Problem set, Chapter 1: The Fundamental Theorem of Arithmetic

Damien Lefebvre

19 June 2016 - 25 June 2016

1 8 Completed Exercises

Exercise 1.

If $(a, b) = 1$, then

$$ax + by = 1 \tag{1}$$

where x and y are integers.
If $c|a$, then $c|ax$. Similarly, if $d|b$, then $d|by$.
This implies

$$ax = cq_1 \tag{2}$$

$$by = dq_2 \tag{3}$$

where q_1 and q_2 are integers.
Solving for equation 2 and 3 in equation 1, we find

$$ax + by = cq_1 + dq_2 = 1 \tag{4}$$

Since q_1 and q_2 are integers, this is equivalent to $(c, d) = 1$. ■

Exercise 2.

Euclid's lemma: if $a|bc$ and if $(a, b) = 1$, then $a|c$.
Suppose $a|bc$. If $(a, b) = 1$, then by Euclid's lemma we must have $a|c$.
But since $(a, c) = 1$, this is a contradiction. So $a \nmid bc$.
Therefore, we must have $(a, bc) = 1$. ■

Exercise 6.

Let $(a, b) = 1$ and $d|(a + b)$.

- Let $(a, d) = k$, so $k|a$ and $k|d$.
  - If $k|d$ and $d|(a + b)$, then $k|(a + b)$.
  - Since $k|a$ and $k|(a + b)$, we have
    - $a = kq_1$ and $a + b = kq_2$, which can be rewritten as $a = kq_2 - b$
    - we find $kq_1 = kq_2 - b$, or $b = kq_2 - kq_1 = k(q_2 - q_1)$.

- Therefore $k|b$. But if $k|a$ and $k|b$, since $(a, b) = 1$, then $k = 1$.

- The same reasoning with $(b, d) = j$, yields $j = 1$.

Therefore $k = j = 1$ and $(a, d) = (b, d) = 1$. ■

Exercise 9.

(a)

Let $a = 2$ and $b = 3$, where $a \nmid b$. We have $a^2 = 2^2 = 4$ and $b^2 = 3^2 = 9$, with $a^2 \leq b^2$.
We choose $n = 36 = 4 \cdot 9$ such that $a^2|n$ and $b^2|n$.
However, $a \nmid b$, so this is a counter example. ■

(b)

We keep the same counter example as (a).
The divisors of n=36 is the set D such that $D = (1, 2, 3, 4, 6, 9, 12, 18, 36)$.
We see that $b^2 = 9$ is the largest square divisor of $n = 36$, different from n.
Yet we still have $a^2|n$ and $a \nmid b$, so this too is a counter example. ■

Exercise 11.

Let $k = n^2$, then $n^4 + 4 = (n^2)^2 + 4 = k^2 + 4$.
We observe that $(k + 2)^2 = k^2 + 4k + 4$. We find:

$$\begin{aligned} k^2 + 4 &= (k + 2)^2 - 4k \\ &= (k + 2)^2 - (2\sqrt{k})^2 \\ &= (n^2 + 2)^2 - (2n)^2 \\ &= (n^2 + 2 + 2n)(n^2 + 2 - 2n) \end{aligned} \tag{5}$$

So $n^4 + 4$ is composite. ■

Exercise 15.

Every $n \geq 12$ can be expressed as $n = 12 + k$, where k is an integer, either composite or prime.

- If k is composite, then n is the sum of two composite numbers (12 and k).

- If k is prime, we have either $k = 2$ or $k > 2$.

  - If $k = 2$, then $n = 12 + k = 12 + 2 = 14$, so n is the sum of two composite numbers (10 and 4).
  - If $k > 2$, since k is prime, then k is odd so $k = 2a + 1$, where a is an integer.

We find:

$$\begin{aligned} n &= 12 + k \\ &= (9 + 3) + k \\ &= 9 + (k + 3) \\ &= 9 + ((2a + 1) + 3) \\ &= 9 + (2a + 4) \\ &= 9 + 2(a + 2) \end{aligned} \tag{6}$$

So n is the sum of two composite numbers (9 and $2(a + 2)$). ■

Exercise 20.

$$\begin{aligned} 1890 &= 2 \cdot 826 + 238 \\ 826 &= 3 \cdot 238 + 112 \\ 238 &= 2 \cdot 112 + 14 \\ 112 &= 8 \cdot 14 + 0 \end{aligned} \tag{7}$$

So $(1890, 826) = 14$. Reversing the order of operations:

$$\begin{aligned} 14 &= 238 - 2 \cdot 112 \\ &= 238 - 2(826 - 3 \cdot 238) \\ &= 7 \cdot 238 - 2 \cdot 826 \\ &= 7(1890 - 2 \cdot 826) - 2 \cdot 826 \\ &= 7 \cdot 1890 - 16 \cdot 826 \end{aligned} \tag{8}$$

So $14 = 7 \cdot 1890 - 16 \cdot 826$. ■

Exercise 21.

(a)

Let $d_i = min\{a_i, b_i\}$.

$$[a, b] = \frac{\mid ab \mid}{(a, b)} = \frac{\prod_{i=1}^{\infty} p_i^{a_i + b_i}}{\prod_{i=1}^{\infty} p_i^{d_i}} = \prod_{i=1}^{\infty} p_i^{a_i + b_i - d_i} \tag{9}$$

We notice $a_i + b_i - d_i = a_i + b_i - min\{a_i, b_i\} = max\{a_i, b_i\}$. ■

(b)

We find:

$$(aDb)Mc = \frac{c(aDb)}{(aDb)Dc} = \frac{(acDbc)}{aD(bDc)} = \frac{(acDbc)}{aDbDc} \tag{10}$$

We have:

$$(aMc) = \frac{ac}{(aDc)} \tag{11}$$

$$(bMc) = \frac{bc}{(bDc)} \tag{12}$$

$$(aMc)D(bMc) = (\frac{ac}{(aDc)})D(\frac{bc}{(bDc)}) = \frac{(acDbc)}{(aDc)D(bDc)} \tag{13}$$

We simplify the denominator:

$$(aDc)D(bDc) = aDcDbDc = aDbD(cDc) \tag{14}$$

Since (cDc)=c, we conclude:

$$(aDb)Mc = (aDc)D(bDc) \tag{15}$$

■

(c)
Note: I am not entirely comfortable with some of the properties I am using here, that were not mentioned in the textbook.

$$(aMb)Dc = (\frac{ab}{(aDb)})Dc = \frac{(ab)Dc}{(aDb)Dc} \tag{16}$$

Using the same reasoning as in (b), we find:

$$(aDc)M(bDc) = \frac{(aDc)(bDc)}{(aDc)D(bDc)} = \frac{(aDc)(bDc)}{(aDcDbDc)} = \frac{(ab)Dc}{(aDb)Dc} \tag{17}$$

We conclude:

$$(aMb)Dc = (aDc)M(bDc) \tag{18}$$

■

2 6 Incomplete Exercises

Exercise 12.

(a)
We have $a^n|b^n$ so $\frac{b^n}{a^n} = q$, where q is an integer.

$$\frac{b^n}{a^n} = \frac{b}{a} \cdot \frac{b^{n-1}}{a^{n-1}} = q \text{so} \frac{b}{a} = q \cdot \frac{a^{n-1}}{b^{n-1}} \tag{19}$$

So $\frac{b}{a} = q \cdot \frac{a^{n-1}}{b^{n-1}}$.
If the expression on the right is an integer, then $a|b$.

(b)
Choosing $a = n = 2$ and $b = 3$, we have $a^n = 2^2 = 4$ and $2b^n = 2 \cdot 3^2 = 18$.

But $4 \nmid 18$, so this is a counter example. ■

Exercise 18.

Let $A_n = a^{2^n} + 1$, so $A_m = a^{2^m} + 1$ and $A_m - 2 = a^{2^m} - 1$.
If $m > n$, then $2^m > 2^n$ and $a^{2^m} > a^{2^n}$ if $a > 1$.
We have $(a^{2m} + 1, a^{2n} + 1) = (A_m, A_n)$.

Exercise 22.

$$(a + b, [a, b]) = (a + b)D(aMb) \tag{20}$$

Let c=(a+b), then:

$$(a + b)D(aMb) = cD(aMb) = (aMb)Dc \tag{21}$$

Using Exercise 21, (c):

$$(a + b)D(aMb) = (aDc)M(bDc) = (aD(a + b))M(bD(a + b)) \tag{22}$$

We have aD(a+b)=(aDa)+(aDb)=a+(aDb). Similarly, bD(a+b)=(bDa)+b.

$$(aD(a + b))M(bD(a + b)) = (a + (aDb))M((bDa) + b) \tag{23}$$

Let d=(aDb)=(bDa), then:

$$\begin{aligned}(a + (aDb))M((bDa) + b) &= (a + d)M(d + b)\\ &= aMd + aMb + dMd + dMb\\ &= aMb + dM(a + b) + d\\ &= aMb + dMc + d\end{aligned} \tag{24}$$

Exercise 26.

If $(a, b) = 1$ and $x^a = y^b$, then $x = n^b$ and $y = n^a$ for some n.
Hint: Use Exercises 25 and 13.
Exercise 25 says: if (a,b)=1 there exist $x, y > 0$ such that $ax - by = 1$.
We replace x and y in this equation:

$$ax - by = an^b - bn^a = n(an^{b-1} - bn^{a-1}) = 1 \tag{25}$$

Exercise 13 says: if $(a, b) = 1$ and $(a/b)^m = n$, then $b = 1$.

Exercise 28.

If $m = n$, then we find $(a^m - 1, a^m - 1) = a^{(m,m)} - 1 = a^m - 1$, so the identity holds.
If $m > n$, then $(a^m, a^n) = a^n$ and $(a^m - 1, a^n - 1) \geq a^n - 1$.
We have $n \geq (m, n)$ so $a^n \geq a^{(m,n)}$ and $a^n - 1 \geq a^{(m,n)} - 1$.
This gives $(a^m - 1, a^n - 1) \geq a^n - 1 \geq a^{(m,n)} - 1$.

To complete the proof, show that: $(a^m - 1, a^n - 1) \leq a^{(m,n)} - 1$.
Note: If $(m, n) = 1$, then $a^{(m,n)} - 1 = a - 1$.

Exercise 30.

An integer has the form $\frac{a}{b}$ where $b|a$. We should expand the harmonic series:

$$\sum_{k=1}^{n} \frac{1}{k} \tag{26}$$