Discrete Mathematics: Combinatorics and Graph Theory

Homework 2 Solution

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) $a = b$
   $\{(0, 0), (1, 1), (2, 2), (3, 3)\}$

   (b) $a + b = 4$
   $\{(1, 3), (2, 2), (3, 1), (4, 0)\}$

   (c) $a > b$
   $\{(1, 0), (2, 0), (2, 1), (3, 0), (3, 1), (3, 2), (4, 0), (4, 1), (4, 2), (4, 3)\}$

   (d) $a|b$
   $\{(1, 0), (1, 1), (1, 2), (1, 3), (2, 0)\,(2, 2), (3, 0), (3, 3)\}$

   (e) $gcd(a, b) = 1$
   $\{(0, 1), (1, 0), (1, 1), (1, 2), (1, 3), (2, 1), (2, 3), (3, 1), (3, 2), (4, 1), (4, 3)\}$

   (f) $lcm(a, b) = 2$
   $\{(1, 2), (2, 1), (2, 2)\}$

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) $\{(2, 2), (2, 3), (2, 4), (3, 2), (3, 3), (3, 4)\}$
   Not reflexive , not symmetric , not antisymmetric, transitive.

   (b) $\{(1, 1), (1, 2), (2, 1), (2, 2), (3, 3), (4, 4)\}$
   Reflexive, symmetric, not antisymmetric, transitive.

   (c) $\{(2, 4), (4, 2)\}$
   Not reflexive, symmetric, not antisymmetric, not transitive.

   (d) $\{(1, 2), (2, 3), (3, 4)\}$
   Not reflexive, not symmetric, antisymmetric, not transitive.

   (e) $\{(1, 1), (2, 2), (3, 3), (4, 4)\}$
   Reflexice, symmetric, antisymmetric, transitive.

   (f) $\{(1, 3), (1, 4), (2, 3), (2, 4), (3, 1), (3, 4)\}$
   Not reflexive, not symmetric, not antisymmetric, not transitive.

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

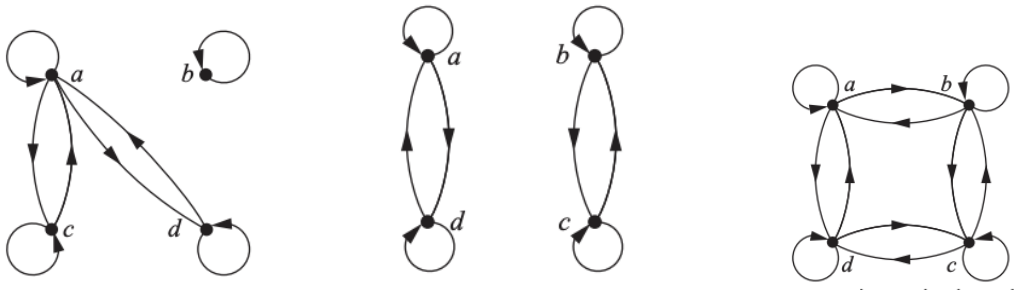

Figure 1: Three relations R_1 (left) R_2 (center) and R_3 (right) represented as digraphs.

Left is reflexive (there is a loop at each vertex), symmetric (every edge is accompanied by an edge pointing in the opposite direction) but not transitive (since edges (c, d) and (d, c) are missing). Center is an equivalence relation, right is reflexive and symmetric but not transitive.
Write the elements of each relation as a set and a binary matrix. If each is not an equivalence relation, 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)* $m = 8$?
      i. $[4]_2 = \{i | i \equiv 4 \pmod 2 = \{\cdots, -2, 0, 2, 4 \cdots\}$
      ii. $[4]_3 = \{i | i \equiv 4 \pmod 3 = \{\cdots, -5, -2, 1, 4, 7, \cdots\}$
      iii. $[4]_6 = \{i | i \equiv 4 \pmod 6 = \{\cdots, -14, -8, -2, 4, 10, \cdots\}$
      iv. $[4]_8 = \{i | i \equiv 4 \pmod 8 = \{\cdots, -20, -12, -4, 4, 12, \cdots\}$

   (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)* $n = -3$?
      i. $[2]_5 = \{i | i \equiv 2 \pmod 5 = \{\cdots, -8, -3, 2, 7, 12, \cdots\}$
      ii. $[3]_5 = \{i | i \equiv 3 \pmod 5 = \{\cdots, -7, -2, 3, 8, 13, \cdots\}$
      iii. $[6]_5 = \{i | i \equiv 6 \pmod 5 = \{\cdots, -9, -4, 1, 6, 11, \cdots\}$
      iv. $[-3]_5 = \{i | i \equiv -3 \pmod 5 = \{\cdots, -8, -3, 2, 7, 12, \cdots\}$

5. Find all solutions to the following linear congruences:

   (a) $5x \equiv 12 \pmod{23}$
   Note that $gcd(5, 23) = 1$ so there is one solution mod 23. Using EEA:

$$\begin{aligned}
23 = 4 \times 5 + 3 \quad &\Rightarrow \quad 3 = 23 - 4 \times 5 \\
5 = 1 \times 3 + 2 \quad &\Rightarrow \quad 2 = 5 - 1 \times 3 \quad \Rightarrow \quad 2 = 5 - (23 - 4 \times 5) \times 1 = (5)5 + (-1)23 \\
3 = 1 \times 2 + 1 \quad &\Rightarrow \quad 1 = 3 - 1 \times 2 \quad \Rightarrow \quad 1 = (23 - 4 \times 5) - 1 \times (5 \times 5 - 1 \times 23) \\
&\Rightarrow 1 = -9 \times 5 + 2 \times 23
\end{aligned}$$

   Therefore -9 is the inverse to $5x \equiv 12 \pmod{23} \Rightarrow (-9)5x \equiv (-9)12 \pmod{23} \Rightarrow x \equiv -108 \pmod{23} \Rightarrow x \equiv 7 \pmod{23}$.

   (b) $210x \equiv 40 \pmod{212}$
   Factoring:

$$105x \equiv 20 \pmod{106}$$

Using the EEA:

$$106 = 1 \times 105 + 1 \Rightarrow 1 = 106 - 1 \times 105$$

Therefore -1 is an inverse and $x \equiv -20 \pmod{106}$ or $x \equiv 86 \pmod{106}$. Converting to our modulus $x \equiv 86 \pmod{212}$ or $x \equiv 192 \pmod{212}$.

(c) $33x \equiv 7 \pmod{143}$
$gcd(33, 143) = 11$ but $11 \nmid 7$ therefore no solutions.

(d) $124x \equiv 132 \pmod{900}$
The $gcd(124, 900) = 4$ therefore we can simplify to obtain $31x \equiv 33 \pmod{225}$. The $gcd(a, m) = 1$ hence we acn find an inverse of 31 $\pmod{225}$

$$\begin{aligned} 225 = 7 \times 31 + 8 \quad &\Rightarrow \quad 8 = 225 - 7 \times 31 \\ 31 = 3 \times 8 + 7 \quad &\Rightarrow \quad 7 = 31 - 3 \times 8 \\ 8 = 1 \times 7 + 1 \quad &\Rightarrow \quad 1 = 8 - 1 \times 7 \end{aligned}$$

Backsubstituting we find that $1 = 31(-1) + (225 + 31(-7)) \times 4 = 4 \times 225 - 29 \times 31$. Therefore -29 is an inverse of 31 $\pmod{225}$.

$$\begin{aligned} (-29)31x &\equiv (-29)33 \pmod{225} \\ x &\equiv -957 \pmod{225} \\ x &\equiv 168 \pmod{225} \end{aligned}$$

We can obtain other solutions by adding 225: $x \equiv 168 + 225 = 393, x \equiv 168 + 2 \times 225 = 618, x \equiv 168 + 3 \times 225 = 843$, all $\pmod{900}$.

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.
   First note that R is reflexive since any coloring can be obtained from itself via rotation by 360 degrees. To see that R is symmetric and transitive, note that each rotation is the composition of two reflections and conversely the composition of two reflections is a rotation. Therefore $(C_1, C_2) \in R$ iff C_2 can be obtained from C_1 by composition of reflections. Hence if $(C_1, C_2) \in R$ then $(C_2, C_1) \in R$ (the inverse of a composition of reflections is also a composition of reflections) and R is symmetric. To check whether R is transitive, we note that if $(C_1, C_2) \in R$ and $(C_2, C_3) \in R$ then the composition of reflections in each case produces a composition of reflections so that $(C_1, C_3) \in R$.

   (b) What are the equivalence classes of R?
   Each coloring corresponds to a sequence of length four, with R and B denoting the colors. The equivalence classes are as follows:

$$\{RRRR\}, \{BBBB\}, \{RRRB, RRBR, RBRR, BRRR\}, \{RBBR, BRRB\}$$

$$\{BBBR, BBRB, BRBB, RBBB\}, \{RRBB, BRBR, BBRR, RBRB\}$$

7. Prove that if $a_0 \equiv a \ (mod\ n)$ and $b_0 \equiv b \ (mod\ n)$ then $(a_0 \ (mod\ n)) \cdot (b_0 \ (mod\ n)) \equiv (a \cdot b) \ (mod\ n)$.
   By the EEA there exist integers q_a, q_b, r_a, r_b such that $a = q_a n + r_a$ and $b = q_b n + r_b$. Plugging into the RHS:

$$(q_a n + r_a)(q_b n + r_b) \pmod{n} = (q_a q_b n^2 + q_a r_b n + q_b r_a n + r_a r_b) \pmod{n}$$

   All therms are divisible by n except for the remainder $r_a r_b$, therefore ab mod n = $r_a r_b$ mod n.

8. Solve the following system of congruences:

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

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

   Set $N = 5 \times 7 \times 11 = 385$. Then $N_1 = N/5 = 77, N_2 = N/7 = 55, N3 = N/11 = 35$. Working out the multiplicative inverses for each N_i modulo n_i. $N_1 \equiv 77 \equiv 2 \pmod 5 \Rightarrow x_1 = 3$.

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

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

   Reduce the above:

   $$x \equiv 3 \pmod 7$$
   $$x \equiv 3 \pmod 5$$
   $$x \equiv 4 \pmod{12}$$

   Set $N = 7 \times 5 \times 12 = 756$. Then $N_1 = 5 \times 12 = 60 \equiv 4 \pmod 7$, $N_2 = 7 \times 12 = 84 \equiv 4 \pmod 5$, and $N_3 = 7 \times 5 = 35 \equiv 11 \pmod{12}$. Putting terms together we see that $x = 2 \times 60 \times 2 + 4 \times 84 \times 3 + 11 \times 35 \times 4 = 2908$. Therefor any solution $x \equiv 2908 \equiv 388 \pmod{420}$.

   (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.
   Out of 1500 soldiers, the number x of soldiers that remain satisfies $x \equiv 1 \pmod 5$, $x \equiv 3 \pmod 7$, and $x \equiv 3 \pmod{11}$. We can thus apply the CRT as follows:

i	a_i	n_i	N_i	$N_i \pmod{n_i}$	y_i
1	1	5	77	2	3
2	3	7	55	-1	-1
3	3	11	35	2	6

   We can obtain an integer satisfying the above by computing:

   $$x = \sum a_i N_i y_i = 1 \times 77 \times 3 + 3 \times 55 \times -1 + 3 \times 35 \times 6 = 231 - 165 + 630 = 696$$

   The set of solutions is the set of integers that differ from 696 by a multiple of N, where $N = 5 \times 7 \times 11 = 385$. Since only a few soldiers deserted, the number remaining should be the largest integer less than 1500 that is congruent to 696 modulo 385. Since $696 + 2 \times 385 = 1466$, we conclude that 34 soldiers deserted.

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?
    Suppose the $gcd(a, b) = d$. Then $d \mid a$ and $d \mid b \iff d \mid b$ and $d \mid a$. Therefore $gcd(a, b) = gcd(b, a) = d$ and f is commutative.

To show that f is associative we need to prove $gcd(a, gcd(b, c)) = gcd(gcd(a, b), c)$. Note that $d \mid gcd(a, b)$ and $d \mid c \Rightarrow d \mid gcd(gcd(a, b), c)$ and $d \mid a$ and $d \mid b$. Therefore $d \mid c, d \mid a$ and $d \mid b \Rightarrow d \mid (gcd(a, gcd(b, c))\ \forall a, b, c \in \mathbb{Z}$. This implies that $gcd(a, gcd(b, c) = gcd(gcd(a, b), c)$ for any $d \mid a$, $d \mid b$, $d \mid c$ and thus f is associative.
If the identity element exists, then $gcd(a, e) = a$ so $a \mid a$ and $a \mid e$ but $a \nmid e$. Therefore $\nexists e$ such that $gcd(a, e) = a$.

(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?
$|A| = 32 \times 38 = 1216$. The identity element for f is $p^{31}q^{37}$.

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

(a) Expand $(a + b)^5$

$$\binom{5}{0}a^5 + \binom{5}{1}a^4b^1 + \binom{5}{2}a^3b^2 + \binom{5}{3}a^2b^3 + \binom{5}{4}a^1b^4 + \binom{5}{5}b^5$$

(b) Expand $(x + 2)^6$

$$\binom{6}{0}x^6 + \binom{6}{1}x^5 2^1 + \binom{6}{2}x^4 2^2 + \binom{6}{3}6^3 2^3 + \binom{6}{4}x^2 2^4 + \binom{6}{5}x 2^5 + \binom{6}{6}2^6$$

(c) Expand $(2x + 3)^4$

$$\binom{4}{0}(2x)^4 + \binom{4}{1}(2x)^3 3^1 + \binom{4}{2}(2x)^2 3^2 + \binom{4}{3}(2x)^1 2^3 + \binom{4}{4}3^4$$

(d) Expand $(\sqrt{2} + 1)^5 + (\sqrt{2} - 1)^5$ and simplify.

$$\begin{aligned}&\binom{5}{0}\sqrt{2}^5 + \binom{5}{1}\sqrt{2}^4 + \binom{5}{2}\sqrt{2}^3 + \binom{5}{3}\sqrt{2}^2 + \binom{5}{4}\sqrt{2}^1 + \binom{5}{5}1\\ &+\binom{5}{0}\sqrt{2}^5 - \binom{5}{1}\sqrt{2}^4 + \binom{5}{2}\sqrt{2}^3 - \binom{5}{3}\sqrt{2}^2 + \binom{5}{4}\sqrt{2}^1 - \binom{5}{5}1\\ &= 2(1 \times 4\sqrt{2} + 10 \times 2\sqrt{2} + 5 \times \sqrt{2}) = 58\sqrt{2}\end{aligned}$$

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?
The result is an example of Catalan numbers which obey the following combinatorial identity:

$$\text{For } n \geq 0\,,\ \text{there are } \mathcal{C}_n = \frac{1}{1+n}\binom{2 \times n}{n} \text{ paths from } (0, 0) \text{ to } (n, n)$$

Plugging in for $(0, 0)$ to $(3, 3)$ and $(0, 0)$ to $(4, 4)$ we have:

$$\mathcal{C}_3 = \frac{1}{1+3}\binom{2 \times 3}{3} = 5 \qquad , \qquad \mathcal{C}_4 = \frac{1}{1+4}\binom{2 \times 4}{4} = 14$$

For $n \geq 0$, since we never fall below the line $y = x$ the first move is U and the last move is R.

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.
We can prove this using a result similar to the Fundamental Theorem of Algebra by using induction on degree.

Base case: We will examine a polynomial of degree 1 (mod p) of the form $ax - b = 0$ (mod p). Here a, b are elements of arithmetic mod p and $a \neq 0$. It follows that a has an inverse a^{-1} (mod p) so the unique root is $x = a^{-1}b$. Therefore the result holds for the base case.

Inductive Hypothesis: Assume every polynomial of degree k over $\mathbb{Z}_p$ has at most k roots.

Inductive Step: Let P be a polynomial of degree $k+1$. If P does not have a root then the statement holds trivially. Assume P has a root a so that $P(a) = 0$. Using the division algorithm we can write $P(x) = (x - a)Q(x) + R$ where $Q(x)$ is a degree k polynomial, R is a degree 0 polynomial. Since a is a root $\Rightarrow P(a) = 0 \Rightarrow R = 0 \Rightarrow P(x) = (x - a)Q(x)$. Note that mod p arithmetic has no divisors of zero since p is prime. Therefore, the only roots of P (mod p) are roots of $(x - a)$ (mod p) and roots of Q (mod p). Since $x - a$ has one root, and Q has at most k roots (by the inductive hypothesis), it follows that P has at most k+1 roots.

14. For every positive integer n, show that:

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

This follows from the fact that $\binom{n}{k} = \binom{n}{n-k}$. To show, expand into factorials and cancel terms.

15. Prove the hexagon property:

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

Expand into factorials. Both products are equal to $f(n)/f(n-k)f(k)$ where $f(n) = (n+1)!n!(n-1)!$.

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

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

Let $\epsilon_p(a)$ be the exponent by which the prime p divides a, and let $m = n - k$. The identity to be proved reduces to:

$$\begin{aligned}&\min(\epsilon_p(m) - \epsilon_p(m+k),\ \epsilon_p(m+k+1) - \epsilon_p(k+1),\ \epsilon_p(k) - \epsilon_p(m+1))\\ &= \min(\epsilon_p(k) - \epsilon_p(m+k),\ \epsilon_p(m) - \epsilon_p(k+1),\ \epsilon_p(m+k+1) - \epsilon_p(m+1))\end{aligned}$$

Let's write this compactly as $\min(x_1, y_1, z_1) = \min(x_2, y_2, z_2)$. Notice that $x_1 + y_1 + z_1 = x_2 + y_2 + z_2$. The general relation $\epsilon_p(a) < \epsilon_p(b) \Rightarrow \epsilon_p(a) = \epsilon_p(|a \pm b|)$ allows us to conclude that $x_1 \neq x_2 \Rightarrow \min(x_1, x_2) = 0$. The same holds for (y_1, y_2) and (z_1, z_2). It is now straightforward to complete the proof.

17. Let p be prime. Show that $\binom{p}{k}$ (mod p) $= 0$ for $0 < k < p$. What does this imply about the binomial coefficients $\binom{p-1}{k}$?
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 $p \mid \binom{p}{i}$. Since $\binom{p}{k} = \binom{p-1}{k} + \binom{p-1}{k-1}$, it follows that $\binom{p-1}{k} \equiv (-1)^k$ (mod p).

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 definition 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:

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

Multiplying and dividing the above gives:

$$\frac{(-1/2)!}{x!(x-1/2)!} = \lim_{n\to\infty} \binom{n+x}{n}\binom{n+x-1/2}{n} n^{-2x} \binom{n-1/2}{n}$$

Applying the duplication formula $\binom{n-1/2}{n} = \binom{2n}{n}/2^{2n}$:

$$= \lim_{n\to\infty} \binom{2n+2x}{2n} n^{-2x}$$

Also $1/(2x)! = \lim_{n\to\infty} \binom{2n+2x}{2n}(2n)^{-2x}$, therefore the equivalent Gamma function is:

$$\Gamma(x)\Gamma(x+1/2) = \Gamma(2x)\Gamma(1/2)/2^{2x-1}$$

19. Prove that the set S of polynomials of degree k with coefficients in $\mathbb{Z}_p$ form a group under addition modulo p.
The definition of addition of polynomials and addition modulo p imply that the sum of two elements of S is in S. The identity element is the polynomial with coefficients all 0. The inverse of $f \in S$ is the polynomial whose coefficients are the inverses of $\mathbb{Z}_p$ of the coefficients of f. Associativity of addition of elements of S follows from associativity of addition modulo p for each coefficient.

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 $[a]^p$.
    Let R be the relation on $[a]^p$ defined by putting $(x, y) \in R$ if the p-tuple y arises from x by a cyclic shift.
    Every p-tuple is a cyclic shift of itself, so R is reflexive. The inverse of a cyclic shift is a cyclic shift, so R is symmetric. The compisition of two cyclic shifts is a cyclic shift, so R is transitive. Hence R is an equivalence relation.

    (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.
    To obtain a set S of size $a^p - a$, discard from $[a]^p$ the a elements that use only one value. Each forms an equivalence class of size 1 under R. If the remaining equivalence classes partition S into sets of size p, then p divides $[a]^p - a$.
    If $x \in S$, then p cyclic shifts apply to x, so each class has size at most p. By way of contradiction, suppose that some class has size less than p. In shifting an element by $0, 1, \cdots, p-1$ positions to obtain all members of the class, some member must appear twice. If y appears when we shift x by i or j, then shifting y by $j - i$ positions does not change it. Let $b = j - i$; shifting y by any multiple of b positions also leaves it unchanged. By Fermat's Little Theorem, 1 is a multiple of b modulo p. We conclude that shifting y by one position leaves it unchanged. This requires that each entry in y is the same as the next, but we explicitly omitted such p-tuples from S. The contradiction implies that R partitions S into equivalence classes of size p. □