Objective: The goal of this worksheet is to gain familiarity with properties of divisibility and see how and when induction can be helpful in proving statements about divisibility.

1. Show that every integer falls into one of the following categories:

   (a) Even: $n = 2j$ for some $j \in \mathbb{Z}$

   (b) Threven: $n = 3k$ for some $k \in \mathbb{Z}$

   (c) Plus one: $n = 6r + 1$ for some $r \in \mathbb{Z}$

   (d) Plus five: $n = 6s + 5$ for some $s \in \mathbb{Z}$

   Are these categories disjoint?

   Let $n \in \mathbb{Z}$ and write $n = 6q + r$ where $0 \leqslant r < 6$. We consider the possibilities for r:
   Case 1: $r = 0$.

   In this case, $n = 6q = 2 \cdot (3q)$, so n is even. Note also that $n = 3 \cdot (2q)$, so n is also threven. In particular, these two categories are not disjoint.

   Case 2: $r = 1$

   In this case, $n = 6q + 1$, so n is of the "plus one" form.

   Case 3: $r = 2$
   In this case, $n = 6q + 2 = 2(3q + 1)$, so n is even.

   Case 4: $r = 3$
   In this case, $n = 6q + 3 = 3(2q + 1)$, so n is threven.

   Case 5: $r = 4$

   In this case, $n = 6q + 4 = 2(3q + 2)$, so n is even.

   Case 6: $r = 5$
   In this case, $n = 6q + 5$, so n is of the "plus five" form.

   This covers all possible values for r, so every n is either even, threven, plus one, or plus five. Checking that the categories are disjoint except for even and threven is tedious, so we present the hardest proof here and leave the rest to the reader.

   Claim: No integer n is both "plus one" and "plus five."

   Proof: By contradiction, suppose $n = 6r+1 = 6s+5$ for integers r and s. Then $6(r-s) = 4$. However, 4 is not a multiple of 6, so this is a contradiction. Hence, no integer is both "plus one" and "plus five."

2. Show that for all $n \in \mathbb{Z}$, $6 \mid n(n+1)(2n+1)$

   Note that either n or $n+1$ is divisible by 2, so $n(n+1)(2n+1)$ must be divisible by 2.

   We next argue that $n(n+1)(2n+1)$ is divisible by 3. Write $n = 3q + r$ for $0 \leqslant r < 3$ and consider the possibilities for r:

   Case 1: $r = 0$

   In this case, $n = 3q$, so $n(n+1)(2n+1) = 3q(3q+1)(6q+1)$, which is a multiple of 3.

   Case 2: $r = 1$

   In this case, $n = 3q+1$, so $n(n+1)(2n+1) = (3q+1)(3q+2)(6q+3) = 3(3q+1)(3q+2)(2q+1)$, which is a multiple of 3.

   Case 3: $r = 2$

   In this case, $n = 3q+2$, so $n(n+1)(2n+1) = (3q+2)(3q+3)(6q+5) = 3(3q+2)(q+1)(6q+5)$, which is again a multiple of 3.

   In all cases, $n(n+1)(2n+1)$ is a multiple of 3.

   Since $n(n+1)(2n+1)$ is a multiple of both 2 and 3 (and since 2 and 3 are distinct primes), $n(n+1)(2n+1)$ must be a multiple of 6.

   Question: How are we relying on the fact that 2 and 3 are distinct primes? Can you find integers a, b, and c with $a \mid c$, $b \mid c$, but $ab \nmid c$?

3. Show that the product of two integers of the form $4k+1$ is again of this form. Show that the product of two integers of the form $4k+3$ is of the form $4k+1$

   Note that
   $$(4k+1)(4n+1) = 16kn + 4k + 4n + 1 = 4(4kn + k + n) + 1$$
   Hence, the product of two integers which are each one more than a multiple of four is again one more than a multiple of four.

   Note that
   $$(4k+3)(4n+3) = 16kn + 12k + 12n + 9 = 4(4kn + 3k + 3n + 2) + 1$$
   Hence, the product of two integers which are each three more than a multiple of four is one more than a multiple of four.

4. The nth Fibonacci number is defined as follows:

$$F_0 = 0 \qquad F_1 = 1 \qquad F_n = F_{n-1} + F_{n-2}$$

(a) Compute the first 6 Fibonacci numbers.

n	0	1	2	3	4	5
F_n	0	1	1	2	3	5

(b) Show that F_n is even if and only if $3 \mid n$

We prove this by strong induction on n. Note that F_0 is even and $3 \mid 0$. F_1 and F_2 are both odd and $3 \nmid 1$ and $3 \nmid 2$, so the claim holds for $n = 0, 1, 2$.

Suppose that F_k is even if and only if $3 \mid k$ for all $k < n$. We aim to show that F_n is even if and only if $3 \mid n$.

Suppose that $3 \nmid n$. Then exactly one of $n - 1$ or $n - 2$ is a multiple of 3. Since $n - 1$ and $n - 2$ are both less than n, we can apply the induction hypothesis to conclude that exactly one of F_{n-1} and F_{n-2} is even and exactly one is odd. But then $F_n = F_{n-1} + F_{n-2}$ must be odd.

Now suppose that $3 \mid n$. Then $F_n = F_{n-1} + F_{n-2}$ and we can again apply the induction hypothesis to F_{n-1} and F_{n-2}. Since neither $n - 1$ nor $n - 2$ is a multiple of 3, we find that both F_{n-1} and F_{n-2} are odd, so F_n must be even.

Therefore $3 \mid n$ if and only if n is even.

By induction, the claim holds for all n.

5. Compute $(29, 11), (100, 7)$, and $(-356, 16)$

Let D_n denote the set of divisors for n. Then we have

$$
\begin{aligned}
D_{29} &= \{\pm 1, \pm 29\} \\
D_{11} &= \{\pm 1, \pm 11\} \\
D_{100} &= \{\pm 1, \pm 2, \pm 5, \pm 10, \pm 20, \pm 50, \pm 100\} \\
D_{7} &= \{\pm 1, \pm 7\} \\
D_{-356} &= \{\pm 1, \pm 2, \pm 4, \pm 89, \pm 178, \pm 356\} \\
D_{16} &= \{\pm 1, \pm 2, \pm 4, \pm 8, \pm 16\}
\end{aligned}
$$

We can see that the only common divisors of 29 and 11 are ± 1, so $1 = (29, 11)$.

We can see that the only common divisors of 7 and 100 are ± 1, so $1 = (100, 7)$.

Finally, the common divisors of 16 and -356 are ± 1, ± 2, and ± 4, so $4 = (-356, 16)$.

6. For $a, b \in \mathbb{Z}$, what are $(a, 0)$, $(a, 1)$, (a, a), and (a, ab)?

Every integer divides 0, so the common divisors of a and 0 are exactly the divisors of a. Hence, the greatest common divisor of a and 0 is the greatest divisor of a, which is $|a|$. So $(a, 0) = |a|$.

The only divisors of 1 are ± 1. Since ± 1 both divide every integer, the common divisors of a and 1 are ± 1 and the greatest common divisor must be 1. Thus, $(a, 1) = a$.

The common divisors of a and a are merely the divisors of a. Hence, the greatest common divisor of a and itself is $|a|$, i.e. $(a, a) = |a|$.

Every divisor of a is also a divisor of ab. Hence, the common divisors of a and ab are the divisors of a, the largest of which is $|a|$. Consequently, $(a, ab) = |a|$.

7. Suppose that $a, b \in \mathbb{Z}$ and $(a, b) = 1$. Show that $(a+b, a-b) = 1$ or 2. When is this GCD 1? When is it 2?

   Suppose that $d \mid a+b$ and $d \mid a-b$. Then d divides every linear combination of $a+b$ and $a-b$. In particular, $d \mid (a+b)+(a-b) = 2a$ and $d \mid (a+b)-(a-b) = -2b$. Since a and b share no common factors, we conclude that $d \mid 2$, so $d = 1$ or $d = 2$.

   If $(a+b, a-b) = 2$, then $a+b$ and $a-b$ must both be even, i.e. either a and b are both even or a and b are both odd. The converse is also true, so $(a+b, a-b) = 2$ if and only if a and b are both even or both odd.