Silvain Rideau silvain.rideau@berkeley.edu
1091 Evans www.normalesup.org/~srideau/en/teaching

Solutions to homework 1

Due September 6th

Problem 1 (Equivalence relation) **:**
Let $f : X \to Y$ be a function and let $x_1 \sim x_2$ hold if $f(x_1) = f(x_2)$.

1. Show that $\sim$ is an equivalence relation on X.

   Solution: Since, for all $x \in X$, $f(x) = f(x)$, we do have that $\sim$ is reflexive. For all $x_1, x_2 \in X$, if $f(x_1) = f(x_2)$, then $f(x_2) = f(x_1)$, so $\sim$ is symmetric. Finally, if $x_1, x_2, x_3 \in X$ are such that $f(x_1) = f(x_2)$ and $f(x_2) = f(x_3)$, then we do have $f(x_1) = f(x_3)$ and hence $\sim$ is transitive.

2. Assume that f is surjective. Show that there exists a bijection $g : Y \to \{\overline{x} : x \in X\}$, where $\overline{x}$ denotes the $\sim$-class of x.

   Solution: Let $g(\overline{x}) = f(x)$. First we have to check that g is well defined. But if $\overline{x_1} = \overline{x_2}$, then $x_1 \sim x_2$ and, by definition $f(x_1) = f(x_2)$. So g is well defined. Since f is surjective, for all $y \in Y$, we can find $x \in X$ such that $f(x) = y$, but then $g(\overline{x}) = f(x) = y$ and therefore g is surjective. Finally if $g(\overline{x_1}) = g(\overline{x_2})$, then we have $f(x_1) = g(\overline{x_1}) = g(\overline{x_2}) = f(x_2)$. It follows that $x_1 \sim x_2$ and hence $\overline{x_1} = \overline{x_2}$. So g is injective.

Problem 2 :

1. Which are the $x \in \mathbb{Z}$ such that there exists $y \in \mathbb{Z}$ with $x \equiv y^2 \mod 9$.

   Solution: We have $0^2 \equiv 0 \mod 9$, $1^2 \equiv 1 \mod 9$, $2^2 \equiv 4 \mod 9$, $3^2 \equiv 0 \mod 9$, $4^2 \equiv 7 \mod 9$, $5^2 \equiv (-4)^2 \equiv 7 \mod 9$, $6^2 \equiv (-3)^2 \equiv 0 \mod 9$, $7^2 \equiv (-2)^2 \equiv 4 \mod 9$ and $8^2 \equiv (-1)^2 \equiv 1 \mod 9$. So the squares in $\mathbb{Z} \mod 9\mathbb{Z}$ are $\overline{0}$, $\overline{1}$, $\overline{4}$ and $\overline{7}$.

2. Which are the $x \in \mathbb{Z}$ such that there exists $y, z \in \mathbb{Z}$ with $x \equiv y^2 + z^2 \mod 9$.

   Solution: We have four squares and therefore sixteens sums of two squares to compute. Because addition is Abelian, we can get away with computing only ten of them: $0+0 \equiv 0 \mod 9$, $0+1 \equiv 1 \mod 9$, $0+4 \equiv 4 \mod 9$, $0+7 \equiv 7 \mod 9$, $1+1 \equiv 2 \mod 9$, $1+4 \equiv 5 \mod 9$, $1+7 \equiv 8 \mod 9$, $4+4 \equiv 8 \mod 9$, $4+7 \equiv 2 \mod 9$ and $7+7 \equiv 5 \mod 9$. So every element of $\mathbb{Z} \mod 9\mathbb{Z}$ except for $\overline{3}$ and $\overline{6}$, is a sum of two squares.

3. Show that if $x, y, z \in \mathbb{Z}$ are such that $x^2 + y^2 \equiv 12 \cdot z^2 \mod 9$, then $x \equiv y \equiv z \equiv 0 \mod 3$.

   Solution: If $x^2 + y^2 \equiv 12 \cdot z^2 \mod 9$ then we have an element of $\mathbb{Z} \mod 9\mathbb{Z}$ which is both a sum of two squares and a multiple of $\overline{3}$. Since, according to our previous computation, the only multiple of $\overline{3}$ that is a sum of two squares is $\overline{0}$, it follows that $x^2 + y^2 \equiv 12 \cdot z^2 \equiv 3 \cdot z^2 \equiv 0 \mod 9$. But if one checks our previous computation, the only way $x^2 + y^2 \equiv 0 \mod 9$ is if x and y are both congruent to either 0 or 3 mod 9. In both cases, it means that $x \cong y \equiv 0 \mod 3$.

   Moreover, if $3 \cdot z^2 \equiv 0 \mod 9$ then it means that 9 divides $3 \cdot z^2$ and hence 3 divides z^2. But since 3 is prime, it follows that 3 divides z. So we also have $z \equiv 0 \mod 3$.

4. Show that if there exists x, y, $z \in \mathbb{Z}_{>0}$ such that $x^2 + y^2 = 12 \cdot z^2$ then there exists x', y', $z' \in \mathbb{Z}_{>0}$ such that $(x')^2 + (y')^2 = 12 \cdot (z')^2$, $x' < x$, $y' < y$ and $z' < z$.

   Solution: By the previous question, we have that $x \equiv y \equiv z \equiv 0 \mod 3$ and therefore there exists x', y' and $z' \in \mathbb{Z}$ such that $x = 3x'$, $y = 3y'$ and $z = 3z'$. Since x is positive, so is x' and since $x \neq 0$, $x' < 3x' = x$. The same holds for y' and z'. Moreover, we have $x^2 + y^2 = 9 \cdot (x')^2 + 9 \cdot (y')^2 = 12 \cdot z^2 = 12 \cdot 9 \cdot (z')^2$ so $(x')^2 + (y')^2 = 12 \cdot (z')^2$.

5. Conclude that if x, y, $z \in \mathbb{Z}$ are such that $x^2 + y^2 = 12 \cdot z^2$ then they are all equal to 0.

   Solution: Let $x \in \mathbb{Z}_{>0}$ be minimal such that there exists y, $z \in \mathbb{Z}_0$ such that $x^2 + y^2 = 12 \cdot z^2$. By the previous question, we can find $x' < x$ with the same property, contradicting the minimality of x. It follows that there exists no such x. Now if we have a triplet $(x, y, z) \in \mathbb{Z} \setminus \{0\}$, taking the opposite of the negatives ones, we may assume they are all positive, which we proved is not possible. It follows that the only solution is the triplet $(0, 0, 0)$.

Problem 3 :
Let G be a non empty finite set and $\cdot$ a binary operation on G such that:

- The operation $\cdot$ is associative;
- For all x, y and $z \in G$ if $x \cdot y = x \cdot z$ then $y = z$ and if $y \cdot x = z \cdot x$ then $y = z$.

1. Show that there exists $e \in G$ such that for all $x \in G$, $e \cdot x = x$.

   (*Hint:* Show that for some $a \in G$, there exists e such that $e \cdot a = a$ and that any $x \in G$ can be written as $a \cdot y$ for some $y \in G$.)

   Solution: Pick any $a \in G$. Let $f : G \to G$ be the function sending x to $a \cdot x$ and let g be the function sending x to $x \cdot a$. The second property of G exactly says that f and g are injective. Because G is finite they are also surjective. In particular, there exists an $e \in G$ such that $g(e) = a$, i.e. $e \cdot a = a$, and for all $x \in G$ there exists a $y \in G$ such that $f(y) = x$, i.e. $a \cdot y = x$. Now $e \cdot x = e \cdot a \cdot y = a \cdot y = x$.

2. Show that we also have $x \cdot e = x$ for all $x \in G$.

   (*Hint:* Show that there exists e' such that $x \cdot e' = x$ for all $x \in G$ and that $e' = e$).

   Solution: By the symmetric proof as above there exists e' such that for all $x \in G$, $x \cdot e' = x$ (take e' such that $f(e') = a$ and use that for all x, there exists y such that $x = g(y)$). But now $e' = e \cdot e' = e$.

3. Show that $(G, \cdot)$ is a group.

   Solution: We know by hypothesis that $\cdot$ is associative and we have just shown that there exists a neutral element. There only remains to show that every element has an inverse. Let a be any element in G and let us consider the same functions f and g as above. There exists y and z such that $a \cdot y = f(y) = e = g(z) = z \cdot a$. But now $z = y \cdot a \cdot z = y$ and hence a has an inverse.