MATH 320 S26, Exam 1 Solutions

1. Find the set of common divisors of $8, 28$, and use this to find $\gcd(8, 28)$.

   Factoring into primes, we have $8 = 2^3$ and $28 = 2^2 7^1$, so the set of common divisors is $\{1, -1, 2, -2, 4, -4\}$. The largest of these is 4, which is therefore the gcd.

2. Find $q, r \in \mathbb{Z}$ so that $(-22, 7) \to DA \to (q, r)$.

   It is true that $-22 = (-3)7 + (-1)$, so $q = -3, r = -1$ does satisfy $a = bq + r$. However, it does NOT satisfy $0 \leq r < b$, so this is not what the division algorithm gives us. Instead we have $-22 = (-4)7 + 6$, so we want $q = -4, r = 6$.

3. Let $a, b \in \mathbb{Z}$, not both zero. Set $d = \gcd(a, b)$. Prove that $\gcd(\frac{a}{d}, \frac{b}{d}) = 1$.

   SOLUTION 1: Set $k = \gcd(\frac{a}{d}, \frac{b}{d})$. We know $k \geq 1$ since 1 is a common divisor of $\frac{a}{d}$ and $\frac{b}{d}$. Assume by way of contradiction that $k > 1$. Since k is a common divisor of $\frac{a}{d}, \frac{b}{d}$, there must be $u, v \in \mathbb{Z}$ such that $ku = \frac{a}{d}$ and $kv = \frac{b}{d}$. Multiplying each by d, we get $kdu = a$ and $kdv = b$. This proves that integer kd is a common divisor of a, b, and $kd > d$ (since $k > 1$ and $d > 0$), a contradiction.

   SOLUTION 2: Apply Bezout's Lemma to get $u, v \in \mathbb{Z}$ satisfying $au + bv = \gcd(a, b) = d$. Divide both sides by d to get $\frac{a}{d}u + \frac{b}{d}v = 1$. By the converse to Bezout's Lemma, $\gcd(\frac{a}{d}, \frac{b}{d}) | 1$. Since the only divisors of 1 are $1, -1$, and $\gcd \geq 1$ (since 1 divides everything), in fact $\gcd(\frac{a}{d}, \frac{b}{d}) = 1$.

4. Use the Euclidean algorithm to find $\gcd(30, 17)$ and also to find $u, v \in \mathbb{Z}$ with $30u + 17v = \gcd(30, 17)$.

   Step 1: $30 = 1 \cdot 17 + 13$
   Step 2: $17 = 1 \cdot 13 + 4$
   Step 3: $13 = 3 \cdot 4 + 1$
   Step 4: $4 = 4 \cdot 1 + 0$.
   Having reached 0, we go to the preceding step to learn that $1 = \gcd(30, 17)$. Now we reverse our steps to find u, v.
   Step 5: $1 = 1 \cdot 13 - 3 \cdot 4$
   Step 6: $1 = 1 \cdot 13 - 3 \cdot (17 - 1 \cdot 13) = 4 \cdot 13 - 3 \cdot 17$
   Step 7: $1 = 4 \cdot (30 - 1 \cdot 17) - 3 \cdot 17 = 4 \cdot 30 - 7 \cdot 17$
   That is, $\gcd(30, 17) = 4 \cdot 30 - 7 \cdot 17$.
   Hence $u = 4, v = -7$.

5. Let $a, b, c \in \mathbb{Z}$, all nonzero. Suppose that $c|a$ and $c|b$. Prove that $c| \gcd(a, b)$.

   Apply Bezout's lemma to get $u, v \in \mathbb{Z}$ with $au + bv = \gcd(a, b)$. Since $c|a$ there is some $s \in \mathbb{Z}$ with $cs = a$. Since $c|b$ there is some $t \in \mathbb{Z}$ with $ct = b$. Substituting in, we get $\gcd(a, b) = (cs)u + (ct)v = c(su + tv)$. Since $su + tv \in \mathbb{Z}$, we have $c| \gcd(a, b)$.

6. Let $a, b, c \in \mathbb{Z}$. Suppose that $a|bc$ and that $\gcd(a, b) = 1$. Prove that $a|c$.

   First, since $a|bc$, there is some $k \in \mathbb{Z}$ with $ak = bc$. Now apply Bezout's lemma to get $u, v \in \mathbb{Z}$ with $au + bv = 1 = \gcd(a, b)$. Multiply both sides by c to get $c = c \cdot 1 = acu + bcv = acu + akv = a(cu + kv)$. Since $cu + kv \in \mathbb{Z}$, we have $a|c$.

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

   Since $a \equiv b \pmod{n}$, we have $n|(a - b)$, and hence there is some $k \in \mathbb{Z}$ with $nk = a - b$. Multiply both sides by c to get $nkc = ac - bc$. Since $kc \in \mathbb{Z}$, we have $n|(ac - bc)$, and so $ac \equiv bc \pmod{n}$.

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

Harder direction: Suppose that $a \equiv b \pmod{n}$. Hence $a \in [b]$. If $c \in [a]$, then $c \equiv a \pmod{n}$. Since $\equiv$ is transitive (by exercise 1.14, or you can prove this as a lemma), then $c \equiv b \pmod{n}$, so $c \in [b]$. This proves that $[a] \subseteq [b]$. But also $\equiv$ is symmetric (by exercise 1.14 again, or you can prove it separately if you wish), $b \equiv a \pmod{n}$. We repeat everything: $b \in [a]$, if $c \in [b]$ then $c \equiv b \pmod{n}$ and by transitivity $c \equiv a$ so $c \in [a]$, hence $[b] \subseteq [a]$.
Easier direction: Suppose that $[a] = [b]$. Since $\equiv$ is reflexive (by exercise 1.14, or you can prove this as a lemma), $a \in [a]$, so $a \in [b]$ and therefore $a \equiv b \pmod{n}$.

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

We begin by applying the preceding exam problem (or exercise 1.16) to conclude that $a \equiv n-1 \pmod{n}$. Hence $n|(a-(n-1))$, and there is some $k \in \mathbb{Z}$ with $nk = a - n + 1$.

SOLUTION 1: Rearranging, we get $1 = nk + n - a = n(k+1) + a(-1)$. Since $k+1, -1 \in \mathbb{Z}$, we apply the converse of Bezout's lemma to conclude that $\gcd(a, n)|1$. The only divisors of 1 are ± 1. (Alternate: by exercise 1.1, this means $\gcd(a, n) = |\gcd(a, n)| \leq |1| = 1$). But also $\gcd(a, n) \geq 1$ since 1 is a common divisor of a, n. Hence $\gcd(a, n) = 1$.

SOLUTION 2: Rearranging, we get $a = nk + (n-1)$. Hence $(a, n) \to DA \to (k, n-1)$. Hence, by exercise 1.7, $\gcd(a, n) = \gcd(n, n-1)$. Next, we have $n = 1(n-1)+1$, so $(n, n-1) \to DA \to (1, 1)$. By exercise 1.7 again, $\gcd(n, n-1) = \gcd(n-1, 1)$. The only divisors of 1 are ± 1, but gcd is always positive, so $\gcd(n-1, 1) = 1$ and so $\gcd(a, n) = \gcd(n, n-1) = \gcd(n-1, 1) = 1$.

10. Let $a, b \in \mathbb{Z}$ with $\gcd(a, b) = 1$. Prove that, for all positive $n \in \mathbb{Z}$, that $\gcd(a, b^n) = 1$.

SOLUTION 1: Proof by induction on n.
Base case ($n = 1$): $\gcd(a, b^1) = \gcd(a, b)$, which is 1 by hypothesis.
Inductive case: Let $n \geq 1$, and suppose that $\gcd(a, b^n) = 1$. Set $d = \gcd(a, b^{n+1})$. Since d is a common divisor of a, b^{n+1}, we have $d|b^{n+1} = b \cdot b^n$.

Lemma: $\gcd(b, d) = 1$
Proof: Set $k = \gcd(b, d)$. Since $k|d$, there is $u \in \mathbb{Z}$ with $ku = d$. Since $d|a$ there is $v \in \mathbb{Z}$ with $dv = a$. Hence $kuv = a$, so $k|a$. But also $k|b$, so $k \leq \gcd(a, b) = 1$.

Now, we apply the lemma and also exam question 6 (or exercise 1.18) to get $d|b^n$. Now d is a common divisor of a and b^n, hence $d \leq \gcd(a, b^n)$, which is 1 by the inductive hypothesis. Also $d \geq 1$ since 1 is a common divisor of a and b^{n+1}. Hence $d = 1$.

SOLUTION 2: We know 1 divides both a, b^n, so $\gcd(a, b^n) \geq 1$. Suppose, by way of contradiction, that $\gcd(a, b^n) > 1$. Since $\gcd(a, b^n)$ is an integer it's at least 2. Then, by the positive fundamental theorem of arithmetic, there is some prime p that divides $\gcd(a, b^n)$. Therefore p is a common divisor of a and b^n. Since $p|b^n = b \cdot b \cdots b$, by exercise 1.4, $p|b$ (it must divide one of the multiplicands, all of which are b). Since also $p|a$, p is a common divisor of a, b. Hence, $\gcd(a, b) \geq p \geq 2$, a contradiction.

SOLUTION 3: If $b \in \{-1, 0, 1\}$, then $b^n = \pm b$, so $\gcd(a, b^n) = \gcd(a, b) = 1$. Otherwise, $|b| \geq 2$, so by the fundamental theorem of arithmetic we may write $b = \pm p_1^{m_1} p_2^{m_2} \cdots p_k^{m_k}$. By exercise 1.12, none of $p_1, p_2, \ldots, p_k$ divide a. Now, $b^n = \pm p_1^{nm_1} p_2^{nm_2} \cdots p_k^{nm_k}$. We know 1 divides both a, b^n, so $\gcd(a, b^n) \geq 1$. Suppose, by way of contradiction, that $\gcd(a, b^n) > 1$. Since $\gcd(a, b^n)$ is an integer it's at least 2. Then, by the positive fundamental theorem of arithmetic, there is some prime p that divides $\gcd(a, b^n)$. Then p must divide b^n, and by the uniqueness part of the fundamental theorem of arithmetic, p must be one of $p_1, p_2, \ldots, p_k$. However, we proved already that none of these divide a, so we have a contradiction.