MATH 320 Unit 1 Exam Name:

Instructions:

Please write your answers on separate paper. Please write clearly and legibly, using a large font and plenty of white space (I need room to put my comments). Staple all your pages together, with your problems in order, when you turn in your exam. Make clear what work goes with which problem. Put your name on every page. To get credit, you must show adequate work to justify your answers. If unsure, show the work. No outside materials are permitted on this exam – no notes, papers, books, calculators, phones, smartwatches, or computers – only pens and pencils. You may freely use the contents of the box below, but not any other results we may have proved. Each problem is out of 10 points, 40 points maximum. You have 30 minutes.

1. Use the Euclidean algorithm to find $\gcd(29,18)$ and also to find $u, v \in \mathbb{Z}$ with $29u + 18v = \gcd(29, 18)$.
2. Let $a, c, n \in \mathbb{Z}$ with $n \geq 1$. Define q_a, r_a, q_c, r_c via $(a, n) \to DA \to (q_a, r_a)$ and $(c, n) \to DA \to (q_c, r_c)$. Prove that $r_a = r_c$ if and only if $a \equiv c \pmod{n}$.
3. Let $a, b \in \mathbb{Z}$, not both zero. Prove that $\gcd(a, b) = \gcd(a, b + a)$.
4. Let $a, n \in \mathbb{Z}$ with $n \geq 2$. Suppose that $[a] = [n-1]$ modulo n. Prove that $\gcd(a, n) = 1$.

Given $m, n \in \mathbb{Z}$, we say that m *divides* n, writing $m|n$, if there is some $k \in \mathbb{Z}$ with $mk = n$. We then call m a *divisor* of n. Given $r, s, t \in \mathbb{Z}$, we say that r is a *common divisor* of s and t if $r|s$ and $r|t$.

Given $p \in \mathbb{Z}$ with $p \notin \{-1, 0, 1\}$, we say that p is *prime* if it satisfies:

$$\forall a, b \in \mathbb{Z}, \text{ if } p|ab \text{ then } \big(p|a \text{ or } p|b\big).$$

Bonus Theorem: Let $a, b \in \mathbb{Z}$. If $a|b$ and $b|a$ then $|a| = |b|$.

Division Algorithm Theorem: Let $a, b \in \mathbb{Z}$ with $b \geq 1$. Then there exist unique $q, r \in \mathbb{Z}$ with $a = bq + r$ and $0 \leq r < b$. We write $(a, b) \to DA \to (q, r)$.

Let $a, b \in \mathbb{Z}$, not both zero. We define their *greatest common divisor* $\gcd(a, b)$ as the largest of their common divisors. (this must exist since 1 is always a common divisor)

Let $a_1, a_2 \in \mathbb{Z}$ with $a_2 \geq 1$. We define the *Euclidean algorithm* as $(a_1, a_2) \to DA \to (q_1, a_3)$, then $(a_2, a_3) \to DA \to (q_2, a_4)$, and so on until $(a_k, a_{k+1}) \to DA \to (q_k, 0)$.

Bézout's Lemma: Let $a, b \in \mathbb{Z}$, not both zero. Then there exist $u, v \in \mathbb{Z}$ with $au + bv = \gcd(a, b)$. Conversely, for any $x, y \in \mathbb{Z}$, we must have $\gcd(a, b)|(ax + by)$.

Positive Fundamental Theorem of Arithmetic: Let $n \in \mathbb{Z}$ with $n \geq 2$. Then n has a factorization into positive primes, that is unique up to order.

Let $a, b, n \in \mathbb{Z}$ with $n \geq 1$. We say *a is congruent to b modulo n*, writing $a \equiv b \pmod{n}$, if $n|(a-b)$.

Let $a, n \in \mathbb{Z}$ with $n \geq 1$. The *congruence (or equivalence) class of a modulo n*, written $[a]$, is the set $\{b \in \mathbb{Z} : b \equiv a \pmod{n}\}$.