Homework 4

Dean Quach
MATH 3003 - Theory of Numbers

Februrary 17, 2023

I hilariously messed up, I normally have my homework done early... but this time I had done the wrong section. I had done these exercises, but in section 3.4 (instead of 3.3). This is why I didn't print it this morning. (Also to save paper is a better excuse :)

Exercise 3.3.1. Find the greatest common divisor of each of the following pairs of integers.

Part (a) 15, 35
Sol^n :
The positive divisors 15 $:= A = \{1, 3, 5, 15\}$.
The positive divisors 35 $:= B = \{1, 5, 7, 35\}$.

$$\text{So } gcd(15, 35) = max(A \cap B) = 5. \quad \square$$

Part (b) 0, 111
Sol^n :
Notice all numbers are divisors of 0 since $c \mid 0, \ \forall c \in \mathbb{Z}$

$$\text{So of course, } gcd(0, 111) = |111| = 111. \quad \square$$

Part (c) -12, 18
Sol^n :
The positive divisors -12 $:= A = \{1, 2, 3, 4, 6, 12\}$.
The positive divisors 18 $:= B = \{1, 2, 3, 6, 9, 18\}$.

$$\text{So } gcd(-12, 18) = max(A \cap B) = 6. \quad \square$$

Part (d) 99, 100
Sol^n :
The positive divisors 99 $:= A = \{1, 3, 9, 11, 22, 99\}$.
The positive divisors 100 $:= B = \{1, 2, 4, 5, 10, 20, 25, 50, 100\}$.

$$\text{So } gcd(99, 100) = max(A \cap B) = 1. \quad \square$$

Part (e) 11, 121
Sol^n :
The positive divisors 11 $:= A = \{1, 11\}$.
The positive divisors 121 $:= B = \{1, 11, 121\}$.

$$\text{So } gcd(11, 121) = max(A \cap B) = 11. \quad \square$$

Part (f) 100, 102
Sol^n :
The positive divisors 100 $:= A = \{1, 2, 4, 5, 10, 20, 25, 50, 100\}$.
The positive divisors 18 $:= B = \{1, 2, 3, 6, 17, 34, 51, 102\}$.

$$\text{So } gcd(100, 102) = max(A \cap B) = 2. \quad \square$$

Exercise 3.3.8. Show that the greatest common divisor of an even number and an odd number is odd.

Proof. Let $a, b \in \mathbb{Z}$ such that a is even and b is odd.
Then $a = 2n$, for some $n \in \mathbb{Z}$. Also $b = 2m + 1$ for some $m \in \mathbb{Z}$.
Now consider $gcd(a, b)$.

BWOC, assume that $gcd(a, b)$ is even, and let $gcd(a, b) = d$.
Now we know $2 \mid d$. Also by the definition of gcd, we know $d \mid a \ \wedge \ d \mid b$.
Notice, by transitivity, $2 \mid d \ \wedge \ d \mid a \implies 2 \mid a$.
But then, by transitivity, $2 \mid d \ \wedge \ d \mid b \implies 2 \mid b$.
Contradiction! Since b is odd $\implies 2 \nmid b$.

Therefore, $gcd(a, b)$ is odd. *q.e.d.*

Exercise 3.3.9. Show that if a and b are integers, not both 0, and c is a nonzero integer, then $gcd(ca, cb) = |c| gcd(a, b)$.

Proof. Let $a, b \in \mathbb{Z}$ such that they cannot both be 0. Also let $c \in \mathbb{Z} \backslash \{0\}$.
Then $gcd(ca, cb) = d$, where $d \in \mathbb{Z}_{\geq 0}$.

Now by Bezout's Thm., we know

$$\begin{aligned} d &= n(ca) + m(cb), \text{ for some } n, m \in \mathbb{Z} \\ &= c(na) + c(mb) \\ &= c(na + mb) \end{aligned}$$

Small note, we let $c \in \mathbb{Z}\{0\}$ which includes $\mathbb{Z}_{<0}$. And since $gcd \implies max$,
even though divisors of a and b are both positive and negative,
we only need to consider the positive divisors. Hence, $d = |c|(na + mb)$.

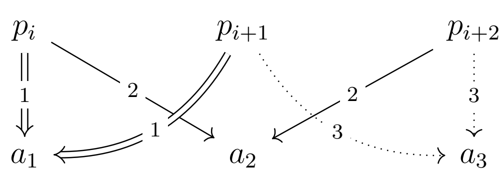
Therefore $gcd(ca, cb) = |c| gcd(a, b)$. *q.e.d.*

Exercise 3.3.10. Show that if a and b are integers, with $gcd(a,b) = 1$, then $gcd(a+b, a-b) = 1 \ \vee \ 2$.

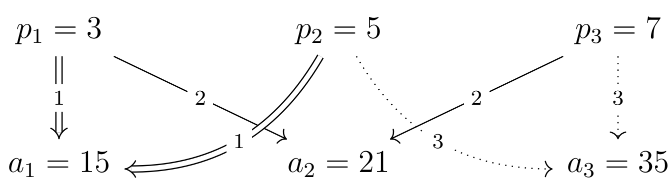
Proof. Let $a, b \in \mathbb{Z}$ such that $gcd(a,b) = 1$. Also let $d = gcd(a+b, a-b)$.
Then $d \mid a+b \ \wedge \ a-b$
and then $d \mid (a+b)n + (a-b)m$, for some $n, m \in \mathbb{Z}$. Observe $d \mid 2$ since $d = gcd(2a, 2b) = 2gcd(a,b) = 2(1) = 2$. Also we know $d \mid (a+b)n + (a-b)m$. So one can choose $m = n = 1 \implies 2 \mid 2a$, and $m = 1, n = -1 \implies 2 \mid 2b$.
Therefore $d \mid 2 \implies d = \{1, 2\}$. *q.e.d.*

Exercise 3.3.17. Find a set of three integers that are mutually relatively prime, but any two of which are not relatively prime. (No ex.'s from text)

Sol^n :
This may already exist, but I had found an interesting way to generate sets of integers $\{a_1, a_2, a_3\}$ with these properties. Let p_i be a prime number. Then consider the following diagram.



I cannot prove this, nor do I want to. But it generates the triple of integers when you multiple the two primes on each arrow type/numbered. For example, the textbook one (which I had accidentally recreated using this method):



Which of course has the properties

- $gcd(15, 21, 35) = 1$
- $gcd(15, 21) = 3 \neq 1$
- $gcd(15, 35) = 5 \neq 1$
- $gcd(21, 35) = 7 \neq 1$

I, of course, then checked if this was an example from the text, and indeed was. So I chose a few more primes. (I had also checked for *gcd* properties by hand, but the question doesn't technically ask for it (and I'm lazy).

$$\begin{tikzcd}
p_1 = 13 \arrow[d, Rightarrow, "1"] \arrow[dr, "2"] & p_2 = 17 \arrow[dl, Rightarrow, bend left, "1"] \arrow[dr, dotted, bend right, "3"] & p_3 = 23 \arrow[dl, "2"] \arrow[d, dotted, "3"] \\
a_1 = 221 & a_2 = 299 & a_3 = 391
\end{tikzcd}$$

Which of course has the properties

- $gcd(221, 299, 391) = 1$
- $gcd(221, 299) = 13 \neq 1$
- $gcd(221, 391) = 17 \neq 1$
- $gcd(299, 391) = 23 \neq 1$

So one possible set of three integers that are mutually relatively prime, but any two of which are not relatively prime, are {221,299,391}. $\square$

Exercise 3.3.24. Show that if k is a positive integer, then $3k + 2$ and $5k + 3$ are relatively prime.

Proof. Let $k \in \mathbb{Z}_{>0}$. And set $gcd(3k + 2, 5k + 3) = d$ for some $d \in \mathbb{Z}$.
Then $d \mid n(3k + 2) + m(5k + 3)$, for some $n, m \in \mathbb{Z}$. WNTS the dividend is equal to 1.
Well take $n = 5,\ m = -3$. Then
$n(3k + 2) + m(5k + 3) = 5(3k + 2) + (-3)(5k + 3) = 1$
Hence, $d \mid 1 \implies d = 1$. So $gcd(3k + 2, 5k + 3) = d = 1$

Therefore $3k + 2$ and $5k + 3$ are relatively prime. *q.e.d.*

Exercise 3.3.25. Show that if $8a + 3$ and $5a + 2$ are relatively prime for all integers a.

Proof. [1]

$$\begin{aligned}
gcd(8a + 3, 5a + 2) &= gcd((8a + 3) + (-1)(5a + 2), 5a + 2) \\
&= gcd(3a + 1, 5a + 2) = gcd(5a + 2, 3a + 1) \\
&= gcd((5a + 2) + (-1)(3a + 1), 3a + 1) \\
&= gcd(2a + 1, 3a + 1) = gcd(3a + 1, 2a + 1) \\
&= gcd(3a + 1 - (2a + 1), 2a + 1) \\
&= gcd(a, 2a + 1 + (-2)(a)) \\
&= gcd(a, 1) = 1.
\end{aligned}$$

Therefore

$$gcd(8a + 3, 5a + 2) = 1.$$

q.e.d.

[1] ($gcd(a + cb, b) = gcd(ab)$), Also the gcd being commutative steps (on the right) might be overkill.