Discrete Mathematics: Combinatorics and Graph Theory

Homework 2: Due 11/2

Instructions. Solve any 10 questions. Typeset or write neatly and show your work to receive full credit.

1. List the ordered pairs in the relation R from $A = \{0, 1, 2, 3, 4\}$ to $B = \{0, 1, 2, 3\}$, where $(a, b) \in R$ if and only if:

   (a) $a = b$

   (b) $a + b = 4$

   (c) $a > b$

   (d) $a|b$

   (e) $gcd(a, b) = 1$

   (f) $lcm(a, b) = 2$

2. For each of these relations on the set $\{1, 2, 3, 4\}$, decide whether it is reflexive, whether it is symmetric, whether it is antisymmetric, and whether it is transitive.

   (a) $\{(2, 2), (2, 3), (2, 4), (3, 2), (3, 3), (3, 4)\}$

   (b) $\{(1, 1), (1, 2), (2, 1), (2, 2), (3, 3), (4, 4)\}$

   (c) $\{(2, 4), (4, 2)\}$

   (d) $\{(1, 2), (2, 3), (3, 4)\}$

   (e) $\{(1, 1), (2, 2), (3, 3), (4, 4)\}$

   (f) $\{(1, 3), (1, 4), (2, 3), (2, 4), (3, 1), (3, 4)\}$

3. Determine whether the three relations shown below in the three directed graphs is an equivalence relation.

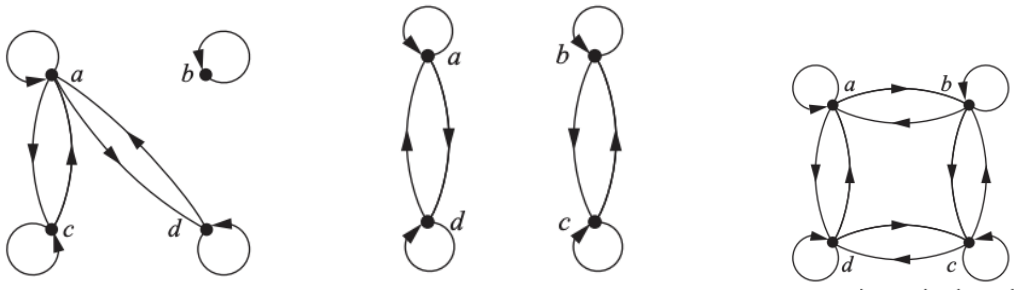

Figure 1: Three relations R_1 (left) R_2 (center) and R_3 (right) represented as digraphs.

   Write the elements of each relation as a set and a binary matrix. If each is not an equivalence class, specify and draw the reflexive R_r^+, symmetric R_s^+ and transitive R_t^+ closure.

4. Establish the congruence classes for the following:

   (a) What is the congruence class $[4]_m$ when *i)* $m = 2$? *ii)* $m = 3$? *iii)* $m = 6$? *iv)* $m = 8$?

   (b) What is the congruence class $[n]_5$ (that is, the equivalence class of n with respect to congruence modulo 5) when *i)* $n = 2$? *ii)* $n = 3$? *iii)* $n = 6$? *iv)* $n = -3$?

5. Find all solutions to the following linear congruences:

(a) $5x \equiv 12 \pmod{23}$
(b) $210x \equiv 40 \pmod{212}$
(c) $33x \equiv 7 \pmod{143}$
(d) $124x \equiv 132 \pmod{900}$

6. Let R be the relation on the set of all colorings of the 2×2 checkerboard where each of the four squares is colored either red or blue so that (C_1, C_2), where C_1 and C_2 are 2×2 checkerboards with each of their four squares colored blue or red, belongs to R if and only if C_2 can be obtained from C_1 either by rotating the checkerboard or by rotating it and then reflecting it.

   (a) Show that R is an equivalence relation.
   (b) What are the equivalence classes of R?

7. Prove that if $a_0 \equiv a \ (mod\ n)$ and $b_0 \equiv b \ (mod\ n)$ then $(a_0 \ (mod\ n)) \cdot (b_0 \ (mod\ n)) \equiv (a \cdot b) \ (mod\ n)$.

8. Solve the following system of congruences:

   (a) Use the Chinese Remainder Theorem to find an x such that:

$$x \equiv 2 \pmod{5}$$
$$x \equiv 3 \pmod{7}$$
$$x \equiv 10 \pmod{11}$$

   (b) Find all solutions x, if they exist, to the system of equivalences:

$$2x \equiv 6 \pmod{14}$$
$$3x \equiv 9 \pmod{15}$$
$$5x \equiv 20 \pmod{60}$$

   (c) Use the Chinese Remainder Theorem to compute $46^{51} \pmod{55}$ by hand.

9. 1500 soldiers arrive in training camp. A few soldiers desert the camp. The drill sergeants divide the remaining soldiers into groups of five and discover that there is one left over. When they divide them into groups of seven, there are three left over. When they divide them into groups of eleven, there are again three left over. Determine the number of deserters.

10. Consider the following questions on closed binary operations:

    (a) Let $f : \mathbb{Z}^+ \times \mathbb{Z}^+ \to \mathbb{Z}^+$ be the closed binary operation defined by $f(a, b) = gcd(a, b)$. (a) is f commutative? (b) Is f associative? (c) Does f have an identity element?
    (b) For distinct primes p, q, let $A = \{p^m q^n | 0 \leq m \leq 31\,,\, 0 \leq n \leq 37\}$. (a) What is $|A|$? (b) If $f : A \times A \to A$ is the closed binary operation defined by $f(a, b) = gcd(a, b)$, does f have an identity element?

11. Apply the Binomial theorem to work out the following:

    (a) Expand $(a + b)^5$
    (b) Expand $(x + 2)^6$
    (c) Expand $(2x + 3)^4$
    (d) Expand $(\sqrt{2} + 1)^5 + (\sqrt{2} - 1)^5$ and simplify.

12. In how many ways can one travel in the xy plane from (0,0) to (3,3) using the moves $R : (x, y) \to (x + 1, y)$ and $U : (x, y) \to (x, y + 1)$, if the path taken may touch but *never* fall below the line $y = x$? In how many ways from $(0, 0)$ to $(4, 4)$? Generalize the results from $(0, 0)$ to (a, b). What can one say about the first and last moves of the paths?

13. Let p be prime and let $f(x)$ be a polynomial over $\mathbb{Z}_p$ (the set of integers mod p) of degree n. Prove that $f(x)$ has at most n roots.

14. For every positive integer n, show that:

$$\binom{n}{0} + \binom{n}{2} + \binom{n}{4} + \cdots = \binom{n}{1} + \binom{n}{3} + \binom{n}{5} + \cdots$$

15. Prove the hexagon property:

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

16. Prove that Pascal's triangle has a more surprising hexagon property:

$$gcd\left(\binom{n-1}{k-1}, \binom{n}{k+1}, \binom{n+1}{k}\right) = gcd\left(\binom{n-1}{k}, \binom{n+1}{k+1}, \binom{n}{k-1}\right)$$

17. Let p be prime. Show that $\binom{p}{k} \pmod p = 0$ for $0 < k < p$. What does this imply about the binomial coefficients $\binom{p-1}{k}$?

18. We can define the reciprocal of a factorial as follows:

$$\frac{1}{z!} = \lim_{n\to\infty} \binom{n+z}{n} n^{-z}$$

Show that the above definitiion is consistent with the ordinary definition by showing that the limit of the above is $1/m!$ when $z = m$ is a positive integer. Use the above to prove the factorial duplication formula:

$$x!\left(x - \frac{1}{2}\right)! = (2x)!\left(-\frac{1}{2}\right)!/2^{2x}$$

19. Prove that the polynomials of degree k with coefficients in $\mathbb{Z}_p$ form a group under addition modulo p.

20. A cyclic shift of a p-tuple x is a p-tuple obtained by adding a constant (modulo p) to the indices of the elements of x; shifting x by p + i positions produces the same p-tuple as shifting x by i positions. For $a \in \mathbb{N}$, let R be the relation on $[a]^p$ (the set of p-tuples with entries in $\{1, \cdots, a\}$) defined by putting $(x, y) \in \mathbb{R}$ if the p-tuple y can be obtained from x by a cyclic shift.

    (a) Prove that R is an equivalence relation on $[a]^p$.

    (b) Prove that p divides $a^p - a$ when p is prime. Hint: Partition a set of size $a^p - a$ into subsets of size p.