# Problem set 8

# Equivalence Relations and modular arithmetic

**I**  Let R be a relation on a set *S*. What does it mean for R to be *reflexive*? *symmetric*? *transitive*? What is an *equivalence relation* on *S*? Explain how an equivalence relation corresponds to a partition on the set S. What does the term *equivalence class* mean?

1. Determine which of the three properties “reflexive,” “symmetric,” and “transitive,” apply to each of the following relations on Z, the set of integers. For each relation that is an equivalence relation, describe the equivalence classes.

a R b iff

1. a = b
2. a < b
3. a < b
4. a | b
5. |a| = |b|
6. a2 + a = b2 + b
7. a < |b|
8. ab > 0
9. ab 0
10. a + b > 0
11. a ≡ b mod 4
12. a ≡ b mod m (where mN)
13. Do the same as in (A) for the following relations on the set of all people who live in Illinois. p R q iff
    1. p “is a father of” q
    2. p “is a sister of” q
    3. p “is a friend of” q
    4. p “is an aunt of” q
    5. p “is a descendant of” q
    6. p “has the same height” as q
    7. p “likes” q
    8. p “knows” q
    9. p “is married to” q

## II Define a ≡ b mod m (for m > 0). Show that this is an equivalence relation on the set of integers, Z. In the following, assume that *a, b, c, d, m* are integers and that m > 0.

* + 1. Prove that if a ≡ b mod *m*, then
       1. a + c ≡ b + c mod *m*
       2. a – c ≡ b – c mod *m*
       3. ac ≡ bc mod m
    2. Show that if ac ≡ bc mod m (and *c* is not 0) then it need not follow that a ≡ b.

Prove that if d = gcd(c,m) and ac ≡ bc mod m, then a ≡ b mod m/d.

* + 1. Show that as a special case of the above we have:

If *c* and *m* are relatively prime and ac ≡ bc mod m, then a ≡ b mod *m*.

* + 1. Suppose that a ≡ b mod m and c ≡ d mod m. Prove that:

1. a + c ≡ b + d mod m *(addition rule)*
2. a – c ≡ b – d mod m *(subtraction rule)*
3. ac ≡ bd mod m *(multiplication rule)*
4. an bn mod m, for any nN *(exponentiation rule)*
5. a/e ≡ b/e mod m/gcd(m, e) where e is a positive integer that divides both a and b *(division rule)*
   * 1. Define addition and multiplication in Z4 and in Z5.

**III** Using modular arithmetic, find the remainder when

1. 2125 is divided by 7.
2. (12)(29)(408) is divided by 13
3. 71942 is divided is divided by 100
4. (419)(799) is divided by 5.

Restate each of the above as a statement in modular arithmetic.

**IV** (a) If it is now 2:00, what time would it be in 12345 hours?

(b) Is 22225555 + 55552222 divisible by 7?

**V** (a) Show that there is no integer x satisfying the equation 2x + 1 = 5x – 4

(b) Show that there is no integer x satisfying the equation 18x2 + 39x – 7 = 0

(c) Show that the system of equations

11x – 5y = 7

9x + 10y = -3

has no integer solution.

.



[Johann Carl Fredrich Gauss](http://www-gap.dcs.st-and.ac.uk/~history/Mathematicians/Gauss.html) introduced modular arithmetic.

[Course Home Page](http://www.math.luc.edu/~ajs/courses/201fall2015/index.pdf) [Department Home Page](http://www.math.luc.edu/) [Loyola Home Page](http://www.luc.edu/)