Selected Solutions to Homework # 3

• Appendix C # 6: Prove that $3|(4^n - 1)$ for every $n \in \mathbb{Z}_+$.

Proof: If $n = 1$, this is true. Assume that $3|(4^n - 1)$ for some $n \geq 1$. Then, $4^n - 1 = 3m$ for some $m \in \mathbb{Z}$. Consider $4^{n+1} - 1$:

$$4^{n+1} - 1 = 4 \cdot 4^n - 1 = 3 \cdot 4^n + 4^n - 1 = 3 \cdot 4^n + 3m = 3(4^n + m).$$

Therefore, $3|(4^{n+1} - 1)$. By the principle of mathematical induction, $3|(4^n - 1)$ for every $n \geq 1$. Q.E.D.

• Appendix C # 17: We discussed this in class on 01/19/2011.

• Section 1.2 #2: Prove that $b|a$ if and only if $(-b)|a$.

  Don’t forget to prove both implications!

Proof: If $b|a$, then $a = bc$ for some $c \in \mathbb{Z}$. So, $a = (-b)(-c)$. Therefore, $(-b)|a$. Conversely, if $(-b)|a$, then $a = (-b)c$ for some $c \in \mathbb{Z}$. So, $a = b(-c)$. Therefore, $b|a$.

• Section 1.2 #4:

  (a) If $a|b$ and $a|c$, then $a|(b + c)$.
  (b) If $a|b$ and $a|c$, then $a|(br + ct)$ for every $r, t \in \mathbb{Z}$.

  (This is an important exercise in lieu of one of the major concepts we will study in chapter 6: see p. 135; this exercise proves that the set $S = \{n \in \mathbb{Z} : a|n\}$ is an ideal in the ring $R = \mathbb{Z}$.)

If you have questions about this problem, please stop by during office hours or make an appointment to meet with me. If you did not get this problem correct, try re-writing a solution, and bring this new solution to office hours and I will critique your writing and offer some suggestions.

• Section 1.2 #8: Let $a, b \in \mathbb{Z}$. If $r \in \mathbb{Z}$, $r \neq 0$, and $r$ is a solution to $x^2 + ax + b = 0$, prove that $r|b$.

Proof: Since $r$ is a solution to the equation, $r^2 + ar + b = 0$. So, $b = r(-r - a)$. Therefore, $r|b$.

Do you see how to generalize this problem to other polynomials?
Section 1.2 #12: Suppose that \((a, b) = 1\) and \((a, c) = 1\). Decide whether each of the following is true or false. (See the book for statements. The answers are as follows: (a) false, (b) false, (c) true, (d) false. Below, I will state and prove that (c) is true.) The solution is not the most efficient, but it highlights another important exercise in section 1.2.

(c): If \((a, b) = 1\) and \((a, c) = 1\), then \((bc, a) = 1\).

Proof: There exist \(m, n, p, q \in \mathbb{Z}\) such that \(am + bn = 1\) and \(ap + cq = 1\). Multiplying, we have that \(a^2mp + bcnq + apbn + amcq = 1\). Factoring, we have that \(a(amp + pbn + mcq) + bc(nq) = 1\). We now apply the following result (see exercise #27 (a) in section 1.2):

If \(w, x, y, z \in \mathbb{Z}\) and \(wx + yz = 1\), then \((x, y) = 1\).

(This is the converse to (Theorem 1.3) the statement that \((x, y) = 1\) implies there exists integers \(w, z\) such that \(wx + yz = 1\). See part (b) of exercise #27: the converse is not true if the greatest common divisor is greater than 1.)

Since we have not solved exercise #27 (a), we need to do so now before applying it. So, suppose \(w, x, y, z \in \mathbb{Z}\) and \(wx + yz = 1\). If \(d\) is a common divisor of \(x\) and \(y\), then \(d\) divides \(wx + yz\). (This is exercise #4 (b) from this homework.) Therefore \(d\) divides 1. Hence \(d = \pm 1\). Since \(d\) was an arbitrary common divisor, the greatest common divisor is 1.

Returning to the proof of (c), we had shown that \(a(amp + pbn + mcq) + bc(nq) = 1\). By exercise #27 (a), we have that \((a, bc) = 1\). Q.E.D.

You may now use exercise #27 (a) in your solutions to future homework exercises, quiz problems, and exam problems. It is a very useful result.