Discrete Mathematics: Combinatorics and Graph Theory

Practice Exam 2 Solution

Instructions. Solve any 5 questions and state which 5 you would like graded. Note that this is a sample exam, and while it bears some similarity to the real exam, the two are not isomorphic.

1. Consider the following:

   (a) Define a relation R on $\mathbb{Z}$ by $(a,b) \in R$ if $a^2 - b^2 \leq 3$. Verify whether R is (i) reflexive (ii) symmetric and (iii) transitive?
   Reflexive: $\forall a \in \mathbb{Z}, a^2 - a^2 = 0 \leq 3$ therefore R reflexive.
   Symmetric: $\forall (a,b) \in \mathbb{Z}, a^2 - b^2 \leq 3$ does not imply that $b^2 - a^2 \leq 3$ so R is not symmetric. For example, $0^2 - 10^2 \leq 3$ but $10^2 - 0^2 > 3$.
   Transitive: $\forall (a,b,c) \in \mathbb{Z}, a^2 - b^2 \leq 3$ and $b^2 - c^2 \leq 3$ does not imply $a^2 - c^2 \leq 3$ so R is not transitive. For example, $2^2 - 1^2 \leq 3$ and $1^1 - 0^2 \leq 3$ but $2^2 - 0^2 > 3$.

   (b) Let $A = \{1,2,3,4,5\}$ and

   $$R = \{(1,1),(1,3),(1,4),(2,2),(2,5),(3,1),(3,3),(3,4),(4,1),(4,3),(4,4),(5,2),(5,5)\}\,.$$

   Which of the following is an equivalence class?

   $(i)\quad \{1,2,3\} \qquad (ii)\quad \{2,3,5\} \qquad (iii)\quad \{1,3,4\} \qquad (iv)\quad \{1,2\} \qquad (v)\quad \{1,2,3,4,5\}$

   Only (iii) is an equivalence class. The elements $1,3,4$ are related to each other and nothing else.

   (c) If R_1 and R_2 are equivalence relations on the set A, then $R_1 \cap R_2$ is an equivalence relation on A. Prove or disprove.
   If R_1 is an equivalence relation then $\forall x \in A \Rightarrow (x,x) \in R_1$ (since R_1 reflexive). Similarly if R_2 is an equivalence relation then $\forall x \in A \Rightarrow (x,x) \in R_2$ (since R_2 reflexive). Therefore $(x,x) \in R_1 \cap R_2$ hence $R_1 \cap R_2$ is reflexive.
   If $(x,y) \in R_1 \cap R_2$ then $(x,y) \in R_1$ and $(x,y) \in R_2$. Since both R_1 and R_2 are equivalence relations, R_1 and R_2 are both symmetric. It follows that $((y,x) \in R_1) \cap ((y,x) \in R_2))$, therefore $(y,x) \in R_1 \cap R_2$ hence $R_1 \cap R_2$ is symmetric.
   If $(x,y) \in R_1$ and $(y,z) \in R_1$ then $(x,z) \in R_1$ (since R_1 is transitive). Similarly $(x,y) \in R_2$ and $(y,z) \in R_2 \Rightarrow (x,z) \in R_2$ (since R_2 is transitive). If $(x,z) \in R_1$ and $(x,z) \in R_2$ then $(x,z) \in R_1 \cap R_2$ hence $R_1 \cap R_2$ is transitive. It follows that R_1 and R_2 is an equivalence relation.

2. Solve the following:

   (a) $3x \equiv 7 \pmod 4$
   The $gcd(3,4) = 1 \mid 7 \Rightarrow 1$ solution mod 4. Thus $3x + 4y = 7$. A simple solution is $x = 1, y = 1$. Therefore $x = 1 \pmod 4$.

   (b) $6x \equiv 7 \pmod 8$
   The $gcd(6,8) = 2 \nmid 7 \Rightarrow$ no solution

   (c) $8x \equiv 13 \pmod{29}$
   The $gcd(8,29) = 1 \mid 13 \Rightarrow 1$ solution mod 29. We want to find 8^{-1} such that $x \equiv 13 \times 8^{-1} \pmod{29}$. By Bezout's identity $8x + 29y = 1$.

   $$\begin{aligned}
   29 = 3 \times 8 + 5 &\quad\Rightarrow\quad 5 = 29 - 3 \times 8 \\
   8 = 1 \times 5 + 3 &\quad\Rightarrow\quad 3 = 8 - 1 \times 5 = 8 - 1 \times (29 - 3 \times 8) = 4 \times 8 - 1 \times 29 \\
   5 = 1 \times 3 + 2 &\quad\Rightarrow\quad 8 = 5 - 1 \times 3 = (29 - 3 \times 8) - 1 \times (4 \times 8 - 1 \times 29) = 2 \times 29 - 7 \times 8 \\
   3 = 1 \times 2 + 1 &\quad\Rightarrow\quad 1 = 3 - 1 \times 2 = (4 \times 8 - 1 \times 29) - 1 \times (2 \times 29 - 7 \times 8) = 11 \times 8 - 3 \times 29
   \end{aligned}$$

   Therefore $x \equiv 13 \times 8^{-1} \equiv 11 \pmod{29} \equiv 27 \pmod{29}$.

3. Find the smallest positive integer x such that:

$$x \equiv 1 \pmod 3$$
$$x \equiv 2 \pmod 4$$
$$x \equiv 3 \pmod 5$$

Use the CRT: $N = 3 \times 4 \times 5 = 60$. $N_1 = 20x_1 \equiv 1 \pmod 3 \Rightarrow x_1 = 2$ works so $N_1 \equiv 40 \pmod{60}$. $N_2 = 15x_2 \equiv 2 \pmod 4 \Rightarrow x_2 = 2$ works so $N_2 \equiv 30 \pmod{60}$. $N_3 = 12x_3 \equiv 3 \pmod 5 \Rightarrow x_3 = 4$ works so $N_3 \equiv 48 \pmod{60}$. Therefore $x = 2\times4\times5+2\times3\times5+4\times3\times4 = 118 \pmod{60} \equiv 58 \pmod{60}$.

4. Evaluate the following expressions or verify the identities:

(a) $(a+b)^7$

$$\begin{aligned}(a+b)^7 &= \binom{7}{0}a^7b^0 + \binom{7}{1}a^6b^1 + \binom{7}{2}a^5b^2 + \binom{7}{3}a^4b^3 + \binom{7}{4}a^3b^4 + \binom{7}{5}a^2b^5 + \binom{7}{6}a^1b^6 + \binom{7}{7}a^0b^7 \\ &= a^7 + 7a^6b^1 + 21a^5b^2 + 35a^4b^3 + 35a^3b^4 + 21a^2b^5 + 7a^1b^6 + b^7\end{aligned}$$

(b) $\sum_{k=0}^{n} \binom{n}{k} p^k (1-p)^{n-k}$

$$\sum_{k=0}^{n} \binom{n}{k} p^k (1-p)^{n-k} = (p + (1-p))^n = 1^n = 1$$

(c) $\binom{n}{k} = \binom{n}{n-k}$.
Expand using factorials.

$$\binom{n}{n-k} = \frac{n!}{(n-k)!(n-(n-k))!} = \frac{n!}{(n-k)!k!} = \frac{n!}{k!(n-k)!} = \binom{n}{k}$$

(d) $\sum_{k=0}^{n} \binom{n}{k} = 2^n$
Use the binomial theorem:

$$\sum_{k=0}^{n} \binom{n}{k} a^{n-k}b^k = (a+b)^n$$

To get the equality on the RHS plug in $a = 1$ and $b = 1$:

$$\sum_{k=0}^{n} \binom{n}{k} 1^{n-k}1^k = \sum_{k=0}^{n} \binom{n}{k} = (1+1)^n = 2^n$$

(e) $\sum_{i=0}^{n} i\binom{n}{i} = n2^{n-1}$
Use the binomial theorem and set $b = 1$:

$$(x+1)^n = \sum_{i=0}^{n} \binom{n}{i} x^i$$

Differentiate wrt x:

$$n(x+1)^{n-1} = \sum_{i=0}^{n} i\binom{n}{i} x^{i-1}$$

Set $x = 1$:

$$n2^{n-1} = \sum_{i=0}^{n} i\binom{n}{i}$$

5. Let $gcd(a, b) = 1$. Show that $a^{\phi(b)} + b^{\phi(a)} \equiv 1 \pmod{\text{ab}}$.
   By Euler's theorem, $a^{\phi(b)} = 1 \pmod b$ and $b^{\phi(a)} = 1 \pmod a$. Notice that $a \mid a^{\phi(b)} \Rightarrow a^{\phi(b)} \equiv 0 \pmod a$ and $b \mid b^{\phi(a)} \Rightarrow b^{\phi(a)} \equiv 0 \pmod b$. Therefore $a^{\phi(b)} + b^{\phi(a)} \equiv 1 \pmod a$ and $a^{\phi(b)} + b^{\phi(a)} \equiv 1 \pmod b$. Note that when $gcd(a, b) = 1$, if $a|c$ and $b|c$ then $ab|c$. To see this, use Bezout's identity: $ax + by = 1$. Multiply by $c \Rightarrow cax + cby = c$. Since $a|c$ and $b|c$, there exist integers m and n such that $am = c$ and $bn = c$. Substitute for c to produce $bnax + amby = c \Rightarrow ab(nx + my) = c$. Therefore $ab|c$.
   We can apply this small result to conclude that since $a^{\phi(b)} + b^{\phi(a)} \equiv 1 \pmod a$ and $a^{\phi(b)} + b^{\phi(a)} \equiv 1 \pmod b$, $a^{\phi(b)} + b^{\phi(a)} \equiv 1 \pmod{ab}$. □

6. Let p be a prime. Show that $\binom{p}{i} \equiv 0 \pmod p$.
   Expand the binomial:
   $$\binom{p}{i} = \frac{p!}{i!(p-i)!}$$
   Observe that since p is prime, the numerator has a factor of p that cannot be canceled by any term. We can express this as follows:
   $$\binom{p}{i} = p \times \frac{(p-1)!}{i!(p-i)!}$$
   By definition this means that $p \mid \binom{p}{i}$. □