## Homework 7 - Solutions

MAT 200, Instructor: Alena Erchenko

1. Proof. Let $x$ be a rational number, i.e., there exists $p, q \in \mathbb{Z}$ such that $q \neq 0$ and $x=\frac{p}{q}$. Let $y$ be a real number that is irrational. Then, $x+y$ is a real number. We prove that $x+y$ is irrational by contradiction. Assume $x+y$ is rational, i.e., there exists $a, b \in \mathbb{Z}$ such that $b \neq 0$ and $x+y=\frac{a}{b}$. Then, $y=\frac{a}{b}-x=\frac{a}{b}-\frac{p}{q}=\frac{a q-b p}{b q}$. Since $y=\frac{a q-b p}{b q}, a q-b p$ and $b q$ are integer numbers and $b q \neq 0$ because $b \neq 0$ and $q \neq 0$, we have $y$ is a rational number which contradicts that we have $y$ being irrational. Therefore, we obtain that $x+y$ is irrational.
2. Proof. We have $\sqrt{3}$ is a real number. To show that $\sqrt{3}$ is an irrational number, we need to show that $\sqrt{3}$ is not a rational number. We prove it by contradiction.
Assume that $\sqrt{3}$ is a rational. Then, by a fact in our class, we have $\sqrt{3}=\frac{a}{b}$, where $a \in \mathbb{Z}$, $b \in \mathbb{N}$, and $\operatorname{GCF}(a, b)=1$. Notice that $a \in \mathbb{N}$ as $\sqrt{3}>0$ and $b>0$. Since $\sqrt{3}=\frac{a}{b}$, we have $3=\left(\frac{a}{b}\right)^{2}$, so $3 b^{2}=a^{2}$. In particular, we have 3 divides $a^{2}$. Since 3 is a prime, we have that 3 divides $a$ because 3 divides $a^{2}$, so $a=3 k$, where $k \in \mathbb{Z}$. Since $3 b^{2}=a^{2}$ and $a=3 k$ where $k \in \mathbb{Z}$, we obtain $3 b^{2}=9 k^{2}$, so $b^{2}=3 k^{2}$ where $k \in \mathbb{Z}$, i.e., 3 divides $b^{2}$. Since 3 is a prime, we have that 3 divides $b$ because 3 divides $b^{2}$. we obtained that 3 divides $a$ and 3 divides $b$, so $\operatorname{GCF}(a, b) \neq 1$. Therefore, we got a contradiction because we have $\operatorname{GCF}(a, b)=1$, and our assumption that $\sqrt{3}$ is rational was not right. As a result, we obtain that $\sqrt{3}$ is irrational.
3. (a) Proof. We have $x$ is rational, then by a fact in our class, we have $x=\frac{p}{q}$ where $p \in \mathbb{Z}$, $q \in \mathbb{N}$, and $G C F(p, q)=1$. Since $x=\frac{p}{q}$, we have that $x^{3}+a x^{2}+b x+c=0$ can be rewritten as $\left(\frac{p}{q}\right)^{3}+a\left(\frac{p}{q}\right)^{2}+b\left(\frac{p}{q}\right)+c=0$. In particular, we obtain that $p^{3}+a p^{2} q+b p q^{2}+c q^{3}=0$, so $p^{3}=q\left(-a p^{2}-b p q-c q^{2}\right)$. Therefore, we have $q$ divides $p \cdot p^{2}$ since $-a p^{2}-b p q-c q^{2}$ is an integer. Then, there exist $q_{1}, q_{2} \mathbb{N}$ such that $q_{1}$ divides $p, q_{2}$ divides $p^{2}$, and $q=q_{1} q_{2}$. Since $q_{1}$ divides $p, q_{1}$ divides $q$, and $G C F(p, q)=1$, we need to have $q_{1}=1$. Therefore, $q=q_{2}$, i.e., we have that $q$ divides $p^{2}$ and $G C F(p, q)=1$. Since $q$ divides $p^{2}$, there exist $w_{1}, w_{2} \in \mathbb{N}$ such that $w_{1}$ divides $p, w_{2}$ divides $p$, and $q=w_{1} w_{2}$. We have that $w_{1}$ divides $p, w_{1}$ divides $q$, and $G C F(p, q)=1$, so $w_{1}=1$. Similarly, we have to have $w_{2}=1$. Therefore, we need to have $q=1$, so $x=\frac{p}{q}=\frac{p}{1}=p \in \mathbb{Z}$. We obtained that if $x$ is rational, then $x \in \mathbb{Z}$.
(b) Proof. We have that $x$ is a real number. We prove by contradiction, that if $x$ is not an integer, then $x$ is irrational. We are given that $x$ is not an integer. Assume that $x$ is a rational number, then by the previous part of the problem, $x$ has to be an integer, but it contradicts the fact that we are given that $x$ is not an integer. Therefore, our assumption that $x$ is rational is not right, and $x$ is an irrational number.
4. Proof. We prove by induction.

Base case: $n=1$. We have $a$ divides $c b$, then $\exists a_{1}, a_{2} \in \mathbb{Z}$ such that $a_{1}$ divides $c, a_{2}$ divides $b$, and $a=a_{1} a_{2}$. Moreover, we can assume that $a_{2}>0$ because if not then write $a=\tilde{a_{1}} \tilde{a_{2}}$, where $\tilde{a_{1}}=-a_{1}$ and $\tilde{a_{2}}=-a_{2}$, in particular, $\tilde{a_{1}}$ divides $c$ and $\tilde{a_{2}}$ divides $b$.
As a result, $a_{1}$ divides $a$ and $a_{2}$ divides $a$. Since $a_{2}$ divides $b, a_{2}$ divides $a$, and $G C F(a, b)=1$, we have $a_{2}=1$ since $a_{2}>0$. Therefore, $a=a_{1} \cdot 1=a_{1}$ and $a$ divides $c$.

Inductive step: Assume that $a$ divides $c b^{n}$ implies that $a$ divides $c$. We want to prove that $a$ divides $c b^{n+1}$ implies that $a$ divides $c$. Since $c b^{n+1}=\left(c b^{n}\right) b$ and $a$ divides $c b^{n+1}$, we have that $\exists a_{1}, a_{2} \in \mathbb{Z}$ such that $a_{1}$ divides $c b^{n}, a_{2}$ divides $b$, and $a=a_{1} a_{2}$. As a above, we can assume that $a_{2}>0$. Since $a_{2}$ divides $a, a_{2}$ divides $b$, and $\operatorname{GCF}(a, b)=1$, we have $a_{2}=1$. Therefore, $a=a_{1}$ and $a$ divides $c b^{n}$. By inductive hypothesis, we obtain that $a$ divides $c$ because $a$ divides $c b^{n}$.

Therefore, by the principle of mathematical induction, for all $n \in \mathbb{N}$, we have that if $a$ divides $c b^{n}$, then $a$ divides $c$.
5. Proof. First, we show that if 15 divides $n$ then 3 divides $n$ and 5 divides $n$.

If 15 divides $n$, then $n=15 k$ for some integer $k$. In particular, $n=3 \cdot(5 k)=5 \cdot(3 k)$, where $(5 k),(3 k) \in \mathbb{Z}$. Thus, 3 divides $n$ and 5 divides $n$.
Second, we show that if 3 divides $n$ and 5 divides $n$, then 15 divides $n$.
If 3 divides $n$, then $n=3 m$ for some $m \in \mathbb{Z}$. Therefore, in that case if 5 divides $n$, then 5 divides $3 m$. Since 5 is a prime, then 5 divides $m$ and $m=5 l$ for some $l \in \mathbb{Z}$ because 5 does not divide 3 . As a result, $n=3 \cdot(5 l)=15 l$ where $l \in \mathbb{Z}$. Thus, 15 divides $n$.
6. Solution. We have

$$
136=2^{3} \cdot 17, \quad 150=2 \cdot 3 \cdot 5^{2}, \quad 255=3 \cdot 5 \cdot 17, \quad 1980=2^{2} \cdot 3^{2} \cdot 5 \cdot 11
$$

Therefore,

$$
G C F(136,150)=2
$$

and

$$
G C F(255,1980)=3 \cdot 5=15
$$

