MATH 521A: Abstract Algebra
Homework 1 Solutions

1. Prove that $(-\mathbb{N}_0)$, the set of nonpositive integers, is well-ordered.

   Method 1: We know that $\mathbb{Z}$ is well-ordered by $\leqslant$, by a theorem from class. Since $(-\mathbb{N}_0) \subseteq \mathbb{Z}$, we apply the lemma from class and conclude that $(-\mathbb{N}_0)$ is also well-ordered by $\leqslant$.

   Method 2: We define a "backwards" order via: $a \lessdot b$ if $|a| < |b|$ (i.e. $a > b$). Let $S \subseteq (-\mathbb{N}_0)$. The image of S under the absolute value map is in $\mathbb{N}_0$, which is well-ordered. Hence there is some element t in that image that is minimal. But then $|t| < |x|$ for all $x \in S$, i.e. $t \lessdot x$. So t is minimal and $(-\mathbb{N}_0)$ is well-ordered by $\lessdot$.

   For a set T, we say it is *inductively ordered* if there is some special $t \in T$ and some function $f : T \to T$ such that:
   (1) The elements $t, f(t), f(f(t)), \ldots$ are all distinct; and
   (2) $T = \{t, f(t), f(f(t)), \ldots\}$.

2. Prove that $\mathbb{N}_0$ is inductively ordered.

   We take $t = 0$ and $S(x) = x + 1$. Then $\{t, f(t), f(f(t)), \ldots\} = \{0, 1, 2, \ldots\} = \mathbb{N}_0$.

3. Prove that if a set is inductively ordered then it is well-ordered.

   Each element of T is $f^{(n)}(t)$, for some $n \in \mathbb{N}_0$. We define an order on T by comparing "exponents", i.e. via $f^{(n)}(t) \lessdot f^{(m)}(t)$ if $n < m$. For $S \subseteq T$, the exponents of the elements of S are a subset of $\mathbb{N}_0$, and hence have a minimal element $n^\star$. Now for any $s \in S$, either $s = f^{(n^\star)}(t)$ or $f^{(n^\star)}(t) \lessdot s$, so $f^{(n^\star)}(t)$ is minimal in S. Thus T is well-ordered by $\lessdot$.

4. Prove that the square of any integer a is either of the form $4k$ or of the form $4k+1$ for some integer k.

   Let $a \in \mathbb{Z}$. By the division algorithm, there are integers q, r such that $a = 4q + r$, with $0 \le r < 4$. Squaring, we get $a^2 = (4q + r)^2 = 16q^2 + 8qr + r^2 = 4(4q^2 + 2qr) + r^2$. If $r = 0$ or $r = 1$, we are done. If $r = 2$ then $a^2 = 4(4q^2 + 2qr + 1) + 0$, and if $r = 3$ then $a^2 = 4(4q^2 + 2qr) + 9 = 4(4q^2 + 2qr + 2) + 1$.

5. Prove the *Backwards Division Algorithm*: Let a, b be integers with $b > 0$. Then there exist integers q, r such that $a = bq + r$ with $-b < r \le 0$.

   We mimic the proof of Thm 1.1. Set $S = \{a - bx : x \in \mathbb{Z}, a - bx \ge 1\}$. In Thm 1.1 it was proved that there is some $x \in \mathbb{Z}$ such that $a - bx \ge 0$. Adding b to both sides $a - bx + b \ge b \ge 1$, so S is nonempty since it contains $a - b(x-1)$. Apply Well-Ordering Axiom to get minimal $r' \in S$. We have, for some integer q', $r' = a - bq' \ge 1$. We subtract b from both sides to get $r' - b = a - b(q' + 1) \ge 1 - b$. Set $r = r' - b$ and $q = q' + 1$. We have $r = a - bq$, or $a = bq + r$. If $r > 0$ then $r' > b$ so in fact r' was not minimal in S since $r' - b \in S$. Hence $-b < r \le 0$. We were not asked to prove uniqueness, but it can be done similarly to the proof of Thm 1.1.

6. Let $a, b \in \mathbb{N}$ with $a|b$. Prove that $a \leq b$.

Method 1: We use $x \geq y$ if $x - y \geq 0$. There is some $c \in \mathbb{N}$ with $b = ac$. Hence $b - a = ac - a = a(c-1)$. Since $a, c-1$ are each in $\mathbb{N}_0$, their product is in $\mathbb{N}_0$ and so $b \geq a$.

Method 2: We use $x \geq y$ if $\frac{x}{y} \geq 1$. There is some $c \in \mathbb{N}$ with $b = ac$. Hence $\frac{b}{a} = c \in \mathbb{N}$. Hence $\frac{b}{a} \geq 1$, so $b \geq a$.

7. Let a, b be nonzero integers with $a|b$ and $b|a$. Prove that $a = \pm b$.

Since $a|b$ there is some integer c with $b = ca$. Since $b|a$ there is some integer f with $a = fb$. Substituting, we get $b = c(fb)$ and so $1 = cf$. Suppose for the moment that c, f are both positive. We have $c|1$, so by exercise 6, $c \leq 1$. Thus $c = 1 = f$. If c, f are not both positive, they are both negative. However $|c| \cdot |f| = 1$ so again $|c|$ is a natural number dividing 1, and thus $|c| = 1$, so $c = -1 = f$. Hence $c = \pm 1$ and so $b = \pm a$.

8. Let $a, b \in \mathbb{Z}$, not both zero, and let $d = \gcd(a, b)$. Prove that d divides each element of $S = \{am + bn : m, n \in \mathbb{Z}\}$.

We have $a = da', b = db'$ for some integers a', b'. We have $am + bn = da'm + db'n = d(a'm + b'n)$, so $d|(am + bn)$.

9. Use the Euclidean Algorithm to find $\gcd(175, 630)$ and to express this as a linear combination of $175, 630$.

Step 1: $630 = 3 \cdot 175 + 105$. Step 2: $175 = 1 \cdot 105 + 70$. Step 3: $105 = 1 \cdot 70 + 35$
Since $35|70$ we know 35 is the gcd. Now we reverse, back-substituting as we go.
$35 = 1 \cdot 105 - 1 \cdot 70 = 1 \cdot 105 - 1 \cdot (1 \cdot 175 - 1 \cdot 105) = 2 \cdot 105 - 1 \cdot 175 = 2 \cdot (630 - 3 \cdot 175) - 1 \cdot 175 = 2 \cdot 630 - 7 \cdot 175$.

10. Prove that $\gcd(a, b) = \gcd(a, b + at)$, for every $t \in \mathbb{Z}$.

Method 1: Fix t and for convenience, set $d = \gcd(a, b), c = \gcd(a, b + at)$. Since $d|a$ and $d|b$, there are integers a', b' with $a = da', b = db'$. So $b + at = db' + da't = d(b' + a't)$, so $d|(b + at)$ and hence $d|c$ by Cor. 1.3. Similarly, there are a'', f such that $a = a''c, b + at = fc$. Hence $(b + at) - at = fc - a''ct = c(f - a''t)$. Hence $c|b$ and so $c|d$. By exercise 7, $c = \pm d$, so $c = d$ since gcd's are always positive.

Method 2: We have $\gcd(a, b)$ dividing a, and also (by Exercise 8) $\gcd(a, b + at)$, since $b + at$ is a linear combination of a, b. But we can do this the other way, since $a = (-t)a + 1(b + at)$, so $\gcd(a, b + at)$ divides both a and b, so $\gcd(a, b + at)$ divides $\gcd(a, b)$. Now apply exercise 7 as in method 1.