Discrete Mathematics: Combinatorics and Graph Theory

Exam 2 Solution

Instructions. Solve any 5 questions and state which 5 you would like graded. Write neatly and show your work to receive full credit. You must sign the attendance sheet when returning your booklet. Good luck!

1. Answer and verify whether (b) and (c) define equivalence relations:

   (a) How many relations are there on a set A with n elements?
   First note that there are $2^{|A|}$ subsets on a set with $|A|$ elements. A relation R on a set A is defined as $R \subseteq A \times A$. By definition, $|A \times A| = n \times n$. Therefore there are $2^{n\times n}$ relations on A.

   (b) Let A be the power set of S so that $A = \mathcal{P}(S)$. Define the relation R on A as $\forall\,(a,b) \in A$, $(a,b) \in R$ if a and b have the same cardinality. What are the equivalence classes when $S = \{1,2,3\}$?

   (i) Reflexivity: For any set $x \in \mathcal{P}(S)$, $|x| = |x|$. Therefore R is reflexive.
   (ii) Symmetry: For any two sets $x, y \in \mathcal{P}(S)$, if $|x| = |y|$ then $|y| = |x|$. Therefore R is symmetric.
   (iii) Transitivity: For any three sets $x, y, z \in \mathcal{P}(S)$, if $|x| = |y|$ and $|y| = |z|$ then $|x| = |z|$. Therefore R is transitive.

   Enumerate $\mathcal{P}(S) = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1,2\}, \{1,3\}, \{2,3\}, \{1,2,3\}\}$, the equivalence classes are:

   $$[\emptyset] = \emptyset, \qquad [\{1\}] = \{\{1\},\{2\},\{3\}\}, \qquad [\{1,2\} = \{\{1,2\},\{1,3\},\{2,3\}\}, \qquad [\{1,2,3\}] = \{\{1,2,3\}\}$$

   (c) Let $S = \{\frac{p}{q} \,|\, p, q \in \mathbb{Z}, q \neq 0\}$ denote the set of fractions and define relation R on S by $(\frac{a}{c}, \frac{b}{d}) \in R$ iff $ad = bc$. What are the equivalence classes?

   (i) Reflexivity: For any fraction $\frac{a}{b}$, $ab = ba$. Therefore $(\frac{a}{b}, \frac{a}{b}) \in R$ and R is reflexive.
   (ii) Symmetry: If $(\frac{a}{b}, \frac{b}{c}) \in R$, then $ad = bc \Rightarrow c = \frac{ad}{b}$ and $d = \frac{bc}{a} \Rightarrow cd = ba$ and R is symmetric.
   (iii) Transitivity: If $(\frac{a}{b}, \frac{c}{d}) \in R$ and $(\frac{c}{d}, \frac{e}{f}) \in R$, then $ad = bc$ and $cf = de$. Multiply the first equation by $f \Rightarrow adf = bcf$. Note that $cf = de \Rightarrow adf = bde$. Divide by d (which is not 0) to get $af = be$. Therefore $(\frac{a}{b}, \frac{e}{f}) \in R$ and R is transitive.

   The equivalence classes are the rational numbers:

   $$\left[\frac{1}{1}\right] = \left\{\frac{2}{2}, \frac{3}{3}, \cdots, \frac{k}{k}, \cdots\right\}, \qquad \left[\frac{1}{2}\right] = \left\{\frac{2}{4}, \frac{3}{6}, \cdots, \frac{k}{2k}, \cdots\right\}, \qquad \cdots$$

   Each vertex in the Stern-Brocot tree represents an equivalence class. The set of all the equivalence classes is $\mathbb{Q}$.

2. Find all congruence classes of solutions of the following congruences in the given modulus.

   (a) $7x \equiv 20 \pmod{62}$
   Since $gcd(7,62) = 1$, we know there will be a unique solution. The multiplicitive inverse of 7 is $9 \pmod{62}$. To see this, observe that $7 \times 9 = 63 \equiv 1 \pmod{62} \Rightarrow 7^{-1} \equiv 9 \pmod{62}$. Multiply both sides of the congruence by 9:

   $$9 \times 7x = 9 \times 20 \pmod{62}$$

   Therefore $x \equiv 180 \equiv \pmod{62}$ which reduces to $x \equiv 56 \pmod{62}$.

   (b) $6x \equiv 3 \pmod{32}$
   The $gcd(6,32) = 2$. Since $2 \nmid 3$, there are no solutions.

(c) $4x \equiv 6 \pmod{10}$
The $gcd(4, 10) = 2$. Since $2 \mid 6$, we can reduce as follows:

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

Note that $2 \times 4 \equiv 4 \pmod 5$ so $x \equiv 4 \pmod 5$ is a solution. Converting back to congruence classes modulo 10 yields the two solutions:

$$x \equiv 4 \pmod{10} \qquad \text{and} \qquad x \equiv 9 \pmod{10}$$

3. Consider the following:

(a) What are $\phi(16)$, $\phi(20)$, $\phi(31)$ and $\phi(36)$ where $\phi(n)$ is Euler's totient function?
   (i) $\phi(16) = 2^4 - 2^3 = 8$
   (ii) $\phi(20) = \phi(4) \times \phi(5) = (2^2 - 2) \times (5 - 1) = 8$
   (iii) $\phi(31) = 31 - 1 = 30$
   (iv) $\phi(36) = \phi(4) \times \phi(9) = (2^2 - 2) \times (3^2 - 3) = 2 \times 6 = 12$

(b) Given that 881 is prime, simplify $101^{882} \pmod{881}$ (Hint: use Fermat's Little Theorem).

$$101^{882} = 101^{880} + 101^2 \equiv 1 \times 101^2 = 10201 \equiv 510 \pmod{881}$$

(c) Find the multiplicitive inverses of 3, 5, 7, 9 and 15 modulo 26.
We seek an x for each number a such that $ax \equiv 1 \pmod{26}$.

$$\begin{aligned} 3x \equiv 1 \pmod{26} &\Rightarrow 3^{-1} \equiv 9 \pmod{26} \\ 5x \equiv 1 \pmod{26} &\Rightarrow 5^{-1} \equiv 21 \pmod{26} \\ 7x \equiv 1 \pmod{26} &\Rightarrow 7^{-1} \equiv 15 \pmod{26} \\ 9x \equiv 1 \pmod{26} &\Rightarrow 9^{-1} \equiv 3 \pmod{26} \\ 15x \equiv 1 \pmod{26} &\Rightarrow 15^{-1} \equiv 7 \pmod{26} \end{aligned}$$

4. Find the smallest positive integer x such that:

$$\begin{aligned} x &\equiv 5 \pmod 6 \\ x &\equiv 2 \pmod 7 \\ x &\equiv 3 \pmod{11} \end{aligned}$$

Set $N_1 = 7 \times 11$, $N_2 = 6 \times 11$ and $N_3 = 7 \times 6$ with $N = 6 \times 7 \times 11 = 462$. Writing out each term requires factors of 3 and 4 so that $x = 7 \times 11 + 3 \times 6 \times 11 + 4 \times 7 \times 6 \Rightarrow x \equiv 443 \pmod{462}$.

5. Verify the following identities:

(a)

$$B_n(x) \coloneqq \sum_{k=0}^{n} \binom{n}{k} x^k = (1 + x)^n$$

Recall the Binomial Theorem:

$$\sum_{k=0}^{n} \binom{n}{k} x^{n-k} y^k = (x + y)^n$$

Substitute 1 for the x^{n-k} term and rename the variables to show the result

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

(b)

$$B_n(x) \coloneqq \sum_{k=0}^{n} \binom{n}{k} x^k = (1+x)^n$$

Expand the binomial coefficient and cancel terms:

$$\begin{aligned}
\binom{k+r-1}{k} &= \frac{(k+r-1)!}{k!(\cancel{k}+r-1-\cancel{k})!} \\
&= \frac{(k+r-1)!}{k!(r-1)!} \\
&= \frac{(k+r-1)\times(k+r-2)\times\cdots\times(r)\times\cancel{(r-1)}\times\cancel{\cdots}\times\cancel{1}}{k!\times(\cancel{(r-1)}\times\cancel{(r-2)}\times\cancel{\cdots}\times\cancel{1})} \\
&= \frac{(k+r-1)\times(k+r-2)\times\cdots\times(r)}{k!} \\
&= (-1)^k\frac{(-r)\times(-r-1)\times\cdots\times(-r-k+1)}{k!} \\
&= (-1)^k\binom{-r}{k}
\end{aligned}$$

(c)

$$\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}$$

Expand the RHS:

$$\begin{aligned}
\binom{n-1}{k} + \binom{n-1}{k-1} &= \frac{(n-1)!}{(n-\cancel{1}-k+\cancel{1})!(k-1)!} + \frac{(n-1)!}{(n-1-k)!k!} \\
&= \frac{(n-1)!}{(n-k)!(k-1)!} + \frac{(n-1)!}{(n-k-1)!k!}
\end{aligned}$$

Express $(k-1)!$ as $k/k!$ and $(n-k-1)!$ as $(n-k)/(n-k)!$ to simplify the denominator:

$$\begin{aligned}
&= \frac{k(n-1)!}{k!(n-k)!} + \frac{(n-k)(n-1)!}{k!(n-k)!} \\
&= \frac{k(n-1)! + (n-k)(n-1)!}{k!(n-k)!} \\
&= \frac{(\cancel{k}+n-\cancel{k})(n-1)!}{k!(n-k)!} \\
&= \frac{n(n-1)!}{k!(n-k)!} \\
&= \frac{n!}{k!(n-k)!} \\
&= \binom{n}{k}
\end{aligned}$$

6. Derive a closed form expression for the number of surjective functions that exist from a set $\mathcal{S}_1$ to $\mathcal{S}_2$ where $|\mathcal{S}_1| = x$ and $|\mathcal{S}_2| = y$.
First note that there are $\binom{y}{i}$ ways of choosing i elements from the set $\mathcal{S}_2$ of y elements. Also note that there are i^x functions from a set of size x into a set of size i. We wish to consider only surjective functions and so it is necessary to remove functions that only go into a subset of size $y-1$ in $\mathcal{S}_2$. There

are $\binom{y}{y-1}$ such subsets, and for each of them there are $(y-1)^x$ functions. Keeping $y^x - \binom{y}{y-1}(y-1)^x$ results in some functions that are removed more than once that go into a subset of size $< y-1$. These must be added back:

$$S(x,y) = \sum_{i=1}^{y} (-1)^{y-1} \binom{y}{i} i^x$$

7. Prove that the $gcd(a,c) = gcd(b,c) = 1$ if and only if $gcd(ab,c) = 1$.

   (a) Consider the forward conditional if $gcd(a,c) = gcd(b,c) = 1$ then $gcd(ab,c) = 1$. By definition $1 \mid ab$ and $1 \mid c$. We want to show that $\exists x, y \in \mathbb{Z}$ such that $abx + cy = 1$. Since the $gcd(a,c) = gcd(b,c) = 1$, $\exists k, l, m, n \in \mathbb{Z}$ such that

   $$ak + cl = 1, \qquad bm + cn = 1$$

   Multiply the two equations:

   $$abkm + ackn + cblm + ccln = 1$$

   Factorize:

   $$ab(km) + c(akn + blm + cln) = 1$$

   Hence $x = km, y = akn + blm + cln$. This proves the forward conditional.

   (b) Consider the backward conditional if $gcd(ab,c) = 1$ then $gcd(a,c) = gcd(b,c) = 1$. This implies that $\exists x, y \in \mathbb{Z}$ such that

   $$abx + cy = 1$$

   Rewrite as follows

   $$a(bx) + cy = 1, \qquad b(ax) + cy = 1$$

   to highlight that there exist integer solutions k, l, m, n to equations $ak + cl = 1, bm + cn = 1$. By Bezout's identity this implies that $gcd(a,c) = gcd(b,c) = 1$.