3 Assessed Exercise I: Euler's totient function

Euler's totient function, written $\phi(n)$, denotes the number of integers 1, 2, ..., n that are coprime to the positive integer n. So for example $\phi(1) = \phi(2) = 1$ and $\phi(3) = \phi(4) = 2$. The totient function is fundamental to number theory and this exercise establishes some of its elementary properties. See Baker, *A Concise Introduction to the Theory of Numbers* (Cambridge University Press, 1984), page 9. Other books on elementary number theory will also cover this function.

Task 1 *Define the totient function φ of type nat $\Rightarrow$ nat as described above. Note that the cardinality of a finite set can be expressed using the built-in function card, and the two-argument predicate coprime is also available. Greek letters can be inserted using the Symbols palette, but you may give the function the name phi if you prefer.*

Then prove the following two facts. *[5 marks]*

lemma *phi-1*: $\varphi\ 1 = 1$
lemma *phi-2*: $\varphi\ 2 = 1$

Task 2 *The following exercise establishes an alternative characterisation of the totient function.* *[10 marks]*

lemma *phi-altdef*: $\varphi(n) = card\ \{m.\ coprime\ m\ n \wedge m < n\}$

Task 3 *Among the other straightforward properties of the totient function is that $\phi(p) = p - 1$ if p is prime.* *[10 marks]*

lemma *phi-prime* [*simp*]:
assumes *prime p* **shows** $\varphi\ p = (p-1)$

Task 4 *The result above can be generalised to $\phi(p^j) = p^j - p^{j-1}$, where p is prime and $j > 0$.* *[25 marks]*

lemma *phi-prime-power* [*simp*]:
assumes *prime p* $j > 0$ **shows** $\varphi\ (p\ \hat{}\ j) = p\ \hat{}\ j - p\ \hat{}\ (j-1)$

Hint: none of these proofs require induction. Typically they involve manipulations of sets of positive integers, perhaps using equational reasoning.