Solutions of Exercises for Module I

Exercise 1 a) Assume $4 | n^2 + 1$ for some n.

If $n = 2k$ then $4 | 4k^2 + 1$ and $4 | 4^k \Rightarrow$

$$4 | (4k^2 + 1) - (4k^2) \text{ i.e. } 4 | 1 \divideontimes$$

If $n = 2k + 1$ then $4 | 4k^2 + 4k + 1$ and the argument proceeds as above $\divideontimes$

Exercise 1 c) $a | b$ means $\exists\, \alpha$ such that $b = \alpha$ a. Likewise $\exists \beta$ such that $d = \beta$ c $\therefore$ $b\,d = (a\,c)(\alpha\beta)$ and $ac | bd$.

Exercise 1 e) First we prove $\forall\, n \geq 0 (6 | (n)(n+1)(n+2))$

Base case $n = 0$: $6 | 0$ - Ok!

Induction hypothesis : $6 | (n)(n+1)(n+2)$

Induction step :

$$(n+1)(n+2)(n+3) - (n)(n+1)(n+2) = 3\,(n+1)(n+2)$$

But either $n + 1$ or $n + 2$ is even so $2 | (n+1)(n+2)$ and therefore $6 \,| 3(n+1)(n+2)$. Hence

$$6 | (n)(n+1)(n+2) + 3(n+1)(n+2) = (n+1)(n+2)(n+3)$$

If $n = -1, -2$ then $(n)(n+1)(n+2) = 0$ and so

$$6 | (n)(n+1)(n+2)$$

Consider $n \leq -3$. Then

$$(-n)(-n-1)(-n-2) = (m)(m+1)(m+2)$$

where $m = -n - 2 \geq 1$. Thus

$$6 | (m)(m+1)(m+2) = (-n)(-n-1)(-n-2)$$

Finally $6 | -[(-n)(-n-1)(-n-2)] = (n)(n+1)(n+2)$ for $n \leq -3$.

Exercise 1 f) The argument is really the same as for e) with

$$(n+1)(n+2)(n+3)(n+4) - (n)(n+1)(n+2)(n+3)$$
$$= 4\ (n+1)(n+2)(n+3)$$

and from e) we know that $6 \,|(n+1)(n+2)(n+3)$

Exercise 3 a) Induction on n: The base case $n = 2$ is trivial.

Induction Hypothesis: $\ell\text{cm}(a_1, a_2, \ldots, a_m)$ exists and equals ℓ_n where $\ell_2 = \ell\text{cm}(a_1, a_2)$, $\ell_3 = \ell\text{cm}(\ell_2, a_3), \cdots, \ell_n = \ell\text{cm}(\ell_{n-1}, a_n)$

Induction Step: Consider $a_1, a_2, \cdots, a_n, a_{n+1} \in Z^+$ and realize that $\ell\text{cm}(a_1, a_2, \ldots, a_n)$ exists and equals $\ell_n = \ell\text{cm}(\ell_{n-1}, a_n)$ by the induction hypothesis. Now ℓ_n is a common multiple of each $a_1, \ldots, a_n$ so $\ell\text{cm}(\ell_n, a_{n+1})$ is a common multiple of $a_1, a_2, \ldots, a_n, a_{n+1}$. Suppose m is a common multiple of $a_1, a_2, \ldots, a_{n+1}$; it follows that $\ell_n = \ell\text{cm}(a_1, \ldots, a_n) |\, m$. Hence $\ell\text{cm}(\ell_n, a_{n+1}) | m$ as well and so $\ell_{n+1} = \ell\text{cm}(\ell_n, a_{n+1})$ is the least common multiple of $a_1, a_2, \ldots, a_{n+1}$.

It is NOT the case that

$$\gcd(a_1, \ldots, a_m)\,\ell\text{cm}(a_1, \ldots, a_m) = \prod_{i=1}^{m} a_i$$

for all $m \geq 2$. Consider

$\gcd(5, 10, 15) = 5$, $\ell\text{cm}(5, 10, 15) = 30$

and $(5)(10)(15) = 750 \neq 150$.

Exeercise 3 c) Suppose $\exists\, x, y \in Z$ such that $x + y = s$ and $\gcd(x, y) = g$

Of course $g | s$.

Conversely, suppose $g|s$. Set $x = g$ and $y = s - x = s - g$

Since $g|s$ it follows that $\gcd(x, y) = g$

Exercise 3 f) Suppose $g = \gcd(a, b)$, $a' = a' g$ and $b = b' g$

Now $b c = \delta a$

$\Leftrightarrow b' g c = \delta a' g$

or $b' c = \delta a'$. Hence $\gcd(a', b') = 1 \Rightarrow a' | c$

i.e. $[a/\gcd(a, b)] | c$

Conversely, $a'|c \Rightarrow a = a' g | g c$. But $g c | b c$

so $a | bc$

Exercise 5 b) Write $d = \alpha k$. Since $\exists\, x, y \in Z$ such that $x d = a$, $y d = b$ we get $x \alpha k = a$ and $y \alpha k = b$.

Thus $\frac{d}{k} = \alpha \Big| \frac{a}{k}, \frac{b}{k}$ which, in turn, implies $\frac{d}{k} \Big| \gcd\left(\frac{a}{k}, \frac{b}{k}\right)$.

Now $\gcd\left(\frac{a}{k}, \frac{b}{k}\right) \Big| \frac{a}{k}, \frac{b}{k}$ implies $k \gcd\left(\frac{a}{k}, \frac{b}{k}\right) \Big| a, b$.

Thus $k \gcd\left(\frac{a}{k}, \frac{b}{k}\right) \Big| d = \gcd(a, b)$. It follows by cancellation that

$\gcd\left(\frac{a}{k}, \frac{b}{k}\right) \Big| \frac{d}{k}$ and the proof is complete.

Exercise 6 c) Observe that $\gcd(6, 10) = 2$ and $6(-3) + 10(2) = 2$

Also $g(2, 15) = 1$ and $2(-7) + (1)(15) = 1$

Thus

$$[6(-3) + 10(2)]\,(-7) + (1)(15) = 1$$

or, equivalently

$$6(21) + 10(-14) + (15)(1) = 1$$

Exercise 6 d) *i)* First we find $\gcd(482, 1687)$:

$$1687 = 3(482) + 241$$

$$482 = 2(241) + 0$$

so $\gcd(482, 1687) = 241$. Thus

$$\ell\text{cm}(482, 1687) = \frac{(482)(1687)}{\gcd(482,\ 1687)} = \frac{(482)(1687)}{241} = 3374$$

ii) $\gcd(60, 61) = 1 \Rightarrow \ell\text{cm}(60, 61) = (60)(61) = 3660$

Solutions of Submitted Exercises
From Module I

Exercise 1 b) $x = 2k + 1$ and $y = 2\ell + 1 \Rightarrow x^2 + y^2 = 4k^2 + 4\ell^2 + 4k + 4\ell + 2$
so $2 \mid x^2 + y^2$. However the assumption that $4 \mid x^2 + y^2$ leads to the contradiction $4 \mid 2$

Exercise 1 d) $n = 2k + 1 \Rightarrow n^2 = 4(k^2 + k) + 1$ and so
$n^2 - 1 = 4(k^2 + k)$. But $k^2 + k = (k+1)(k)$ is even so $8 \mid n^2 - 1$

Exercise 2 a) Induction on n

$n = 2$: already known from notes

Hypothesis: $d_n = \gcd(d_{n-1}, a_n)$ is a comon divisor of $a_1, a_2, \ldots, a_n$ and if $f \mid a_1, \ldots, a_n$ then $f \mid d_n$.

Induction step: Consider $a_1, \ldots, a_n, a_{n+1}$ and $d_{n+1} = \gcd(d_n, a_{n+1})$.
Now $d_{n+1} \mid d_n, a_{n+1}$ so by the hypothesis $d_{n+1} \mid a_1, \ldots, a_n, a_{n+1}$.
Suppose $f \mid a_1, \ldots, a_n, a_{n+i}$. Then $f \mid a_1, \ldots, a_n$ and $f \mid a_{n+1}$.
Hence, by the hypothesis, $f \mid d_n$ and so $f \mid d_{n+1} = \gcd(d_n, a_{n+1})$.
Also $d_{n+1} \mid d_n$ and $d_{n+1} \mid a_{n+1}$. The hypothesis yields $d_{n+1} \mid a_1, \ldots, a_n$.
In summary, d_{n+1} is a common divisor of $a_1, .., a_{n+1}$ and any other common divisor divides d_{n+1} i.e. $d_{n+1} = \gcd(a_1, \ldots, a_n, a_{n+1})$

As for the ideal statement

$$I = \left\{ \sum_{i=1}^{n} a_i x_i \mid x_i \in Z,\ i = 1, \ldots, n \right\}.$$

is an ideal and is therefore equal to (d) for some $d > 0$. Now $d \mid a_i$ for each i by setting $x_i = 1$ and $x_j = 0,\ j \neq i$.
Hence $d \mid d_n$ - the gcd of $a_1, \ldots, a_n$. Finally $d \in I$ implies that $\exists\ y_1, \ldots, y_n \in Z$ such that $d = \sum_{i=}^{n} a_i y_i$ so $d_n \mid d$

Exercise 2 b) $2 = \gcd(a, 4) = \gcd(b, 4) \Rightarrow a = 2(2k+1)$ and $b = 2(2\ell + 1)$. Thus $a + b = 4(k + \ell) + 4$ so $4 \mid a + b$ and finally $\gcd(a + b, 4) = 4$.

Exercise 3 b) $\exists\ \alpha, \beta, u, v$ such that

$$\alpha\, a + u\, m = 1$$

$$\beta b + v\, m = 1$$

Therefore

$$(\alpha\beta)(ab) + \beta\, u\, b\, m + \alpha\, v\, a\, m + u\, v\, m^2 = 1$$

Thus $\quad d \mid ab$ and $d \mid m \Rightarrow d \mid 1.$

Exercise 4) Base case: $k = 2$. See exercise 3b.

Induction hypothesis: if $\gcd(a_i, b) = 1$ for $i = 1, \ldots, k$ then

$$\gcd\Big(\prod_{i=1}^{k} a_i,\ b\Big) = 1.$$

Induction step: Suppose $\gcd(a_i, b) = 1$ for $i = 1, \ldots, k, k+1$.

Then the hypothesis yields $\gcd\Big(\prod_{i=1}^{k} a_i, b\Big) = 1$ and therefore

$\gcd\Big(\prod_{i=1}^{k+1} a_i,\ b\Big) = 1$ follows by the result for $k = 2$.

Some Exercises

- Prove $\forall a,b \in \mathbb{Z}^+ \ \forall n \geq 2 \quad a^n - b^n \nmid a^n + b^n$:

Suppose $\exists$ $a,b \in \mathbb{Z}^+$ and $n \geq 2$ s.t

$$(a^n - b^n)\,r = a^n + b^n$$

Wlog assume $a > b$ (realize $a \neq b$).

Let $d = \gcd(a,b)$ so that

$$a = a'd, \quad b = b'd$$

and $\therefore$

$$\cancel{d^n}\left((a')^n - (b')^n\right) r = \cancel{d^n}\left((a')^n + (b')^n\right)$$

Claim $\gcd((a')^n, (b')^n) = 1$

Pf of claim: Realize $\gcd(a', b') = 1$. If $\gcd((a')^n, (b')^n) \geq 2$ then $\exists$ a prime p s.t

$$p \mid (a')^n, (b')^n$$

But then $p \mid a', b'$ $\times$

Next realize that

$$(r-1)(a')^n = (r+1)(b')^n$$

But $\gcd((a')^n, (b')^n) = 1 \Longrightarrow$

$$(a')^n \mid r+1$$

and $$(b')^n \mid r-1$$

i.e $\quad \gamma+1 = (a')^n\delta \quad$ some δ

$\quad\gamma-1 = (b')^n\rho \quad$ some ρ

Plugging in we get

$$(b')^n(a')^n\rho = (a')^n(b')^n\delta$$

so $\rho=\delta$, i.e

$$\gamma+1 = (a')^n\delta$$

$$\gamma-1 = (b')^n\delta$$

Subtracting we get

$$2 = \delta\left((a')^n-(b')^n\right)$$

so $(a')^n-(b')^n = 1$ or 2

However $a' \geq b'+1$ so

$$(a')^n = (b')^n + \sum_{k=0}^{n-1}\binom{n}{k}(b')^k$$

$$\geq (b')^n + n(b')^{n-1} + 1$$

so

$$(a')^n-(b')^n \geq n(b')^{n-1}+1 \geq 3 \quad \times$$

Done!

• Prove $\forall\, a,b \geq 2 \quad 2^b - 1 \nmid 2^a + 1$

Proof Suppose

$$2^b - 1 \mid 2^a + 1$$

Claim $b \leq a$

Pf of claim : If $b \geq a+1$ then

$$2^b - 1 \geq 2^{a+1} - 1$$

But

$$2^{a+1} - 1 - (2^a + 1) = 2^a - 2 > 0 \quad (\text{since } a \geq 2)$$

So $\quad 2^b - 1 > 2^a + 1 \quad \rightarrow\!\leftarrow$

Next consider

$$2^a + 1 = 2^{a-b}(2^b - 1) + 2^{a-b} + 1$$

Then, if $2^b - 1 \mid 2^a + 1$ it follows that

$$2^b - 1 \mid 2^{a-b} + 1 \qquad (+)$$

From an intuitive prospective if we continue thus we arrive at $2^b - 1 \mid 2^\alpha + 1$ where $\alpha < b$

A very neat inductive approach is as follows.:

If $\exists\; a \geq b > 0$ s.t $2^b - 1 \mid 2^a + 1$ then $\exists$ a smallest such a. But then $(+)$ provides a $\rightarrow\!\leftarrow$