M403 Homework 5

Enrique Areyan
October 3, 2012

(1.54)

(i) **Proof by contradiction**: suppose that n is square free and is also a rational number. Then, we can write it in lowest terms: $\sqrt{n} = \frac{a}{b}$, where $a.b \in \mathbb{Z}, b \neq 0, gcd(a,b) = 1$. Now,

$$\sqrt{n} = \frac{a}{b} \iff n = \frac{a^2}{b^2} \iff nb^2 = a^2$$

By the last statement we know that $n|a^2 \iff a^2 = np_1$. Also, we can factor n as follow: $n = p \cdot q$ where p is a prime. Replacing this factorization into the last equation we get that $a^2 = (pq)p_1 = p(qp_1) \Rightarrow p|a^2$. By Euclid's lemma $p|a \iff a = pm$. Replacing into the first equation:

$$nb^2 = (pm)^2 = p^2m^2 \iff pqb^2 = p^2m^2 \iff qb^2 = pm^2$$

Since n is square free and p is prime, n is not divisible by p^2. Hence:

$$b^2 = p\frac{m^2}{q} \iff p|b^2$$

By Euclid's lemma, $p|b$. From before we have that $p|a$, which contradicts the fact that $\frac{a}{b}$ is in lowest terms. Therefore, $\sqrt{n}$, where n is square free, is not a rational number.

(ii) **Proof by contradiction**: suppose that $\sqrt[3]{2}$ were rational. Then we can write it in lowest terms, i.e., $\sqrt[3]{2} = \frac{a}{b}$ where $a.b \in \mathbb{Z}, b \neq 0, gcd(a,b) = 1$. Then

$$\sqrt[3]{2} = \frac{a}{b} \iff 2 = \frac{a^3}{b^3} \iff 2b^3 = a^3$$

Since 2 is a prime and $2|2b^3 \iff 2|a^3$, we can apply Euclid's lemma to conclude that $2|a \iff a = 2p$ for some $p \in \mathbb{Z}$. Replacing this into our previous equation:

$$2b^3 = 2^3p^3 \iff b^3 = 4p^3 \iff 4|b^3 \Rightarrow 2|b^3$$

Applying Euclid's lemma again $2|b$, which together with $2|a$ contradicts the fact that $gcd(a,b) = 1$. Hence, it must be the case that $\sqrt[3]{2}$ is irrational.

(1.58) Suppose that given integers r, r' and m, we have that $gcd(r,m) = gcd(r',m) = 1$. This means that for some integers s, s', t, t' we have that $sr + tm = 1$ and $s'r' + t'm = 1$. Consider the following product:

$$1 = (sr+tm)(s'r'+t'm) = ss'rr' + srt'm + s'r'tm + tt'm^2 = ss'rr' + m(srt' + s'r't + tt'm)$$

Let $q = ss' \in \mathbb{Z}$ and $p = srt' + s'r't + tt'm \in \mathbb{Z}$, then $1 = qrr' + pm \iff gcd(rr', m) = 1$. Q.E.D

(1.59) I <u>claim</u> that if $d = sa + tb$ then $d = a(s+nb) + b(t-na)$ for $n \in \mathbb{N}$.
Proof: By simple arithmetic: $a(s+nb)+b(t-na) = as+nab+bt-nab = sa+tb = d$. In particular, this means that there exists infinitely many pairs of integers (s_n, t_n) for which $d = s_na + t_nb$. Simply take $(s_n, t_n) = (s+nb, t-na)$ for $n \in \mathbb{N}$.

(1.60) Suppose that $gcd(a,b) = 1$ and $a|n$ and $b|n$. Then, $n = a \cdot p = b \cdot q$, for some integers p, q. Hence, $a|b \cdot q$. Applying Corollary 1.40, we can conclude that $a|q$, i.e. $q = a \cdot q'$. Replacing this into the above equation for n, we obtain $n = b \cdot a \cdot q' = (a \cdot b) \cdot q'$, which means that $ab|n$.

(1.61) This is a two part proof: (in what follows, $a, a', b, b', c, q \in \mathbb{Z}$)

(i) Suppose $c|a$ and $c|b$. Then $a = ca'$ and $b = cb'$. Consider $b - a = cb' - ca' = c(b' - a') \iff c|b-a$. Hence, the same divisor of a and b divides $b - a$. This means that $gcd(a,b) \leq gcd(b-a, a)$.

(ii) Suppose $c|b-a$ and $c|a$. Then $b - a = cq$ and $a = ca'$. Consider $b = cq - a = cq - ca' = c(q - a') \iff c|b$. Hence, the same divisor of $b - a$ and a divides b. This means that $gcd(b-a, a) \leq gcd(a.b)$.

Together, (i) and (ii) imply that $gcd(a, b) = gcd(b - a, a)$

(1.62) I am going to do this proof same as before (1.60). (In what follows, $a, b, c, e, k, p_1, p_2, p_3, p_4, p_5 \in \mathbb{Z}$) Also, let $e = gcd(b, c)$. By definition, $e|b \iff b = ep_3$ and $e|c \iff c = ep_4$.

(i) Suppose $k|ab$ and $k|ac$. Then, $ab = kp_1$ and $ac = kp_2$. Consider $ab = aep_3 = kp_1$ and $ac = aep_4 = kp_2$ $\Rightarrow ae = kp_2p_3 \iff k|ae$.

(ii) Suppose that $k|ae$. Then, $ae = kp_5$. Consider, $ab = \frac{kp_5}{e}ep_3 = kp_5p_3 \iff k|ab$. Likewise, $ac = \frac{kp_5}{e}ep_4 = kp_5p_4 \iff k|ac$

Together, (i) and (ii) imply that $a \cdot gcd(b, c) = gcd(ab, ac)$

(1.64) **Proof by Induction**. Let $S(n) : F_{n+1}$ and F_n are relatively prime, i.e., $gcd(F_{n+1}, F_n) = 1$.

Base Case $S(1) : F_2 = 1; F_1 = 0 \Rightarrow gcd(F_2, F_1) = gcd(1, 0) = 1$. Base case holds true.

Inductive Step. Assume $S(n)$ true. We want to show that $S(n + 1)$ is true, i.e. $gcd(F_{(n+1)+1}, F_{n+1}) \stackrel{?}{=} 1$. We begin as follow:

$$\begin{array}{lcll} gcd(F_{n+2}, F_{n+1}) & = & gcd(F_{n+2} - F_{n+1}, F_{n+1}) & \text{By exercise (1.61)} \\ & = & gcd(F_n, F_{n+1}) & \text{By definition of Fibonacci sequence.} \\ & = & 1 & \text{by IH. Q.E.D.} \end{array}$$

(1.66)

(i) Let $d = gcd(a, b, c)$ and let $e = gcd(b, c)$ and $f = gcd(a, gcd(b, c))$. By definition $d|a, d|b$, and $d|c$. Also, by definition $e|b, e|c, f|a$, and $f|e$. From $f|e$ and $e|b$ we conclude that $f|b$. Likewise, from $f|e$ and $e|c$ we conclude that $f|c$. Therefore, of f we have that $f|a, f|b$, and $f|c$. But from definition if f is a common divisor of a, b, c, which we just showed, then $f|d$.

Also, from $d|b$ and $d|c$ we can conclude that, $d|gcd(b, c) \iff d|e$, i.e., a common divisor divides the gcd. Applying this same reasoning but with premises $d|a$ and $d|e$ we obtain that $d|gcd(a, e) \iff d|f$.

Therefore, we have that $f|d$ and $d|f$, and we can conclude that $f = \pm d$. However, these are defined as the greatest common divisor, so we can conclude that $f = d$.

(ii) $(120, 168, 328) = (120, (328, 168)) = (120, (168, 160)) = (120, (160, 8)) = (120, 8) = 8$

(1.67)

(i) Let $z = q + ip$ be a complex number such that $q > p$ and $q, p \in \mathbb{Z}^+$. Then, on the one hand:

$$\begin{array}{lcl} |z^2| & = & |z \cdot z| \\ & = & |(q + ip)(q + ip)| \\ & = & |q^2 + 2ipq - p^2| \\ & = & |(q^2 - p^2) + 2ipq| \\ & = & \sqrt{(q^2 - p^2)^2 + (2pq)^2} \end{array}$$

On the other:

$$\begin{array}{lcl} |z|^2 & = & |q + ip|^2 \\ & = & \sqrt{q^2 + p^2}^2 \\ & = & q^2 + p^2 \end{array}$$

So, if $|z^2| = |z|^2 \iff \sqrt{(q^2 - p^2)^2 + (2pq)^2} = q^2 + p^2 \iff (q^2 - p^2)^2 + (2pq)^2 = (q^2 + p^2)^2$, which shows that $(q^2 - p^2, 2pq, q^2 + p^2)$ is a Pythagorean triple by letting $a = q^2 - p^2, b = 2pq$ and $c = q^2 + p^2$

(ii) Suppose that $(9, 12, 15)$ is a Pythagorean triple of the type given in (i). Then, there exists $p, q \in \mathbb{Z}^+$ with $q > p$ such that:

$$(q^2 - p^2, 2pq, q^2 + p^2) = (9, 12, 15)$$

Meaning that: $q^2 - p^2 = 9$ and $2pq = 12$ and $q^2 + p^2 = 15$. From the second equation we get that $pq = 6$, whose only positive integer solutions are $q = 3, p = 2$ OR $q = 6, p = 1$. Neither one of these solutions satisfy the other equations and hence, $(9, 12, 15)$ is not of type given in (i).