Solutions 4

#1 Suppose that $G = \langle g \rangle$ is a cyclic group of order 144. What is the order of g^{60}?

The question is to find the smallest positive integer n so that $(g^{60})^n = e$. We have shown that $g^{60n} = e$ if and only if $60n = 0 \bmod |g|$. That is, we want the smallest positive solution of $60x = 0 \bmod 144$. That is, we want $144|60n$. The gcd of 144 and 60 is easily found (for example, by the Euclidean Algorithm) to be 12. Taking this common factor out, we are trying to solve $12|5n$. This requires that $12|n$. Thus, $n = 12$ is the smallest solution. That is, $g^{60} = 12$.

#2 Find all elements of order 10 in $\mathbf{Z}/100$ with addition.

The element $g = 1$ is a generator of $\mathbf{Z}/100$. The order of $n \cdot 1$ is (by definition) the smallest ℓ so that $\ell \cdot n = 0 \bmod 100$. That is, $\ell = 100/\gcd(n, 100)$. We want to find all n in the range $0, \ldots, 99$ so that $10 = \gcd(n, 100)$. In particular, 10 must divide n, but $n/10$ must have no factor of 2 or 5. Write $n = 10m$. Then $0 \leq m < 9$. For $n/10$ to be coprime to 10 means that m is coprime to 10. Thus, m can be in the list $1, 3, 7, 9$ only. That is, $n = 10, 30, 70, 90$ are the integers mod 100 which have (additive) order exactly 10.

#3 Let p be a prime congruent to 21 mod 25. Prove that, for any non-zero 5^{th} power $b \in \mathbf{Z}/p^\times$, $b^{(p+4)/25}$ is a 5^{th} root of b mod p.

We want to check that $(b^{(p+4)/25})^5 = b$. Let $a^5 = b$. Then

$$(b^{(p+4)/25})^5 = ((a^5)^{(p+4)/25})^5 = a^{p+4} = a^{p-1} \cdot a^5 = 1 \cdot b$$

where we invoke Fermat's little theorem to know that $a^{p-1} = 1$.