# M403 Homework 4

**Enrique Areyan**
**September 21, 2012**

(1.46)

(i) **False**. Suppose for a contradiction that $6|2$. Then, $2 = 6 \cdot q$ for some $q \in \mathbb{Z}$. But, solving for $q$ we get that $q = \frac{1}{3} \notin \mathbb{Z}$, a contradiction. Hence $2 \nmid 6$.

(ii) **True**. $6 = 2 \cdot 3$ and $3 \in \mathbb{Z}$. Hence, $2|6$.

(iii) **True**. $0 = 6 \cdot 0$ and $0 \in \mathbb{Z}$. Hence, $6|0$.

(iv) **False**. Suppose for a contradiction that $0|6$. Then $6 = 0 \cdot q$ for some $q \in \mathbb{Z}$. But, $6 = 0 \cdot q = 0$, which is clearly a contradiction. Hence $0 \nmid 6$.

(v) **True**. $0 = 0 \cdot q$ for some $q \in \mathbb{Z}$, pick any $q$. Hence, $0|0$.

(vi) **True**. Suppose for a contradiction that there is a $c > 1 \in \mathbb{Z}$ for which $g.c.d(n, n+1) = c$. (I do not have to worry about $c$ being negative because I know that at least 1 divides both $n$ and $n+1$ and hence 1 is a lower bound on the g.c.d.). This would mean that $c|n$ and $c|n+1$, i.e., $n = c \cdot q$ for some $q \in \mathbb{Z}$ and $n+1 = c \cdot p$ for some $p \in \mathbb{Z}$. Using these equations we obtain:

$$\begin{array}{lcll} n+1 & = & c \cdot p & \\ c \cdot q + 1 & = & c \cdot p & \Longrightarrow \\ 1 & = & c \cdot p - c \cdot q & \\ 1 & = & c(p-q) & \end{array}$$

Now we have to consider three cases:

(i) $p - q = 0$. This would mean that $1 = c \cdot 0 = 0$ . A contradiction.

(ii) $p - q < 0$. This would mean that $1 < 0$. A contradiction.

(iii) $p - q > 0$. This would mean that $1 > 1$. A contradiction.

Therefore, our assumption is wrong, and the case is that $g.c.d(n, n+1) = 1$ for every natural number $n$.

(vii) **False**. Let $n = 13$, then $n + 2 = 15$ but $g.c.d(13, 15) = 1 \neq 2$.

(1.49)

$$f_1 = p_1 + 1 = 2 + 1 = 3$$

$$f_2 = p_1 \cdot p_2 + 1 = 2 \cdot 3 + 1 = 7$$

$$f_3 = p_1 \cdot p_2 \cdot p_3 + 1 = 2 \cdot 3 \cdot 5 + 1 = 31$$

$$f_4 = p_1 \cdot p_2 \cdot p_3 \cdot p_4 + 1 = 2 \cdot 3 \cdot 5 \cdot 7 + 1 = 211$$

$$f_5 = p_1 \cdot p_2 \cdot p_3 \cdot p_4 \cdot p_5 + 1 = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 + 1 = 2311$$

$$f_6 = p_1 \cdot p_2 \cdot p_3 \cdot p_4 \cdot p_5 \cdot p_6 + 1 = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 + 1 = 30031$$

We can see that $f_1, f_2, f_3, f_4$ and $f_5$ are all prime. But, $f_6 = 30031 = 59 \cdot 509$, not prime. Hence, the smallest $k$ is $k = 6$

(1.50) Let $d, d' \in \mathbb{Z} \backslash \{0\}$. Suppose that $d|d'$ and $d'|d$. Then, $d' = d \cdot q$, for some $q \in \mathbb{Z}$ and $d = d' \cdot p$ for some $p \in \mathbb{Z}$. Replace the former into the latter:

$$d = d \cdot q \cdot p \Longrightarrow q \cdot p = 1 \Longrightarrow q = 1 \text{ and } p = 1 \text{ OR } q = -1 \text{ and } p = -1$$

Replacing these solutions back into the original equations, we obtain that $d' = \pm d$.

(1.51) To prove the statement we can apply corollary 1.37. Let $I = \{x : \zeta^x = 1\}$. First we need to check that the conditions of the corollary hold for $I$.

(i) Since by definition $\zeta^0 = 1$, then $0 \in I$

(ii) Let $a, b \in I$. By definition of membership, $\zeta^a = 1 = \zeta^b$. Divide to obtain: $\frac{\zeta^a}{\zeta^b} = 1 \Rightarrow \zeta^{a-b} = 1$, which means that $a - b \in I$

(iii) Let $a \in I$ and $q \in \mathbb{Z}$. By definition of membership, $\zeta^a = 1$. Raise both sides of this equation to $q$: $(\zeta^a)^q = 1^q \Rightarrow \zeta^{aq} = 1$, hence $aq \in I$

The conditions of corollary 1.37 hold, therefore, there exists $d \in \mathbb{Z}$ with $d > 0$ such that $I = \{d \cdot q : q \in \mathbb{Z}\}$. In particular, this means that for any $x$ such that $\zeta^x = 1$, $x$ can be written as $x = d \cdot q$, for $q \in \mathbb{Z}$, or in other words, $d|x$.

(1.56) Let $a.b$ be integers and $s \cdot a + t \cdot b = 1$, for $s, t \in \mathbb{Z}$. Suppose that $gcd(a, b) = c$ for $c > 1$. By definition, $c|a$ and $c|b$, i.e., $a = c \cdot q$ for some $q \in \mathbb{Z}$ and $b = c \cdot p$ for some $p \in \mathbb{Z}$. If we replace these equations into the above linear combination, we obtain: $s(c \cdot q) + t(c \cdot p) = 1 \iff c(s \cdot q + t \cdot p) = 1 \Rightarrow s \cdot q + t \cdot p \neq 0$. Moreover, $\frac{1}{s \cdot q + t \cdot p} = c$ implies that $|c| \leq 1$, contradicting our assumption that $c > 1$. Therefore, $gcd(a, b) = 1$. Q.E.D.

(1.57) Let $d = gcd(a, b)$. By theorem 1.35, we have that $d = s \cdot a + t \cdot b$, for some $s, t \in \mathbb{Z}$. We can divide by $d$ because by definition of g.c.d, $d$ is at least 1. Hence,

$$\frac{d}{d} = \frac{s \cdot a + t \cdot b}{d} \iff 1 = s\frac{a}{d} + t\frac{b}{d}$$

By definition of g.c.d, $d|a$ and $d|b$, therefore both $\frac{a}{d}$ and $\frac{b}{d}$ are integers.
Applying the result of the previous exercise, we conclude that $\frac{a}{d}$ and $\frac{b}{d}$ are relatively prime. Q.E.D.