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?

(A) Determine which of the three properties "reflexive," "symmetric," and "transitive," apply to each of the following relations on $\mathbb{Z}$, the set of integers. For each relation that is an equivalence relation, describe the equivalence classes.

a R b iff

1. $a = b$
2. $a \leq b$
3. $a < b$
4. $a \mid b$
5. $|a| = |b|$
6. $a^2 + a = b^2 + b$
7. $a < |b|$
8. $ab > 0$
9. $ab \geq 0$
10. $a + b > 0$
11. $a \equiv b \mod 4$
12. $a \equiv b \mod m$ (where $m \in \mathbb{N}$)

(B) 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 $a \equiv b \bmod m$ (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 $m > 0$.

(A) Prove that if $a \equiv b \bmod m$, then

1. $a + c \equiv b + c \bmod m$
2. $a - c \equiv b - c \bmod m$
3. $ac \equiv bc \bmod m$

(B) Show that if $ac \equiv bc \bmod m$ (and *c* is not 0) then it need not follow that $a \equiv b$.

Prove that if $d = \gcd(c,m)$ and $ac \equiv bc \bmod m$, then $a \equiv b \bmod m/d$.

(C) Show that as a special case of the above we have:

If *c* and *m* are relatively prime and $ac \equiv bc \bmod m$, then $a \equiv b \bmod m$.

(D) Suppose that $a \equiv b$ mod m and $c \equiv d$ mod m. Prove that:

1. $a + c \equiv b + d$ mod m *(addition rule)*

2. $a - c \equiv b - d$ mod m *(subtraction rule)*

3. $ac \equiv bd$ mod m *(multiplication rule)*

4. a^n b^n mod m, for any $n \in \mathbb{N}$ *(exponentiation rule)*

5. $a/e \equiv b/e$ mod m/gcd(m, e) where e is a positive integer that divides both a and b *(division rule)*

(E) Define addition and multiplication in $\mathbb{Z}_4$ and in $\mathbb{Z}_5$.

III Using modular arithmetic, find the remainder when

(a) 2^{125} is divided by 7.

(b) (12)(29)(408) is divided by 13

(c) 7^{1942} is divided is divided by 100

(d) $(4^{19})(7^{99})$ 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 $2222^{5555} + 5555^{2222}$ 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 $18x^2 + 39x - 7 = 0$

(c) Show that the system of equations

$$11x - 5y = 7$$
$$9x + 10y = -3$$

has no integer solution.

.

Johann Carl Fredrich Gauss introduced modular arithmetic.