Homework Assignment #1: Solutions to Selected Exercises

Part I. Apostol Chapter 1 (pp. 21–23): Exercises 2, 10, 11, 16, 18, 19, 20.

Exercise 2. Prove that, if $(a, b) = (a, c) = 1$, then $(a, bc) = 1$.

SOLUTION: Suppose $(a, b) = (a, c) = 1$. If $(a, bc) > 1$, then a and bc have a common factor $d > 1$. Since $d|a$ implies (d, b) divides (a, b), and since $(a, b) = 1$ by assumption, We must have $(d, b) = 1$. But then, since $d|bc$, we must have $d|c$, by Theorem 1.5 (Euclid's Lemma). But then $d|a$ and $d|c$, contradicting the fact that $d > 1$ and $(a, c) = 1$.

So it must be that $(a, bc) = 1$.

Exercise 10. Given x and y, let $m = ax + by$, $n = cx + dy$, where $ad - bc = \pm 1$. Prove that $(m, n) = (x, y)$.

SOLUTION: Under the given assumptions note that, if $d|x$ and $d|y$, then $d|(ax + by)$ and $d|(cx + dy)$; that is, $d|m$ and $d|n$. So $d|(m, n)$. So $(x, y)|(m, n)$.

On the other hand, the equations $m = ax + by$ and $n = cx + dy$ have solution

$$x = \frac{dm - bn}{ad - bc} = \pm(dm - bn); \qquad y = \frac{-cm + an}{ad - bc} = \pm(-cm + an),$$

since we're assuming that $ad - bc = \pm 1$. So $d|m$ and $d|n$ implies that $d|x$ and $d|y$. That is, $(m, n)|(x, y)$.

Since $(x, y)|(m, n)$ and $(m, n)|(x, y)$, and since greatest common divisors are positive, we conclude that $(m, n) = (x, y)$.

Exercise 11. Prove that $n^4 + 4$ is composite if $n > 1$.

SOLUTION: We will show that, for any $k \in \mathbb{Z}_+$ and $r \in \{0, 1, 2, 3, 4\}$, $(5k + r)^4 + 4$ is composite as long as it's not the case that $k = 0$ and $r = 1$. This will be enough because any $n > 1$ can be written as $n = 5k + r$ for such a k and such an r.

First we consider the case $r = 0$. We note that

$$(5k)^4 + 4 = (2 - 10k + 25k^2)(2 + 10k + 25k^2),$$

so we're done in this case. (It's readily checked that neither factor on the right can equal 1.)

On the other hand, suppose $r \neq 0$. We have

$$\begin{aligned}(5k + r)^4 + 4 &= 4 + 625k^4 + 500k^3 r + 150k^2 r^2 + 20kr^3 + r^4 \\ &= (r^4 + 4) + 5(125k^4 + 100k^3 r + 30k^2 r^2 + 4kr^3).\end{aligned}$$

Clearly, this is larger than 5 as long as $k \neq 0$, and is divisible by 5 as long as $r^4 + 4$ is. But $1^4 + 4 = 5$, $2^4 + 4 = 20$, $3^4 + 4 = 85$, and $4^4 + 4 = 260$, so we're done.

Exercise 16. Prove that if $2^n - 1$ is prime, then n is prime.

SOLUTION: If $n = ab$ where $a, b > 1$, then

$$2^n - 1 = (2^{ab}) - 1 = (2^a)^b - 1 = (2^a - 1)(1 + 2^a + (2^a)^2 + \cdots + (2^a)^{b-1}),$$

by the formula for a finite geometric sum.

Exercise 18. If $m \neq n$ compute the gcd $(a^{2^m}+1, a^{2^n}+1)$ in terms of a. [Hint: let $A_n = a^{2^n}+1$ and show that $A_n | (A_m - 2)$ if $m > n$.]

SOLUTION: If $m > n$, then

$$A_m - 2 = a^{2^m} - 1 = (a^{2^{m-1}} + 1)(a^{2^{m-1}} - 1).$$

The term in parentheses on the far right can further be factored, as $(a^{2^{m-2}}+1)(a^{2^{m-2}}-1)$. We may continue factoring in this manner, to get

$$A_m - 2 = a^{2^m} - 1 = (a^{2^{m-1}}+1)(a^{2^{m-2}}+1)(a^{2^{m-3}}+1)\cdots(a^{2^n}+1)(a^{2^n}-1).$$

The term on the far right is A_n. So $A_n|(A_m-2)$, say $A_m = qA_n + 2$. Now let $d = (A_m, A_m)$. Then $d|A_m$ and $d|A_n$, so $d|2$, so $d = 1$ or $d = 2$. But $d \neq 2$ since A_n and A_m are odd. So $d = (A_n, A_m) = 1$.

Exercise 19. The *Fibonacci sequence* 1, 1, 2, 3, 5, 8, 13, 21, 34,... is defined by the recursion formula $a_{n+1} = a_n + a_{n-1}$, with $a_1 = a_2 = 1$. Prove that $(a_n, a_{n+1}) = 1$ for each n.

SOLUTION: We prove this by induction on n. It's certainly true for $n = 1$ $(1,1) = 1$. Now assume it's true for $n = k$. Then $(a_{k+1}, a_{k+2}) = (a_{k+1}, a_{k+1} + a_k)$. But for general integers r and s, $(r, r+s) = (r, s)$, since $d|r$ and $d|s \Leftrightarrow d|r$ and $d|(r+s)$. So

$$(a_{k+1}, a_{k+2}) = (a_{k+1}, a_{k+1} + a_k) = (a_{k+1}, a_k) = (a_k, a_{k+1}) = 1$$

by the induction hypothesis, and we're done.

Exercise 20. Let $d = (826, 1890)$. Use the Euclidean algorithm to compute d, then express d as a linear combination of 826 and 1890.

SOLUTION:

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

So

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

Part II.

(a) Use mathematical induction to prove that, for any positive integer n, the product of any n integers of the form $4\ell + 1$ (where ℓ is a positive integer) is itself of the form $4\ell + 1$.

SOLUTION: It's true for $n = 1$. Now assume it's true for $n = k$. If $m_1, m_2, \ldots, m_k, m_{k+1} \in \mathbb{Z}$ are of the form $4\ell + 1$, then by induction, there exist integers $r, s \in \mathbb{Z}$ such that

$$m_1 m_2 \cdots m_k \cdot m_{k+1} = (m_1 m_2 \cdots m_k) \cdot m_{k+1} = (4r + 1)(4s + 1) = 4(4s + r + s) + 1;$$

that is, the desired result is true for $n = k + 1$ as well. So we're done by induction.

(b) Show that there are infinitely many primes of the form $4\ell + 3$ (for ℓ a positive integer). You may want to use the result of part (a) of this exercise.

SOLUTION: Suppose there are only finitely many such primes, call them $p_1, p_2, \ldots, p_K$, in ascending order. Let

$$M = 4p_1 p_2 \cdots p_k - 1 = 4(p_1 p_2 \cdots p_K - 1) + 3.$$

Then clearly $M > 1$ and M is of the form $4\ell + 3$. Every integer > 1 is divisible by a prime, so M must be divisible by one of the primes p_j, for some $1 \leq j \leq K$. (M is of the form $4\ell + 3$, so it can't be divisible *only* by primes of the form $4\ell + 1$, because then it too would be of that form, by part (a).) But if p_j divides M then, since p_j also divides $4p_1 p_2 \cdots p_k$, it must divide

$$M - 4p_1 p_2 \cdots p_k = -1,$$

a contradiction. So there must be infinitely many primes of the given form.