamma_i = \min\{\alpha_i, \beta_i\}$ for all $i$. Likewise, through an argument very similar to Corollary 23.4.3 (which was discussed in class), we have $\operatorname{lcm}(a, b) \;=\; p_1^{\lambda_1} p_2^{\lambda_2} \cdots p_r^{\lambda_r}$, where $\lambda_i = \max\{\alpha_i, \beta_i\}$ for all $i$. Thus,

$$\begin{aligned}\gcd(a,b) \cdot \operatorname{lcm}(a,b) \quad &= \quad \prod_{i=1}^{r} p^{\gamma_i} \cdot \prod_{i=1}^{r} p^{\lambda_i} \quad = \quad \prod_{i=1}^{r} p^{\gamma_i + \lambda_i} \quad \underset{(*)}{=} \quad \prod_{i=1}^{r} p^{\alpha_i + \beta_i} \\ &= \quad \prod_{i=1}^{r} p^{\alpha_i} \cdot \prod_{i=1}^{r} p^{\beta_i} \quad = \quad a \cdot b.\end{aligned}$$

Here $(*)$ is by Question #7. □

$(\frac{10}{200})$ 9. (a) Use the *Euclidean algorithm* to compute the greatest common divisor of 180 and 21.

$(\frac{10}{200})$ (b) Express $\gcd(180, 21)$ as an *integer-linear combination* of 180 and 21.

**Solution:**

$$\begin{array}{rcl} 180 &=& 8\cdot 21+12 \implies 12 = 180-8\cdot 21; \\ 21 &=& 1\cdot 12+9 \implies 9 = 21-12 = 21-(180-8\cdot 21) = 9\cdot 21-180; \\ 12 &=& 1\cdot 9+3 \implies 3 = 12-9 = (180-8\cdot 21)-(9\cdot 21-180) = 2\cdot 180-17\cdot 21; \\ 9 &=& 3\cdot 3+0 \implies 3 = \gcd(180,12). \end{array}$$

Thus, $\gcd(180, 21) = \boxed{3} = \boxed{2\cdot 180-17\cdot 21}$. □

$(\frac{10}{200})$ 10. Prove: If $n \geq 4$, then $n! > 2^n$. (**Hint:** *Use induction.*)

**Solution:** (by induction on $n$)

**Base case** ($n = 4$): $4! = 4\cdot 3\cdot 2 = 24 > 16 = 2^4$.

**Induction:** Suppose $n \geq 4$ and $n! > 2^n$. Then

$$(n+1)! = (n+1)\cdot n! \underset{(*)}{>} (n+1)\cdot 2^n \underset{(\dagger)}{\geq} 4\cdot 2^n > 2\cdot 2^n = 2^{n+1},$$

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

$(\frac{10}{200})$ 11. Let $\mathbf{X} \subset \mathbb{R}$ be countable, and let $\mathbf{X}^{\complement} := \mathbb{R} \setminus \mathbf{X}$. Is $\mathbf{X}^{\complement}$ countable or uncountable? Justify your answer.

**Solution:** $\mathbf{X}^{\complement}$ is uncountable. To see this, by contradiction suppose $\mathbf{X}^{\complement}$ was countable. Then $\mathbb{R} = \mathbf{X} \sqcup \mathbf{X}^{\complement}$ would be a union of two countable sets, so $\mathbb{R}$ would also also be countable. But this is false. Thus, by contradiction, $\mathbf{X}^{\complement}$ must be uncountable. □

12. Define $\phi : \mathbb{N}^3 \longrightarrow \mathbb{N}$ by $\phi(x, y, z) = 2^x 3^y 5^z$.

$(\frac{15}{200})$ (a) Is $\phi$ *injective*? Why or why not?

**Solution:** Yes. Let $(x_1, y_1, z_1)$ and $(x_2, y_2, z_2)$ be elements of $\mathbb{N}^3$. If $\phi(x_1, y_1, z_1) = \phi(x_2, y_2, z_2)$, then $2^{x_1}3^{y_1}5^{z_1} = 2^{x_2}3^{y_2}5^{z_2}$, which implies that $x_1 = x_2$, $y_1 = y_2$, and $z_1 = z_2$, because prime factorizations are unique (by the Fundamental Theorem of Arithmetic). □

$(\frac{15}{200})$ (b) Is $\phi$ *surjective*? Why or why not?

**Solution:** No. For example, 7 is not in the image of $\phi$. To see this, suppose $\phi(x, y, z) = 7$. This means that $7 = 2^x 3^y 5^z$. But this contradicts the fact that 7 is prime.

More generally, any number divisibly by *any* prime greater than 5 is not in the image of $\phi$, because prime factorizations are unique (by the Fundamental Theorem of Arithmetic). □

$(\frac{10}{200})$ (c) **(Bonus)**. Let $\mathbb{Q}^* := \mathbb{Q} \setminus \{0\}$. Define $\Phi : \mathbb{Z}^3 \longrightarrow \mathbb{Q}$ by $\phi(x, y, z) = 2^x 3^y 5^z$. Is $\Phi$ a *group homomorphism* from $(\mathbb{Z}^3, +)$ into $(\mathbb{Q}^*, \cdot)$? Why or why not?

**Solution:** Yes.. Let $(x_1, y_1, z_1)$ and $(x_2, y_2, z_2)$ be elements of $\mathbb{Z}^3$. Then

$$\begin{aligned} \Phi(x_1+x_2, y_1+y_2, z_1+z_2) &= 2^{x_1+x_2}3^{y_1+y_2}5^{z_1+z_2} = 2^{x_1}3^{y_1}5^{z_1}\cdot 2^{x_2}3^{y_2}5^{z_2} \\ &= \Phi(x_1, y_1, z_1)\cdot \Phi(x_2, y_2, z_2). \end{aligned}$$

□