Solutions to Analytic Number Theory by Apostol

Aakash Ghosh

March 29, 2022

Contents

1 The Fundamental Theorem of Arithmetic **2**

Chapter 1

The Fundamental Theorem of Arithmetic

In these exercises lower case latin letters $a, b, c, ..., x, y, z$ represent integers. Prove each of the statements in Exercises I through 6.

> **1.1. lf $(a, b) = 1$ and if $c|a$ and $d|b$, then $(c, d) = 1$.**

Solution: Assume to the contrary that $(c, d) = m \neq 1$. Write $c = k_c m, d = k_d m$ Then $a = ck_a = k_a k_c m$, $b = k_b k_d m$. Then (a, b) is at least m, which is a contradiction.

Alt Solution: We can write $a = k_1 c$ and $b = k_2 d$. Then as $(a, b) = 1$ there exists x, y such that $ax + by = 1 \Rightarrow c(k_1 x) + d(k_2 y) = 1$ which implies $(c, d) = 1$.

> **1.2. If $(a, b) = (a, c) = 1$, then $(a, bc) = 1$.**

Solution : Assume to the contary that $(a, bc) \neq 1$. Then there exist prime p which divides (a, bc) therefore, $p|a$ and $p|bc$. But if $p|bc$ then $p|b$ or $p|c$. But either case will lead to contradiction as this implies either b or c share a common factor with a (which is p).

Alt Solution: There exist $x_1 y, y_1$ and x_2, y_2 such that:

$$ax_1 + by_1 = 1 \quad ax_2 + cy_2 = 1$$

Multiply them to get:

$$a(ax_1x_2 + bx_2y_1 + cx_1y_2) + bc(y_1y_2) = 1$$

Which implies $(a, bc) = 1$

> **1.3. lf $(a, b) = 1$, then $(a^m, b^n) = 1$ for all $n, k \geq 1$**

Solution : Assume to the contary that $(a^m, b^n) \neq 1$. Then there exist prime p which divides (a^n, b^m) therefore, $p|a^n$ and $p|b^m$. As $p|b^m$ then $p|b$. Similarly, $p|a$. This leads to contradiction as this implies either a and b share a common factor (which is p).

> **1.4. If $(a, b) = 1$, then $(a + b, a - b)$ is either 1 or 2.**

Solution : As $(a,b)=1$, there exist (x,y) such that $ax+by=1$. Then:

$$\begin{aligned}
&ax+by=1\\
\Rightarrow&\frac{(a+b)+(a-b)}{2}x+\frac{(a+b)-(a-b)}{2}y=1\\
\Rightarrow&(a+b)\frac{(x+y)}{2}+(a-b)\frac{(x-y)}{2}=1\\
\Rightarrow&(a+b)(x+y)+(a-b)(x-y)=2
\end{aligned}$$

Note if $a'x'+b'y'=m$ then $(a',b')|m$, Therefore, $(a+b,a-b)|2$ or $(a+b,a-b)$ is 1 or 2.

1.5 If $(a,b)=1$, then $(a+b,a^2-ab+b^2)$ is either 1 or 3.

1.6. If $(a,b)=1$ and if $d|(a+b)$, then $(a,d)=(b,d)=1$.

Solution : As $(1,b)=1$, there exists x,y such that $ax+by=1$. Write $a+b=dk$. Then:

$$ax+by=1\Rightarrow a(x-y)+(a+b)y=1\Rightarrow a(x-y)+d(ky)=1$$

Therefore, $(a,d)=1$. Replace a with b everywhere above to get $(b,d)=1$.

1.7. A rational number a/b with $(a,b)=1$ is called a reduced fraction. If the sum of two reduced fractions is an integer, say $(a/b)+(c/d)=n$, prove that $|b|=|d|$.

Solution : By altering sign of a,c we can keep $b,d>0$. We have: $ad+bc=nbd\Rightarrow ad=b(nd-c)$, Now, as $(a,b)=1$, $b|d$. Similarly, $d|b$ and thus $d=\pm b$ and $|d|=|b|$

1.8 An integer is called *squarefree* if it is not divisible by the square of any prime. Prove that for every $n\geq 1$ there exist uniquely determined $a>0$ and $b>0$ such that $n=a^2b$, where b is square free.

Solution : Let $n=\prod p_i\alpha_i$ where each p_i is prime. We write $\alpha_i=2\beta_i+r_i$ where $\beta_i>0$ and $0\leq r_i<2$. Then set $a=\prod p_i^{\beta_i}$ and $b=\prod p_i^{r_i}$. It follows b is square free as if $p_i^2|b$ then $r_i\geq 2$ which leads to a contradiction. Being unique follows from construction.

1.9. For each of the following statements, either give a proof or exhibit a counter example.
1. **If $b^2|n$ and $a^2|n$ and $a^2<b^2$ then $a|b$**
2. **If b^2 is the largest square divisor of n, then $a^2|n$ implies $a|b$.**

Solutions:

1. No. Set $n=36$, $a=2$, $b=3$.
2. Yes. If $n=\prod p_i^{\alpha_i}$ then $b=\prod p_i^{\beta_i}$ where α_i ,p_i and β_i are as defined in above problem. If $a^2|n$ and if $a=\prod p_i^{a_i}$ then $2a_i\leq\alpha_i\Rightarrow a_i<\beta_i$. Therefore, $a_i|\beta_i$ and $a|b$.

1.10. Given x and y, let $m=ax+by$, $n=ex+dy$, where $ad-be=\pm 1$. Prove that $(m,n)=(x,y)$.

Solution: By the equations given, $(a,b)|m$ and $(a,b)|n$. Therefore, $(a,b)|(m,n)$. Now $md-nb=(ad-be)x=\pm x$. So, $((m,n)|x$ and in a similar way we get, $(m,n)|y$. So $(m,n)|(x,y)$ and $(m,n)=(x,y)$.

1.11. Prove that n^4+4 is composite if $n>1$.

Solution : Note:

$$n^2 + 4 = n^4 + 4n^2 + 4 - 4n^2 = (n^2 + 2)^2 - 4n^2 = (n^2 - 2n + 2)(n^2 + 2n + 2)$$

For $n > 1$, the quardratics are posative, and so being composite follows.

In Exercises 12, 13, and 14, a, b, c, m, n denote positive integers.

1.12. For each of the following statements either give a proof or exhibit a counter example.

1. **If $a^n | b^n$ then $a|b$.**
2. **$n^n | m^m$, then $n|m$.**
3. **If $a^n | 2b^n$ and $n > 1$ then $a|b$.**

Solution :

1. Let $a = \prod p_i^{a_i}$ and $b = \prod p_i^{b_i}$. Then $a^n | b^n \Rightarrow na_i | nb_i \Rightarrow a_i | b_i \Rightarrow a|b$
2. Change