MATH 521A: Abstract Algebra
Exam 1 Solutions

1. Richard Dedekind, a pioneer of ring theory, was born in 1831 and died in 1916. Use the Euclidean Algorithm to find $\gcd(1831, 1916)$ and to express that gcd as a linear combination of $1831, 1916$.

   We first calculate $1916 = 1 \cdot 1831 + 85$, $1831 = 21 \cdot 85 + 46$, $85 = 1 \cdot 46 + 39$, $46 = 1 \cdot 39 + 7$, $39 = 5 \cdot 7 + 4$, $7 = 1 \cdot 4 + 3$, $4 = 1 \cdot 3 + 1$. Hence the gcd is 1, and $1 = 4 - 3 = 4 - (7 - 4) = 2 \cdot 4 - 7 = 2 \cdot (39 - 5 \cdot 7) - 7 = 2 \cdot 39 - 11 \cdot 7 = 2 \cdot 39 - 11 \cdot (46 - 39) = 13 \cdot 39 - 11 \cdot 46 = 13 \cdot (85 - 46) - 11 \cdot 46 = 13 \cdot 85 - 24 \cdot 46 = 13 \cdot 85 - 24 \cdot (1831 - 21 \cdot 85) = -24 \cdot 1831 + 517 \cdot 85 = -24 \cdot 1831 + 517(1916 - 1831) = 517 \cdot 1916 - 541 \cdot 1831$.

2. Let $a, m, n \in \mathbb{N}$ with $\gcd(m, n) = 1$. Prove that $mx \equiv a \pmod{n}$ has a solution x.

   Because $\gcd(m, n) = 1$, there are integers s, t such that $ms + nt = 1$. Multiplying both sides by a we get $msa + nta = a$, which rearranges as $m(sa) - a = n(-ta)$. We take $x = sa$, and have $mx - a = n(-ta)$. Since $-ta$ is an integer, $n|(mx - a)$. Hence $mx \equiv a \pmod{n}$, as desired.

3. Let $n \in \mathbb{N}$, and suppose that $[a]$ is a nonzero element of $\mathbb{Z}_n$. Prove that $[a]$ is a unit if and only if $[a]$ is *not* a zero divisor.

   There are two directions to prove, and generally the two proofs will require different methods.

   Suppose first that $[a]$ is a unit. Hence there is some $[b] \in \mathbb{Z}_n$ such that $[b] \odot [a] = [1]$. Now suppose, by way of contradiction, that $[a]$ is also a zero divisor. Then there is some nonzero $[c] \in \mathbb{Z}_n$ such that $[a] \odot [c] = [0]$. But now $[c] = [1] \odot [c] = ([b] \odot [a]) \odot [c] = [b] \odot ([a] \odot [c]) = [b] \odot [0] = [0]$, a contradiction. Hence $[a]$ is not a zero divisor.

   Suppose now that $[a]$ is not a unit. Set $d = \gcd(a, n)$. We may write $a = da', n = dn'$. By Theorem 2.10, we know that $d > 1$, and hence $1 < n' < n$ and in particular $[n'] \neq [0]$. We have $[a] \odot [n'] = [da'] \odot [n'] = [da'n'] = [a'n] = [0]$, hence $[a]$ is a zero divisor.

4. Let p be a positive prime. Use the Fundamental Theorem of Arithmetic to prove that there do not exist $a, b \in \mathbb{N}$ with $a^2 = pb^2$.

   By considering all the primes that divide either a, b, or p, we write $a = p^{s_0} p_1^{s_1} \cdots p_k^{s_k}$, $b = p^{t_0} p_1^{t_1} \cdots p_k^{t_k}$, $p = p^1 p_1^0 \cdots p_k^0$. Suppose by way of contradiction that $a^2 = pb^2$. Then we have $p^{2s_0} p_1^{2s_1} \cdots p_k^{2s_k} = (p^1)(p^{2t_0} p_1^{2t_1} \cdots p_k^{2t_k})$. By the FTA, these are unique up to order and units. In particular, looking at the power of p, on the left we have $2s_0$ and on the right we have $1 + 2t_0$. These cannot be equal, since the former is even and the latter is odd. This contradiction proves the desired result.

5. Working in $\mathbb{Z}_{21}$, find the multiplicative inverse of $[8]$, and use this to solve the modular equation $[8] \odot [x] = [13]$.

   There are twelve units in $\mathbb{Z}_{21}$, so we just try them all to see which multiplies by $[8]$ to give $[1]$.
   ALTERNATIVE: Use Euclidean Algorithm to find s, t with $8s + 21t = 1$. Then $[s] = [8]^{-1}$.
   It turns out that $[8]^{-1} = [8]$. Hence we compute $[8] \cdot [8] \cdot [x] = [8] \cdot [13]$, so $[x] = [8] \cdot [13] = [20]$.

6. Working in $\mathbb{Z}_n$, prove that the following holds for all a, b, c, d:

   $$([a] \oplus [b]) \odot ([c] \oplus [d]) = ([a] \odot [c]) \oplus ([a] \odot [d]) \oplus ([b] \odot [c]) \oplus ([b] \odot [d])$$

   For convenience, set $[e] = [c] \oplus [d]$, and apply the distributive property to get

   $$([a] \oplus [b]) \odot [e] = ([a] \odot [e]) \oplus ([b] \odot [e]) \quad (1)$$

   We now apply the distributive property two more times, to get

   $$[a] \odot [e] = ([a] \odot [c]) \oplus ([a] \odot [d]) \quad (2)$$

   $$[b] \odot [e] = ([b] \odot [c]) \oplus ([b] \odot [d]) \quad (3)$$

   Now we plug (2) and (3) into (1) to get the desired result.