# Solutions 9

**#1** Find all idempotent elements in $\mathbf{Z}/(17 \cdot 19)$.

For $x$ to be an idempotent is that $x$ satisfies $x^2 = x \bmod 17{\cdot}19$. By Sun Ze, this is equivalent to $x^2 = x \bmod 17$ and $x^2 = x \bmod 19$. Since $\mathbf{Z}/17$ and $\mathbf{Z}/19$ are fields (17 and 19 being prime), there are at most two solutions to quadratic equations in $\mathbf{Z}/17$ and $\mathbf{Z}/19$. And here we can see 2 obvious solutions: 0 and 1. Thus, all idempotents in $\mathbf{Z}/17 \cdot 19$ are solutions to

$$x = 0 \text{ or } 1 \bmod 17 \quad \text{and} \quad x = 0 \text{ or } 1 \bmod 19$$

The two obvious solutions are 0 and 1. The non-obvious solutions are the solutions to (first) $x = 0 \bmod 17$ and $x = 1 \bmod 19$ and (second) $x = 1 \bmod 17$ and $x = 0 \bmod 19$. From Euclid, $9 \cdot 17 - 8 \cdot 19 = 1$, so $x_1 = 9 \cdot 17 \cdot 0 - 8 \cdot 19 \cdot 1 = -8 \cdot 19$ and $x_2 = 9 \cdot 17 \cdot 1 - 8 \cdot 19 \cdot 0 = 9 \cdot 17$ are the two unobvious idempotents mod $17 \cdot 19$.

**#2** Show that there are no (non-zero) nilpotent elements in $\mathbf{Z}/(p \cdot q)$ for distinct primes $p, q$.

Suppose $x$ were a nilpotent element in $\mathbf{Z}/(pq)$. Then for some $n \geq 1$ it would be that $x^n = 0 \bmod pq$. That is, $pq|x^n$. Since $p, q$ are relatively prime, this is equivalent to $p|x^n$ and $q|x^n$. Since $p$ is prime, by the "Crucial Lemma" (in proving unique factorization) if $p|ab$ then $p|a$ or $p|b$. Thus, since $p|x^n$ necessarily $p|x$. Similarly, $q|x$. Again, since $p, q$ are relatively prime, $pq|x$. That is, $x = 0 \bmod pq$. So 0 is the only nilpotent element here. *Done.*

**#3** Prove that there is no field with 35 elements.

Suppose $k$ were a field with $p \cdot q$ elements with $p, q$ distinct primes. By Cauchy's theorem applied to the group $k$-with-addition, there is an element $x$ of (additive) order $p$, and an element $y$ of (additive) order $q$. Certainly neither $x$ nor $y$ is 0, since the order of 0 is 1. Let $z = xy$. Then since neither $x$ nor $y$ is 0, and since $k$ is a field, $z \neq 0$. As usual, for an ordinary integer $n$ and $w \in k$, $n \cdot w$ is merely an abbreviation for adding together $n$ copies of $w$. Then

$$p \cdot (xy) = (px) \cdot y = 0 \cdot y = 0$$

and also

$$q \cdot (xy) = x \cdot (qy) = x \cdot 0 = 0$$

Let $s, t$ be integers so that $sp + tq = 1$. Then

$$xy = 1 \cdot (xy) = (sp + tq) \cdot (xy) = s(px)y + tx(qy) = 0 + 0 = 0$$

contradiction.

Note that what we've actually proven is that the number of elements in a finite field cannot be divisible by two distinct primes.