

# Homework

Jon Allen

September 10, 2014

- 1.1 14. For what positive integers  $n$  is it true that  $(n, n+2) = 2$ ? Prove your claim.

## claim

The statement is true for all even integers.

## proof

First let's note that by the definition of even and odd integers, two does not divide an odd integer. Because two is not a divisor of an odd integer, it cannot be a greatest common divisor with any other integer. It follows then that  $n$  must be even. That is to say there exists some  $k \in \mathbb{Z}$  such that  $n = 2k$ .

Now we show that the fact that  $n$  is even is enough for  $\gcd(n, n+2) = 2$ . Let's take an integer  $d \neq 2$  where  $d = \gcd(n, n+2)$ . Now by definition  $d|n$ . Because  $n$  is even we have  $d|2k$ . Because  $d \neq 2$  there must exist some integer  $a$  such that  $k = ad$  and then  $d|2ad$ . Now because  $d$  also divides  $n+2$  we have  $d|2ad+2$  which is to say there exists some integer  $b$  such that  $bd = 2ad+2$ . This is true only if  $d|2$ . Because  $d \neq 2$  we see that  $d = 1$ . However we defined  $d = \gcd(n, n+2)$  and we know that  $2|n$  and  $2|(n+2)$  and obviously  $2 > 1$  so we have a contradiction. Therefore if  $n$  is even, then  $\gcd(n, n+2) = 2$ .  $\square$

16. Let  $a, b, c$  be integers, with  $b > 0, c > 0$ , and let  $q$  be the quotient and  $r$  the remainder when  $a$  is divided by  $b$ .

(a) Show that  $q$  is the quotient and  $rc$  is the remainder when  $ac$  is divided by  $bc$ .

## proof

We observe that dividing  $a$  by  $b$  we are guaranteed to be able to find  $a = bq + r$  such that  $0 \leq r < b$ . Let's multiply this by  $c$ . We get  $c(a) = c(bq+r)$ . Now distributing and rearranging we see that  $ac = (bc)q + rc$ . We see from this that  $q$  is a quotient and  $rc$  is a remainder. Observe however that these may not be the quotient and remainder that are guaranteed by the division algorithm.

To guarantee this, we must show that  $rc < bc$ . Note that  $c > 0$  and  $0 \leq r < b$ . Again multiplying by  $c$  we have  $0 \leq rc < bc$  and therefore  $rc$  is the remainder guaranteed by the division algorithm. By extension  $q$  must also be the quotient guaranteed by the division algorithm.  $\square$

- (b) Show that if  $q'$  is the quotient when  $q$  is divided by  $c$  then  $q'$  is the quotient when  $a$  is divided by  $bc$ . (Do not assume that the remainders are zero.)

## proof

We let  $q = cq' + r'$  where  $r'$  is the remainder when  $q$  is divided by  $c$ . Let us multiply both sides of the equation by  $b$  to get  $bq = bcq' + br'$ . We note that  $a = bq + r$  and substitute in

$bq$  to obtain  $a = bcq' + br' + r$ . Now we see that  $q'$  is a quotient when  $a$  is divided by  $bc$ . We must show that  $0 \leq br' + r < bc$  to prove that  $br' + r$  is the remainder guaranteed by the division algorithm and by extension,  $q'$  is the quotient guaranteed by the division algorithm. We know  $0 \leq r' < c$  and  $0 \leq r < b$  so  $r'$  is at most  $c - 1$  and  $r$  is at most  $b - 1$ . This means that  $br' + r \leq b(c - 1) + b - 1$ . Simplifying we have  $br' + r \leq bc - 1$  or  $br' + r < bc$ . Similarly  $0 \leq b(0) + 0 = 0$  so  $0 \leq br' + r < bc$  and we have our result.  $\square$

21. Prove that the sum of the cubes of any three consecutive positive integers is divisible by 3.

**proof**

Let  $a \in \mathbb{Z}^+$ . We seek to show that there exists some integer  $b$  such that  $3b = a^3 + (a+1)^3 + (a+2)^3$ .

$$\begin{aligned} 3b &= a^3 + (a+1)^3 + (a+2)^3 \\ &= a^3 + a^3 + 3a^2 + 3a + 1 + a^3 + 3 \cdot 2a^2 + 3 \cdot 2^2a + 2^3 \\ &= 3a^3 + 9a^2 + 15a + 9 \\ &= 3(a^3 + 3a^2 + 5a + 3) \\ b &= a^3 + 3a^2 + 5a + 3 \end{aligned}$$

Note that this works with all  $a \in \mathbb{Z}$ , it does not require  $a \in \mathbb{Z}^+$ .  $\square$

- 1.2 12. Let  $a, b, c$  be nonzero integers. Show that  $\gcd(a, b) = 1$  and  $\gcd(a, c) = 1$  if and only if  $\gcd(a, \text{lcm}[b, c]) = 1$

**proof**

I could prove this using the  $a = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_n^{\alpha_n}$  representation of prime factorizations used in the book, but I think it will be easier to see if we think of prime factorizations as sets instead. If we have some integer  $a = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_n^{\alpha_n}$  where  $p_i$  is prime and  $\alpha_i$  is the number of times that factor occurs in the prime factorization, then we can imagine some set  $F(a) = \{p_{ij} : 1 \leq i \leq n, 1 \leq j \leq \alpha_i\}$ . For example  $F(8) = \{2_1, 2_2, 2_3\}$ ,  $F(12) = \{2_1, 2_2, 3_1\}$ . Now we reformulate Proposition 1.2.10 to say that  $\gcd(a, b)$  is the intersection of the sets of prime factors for  $a$  and  $b$ . We see this as  $\min\{\alpha_i, \beta_i\}$  will only include elements that are in both  $F(a)$  and  $F(b)$ . That is to say  $\gcd(a, b) = F(a) \cap F(b)$ . Similarly  $\text{lcm}[a, b]$  is the union of  $F(a)$  and  $F(b)$ . This is also true as  $\max\{\alpha_i, \beta_i\}$  will include all elements in  $F(a)$  and  $F(b)$ . Note that if  $F(a) \cap F(b) = \emptyset$  then there are no prime factors and  $\gcd(a, b) = 1$ . The result falls very naturally out of this reformulation:

$$\begin{aligned} \gcd(a, b) &= F(a) \cap F(b) = \emptyset \\ \gcd(a, c) &= F(a) \cap F(c) = \emptyset \\ \gcd(a, \text{lcm}[b, c]) &= F(a) \cap (F(b) \cup F(c)) \\ &= (F(a) \cap F(b)) \cup (F(a) \cap F(c)) \\ &= \emptyset \cup \emptyset \end{aligned}$$

Since the set of prime factors is empty, we see that  $\gcd(a, \text{lcm}[b, c]) = 1$ .  $\square$

23. Show that if  $n$  is a positive integer such that  $2^n + 1$  is prime, then  $n$  is a power of 2.

**proof**

Because  $n$  is a power of two, its prime factorization is  $2^m$  for some integer  $m \geq 0$  and all of its factors are therefore even. Let us assume that  $n$  is not a power of two, then it must have some odd prime factor  $p = 2k + 1$ . We'll say that  $n = (2k + 1)q$ .

$$2^n + 1 = 2^{q(2k+1)} + 1$$

$$\begin{aligned}
&= (2^q)^{2k+1} + 1 \\
&= (2^q + 1)(2^{q2k} - 2^{q(2k-1)} + \dots + 1)
\end{aligned}$$

Now because we defined  $p$  to be prime we know that  $p \geq 2$  and therefore  $k \geq 1$ . This means that we have found a factor for  $2^n + 1$  when  $n$  is not a power of two. Therefore, if  $n$  is a power of two, then  $2^n + 1$  must not have any factors and is therefore prime.  $\square$