1. *Suppose that m is a positive integer and that k is relatively prime to $\varphi(m)$. Suppose also that m has a primitive root. Use Theorem 9.17 (or other methods) to show that the function*

$$f : \left(\mathbb{Z}\big/m\mathbb{Z}\right)^{\times} \to \left(\mathbb{Z}\big/m\mathbb{Z}\right)^{\times}$$
$$x \mapsto x^k$$

is injective.

Approach 1

Suppose $x, y \in (\mathbb{Z}/m\mathbb{Z})^{\times}$ and that $f(x) \equiv f(y) \mod m$. Then $x^k \equiv y^k \mod m$. Set $a = y^k$ and consider the equation $X^k \equiv a \mod m$. There is a solution to this equation since $X = y$ satisfies $X^k \equiv a \mod m$. Since m has a primitive root, theorem 9.17 applies to yield that there are exactly $(k, \varphi(m)) = 1$ incongruent solutions modulo m. Since x and y are both solutions, yet there is only one distinct solution modulo m, x and y must not be distinct. Hence, $x \equiv y \mod m$ and so f is injective.

Approach 2

Suppose $x, y \in (\mathbb{Z}/m\mathbb{Z})^{\times}$ and that $f(x) \equiv f(y) \mod m$. Then $x^k \equiv y^k \mod m$. Since m has a primitive root (say r) we can take indices on both sides to find that $k\,\mathrm{ind}_r(x) \equiv k\,\mathrm{ind}_r(y) \mod \varphi(m)$. Since k is relatively prime to the modulus $\varphi(m)$, we can divide both sides by k to find that $\mathrm{ind}_r(x) \equiv \mathrm{ind}_r(y) \mod \varphi(m)$. By problem 2 on Homework 6, however, this implies that $x \equiv y \mod m$. Therefore, f is injective.

2. *Suppose that k and n are positive integers. In this problem, you will show that the set*

$$S = \{0, 1^k, 2^k, 3^k, \dots, (n-1)^k\}$$

forms a complete set of residues modulo n if n is square-free and $(k, \lambda(n)) = 1$. The converse is true too, but I won't make you show that here.

(a) *Show that the only element of S which is congruent to 0 modulo n is 0.*

Suppose by contradiction that $x^k \equiv 0 \mod n$ for some $1 \leqslant x \leqslant n-1$. Then $n \mid x^k$ so every prime factor of n is also a prime factor of x. However, n is square-free so it must be the case that $n \mid x$. But this contradicts the fact that $1 \leqslant x \leqslant n-1$. Hence, we cannot have $x^k \equiv 0 \mod n$ for some $1 \leqslant x \leqslant n-1$.

(b) *Suppose $1 \leqslant x, y \leqslant n-1$ and p is a prime factor of n. Show that if $x^k \equiv y^k \mod n$, then $x \equiv y \mod p$.*

Since $p \mid n$, we have $x^k \equiv y^k \mod p$. We consider two cases.

<u>Case 1</u>: $p \mid x$

In this case, we have $0 \equiv x^k \equiv y^k \mod p$, so $p \mid y^k$. But then $p \mid y$ so $x \equiv 0 \equiv y \mod p$.

<u>Case 2</u>: $p \nmid x$

In this case, we cannot have $p \mid y$ either, else we will have $p \mid x$ as in case 1. Since k is relatively prime to $\lambda(n)$ which is a multiple of $\lambda(p) = \varphi(p)$, k is relatively prime to $\varphi(p)$. Moreover, p (being prime) has a primitive root. Hence, by problem 1, the fact that $x^k \equiv y^k \mod p$ implies that we must have $x \equiv y \mod p$.

(c) *Conclude that S forms a complete set of residues modulo n.*

Since $|S| = n$, it suffices to show that the elements of S are distinct modulo n. By part (a), no nonzero elements are congruent to 0 modulo n. By part (b), if two nonzero elements of S (say, x^k and y^k) are congruent modulo n, then $x \equiv y \mod p$ for every prime factor of n. Applying Sun-Tsu's theorem together with the fact that n is square-free yields that if $x^k \equiv y^k \mod n$, then $x \equiv y \mod n$. Hence, the elements of S are distinct modulo n and so S constitutes a complete set of residues modulo n.

3. (a) *Suppose $f(x_1, \ldots, x_n)$ is a polynomial with integer coefficients. Show that if there exist integers $(k_1, \ldots, k_n)$ so that $f(k_1, \ldots, k_n) = 0$, then there exists a solution to $f(x_1, \ldots, x_n) \equiv 0 \mod m$ for every positive integer m. What is the contrapositive of this statement?*

If $f(k_1, \ldots, k_n) = 0$, then for any positive integer m, $f(k_1, \ldots, k_n) \equiv 0 \mod m$, so there exists a solution to $f(x_1, \ldots, x_n) \equiv 0 \mod m$.

The contrapositive of this statement is that if there exists an m for which $f(x_1, \ldots, x_n) \equiv 0 \mod m$ has no solutions, then there do not exist integers $k_1, \ldots, k_n$ so that $f(x_1, \ldots, x_n) = 0$.

(b) *Show that there are no solutions in integers to $x^2 + y^2 = 3z^2$*

Suppose by contradiction that there exist integers p, q, r so that $p^2 + q^2 = 3r^2$. Then if $d = \gcd(p, q, r)$ and we write $p = dp'$, $q = dq'$, and $r = dr'$, we have $1 = \gcd(p', q', r')$ and

$$(dp')^2 + (dq')^2 = 3(dr')^2$$

implying that $(p')^2 + (q')^2 = 3(r')^2$. Looking at this equation mod 3, we find that $(p')^2 + (q')^2 \equiv 0 \mod 3$. Since the squares mod 3 are either 0 or 1, the only way that $(p')^2 + (q')^2 \equiv 0 \mod 3$ is if $p' \equiv q' \equiv 0 \mod 3$.

Now that we see that p' and q' are divisible by 3, we see that $(p')^2 + (q')^2 = 3(r')^2$ is divisible by 9. Hence, $(r')^2$ is divisible by 3, implying that r' is divisible by 3. But this contradicts the hypothesis that $1 = \gcd(p', q', r')$.

Therefore, there are no integer solutions to $x^2 + y^2 = 3z^2$.

4. *Classify all right triangles whose sides have integer lengths and whose area equals its perimeter.*

Consider a right triangle with side lengths a, b, and c so that $a^2 + b^2 = c^2$ and suppose that the area of this triangle equals its perimeter. By the classification of Pythagorean triples, we know that there exist positive integers $m > n$ so that $a = m^2 - n^2$, $b = 2mn$, and $c = m^2 + n^2$. Additionally, the fact that the area of the triangle equals the perimeter indicates that

$$\frac{ab}{2} = a + b + c$$

Replacing a, b, c with their expressions in terms of m and n yields that

$$\frac{(m^2 - n^2)(2mn)}{2} = m^2 - n^2 + 2mn + m^2 + n^2$$

and some arithmetic simplification yields

$$mn(m + n)(m - n) = 2m(m + n)$$

Dividing both sides by the nonzero quantities m and $m + n$ indicates that $n(m - n) = 2$. Since 2 can only be written as a product of positive integers in one way, we must have one of the following cases:

$$n = 1, m - n = 2 \qquad \text{OR} \qquad n = 2, m - n = 1$$

The former case yields $n = 1, m = 3$ (and so $a = 8$, $b = 6$, and $c = 10$) and the latter case yields $n = 2, m = 3$ (and so $a = 5$, $b = 12$, and $c = 13$).