Math 230 **Spring 2019**
Homework 5 **Drew Armstrong**

Problem 1. Fractions. Consider the following set of ordered pairs:

$$S := \{(a,b) : a,b \in \mathbb{Z}, b \neq 0\}.$$

(a) Prove that the following is an *equivalence relation* on the set S:

$$(a,b) \sim (c,d) \quad \Longleftrightarrow \quad ad = bc.$$

(b) Prove that the following two operations are *well-defined* with respect to $\sim$:

$$(a,b) \times (c,d) := (ac, bd)$$
$$(a,b) + (c,d) := (ad + bc, bd).$$

(a) There are three things to show:

- **Reflexive.** For all $(a,b) \in S$ we have $(a,b) \sim (a,b)$ because $ab = ba$.
- **Symmetric.** Consider (a,b) and (c,d) in S such that $(a,b) \sim (c,d)$. By definition this means that $ad = bc$. But then we also have $cb = da$ which means that $(c,d) \sim (a,b)$.
- **Transitive.** Consider $(a,b), (c,d), (e,f) \in S$ and assume that $(a,b) \sim (c,d)$ and $(c,d) \sim (e,f)$. By definition this means that $ad = bc$ and $cf = de$. But then since $d \neq 0$ we have

$$\begin{aligned} ad &= bc \\ (ad)f &= (bc)f \\ (af)d &= b(cf) \\ (af)d &= b(de) \\ (af)d &= (bd)d \\ af &= be, \end{aligned}$$

and hence $(a,b) \sim (e,f)$.

(b) Assume that $(a,b) \sim (a',b')$ and $(c,d) \sim (c',d')$, so that $ab' = a'b$ and $cd' = c'd$. There are two things to show:

- Note that $(ac, bd) \sim (a'c', b'd')$ because
$$(ac)(b'd') = (ab')(cd') = (a'b)(c'd) = (a'c')(bd).$$
- Note that $(ad + bc, bd) \sim (a'd' + b'c', b'd')$ because
$$\begin{aligned} (ad+bc)(b'd') &= (ad)(b'd') + (bc)(b'd') \\ &= (ab')(dd') + (cd')(bb') \\ &= (a'b)(dd') + (c'd)(bb') \\ &= (a'd')(bd) + (b'c')(bd) \\ &= (a'd' + b'c')(bd). \end{aligned}$$

□

Problem 2. Modular Arithmetic. Fix an integer $n \geq 1$. We proved in class that the following is an equivalence relation on $\mathbb{Z}$, called *congruence mod n*:

$$a \sim_n b \quad \Longleftrightarrow \quad n|(a-b).$$

Prove that addition and multiplication of integers are *well-defined* with respect to $\sim_n$:

(a) For all $a, b, a', b' \in \mathbb{Z}$ with $a \sim_n a'$ and $b \sim_n b'$, prove that $a + b \sim_n a' + b'$.
(b) For all $a, b, a', b' \in \mathbb{Z}$ with $a \sim_n a'$ and $b \sim_n b'$, prove that $ab \sim_n a'b'$.

(a) Assume that $a \sim_n a'$ and $b \sim_n b'$, so that $a - a' = nk$ and $b - b' = n\ell$ for some $k, \ell \in \mathbb{Z}$. Then we have

$$(a+b) - (a'+b') = (a-a') + (b-b') = nk + n\ell = n(k+\ell),$$

which implies that $a + b \sim_n a' + b'$.

(b) Assume that $a \sim_n a'$ and $b \sim_n b'$, so that $a - a' = nk$ and $b - b' = n\ell$ for some $k, \ell \in \mathbb{Z}$. Then we have

$$\begin{aligned} ab - a'b' &= ab + 0 - a'b' \\ &= ab + (-ab' + ab') - a'b' \\ &= a(b-b') + (a-a')b' \\ &= an\ell + nkb' \\ &= n(a\ell + kb'), \end{aligned}$$

and hence $ab \sim_n a'b'$. [Remark: That was a good trick. There are other ways two solve this, such as substituting $a = nk + a'$ and $b = n\ell + b'$ into $ab - a'b'$.] □

Problem 3. Linear Congruence Theorem. Fix the modulus $n = 22$. Since $\gcd(7, 22) = 1$ we know from the Linear Congruence Theorem that the equation $7x \sim_{22} 1$ has a solution.

(a) Use the Euclidean Algorithm to find this solution.
(b) Use your answer from part (a) to solve the following linear congruences:

$$\begin{aligned} 7a &\sim_{22} 10, \\ 7b &\sim_{22} 11, \\ 7c &\sim_{22} 12. \end{aligned}$$

(a) In order to solve the congruence $7x \sim_{22} 1$ we consider the equation $7x + 22y = z$ and apply the Euclidean Algorithm:

x	y	z
0	1	22
1	0	7
−3	1	1

We conclude that $7(-3) + 22(1) = 1$ and hence

$$1 \sim_{22} 7(-3) + 22(1) \sim_{22} 7(-3) + 0(1) \sim_{22} 7(-3).$$

In other words, $x \sim_{22} -3$. We can also express this in standard form as $x \sim_{22} 19$.

(b) From part (a) we know that "dividing by 7" is the same as "multiplying by 19" mod 22. This allows us to solve the three congruences quickly:

$$\begin{aligned} 7a &\sim_{22} 10 \\ 19 \cdot 7a &\sim_{22} 19 \cdot 10 \\ 1 \cdot a &\sim_{22} 190 \\ a &\sim_{22} 190 \sim_{22} 14, \end{aligned}$$

$$\begin{aligned} 7b &\sim_{22} 11 \\ 19 \cdot 7b &\sim_{22} 19 \cdot 11 \\ 1 \cdot b &\sim_{22} 209 \\ b &\sim_{22} 209 \sim_{22} 11, \end{aligned}$$

$$\begin{aligned} 7c &\sim_{22} 12 \\ 19 \cdot 7c &\sim_{22} 19 \cdot 12 \\ 1 \cdot c &\sim_{22} 228 \\ c &\sim_{22} 228 \sim_{22} 8. \end{aligned}$$

Problem 4. Fermat's Little Theorem. In this problem you will give an induction proof of Fermat's Little Theorem. You may assume the following statement, which we proved in class. For all $a, b, p \in \mathbb{Z}$ with p prime we have

$$(a+b)^p \sim_p a^p + b^p.$$

Now fix a prime $p \in \mathbb{Z}$ and for any $n \in \mathbb{Z}$ consider the statement $P(n) =$ "$n^p \sim_p n$."

(a) Observe that $P(0)$ and $P(1)$ are true.
(b) If $P(n)$ is true, prove that $P(n+1)$ is also true.
(c) If $P(n)$ is true, prove that $P(-n)$ is also true.

(a) These statements are true because $0^p = 0$ and $1^p = 1$.

(b) Assume for induction that $P(n)$ is true so that $n^p \sim_p n$. Then from the assumption $(a+b)^p \sim_p a^p + b^p$ with $a = n$ and $b = 1$ we have

$$(n+1)^p \sim_p n^p + 1^p \sim_p n + 1,$$

which means that $P(n+1)$ is also true.

(c) Assume that $P(n)$ is true so that $n^p \sim_p n$. Now there are two cases:

- If p is odd then we have $(-n)^p = (-1)n^p \sim_p (-1)n = -n$ and hence $P(-n)$ is true.
- If p is even then since p is prime we must have $p = 2$. In this case we observe that $n \sim_2 -n$ for all $n \in \mathbb{Z}$ because $n - (-n) = 2n$. It follows that

  $$(-n)^2 = n^2 \sim_2 n \sim_2 -n$$

  and hence $P(-n)$ is true. □