Objective: The goal of this worksheet is to help you become more comfortable working with prime numbers and greatest common divisors.

1. Show that if $k \in \mathbb{Z}_{>0}$, then $3k+2$ and $5k+3$ are relatively prime.

   Let $d = (3k+2, 5k+3)$. Note that $5(3k+2) - 3(5k+3) = 1$. Since d divides every linear combination of $3k+2$ and $5k+3$, $d \mid 1$. Since d is positive, we find that $d = 1$ and hence, $3k+2$ and $5k+3$ are relatively prime.

2. Show that if $n \in \mathbb{Z}_{>0}$, then $(n+1, n^2-n+1) = 1$ or 3

   Repeatedly applying the fact that $(a, b) = (a + kb, b)$, we find that

$$\begin{aligned}(n+1, n^2-n+1) &= (n+1, n^2-n+1-n(n+1)) \\ &= (n+1, -2n+1) \\ &= (n+1, -2n+1+2(n+1)) \\ &= (n+1, 3)\end{aligned}$$

   Hence if $d = (n+1, n^2-n+1)$, then $d \mid 3$. Since d is positive, d must be 1 or 3.

3. We say that integers $a_1, \ldots, a_n$ are mutually relatively prime if $(a_1, \ldots, a_n) = 1$. The integers are pairwise relatively prime if $(a_i, a_j) = 1$ when $i \neq j$.

   (a) Can you find four integers which are mutually relatively prime so that any three of them are not mutually relatively prime?

   Yes! Consider the integers $2 \cdot 3 \cdot 5, 2 \cdot 3 \cdot 7, 2 \cdot 5 \cdot 7, 3 \cdot 5 \cdot 7$. These four integers are mutually relatively prime because there is no prime p which divides all four integers. However, if you pick any three of the integers, you will find that those three share a common prime factor, and hence are not mutually relatively prime.

   (b) Can you find four integers which are pairwise relatively prime so that any three of them are not mutually relatively prime?

   No! Say a, b, and c are not mutually relatively prime. Then a, b, and c share a common prime factor, p. In particular, $p \mid (a, b)$, so no matter which d you choose, a, b, c, and d can't be pairwise relatively prime.

4. Write $(630, 156)$ as a linear combination of 630 and 156 in two different ways.

   We first find a way to write 630 and 156 as a linear combination of 630 and 156 using the Extended Euclidean Algorithm. Set $s_0 = 1$, $s_1 = 0$, $t_0 = 0$, $t_1 = 1$, and

   $$s_j = s_{j-2} - q_{j-1}s_{j-1} \qquad t_j = t_{j-2} - q_{j-1}t_{j-1}$$

   Then we have

   $$630 = 4 \cdot 156 + 6 \qquad s_2 = 1 - 4 \cdot 0 \qquad t_2 = 0 - 4 \cdot 1$$
   $$156 = 26 \cdot 6$$

   and so $6 = 1 \cdot 630 + (-4) \cdot 156$. Note that if we add $\frac{156}{(630,156)} = 26$ to 1 and if we subtract $\frac{630}{(630,156)} = 105$ from -4, the added and subtracted terms cancel out and we are left with $6 = 27 \cdot 630 + (-109) \cdot 156$

5. Suppose that n is a positive integer and let p be the smallest prime factor of n. Show that if $p > n^{1/3}$, then $\frac{n}{p}$ is either prime or equal to 1.

   Since $p > n^{1/3}$, we conclude that $\frac{n}{p} < \frac{n}{n^{1/3}} = n^{2/3}$.

   If $\frac{n}{p}$ were composite, then it would have to have a prime factor $\leqslant \sqrt{\frac{n}{p}} < \sqrt{n^{2/3}} = n^{1/3} < p$. But $\frac{n}{p}$ can't have a prime factor less than p because p is the smallest prime factor of n. Hence, $\frac{n}{p}$ is not composite so it is either prime or 1.

6. Suppose that p is prime. Show that if $p \mid ab$, then $p \mid a$ or $p \mid b$.

   We prove the contrapositive. Suppose that $p \nmid a$ and $p \nmid b$. Then we can write $a = pq_a + r_a$ and $b = pq_b + r_b$ where $0 < r_a, r_b < p$ (we can assume that both remainders are nonzero because neither a nor b is a multiple of p). Note now that

   $$ab = (pq_a + r_a)(pq_b + r_b) = p^2 q_a q_b + pr_a + pr_b + r_a r_b = p(pq_a q_b + r_a + r_b) + r_a r_b$$

   Now $r_a r_b$ is not a multiple of p because $0 < r_a, r_b < p$. Hence, $p(pq_a q_b + r_a + r_b) + r_a r_b$ is not a multiple of p, so ab is not a multiple of p.