MATH 215 – Number Theory I (NTI)

We will assume the existence of a set $\mathbb{Z} = \{0, 1, -1, 2, -2, \ldots\}$ of integers satisfying the axioms on sheet AI. We will also assume the existence of the set $\mathbb{N} = \{1, 2, 3, \ldots\}$ of natural numbers. The set $\mathbb{N}$ is naturally a subset of $\mathbb{Z}$ and we will assume that if a, b are natural numbers, then $a + b$ and ab are natural numbers.

Definition 1 *Let a, b be integers. We say that a* **divides** *b if there exists an integer k such that $ak = b$. If a divides b, we write $a|b$.*

Remark 2 *If a divides b, we can also say that a is a* **divisor** *of b, or that b is a* **multiple** *of a.*

Proposition 3 *Let a, b, c be integers. If $a|b$ and $a|c$, then $a|(b + c)$.*

Proposition 4 *Let a, b, c be integers. If $a|b$ and $a|c$, then $a|(b - c)$.*

Conjecture 5 *Let a, b, c be integers. If $a|(b + c)$, then $a|b$ and $a|c$.*

Proposition 6 *Let a, b, c be integers. If $a|b$ and $a|c$, then $a|bc$.*

Proposition 7 *Let a, b, c be integers. If $a|b$, then $a|bc$. [Can we put this statement into words to better understand what it is saying?]*

Proposition 8 *Let a, b, c be integers. If $a|b$ and $b|c$, then $a|c$.*

Proposition 9 *If n is an integer, then $n|0$.*

Corollary 10 *If n and a are integers, then $n|(a - a)$.*

Proposition 11 *Let n, a, b be integers. If $n|(a - b)$, then $n|(b - a)$.*

Proposition 12 *Let n, a, b, c be integers. If $n|(a - b)$ and $n|(b - c)$, then $n|(a - c)$.*

Definition 13 *Let a, b be integers and n a natural number. If $n|(a - b)$, then we say that a* **is congruent to** *b* **modulo** *n and write*

$$a \equiv b \bmod n.$$

Remark 14 *Consider two statements P and Q. We write P* **if and only if** *Q to mean the combination of the statements "If P, then Q" AND "If Q, then P".*

Proposition 15 *Let a be an integer and n a natural number. $n|a$ if and only if $a \equiv 0 \bmod n$.*

Note: In the above proposition, the statement P is $n|a$ and the statement Q is $a \equiv 0 \bmod n$.

Proposition 16 *Let a be an integer and n a natural number. Then $a \equiv a \bmod n$.*

Proposition 17 *Let a, b be integers and n a natural number. If $a \equiv b \bmod n$, then $b \equiv a \bmod n$.*

Proposition 18 *Let a, b, c be integers and n a natural number. If $a \equiv b \bmod n$ and $b \equiv c \bmod n$, then $a \equiv c \bmod n$.*

Proposition 19 *Let a, b, c, d be integers and n a natural number. If $a \equiv b \bmod n$ and $c \equiv d \bmod n$, then $a + c \equiv b + d \bmod n$.*

Proposition 20 *Let a, b, c, d be integers and n a natural number. If $a \equiv b \bmod n$ and $c \equiv d \bmod n$, then $a - c \equiv b - d \bmod n$.*

Proposition 21 *Let a, b, c, d be integers and n a natural number. If $a \equiv b \bmod n$ and $c \equiv d \bmod n$, then $ac \equiv bd \bmod n$.*

Notation 22 *If a does not divide b, we notate this by $a \nmid b$.*

Proposition 23 $2 \nmid 1$.

Proposition 24 *Let a, b be natural numbers. If $a > b$, then $a \nmid b$.*

Definition 25 *Let S be a set of integers and let l be an element of S. We say that l is a* **least element** *of S if $l \leq s$ for every s in S.*

Proposition 26 *Let S be a set of integers and assume that l is a least element of S. If l' is some other least element of S, then $l = l'$.*

Note: Proposition 26 says that the least element of a set (if it exists) is unique.

Conjecture 27 *Every non-empty set of integers has a least element.*

Axiom 28 *If S is a non-empty set of non-negative integers, then S has a least element.*

Remark 29 *The above axiom is referred to as the* **Well-Ordering Principle (WOP)***. We will assume it is true without proof.*

Challenge 30 *Let a be an integer and n a natural number. Show that there exists a unique integer r such that $a \equiv r \bmod n$ and $0 \leq r < n$.*

Hints: Consider the set $S = \{a - kn : k \text{ is an integer and } a - kn \geq 0\}$. Show that S only contains non-negative integers and is non-empty. Use the Well-Ordering Principle to find the smallest element of S and call it r. Show that $a \equiv r \bmod n$ and explain why $0 \leq r < n$.

Question 31 *Why have we labeled the unique integer in Challenge 30 with the letter r? What does this number represent?*

Remark 32 *Let a be an integer and n a natural number. Let r be the unique integer as in Challenge 30. Define the (unique) integer q by the formula $a = nq + r$. (Why have we chosen to use the letter q?) Given the integer a and the natural number n, finding the unique integers q, r such that $a = nq + r$ where $0 \leq r < n$ is called the* **division algorithm**.

Proposition 33 *Let a, b be integers and n a natural number. If $a \equiv b \bmod n$, then $a^2 \equiv b^2 \bmod n$.*

Proposition 34 *Let a, b be integers and n a natural number. If $a \equiv b \bmod n$, then $a^3 \equiv b^3 \bmod n$.*

Proposition 35 *Let a, b be integers and n a natural number. If $a \equiv b \bmod n$, then $a^k \equiv b^k \bmod n$ for every natural number k.*

Problem 36 *For the following pairs of integers a and n, find q and r in the division algorithm.*

- $a = 5$, $n = 2$
- $a = 72$, $n = 5$
- $a = 94$, $n = 100$
- $a = 7814$, $n = 1124$

Definition 37 *Let a and b be positive integers and d an integer such that $d|a$ and $d|b$. Then we say that d is a* **common divisor** *of a and b.*

Definition 38 *Let a and b be integers such that not both of a and b are zero. We say an integer d is a* **greatest common divisor** *of a and b if the following two statements are true:*

1. *$d|a$ and $d|b$; and*
2. *if c is any integer such that $c|a$ and $c|b$, then $c \leq d$.*

Proposition 39 *Let a and b be integers such that not both are zero. Let*

$$D = \{am + bn : m \text{ and } n \text{ are integers, and } am + bn > 0\}.$$

Then the following statements are true:

1. *D is a non-empty set of positive integers.*

2. *D has a least element. Call that least element d.*
3. *There exists integers x and y such that $d = ax + by$.*
4. *$d|a$ and $d|b$. [Hint: Use the division algorithm.]*
5. *If c is any integer such that $c|a$ and $c|b$, then $c|d$.*
6. *If c is any integer such that $c|a$ and $c|b$, then $c \leq d$.*
7. *d is a greatest common divisor of a and b.*
8. *The greatest common divisor is unique.*

Notation 40 *The greatest common divisor of a and b is denoted* $\gcd(a, b)$.

Lemma 41 *Let a, b be natural numbers, and let q, r be the unique integers as defined by $a = bq + r$ where $0 \leq r < b$. If d is a natural number, then $d|a$ and $d|b$ if and only if $d|b$ and $d|r$.*

Proposition 42 *Let a, b be natural numbers, and let q, r be the unique integers as defined by $a = bq + r$ where $0 \leq r < b$. Then* $\gcd(a, b) = \gcd(b, r)$.

Proposition 43 *Let a be a natural number. Then* $\gcd(a, 0) = a$.

Problem 44 *Using the previous two propositions, find the greatest common divisor of the following pairs of natural numbers.*

- $\gcd(7, 2)$
- $\gcd(52, 16)$
- $\gcd(1492, 2014)$
- $\gcd(528740, 615846)$

Remark 45 *The process of finding the greatest common divisor of two natural numbers using the previous two propositions is referred to as the* **Euclidean Algorithm.**

Problem 46 *For each part, find integers m, n such that* $\gcd(a, b) = am + bn$.

- $\gcd(7, 2)$
- $\gcd(52, 16)$
- $\gcd(1492, 2014)$
- $\gcd(528740, 615846)$