MATH 371
HOMEWORK SET 2
DUE 07.11.2012, WEDNESDAY

Remember: x, y, z, etc. a, b, etc., A, B, etc. stand for integers! p stand ALWAYS for a prime number; $\mathbf{Z}$ denotes the set of integers.

(1) Find *all* solutions of the Diophantine equation

$$x^2 + y^2 = 100049.$$

(Hint: 100049 is a prime number!)

Solution 1. The prime 100049 is congruent to 1 modulo 4. Hence we know that the given equation has a solution(for reference see `http://en.wikipedia.org/wiki/Fermat's_theorem_on_sums_of_two_squares`). This question is supposed to be solved by the help of computer. The following sample PARI/GP[1] code will rule you out the two integer solutions $x = 215$ and $y = 232$:

for (i = 1, 316, print((100049 - i ^ 2) ^ (1/2)););

All the solutions will be possible $+$ and/or $-$ combinations of these two numbers.

(2) Find *all* solutions of the Diophantine equation

$$3x^2 + 7y^2 = 75.$$

Solution 2. Note that the discriminant, $\Delta(f)$, of the form $f = (3, 0, 7)$ is $-4 \cdot 3 \cdot 7$. By the inequalities

$$x^2 \leq \frac{4 \cdot 7 \cdot 75}{\Delta(f)} \text{ and } y^2 \leq \frac{4 \cdot 3 \cdot 75}{\Delta(f)},$$

we get $x \leq 5$ and $y \leq 3$. The following table gives all positive solutions:

x	y
5	0
2	3

(3) Prove that $x^2 - 11y^2 = 7$ has no solutions.

Solution 3. Say x_o and y_o are a solution to the above equation. Then reducing the equation modulo 11, we get

$$x^2 \equiv 7 \bmod 11.$$

But a square in $\mathbf{Z}/11\mathbf{Z}$ has to be in the set $\{1, 4, 9, 5, 3\}$, contradiction.

(4) Prove that $x^2 - 5y^2 = 1$ has infinitely many solutions.

Solution 4. First observe that $x = 9$ and $y = 4$ are solutions to the given equation. To produce infinitely many solutions, we find a matrix $U = \begin{pmatrix} p & q \\ r & s \end{pmatrix}$ by solving the system of equations given by the product:

$$U^t \begin{pmatrix} 1 & 0 \\ 0 & -5 \end{pmatrix} U = \begin{pmatrix} 1 & 0 \\ 0 & -5 \end{pmatrix}.$$

Hence $U \in \mathrm{Aut}(f)$. One sees that $U = \begin{pmatrix} 9 & 20 \\ 4 & 9 \end{pmatrix}$. Then the product $\begin{pmatrix} 9 & 20 \\ 4 & 9 \end{pmatrix}^s (9\ 4)^t$ is also a solution; where $s \in \mathbf{Z}$. As we have observed in class, the matrix U, having trace larger than 2 has infinite order.

(5) Let G be a group acting on itself by conjugation (Check your notes for a definition). Describe the orbits of this action if G is abelian.

Solution 5. Recall that conjugation action is defined as $(g, \omega) \mapsto g \cdot \omega := g^{-1}\omega g$. When G is abelian

$$g \cdot \omega = g^{-1}\omega g = \omega g^{-1} g = \omega.$$

So any $g \in G$ acts trivially. Hence the orbits of this action are singletons, i.e. $G \cdot g = \{g\}$.

[1]Please visit `http://pari.math.u-bordeaux.fr/` to get more information and download PARI.

(6) Let G be any group and consider the action of G on itself (i.e. $\Omega = G$ in our notation). Define maps $G \times \Omega \longrightarrow \Omega = G$

a. $g \cdot_L \omega) := g\omega$, and
b. $g \cdot_R \omega) := \omega g$.
i. Show that both maps are in fact actions of G onto itself (a. is called left action, and b. is called right action).
ii. Compare right action and left action when G is abelian?

Solution 6.

i. We'll only show for left action. The proof of right action is similar. There are two conditions to check:

(a) Let $1_G \in G$ denote the identity of G. Then for any $g \in G$, $1_G \cdot_L g = 1_G g = g$.

(b) Let $g_1, g_2 \in G$ be two arbitrary elements. For any $g \in G$ we have:

$$\begin{aligned} (g_1 g_2) \cdot_L g &= (g_1 g_2) g \\ &= g_1(g_2 g) \\ &= g_1(g_2 \cdot_L g) \\ &= g_1 \cdot_L (g_2 \cdot_L g). \end{aligned}$$

ii. Let $g \in G$ and $\omega \in \Omega = G$ be arbitrary. When G is abelian we have:

$$g \cdot_L \omega = g\,\omega = \omega\, g = g \cdot_R \omega.$$

Hence the two actions are *same* when G is abelian.

(7) Let G be any group and let $\mathrm{Aut}(G)$ denote the *group* of automorphisms of G, that is

$$\mathrm{Aut}(G) := \{\varphi : G \longrightarrow G \,|\, \varphi \text{ is an isomorphism}\}.$$

i. Show that the map $\cdot : \mathrm{Aut}(G) \times G \longrightarrow G$ sending (φ, g) to $\varphi \cdot g := \varphi(g)$ defines an action of $\mathrm{Aut}(G)$ onto G.
ii. For every $g \in G$ show that the homomorphism $\varphi_{g_o} : G \longrightarrow G$ sending g to $\varphi_{g_o}(g) := (g_o^{-1}) g g_o$ is an automorphism of G.
iii. Show that the map $\iota : G \longrightarrow \mathrm{Aut}(G)$ sending each $g_o \in G$ to the isomorphism φ_{g_o} ~~is an injective group homomorphism(i.e. a monomorphism.)~~ has kernel $Z(G)$, the center of G.
iv. Show that the image $\iota(G)$ of G in $\mathrm{Aut}(G)$ is a normal subgroup of $\mathrm{Aut}(G)$.

Solution 7. i. There are two conditions to check:

(a) Let $\mathrm{id} \in \mathrm{Aut}(G)$ denote the identity automorphism of G. Then for any $g \in G$, $\mathrm{id}(g) = g$.

(b) Let $\varphi_1, \varphi_2 \in \mathrm{Aut}(G)$ be two arbitrary automorphisms. Then:

$$\begin{aligned} (\varphi_1 \circ \varphi_2) \cdot g &= (\varphi_1 \circ \varphi_2)(g) \\ &= \varphi_1(\varphi_2(g)) \\ &= \varphi_1(\varphi_2 \cdot g) \\ &= \varphi_1 \cdot (\varphi_2 \cdot g). \end{aligned}$$

ii. We need to show that φ_{g_o} is

1. a homomorphism: For any given $g_1, g_2 \in G$ we have

$$\varphi_{g_o}(g_1 g_2) = g_o^{-1})(g_1 g_2) g_o = (g_o^{-1}) g_1 g_o)(g_o^{-1} g_2 g_o) = \varphi_{g_o}(g_1)\varphi_{g_o}(g_2).$$

2. injective$(1-1)$: Let 1_G denote the identity in G. Then the kernel of this morphism is:

$$\begin{aligned} \ker(\varphi_{g_o}) &= \{g \in G \,|\, \varphi_{g_o}(g) = 1_G\} \\ &= \{g \in G \,|\, g_o^{-1} g g_o = 1_G\} \\ &= \{g \in G \,|\, (g_o^{-1} g g_o) g_o^{-1} = 1_G g_o^{-1}\} \\ &= \{g \in G \,|\, g_o^{-1} g = g_o^{-1}\} \\ &= \{g \in G \,|\, g_o(g_o^{-1} g) = g_o g_o^{-1}\} \\ &= \{g \in G \,|\, g = 1_G\} \\ &= \{1_G\}. \end{aligned}$$

3. surjective: Let $g \in G$ be arbitrary. Then the element $g_o g g_o^{-1}$ is mapped by φ_{g_o} onto g. Namely

$$\varphi_{g_o}(g_o g g_o^{-1}) = g_o^{-1}(g_o g g_o^{-1}) g_o = g.$$

iii. Let us now compute once again the kernel:

$$\begin{aligned}
\ker(\iota) &= \{g_0 \in G \,|\, \varphi_{g_o} = \mathrm{id}\} \\
&= \{g_0 \in G \,|\, \varphi_{g_o}(g) = \mathrm{id}(g) = g \,\forall g \in G\} \\
&= \{g_0 \in G \,|\, g_o^{-1} g g_o = g \,\forall g \in G\} \\
&= \{g_0 \in G \,|\, g_o(g_o^{-1} g g_o) = g_o g \,\forall g \in G\} \\
&= \{g_0 \in G \,|\, g g_o = g_o g \,\forall g \in G\} \\
&= Z(G).
\end{aligned}$$

iv. Let $\varphi \in \mathrm{Aut}(G)$ and $\varphi_{g_o} \in \iota(G)$ be arbitrary. Then, for any $g \in G$:

$$\begin{aligned}
(\varphi^{-1} \circ \varphi_{g_o} \circ \varphi)(g) &= \varphi^{-1} \circ \varphi_{g_o}(\varphi(g)) \\
&= \varphi^{-1} \circ (\varphi_{g_o}(\varphi(g))) \\
&= \varphi^{-1}\left(g_o^{-1} \varphi(g) g_o\right) \\
&= \varphi^{-1}\left(g_o^{-1}\right) \varphi^{-1}(\varphi(g)) \varphi^{-1}(g_o) \\
&= \left[\varphi^{-1}(g_o)\right]^{-1} g \varphi^{-1}(g_o) \\
&= \varphi_{\varphi^{-1}(g_o)}(g).
\end{aligned}$$

Hence $\varphi^{-1} \circ \varphi_{g_o} \circ \varphi \in \iota(G)$.