1. **(9 points)** *The following questions will explore this slightly obscure relation property.*

   Definition 1. A relation R on a set S is *antireflexive* if and only if, for all $a \in S$, $(a, a) \notin R$; in other words, $a \not R\, a$ for all $a \in S$.

   (a) **(2 points)** *Demonstrate, either by example or explanation, that there exist relations which are neither reflexive nor antireflexive.*

   If there is *any* element a of S such that $a \not R\, a$, then R is nonreflexive; likewise, if there is *any* $b \in S$ such that $b\, R\, b$, then R is not antireflexive. There are several such relations on sets of 2 or more elements; the simplest one is $R = \{(b, b)\}$ on the set $S = \{a, b\}$.

   (b) **(7 points)** Prove that for a set S, if $R \subseteq S \times S$ is an antireflexive, symmetric, and transitive relation, then $R = \emptyset$.

   Proof. We shall proceed by contradiction; suppose R is antireflexive, symmetric, and transitive, but $R \neq \emptyset$. Since R is not empty, there is some $(a, b) \in R$, i.e. there are some $a, b \in S$ so that $a\, R\, b$. By symmetry, it is also true that $b\, R\, a$. Then transitivity on the two true statements $a\, R\, b$ and $b\, R\, a$ yields that $a\, R\, a$, but by antireflexivity, R must also satisfy the contradictory condition $a \not R\, a$. □

2. **(25 points)** *The following proofs concern unions and intersections of relations; if R_1 and R_2 are considered as subsets of $S \times S$, we may take $R_1 \cup R_2$ and $R_1 \cap R_2$ to represent the ordinary operations on these sets.*

   (a) **(5 points)** *Prove or disprove that, for relations R_1 and R_2 on S, if either R_1 or R_2 is reflexive, then the relation $R_1 \cup R_2$ is reflexive.*

   Proposition 1. *For relations R_1 and R_2 on the set S, if either R_1 or R_2 is reflexive, then $R_1 \cup R_2$ is reflexive.*

   Proof. Without loss of generality, we may consider the specific premise that R_1 is reflexive, so that for every element a of S, $(a, a) \in R_1$. Since $R_1 \subseteq (R_1 \cup R_2)$, it thus follows that for every element a of S, $(a, a) \in (R_1 \cup R_2)$, so $R_1 \cup R_2$ is reflexive. □

   As a point of interest, the converse is *not* true: $R_1 \cup R_2$ could be reflexive even if each of R_1 and R_2 are not themselves reflexive. For instance, if $S = \{a, b\}$, $R_1 = \{(a, a)\}$, and $R_2 = \{(b, b)\}$, then neither R_1 nor R_2 is reflexive, but $R_1 \cup R_2$ is.

   (b) **(5 points)** *Prove or disprove that, for relations $R5_1$ and R_2 on S, if both R_1 and R_2 are symmetric, then the relation $R_1 \cup R_2$ is symmetric.*

   Proposition 2. *For relations R_1 and R_2 on the set S, if both R_1 and R_2 are symmetric, then $R_1 \cup R_2$ is symmetric.*

   Proof. Symmetry of $R_1 \cup R_2$ is equivalent to the implication that if $(a, b) \in (R_1 \cup R_2)$, then $(b, a) \in (R_1 \cup R_2)$. We may show that an assertion is true by assuming its premise and working to its conclusion; thus we may take as an overall premise for our proof the facts that R_1 is symmetric, R_2 is symmetric, and that some $(a, b) \in (R_1 \cup R_2)$; from this we hope to prove that $(b, a) \in (R_1 \cup R_2)$.

   Since $(a, b) \in (R_1 \cup R_2)$, either $(a, b) \in R_1$ or $(a, b) \in R_2$. Without loss of generality we may consider the case $(a, b) \in R_1$. Since R_1 is symmetric, it thus follows that $(b, a) \in R_1$, and since $R_1 \subseteq (R_1 \cup R_2)$, it follows that $(b, a) \in (R_1 \cup R_2)$. □

(c) **(5 points)** *Prove or disprove that, for relations R_1 and R_2 on S, if both R_1 and R_2 are transitive, then the relation $R_1 \cup R_2$ is transitive.*

We disprove the above statement by counterexample. Consider, for example, the following relations on the real numbers: $R_1 = \{(a,b) \in \mathbb{R}\times\mathbb{R} : a < b\}$ and $R_2 = \{(a,b) \in \mathbb{R}\times\mathbb{R} : a > b\}$. Demonstrably R_1 and R_2 are each transitive, since both the "less than" and "greater than" relations are in fact transitive, but $R_1 \cup R_2 = \{(a,b) \in \mathbb{R}\times\mathbb{R} : a \neq b\}$ is not transitive (as a specific example, $(1,3) \in R_1 \cup R_2$ and $(3,1) \in R_1 \cup R_2$, but $(1,1) \notin R_1 \cup R_2$).

(d) **(5 points)** *Prove that for equivalence relations R_1 and R_2 on S, $R_1 \cap R_2$ is an equivalence relation* (note: this is the intersection, whereas the previous questions discussed the union).

We shall prove reflexivity, symmetry, and transitivity, mostly by modifying our above proofs (hurrah for copy and paste!):

Proposition 3. *For relations R_1 and R_2 on the set S, if both R_1 and R_2 are equivalence relations, then $R_1 \cup R_2$ is an equivalence relation.*

Proof of reflexivity. Since both R_1 and R_2 are reflexive, it follows that for every element a of S, $(a,a) \in R_1$ and $(a,a) \in R_2$. Thus, for every element a of S, $(a,a) \in R_1 \cap R_2$, so $R_1 \cap R_2$ is reflexive. □

Proof of symmetry. Symmetry of $R_1 \cap R_2$ is equivalent to the implication that if $(a,b) \in (R_1 \cap R_2)$, then $(b,a) \in (R_1 \cap R_2)$. We may show that an assertion is true by assuming its premise and working to its conclusion; thus we may take as an overall premise for our proof the facts that R_1 is symmetric, R_2 is symmetric, and that some $(a,b) \in (R_1 \cap R_2)$; from this we hope to prove that $(b,a) \in (R_1 \cap R_2)$.

Since $(a,b) \in (R_1 \cap R_2)$, both $(a,b) \in R_1$ and $(a,b) \in R_2$. Since both R_1 and R_2 are symmetric, it thus follows respectively that $(b,a) \in R_1$ and $(b,a) \in R_2$. Thus $(b,a) \in (R_1 \cup R_2)$. □

Proof of transitivity. Transitivity of $R_1 \cap R_2$ is equivalent to the implication that if $(a,b) \in (R_1 \cap R_2)$ and $(b,c) \in (R_1 \cap R_2)$, then $(a,c) \in (R_1 \cap R_2)$. We may show that an assertion is true by assuming its premise and working to its conclusion; thus we may take as an overall premise for our proof the facts that R_1 is transitive, R_2 is transitive, that some $(a,b) \in (R_1 \cap R_2)$ and $(b,c) \in (R_1 \cap R_2)$; from this we hope to prove that $(a,c) \in (R_1 \cap R_2)$.

Since $(a,b) \in (R_1 \cap R_2)$, both $(a,b) \in R_1$ and $(a,b) \in R_2$; likewise from $(b,c) \in (R_1 \cap R_2)$, both $(b,c) \in R_1$ and $(b,c) \in R_2$. Since both R_1 and R_2 are transitive, it follows from the fact that $(a,b) \in R_1$ and $(b,c) \in R_1$ that $(a,c) \in R_1$ and from the fact that $(a,b) \in R_2$ and $(b,c) \in R_2$ that $(a,c) \in R_2$. Thus $(a,c) \in (R_1 \cup R_2)$. □

(e) **(5 points)** *If $x \in S$ and R_1 and R_2 are equivalence relations of S, what is the relationship between the equivalence classes of x with respect to R_1, R_2, and $R_1 \cap R_2$?*

Let us denote the above equivalence classes $[x]_{R_1} = \{s \in S : (x,s) \in R_1\}$, $[x]_{R_2} = \{s \in S : (x,s) \in R_2\}$, and $[x]_{R_1 \cap R_2} = \{s \in S : (x,s) \in R_1 \cap R_2\}$. Since the condition $(x,s) \in R_1 \cap R_2$ is satisfied if and only if (x,s) is an element of both R_1 and R_2 — i.e., when $s \in [x]_{R_1}$ and $s \in [x]_{R_2}$ — it is fairly easy to see that $[x]_{R_1 \cap R_2} = [x]_{R_1} \cap [x]_{R_2}$.

3. **(6 points)** *Prove or disprove and salvage if possible: for $[a], [b] \in \mathbb{Z}_n$ for a positive integer n, if $[a] \cdot [b] = 0$, then either $[a] = [0]$ or $[b] = [0]$.*

This is a clearly false statement in general: considering $\mathbb{Z}_6$, we might note that $[2] \cdot [3] = [6] = [0]$, but that neither the congruence class $[2]$ nor the congruence class $[3]$ is identical to the congruence class $[0]$. However, this weaker version can be proven:

Proposition 4. *For $[a], [b] \in \mathbb{Z}_n$ for a prime positive integer n, if $[a] \cdot [b] = [0]$, then either $[a] = [0]$ or $[b] = [0]$.*

Proof. Definitionally, $[a] \cdot [b] = [ab]$, so given that $[ab] = [0]$, it follows that $ab \equiv 0 \pmod{n}$, or alternatively that $n \mid (ab - 0)$. From a result in question 1(b) of problem set #3, we can derive from prime n that if $n \mid ab$ then either $n \mid a$ or $n \mid b$. If $n \mid a$, then $a \equiv 0 \pmod{n}$, so $[a] = [0]$; likewise for b. □

4. **(4 point bonus)** *Prove that for a positive integer n, the perfect squares lie in at most $\lceil \frac{n+1}{2} \rceil$ different congruence classes modulo n.*

It is easiest to argue this in terms of two separate cases: when n is even, there are no more than $\frac{n}{2} + 1$ congruence classes containing perfect squares, and when n is odd, there are no more than $\frac{n+1}{2}$ congruence classes containing perfect squares. First, however, let us note that for any k, when considerign the elements of $\mathbb{Z}_n$, it is the case that $[k^2] = [k \cdot k] = [k] \cdot [k]$, and since there are only n different values for $[k]$, it is easy to calculate the specific classes which can contain squares by exhaustively considering each $[k] \cdot [k]$. For instance, modulo 10, we might look at the following 10 products of congruence classes:

$$
\begin{aligned}
[0] \cdot [0] &= [0] \\
[1] \cdot [1] &= [1] \\
[2] \cdot [2] &= [4] \\
[3] \cdot [3] &= [9] \\
[4] \cdot [4] = [16] &= [6] \\
[5] \cdot [5] = [25] &= [5] \\
[6] \cdot [6] = [36] &= [6] \\
[7] \cdot [7] = [49] &= [9] \\
[8] \cdot [8] = [64] &= [4] \\
[9] \cdot [9] = [81] &= [1]
\end{aligned}
$$

so, for instance, every square is congruent to 0, 1, 4, 5, 6, or 9 modulo 10.

The above example illuminates our overall proof strategy. Note that each $[k^2]$ and $[(n-k)^2]$ lie in the same congruence class, which is easy to show: $[(n-k)^2] = [n^2 - 2nk + k^2] = [k^2]$, since $n^2 - 2nk$ is a multiple of n, so as a general rule we can guarantee that two distinct congruence classes have the same square.

Proposition 5. *For a positive integer n, the perfect squares lie in at most $\lceil \frac{n+1}{2} \rceil$ different congruence classes modulo n.*

Proof. In the course of this proof, we shall use $[k]$ to represent the congruence class of k modulo n, and conventionally will consider specifically the labels $\mathbb{Z}_n = \{[0], [1], [2], \ldots, [n-1]\}$. For any integer k, as demonstrated prior to this proof, if $k \in [\ell]$, then $k^2 \in [\ell^2]$, so the congruence classes containing perfect squares are specifically $[0^2]$, $[1^2]$, $\ldots$, $[(n-1)^2]$. It was seen prior to this proof that $[k^2] = [(n-k)^2]$, so we may be certain that some of the above-listed congruence classes are in fact identical. How many of them we can apply this rule to depends on the parity of n:

Case I: n is even. Let $n = 2s$, where s is a positive integer. Then $[1^2] = [(2s-1)^2]$, $[2^2] = [(2s-2)^2]$, and so forth up to $[(s-1)^2] = [(s+1)^2]$. We may thus guarantee that there are at least $s-1$ identical pairs among the list $[0^2]$, $[1^2]$, $\ldots$, $[(n-1)^2]$. Thus there are no more than $n-(s-1) = s+1 = \frac{n}{2}+1$ distinct congruence classes in this list.

Case II: n is odd. Let $n = 2s+1$, where s is a non-negative integer. Then $[1^2] = [(2s)^2]$, $[2^2] = [(2s-1)^2]$, and so forth up to $[s^2] = [(s+1)^2]$. We may thus guarantee that there are at least s identical pairs among the list $[0^2]$, $[1^2]$, $\ldots$, $[(n-1)^2]$. Thus there are no more than $n-s = s+1 = \frac{n+1}{2}$ distinct congruence classes in this list. □

In fact, when n is prime, there are exactly $\left\lceil \frac{n+1}{2} \right\rceil$ congruence classes containing squares; these are called *quadratic residues*. There are simple rules (with rather advanced proofs) for determining which numbers are quadratic residues; the entire theory is detailed elsewhere under the name of *quadratic reciprocity*.

> Ha rossz kedvem van, matematizálok, hogy jó kedvem legyen. Ha jó kedvem van, matematizálok, hogy megmaradjon a jó kedvem. [When I'm in a bad mood, I do mathematics, so that my mood becomes good. When I'm in a good mood, I do mathematics, so that my mood stays good.] —Alfréd Rényi