MATH 320 Unit 1 Exercises

Factorization and Congruence in $\mathbb{Z}$

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 $\{b \in \mathbb{Z} : b \equiv a \pmod{n}\}$. We define $\mathbb{Z}_n$ to be the set of equivalence classes modulo n, which are $\{[0], [1], \ldots, [n-1]\}$. (each have many different names)

For Sep. 4:

1. Let $a, b, c \in \mathbb{Z}$ with $b, c \geq 1$. Suppose that $(a, b) \to DA \to (q, r)$. Prove that $(ac, bc) \to DA \to (q, rc)$.
2. Let $a \in \mathbb{Z}$. Prove that either there is some $k \in \mathbb{Z}$ with $a^2 = 3k$, or there is some $k \in \mathbb{Z}$ with $a^2 = 3k + 1$. HINT: $(a, 3) \to DA$.
3. 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 $n|(a - c)$.
4. Prove the uniqueness part of the Division Algorithm Theorem. That is, suppose $(a, b) \to DA \to (q, r)$ and also $(a, b) \to DA \to (q', r')$. Prove $q = q'$ and $r = r'$.

For Sep. 9:

5. Let $a, b \in \mathbb{Z}$ with $a \neq 0$ and $b \geq 1$. Suppose that $(a, b) \to DA \to (q, r)$. Prove that $\gcd(a, b) = \gcd(b, r)$. HINT: Use one of the Unit 0 exercises.
6. Prove the Euclidean algorithm must terminate at some $(a_k, a_{k+1}) \to DA \to (q_k, 0)$. Prove that that when it does, $a_{k+1} = \gcd(a_1, a_2)$. Use it to find $\gcd(234, 123)$ by hand.
7. If we remember the steps of the Euclidean algorithm, we can reverse them, back-substituting repeatedly, to find u, v to satisfy Bézout's Lemma. Apply this to $(a, b) = (234, 123)$, and also to $(a, b) = (200, 123)$.
8. Let $a, b \in \mathbb{Z}$, not both 0. Set $d = \gcd(a, b)$. Prove that $\gcd\left(\frac{a}{d}, \frac{b}{d}\right) = 1$.

For Sep. 11:

9. Let $a, b \in \mathbb{Z}$, not both 0. Prove that every common divisor of a, b divides $\gcd(a, b)$. Hence, gcd is not only the largest, but also a multiple of all common divisors.

10. Let $a, b, t \in \mathbb{Z}$ with a, b not both 0. Prove that $\gcd(a, b) = \gcd(a, b + at)$.

11. Let $a, b \in \mathbb{Z}$, not both 0. Prove that $\gcd(a, b) = 1$, if and only if there is no prime p with $p|a$ and $p|b$.

12. Prove the uniqueness part of the Fundamental Theorem of Arithmetic. That is, suppose $n = p_1 p_2 \cdots p_j = q_1 q_2 \cdots q_k$, two factorizations into positive primes. Then $j = k$, and we can reorder the q's to get $p_1 = q_1, p_2 = q_2, \ldots, p_j = q_j$. HINT: You may want to use results from both the Unit 0 exercises and the Unit 0 exam.

For Sep. 16:

13. Let $a, b, c, n \in \mathbb{Z}$ with $n \geq 1$. Suppose that $a \equiv b \pmod{n}$. Prove that $a + c \equiv b + c \pmod{n}$ and also $ac \equiv bc \pmod{n}$.

14. Let $n \in \mathbb{Z}$ with $n \geq 1$. Prove that equivalence modulo n is reflexive, symmetric, and transitive. That is, prove that $\forall a, b, c \in \mathbb{Z}$, (i) $a \equiv a$; and (ii) if $a \equiv b$ then $b \equiv a$; and (iii) if $a \equiv b$ and $b \equiv c$ then $a \equiv c$.

15. Let $a, n \in \mathbb{Z}$ with $n \geq 1$. Suppose $(a, n) \to DA \to (q, r)$. Prove that $[a] = [r]$.

16. Let $a, b, n \in \mathbb{Z}$ with $n \geq 1$. Prove that $a \equiv c \pmod{n}$, if and only if $[a] = [c]$.

Extra:

17. Let $a, b, c \in \mathbb{Z}$ with a, b not both zero. Suppose $a|bc$ and $\gcd(a, b) = 1$. Prove that $a|c$.

18. Prove or disprove: If $ab \equiv 0 \pmod{15}$, then $a \equiv 0 \pmod{15}$ or $b \equiv 0 \pmod{15}$. Also, prove or disprove: If $ab \equiv 0 \pmod{17}$, then $a \equiv 0 \pmod{17}$ or $b \equiv 0 \pmod{17}$.

19. Let $a, b \in \mathbb{Z}$. Prove that $a|b$ if and only if $a^2|b^2$. HINT: one direction is much easier.

20. Let $a, n \in \mathbb{Z}$ with $n \geq 2$. Suppose that $[a] = [1]$ modulo n. Prove that $\gcd(a, n) = 1$.

21. Let $a, b, n \in \mathbb{Z}$ with $n \geq 1$, and we work modulo n. Prove that either $[a] = [b]$ or $[a] \cap [b] = \emptyset$.

22. Prove the existence part of the Division Algorithm Theorem. That is, prove that for any $a, b \in \mathbb{Z}$ with $b \geq 1$, there must exist some $q, r \in \mathbb{Z}$ with $(a, b) \to DA \to (q, r)$.

23. Prove the existence part of the Positive Fundamental Theorem of Arithmetic. That is, prove that for any $n \in \mathbb{Z}$ with $n \geq 2$, there is at least one factorization of n into positive primes.

24. Prove Bézout's Lemma.