Ve203 Discrete Mathematics (Fall 2020)

Assigment 3: Division Theory of the Integers, Prime Numbers

Date Due: 2:00 PM, Wednesday, the 30th of September 2020

This assignment has a total of **(29 Marks)**.

Exercise 3.1
Prove Corollary 7.11 of the lecture:

> Let $a, b \in \mathbb{Z}$ with $|a| + |b| \neq 0$. Then
>
> $$T(a, b) = \{n \in \mathbb{Z} : n = ax + by,\ x, y \in \mathbb{Z}\}$$
>
> is the set of all integer multiples of $\gcd(a, b)$.

(2 Marks)

Exercise 3.2
Use the Division Algorithm to show that for any $n \in \mathbb{N}$ there exists a $k \in \mathbb{N}$ such that either $n^2 = 3k$ or $n^2 = 3k + 1$.
(3 Marks)

Exercise 3.3
Let $a \in \mathbb{Z}$ and $n \in \mathbb{N}$. Prove that $\gcd(a, a + n)$ divides n. Deduce that a and $a + 1$ are always relatively prime.
(3 Marks)

Exercise 3.4
Use the Euclidean Algorithm to find $x, y \in \mathbb{Z}$ such that

i) $\gcd(56, 72) = 56x + 72y$,
(2 Marks)

ii) $\gcd(1769, 2378) = 1769x + 2378y$.
(2 Marks)

Exercise 3.5
Find all $x, y \in \mathbb{Z}$ such that

i) $56x + 72y = 40$,
(2 Marks)

ii) $84x - 439y = 156$.
(2 Marks)

Exercise 3.6

i) Suppose $a, b \in \mathbb{N} \setminus \{0\}$ with $\gcd(a, b) = 1$ and let $c \in \mathbb{Z}$. Show that there exist infinitely many solutions $x, y \in \mathbb{N}$ of the Diophantine equation $ax - by = c$.
(3 Marks)

ii) Find $x, y \in \mathbb{N}$ such that $158x - 57y = 7$.
(2 Marks)

Exercise 3.7

Consider the set S of all positive integers of the form $3k+1$: $S = \{n \in \mathbb{N} \colon n = 3k+1,\ k \in \mathbb{N}\}$. An integer in S is said to be prime if it cannot be factored into two smaller integers, each of which belongs to S. (Thus, 10 and 25 are prime, while 16 and 28 are not.)

i) Prove that any member of S is either prime or a product of primes.

   (2 Marks)

ii) Give an example to show that it is possible for an element of S to be factored into primes in more than one way.

   (1 Mark)

Exercise 3.8

Let D be the set of all the primes of the form $4 \cdot n + 3$ for $n \in \mathbb{N}$. We suppose D to be finite and define $d = 4 \cdot (3 \cdot 7 \cdot \dots \cdot p) - 1$, where p is the largest prime in D.

i) Prove that no prime of the form $4 \cdot k + 3$ divides d.

   (1 Mark)

ii) Prove that d is not divisible by $4 \cdot k + 1$.

   (2 Marks)

iii) Conclude that there is an infinite number of primes of the form $4 \cdot n + 3$.

   (2 Marks)

Note: The general version of this result is called Dirichlet's theorem and states that if a and b are non-zero coprime natural numbers then there are an infinite number of primes of the form $an + b$ for $n \in \mathbb{N}$.