INSA de Rouen

STPI - SIB - M2

Tutorial n^{o} 5
Abstract algebraic notions, modular arithmetic.

Exercise 1 *Properties of groups*

1. *Prove that in a group the neutral element is unique. Prove that for any element its inverse is unique as well.*

2. *Let* $(G_1, \star_1), (G_2, \star_2)$ *be groups with neutral elements* e_1 *and* e_2 *respectively, and* $\varphi\colon G_1 \to G_2$ *be a homomorphism.*
   a). Prove that $\varphi(e_1) = e_2$.
   b). Prove that $Ker(\varphi) \equiv \{g \in G_1,\ s.t.\ \varphi(g) = e_2\}$ *is a subgroup of* G_1.
   c). **(Optional) Prove that the quotient* $G_1/Ker(\varphi)$ *is isomorphic to* $\varphi(G)$.
   $(\varphi(G) \equiv \{\bar{g} \in G_2\ s.t.\ \exists g \in G_1, \bar{g} = \varphi(g)\}.)$

Exercise 2 *Subgroups / morphisms*

1. *Describe a set* D_3 *of all the similarity transformations, mapping an equilateral triangle to itself. Prove that* D_3 *equipped with a composition operation is a group. Give explicitly the multiplication table.*

2. *Describe a set* D_6 *of all the similarity transformations, mapping a regular hexagon to itself. Prove that* D_6 *equipped with a composition operation is a group.*

3. *Consider the set of all permutations of 3 elements, i.e. the set of bijective mappings from the set* $\{1, 2, 3\}$ *to itself. How many elements are there in this set? Does this set equipped with the composition operation form a group?*

4. *Consider the set of* n*-th roots of unity for* $n = 3$, *and* $n = 6$. *Prove that these sets equipped with complex multiplication form a group. Give explicitly the multiplication table.*

5. *What are the relations between all the groups described above?*

Exercise 3 *Rings*

1. *Check that* $\mathbb{Z}_{12} \equiv \mathbb{Z}/12\mathbb{Z}$ *equipped with the induced addition and multiplication is a ring. Is it a field? Is there any subring of* Z_{12} *that is a field?*

2. *Consider* $\mathbb{Z}_7 \equiv \mathbb{Z}/7\mathbb{Z}$. *Give explicitly the addition and multiplication tables. For any non-zero element construct its multiplicative inverse.*

3. *Consider* $\mathbb{R}^3$ *equipped with component-wise addition and vector product as a multiplication. Does it form a ring?*

Exercise 4 *Modular arithmetic*

1. *Congruences*
   a). Prove that the congruence is compatible with arithmetic operations in $\mathbb{Z}$, *i.e. prove that if* $a \equiv b (mod\ n)$, $c \equiv d (mod\ n)$, *then* $a \pm c \equiv b \pm d (mod\ n)$, $ac \equiv bd (mod\ n)$, $a^k \equiv b^k (mod\ n)$. *Can we divide the l.h.s. and the r.h.s. of a congruence by the same integer number?*
   b). Compute the remainder of the division of 3^{1789} *by* 25, *of* 63^{987654} *by* 8.
   c). Compute the last digit of 2014^{2014}, $\left(2013^{2014}\right)^{2016}$.
   d). Show that for integer a *and* b, $a^2 + b^2$ *is a multiple of* 7 *if and only if both* a *and* b *are.*

2. *Equations for integer unknowns. We consider an equation* $ax + by = c$ *with* $a, b, c \in \mathbb{Z}$ *and we search for its integer solutions* $(x, y) \in \mathbb{Z}^2$.

a). Show that if a solution exists, then c *is necessarily a multiple of* $gcd(a, b)$.

b). Using the decomposition of $gcd(a, b)$ *show that at least one solution exists.*
Find all the solutions of the equation.

c). Find the integer solutions of the equation $5x - 9y = 3$

d). Find the integer solutions of the equation $123x - 54y = 3$

3. *Systems of congruences*

a). Consider two conditions: $x \equiv a[m]$, $x \equiv b[n]$, *with* $gcd(m, n) = 1$. *Let* $x_0 = bum + avn$, *where* u *and* v *are the coefficients such that* $mu + vn = 1$ – *show that* x_0 *satisfies the system. Show that for any solution* x, $x - x_0$ *is a multiple of* n *and* m. *Formulate the method.*

b). Solve the systems: $\begin{cases} x \equiv 2(mod\ 3) \\ x \equiv 1(mod\ 5) \end{cases}$ $\qquad$ $\begin{cases} 2x \equiv 3(mod\ 5) \\ 3x \equiv 2(mod\ 4) \end{cases}$

4. *Fermat's little theorem. Let* p *be a prime number.*

a). Prove that for any p *and* $0 < k < p$, $\binom{p}{k}$ *is a multiple of* p.

b). Prove that for all integer couples (x, y), $(x + y)^p \equiv x^p + y^p (mod\ p)$

c). Deduce that for any integer a, $a^p \equiv a(mod\ p)$. *(Induction may be helpful).*

d). Show that if a *is not a multiple of* p, *the above statement is equivalent to* $a^{p-1} \equiv 1(mod\ p)$.