MATH 521A: Abstract Algebra
Homework 1 Solutions

1. Set $S = \{-1\} \cup \mathbb{N}_0 = \{-1, 0, 1, 2, 3, \ldots\}$. Prove that S is well-ordered.

   We prove that the usual order $<$ on S is a well-order. Let $T \subseteq S$. If $-1 \notin T$, then $T \subseteq \mathbb{N}_0$, and hence T has a minimal element since $\mathbb{N}_0$ is a well-order. If instead $-1 \in T$, then -1 is a minimal element of T, since $-1 < n$ for all $n \in T \subseteq \mathbb{N}_0$.

2. Suppose that $S = \{s_1, s_2, \ldots, s_k\}$ is a finite set. Prove that S is well-ordered.

   We define the "order of indices" as $s_i \prec s_j$ if $i < j$. For $T \subseteq S$, the indices of T fall into $\{1, 2, \ldots, k\} \subseteq \mathbb{N}$. Since $\mathbb{N}$ is well-ordered, there is some minimal index, and hence some minimal element of T under $\prec$. Note: this same method proves that every countable set is well-ordered.

3. Suppose that S and T are both well-ordered, and that $S \cap T = \emptyset$ (i.e. S, T are disjoint). Prove that $S \cup T$ is well-ordered.

   We define a total order $\prec$, as follows. Let $a, b \in S \cup T$. If $a, b \in S$, then $a \prec b$ if $a <_S b$, i.e. we keep the order in S, for elements from S. Similarly, if $a, b \in T$, then $a \prec b$ if $a <_T b$. However, if $a \in S$ and $b \in T$, we say that $a \prec b$; that is, every element of S is less than every element of T. Now, let $R \subseteq (S \cup T)$. Set $R' = R \cap S$. If R' is empty, then $R \subseteq T$. Hence, R has a minimal element in $\prec$ (since T is well-ordered by $<_T$, which coincides with $\prec$ on R). If instead R' is nonempty, then R' has a minimal element in $\prec$ (since $R' \subseteq S$, and S is well-ordered by $<_S$, which coincides with $\prec$ on R'), and this is the minimal element for all of R, since all other elements of R are in S, and hence larger in $\prec$.

4. Use the division algorithm to prove that every integer is either even or odd.

   Let $n \in \mathbb{Z}$, and we apply the division algorithm with $n, 2$ to get $q, r \in \mathbb{Z}$ with $n = 2q + r$, where $0 \leq r < 2$. If $r = 0$, then n is even. If $r = 1$, then n is odd. There are no other options for r.

5. Use the division algorithm to prove that the square of any integer a is of the form $5k$, of the form $5k + 1$, or of the form $5k + 4$, for some integer k.

   We apply the division algorithm with $a, 5$ to get $q, r \in \mathbb{Z}$ with $a = 5q + r$ and $0 \leq r < 5$. We now have $a^2 = (5q + r)^2 = 25q^2 + 10qr + r^2 = 5s + r^2$, where $s = 5q^2 + 2qr \in \mathbb{Z}$. If $r = 0, 1, 2$ then $r^2 = 0, 1, 4$ and we are done. If instead $r = 3$, then $r^2 = 9$ so $a^2 = 5s + 9 = 5(s + 1) + 4$. Finally, if $r = 4$, then $r^2 = 16$ so $a^2 = 5s + 16 = 5(s + 3) + 1$.

6. Prove the following variant of the division algorithm: Let a, b be integers with $b > 0$. Then there exist integers q, r such that $a = bq + r$ with $0 < r \leq b$.

   We closely mimic the proof in the textbook, with a few subtle changes. Define S to be the set of all integers $a - bx$, where $x \in \mathbb{Z}$ and $a - bx > 0$. Step 1: We prove $S \neq \emptyset$. We take $x = -|a| - 1$, and calculate $a - bx = a + b|a| + b \geq b > 0$. (using $a + b|a| \geq 0$) Hence $a - bx \in S$. Step 2: Let r be minimal in S, since $\mathbb{N}_0$ is well-ordered. Since

$r \in S$, $r > 0$. Set $q \in \mathbb{Z}$ such that $r = a - bq$. Step 3: We prove that $r \le b$. We argue by contradiction; if instead $r > b$, then $r - b = a - b(q+1)$ would be a smaller element of S, which is impossible. Step 4: Uniqueness was not asked for in this problem.

7. Suppose that a, b, c are integers, with $a|b$ and $b|c$. Prove that $a|c$.

   Since $a|b$, there is some $m \in \mathbb{Z}$ with $b = ma$. Since $b|c$, there is some $n \in \mathbb{Z}$ with $c = bn$. Combining, we get $c = bn = (ma)n = (mn)a$, so $a|c$.

8. Determine $\gcd(n, n+2)$ for all integers n.

   Note that $\gcd(n, n+2) = \gcd(n, n+2-n) = \gcd(n, 2)$. But this last is confined to the positive divisors of 2, which are just $1, 2$. If n is even, then $n+2$ is also even, so $\gcd(n, n+2) = 2$. If instead n is odd, then 2 is not a divisor of n, so $\gcd(n, n+2)$ must be 1.

   Let $a, b \in \mathbb{Z}$ with $b \neq 0$. Set $CD(a, b) = \{c \in \mathbb{Z} : c|a \text{ and } c|b\}$, the set of common divisors. Set $PLC(a, b) = \{e \in \mathbb{N} : \exists m, n \in \mathbb{Z}, e = am + bn\}$, the set of positive linear combinations.

9. Prove that $\gcd(a, b)$ is the largest element in $CD(a, b)$, and that each element of $CD(a, b)$ divides $\gcd(a, b)$.

   The first statement is the definition of *greatest* common divisor. Set $d = \gcd(a, b)$, for convenience. Suppose now that $c \in CD(a, b)$. There must be $x, y \in \mathbb{Z}$ with $a = cx$ and $b = cy$. By Theorem 1.2, there are integers u, v with $d = au + bv$. Substituting, we get $d = (cx)u + (cy)v = c(xu + yv)$. Since $xu + yv \in \mathbb{Z}$, in fact $c|d$.

10. Prove that $\gcd(a, b)$ is the smallest element in $PLC(a, b)$, and that $\gcd(a, b)$ divides each element of $PLC(a, b)$.

    The first statement is Theorem 1.2. Set $d = \gcd(a, b)$, for convenience. Suppose now that $e \in PLC(a, b)$, with $d \nmid e$. We apply the division algorithm to e, d to get $q, r \in \mathbb{Z}$ with $e = qd + r$ and $0 \le r < d$. Since $d \nmid e$, in fact $0 < r < d$. Now, since $d, e \in PLC(a, b)$, there are m, m', n, n' with $d = am + bn$ and $e = am' + bn'$. Multiply the first equation by q to get $qd = aqm + bqn$. Subtracting, we have $r = e - qd = (am' + bn') - (aqm + bqn) = a(m' - qm) + b(n' - qn)$. Hence in fact $r \in PLC(a, b)$, and $r < d$, which contradicts Theorem 1.2.