1. Najděte poslední dvě cifry čísla $2012^{2011^{2010^{2009^{2008}}}}$.

   Rešení. Poslední dvě cifry čísla 2012^k, kde $k = 2011^{2010^{2009^{2008}}}$, dostaneme jako řešení rovnice

   $$2012^k \equiv 12^k \equiv x \; mod \, 100$$

   Protože $NSD(100, 2012) = 4 \neq 1$, nemůžeme použít Eulerovu větu přímo. Můžeme ale položit $x = 4y$ a po vydělení 4 dostaneme následující kongruenci:

   $$4^{k-1} \cdot 3^k \equiv y \; mod \, 25$$

   Počítáme tedy dvě kongruence: $4^{k-1} \; mod \, 25$ a $3^k \; mod \, 25$.

   - $NSD(4, 25) = NSD(3, 25) = 1$ a tedy můžeme použít Eulerovu větu. Platí $\varphi(25) = 20$ a tedy $4^{20} \equiv 1 \; mod \, 25$ a $3^{20} = 1 \; mod \, 25$. Potřebujeme tedy vypočítat $2011^{2010^{2009^{2008}}} \; mod \, 20$.
   - Protože $NSD(20, 2011) = 1$, můžeme opět využít Eulerovu větu: $2011^{\varphi(20)} = 2011^8 \equiv 1 \; mod \, 20$. Počítáme tedy $2010^{2009^{2008}} \; mod \, 8$. Vzhledem k tomu, že $2|2010$, tak jistě $2^3|2010^3$, tedy $2010^{2009^{2008}} \equiv 0 \; mod \, 8$ a mužeme dosadit do původní kongruence.
   - Nejprve vypočteme $4^k \; mod \, 25$

     $$4^{2011^{2010^{2009^{2008}}}} \equiv 4^{2011^{2010^{2009^{2008}} \; mod \, 20}} \equiv 4^{2011^{2010^{2009^{2008}} \; mod \, 8}} \equiv 4^{2011^0} = 4 \; mod 25$$

     $$4^k \equiv 4 \; mod \, 25 \; \Rightarrow \; 4^{k-1} \equiv 1 \; mod \, 25$$

   - Dále

     $$3^{2011^{2010^{2009^{2008}}}} \equiv 3^{2011^{2010^{2009^{2008}} \; mod \, 20}} \equiv 3^{2011^{2010^{2009^{2008}} \; mod \, 8}} \equiv 3^{2011^0} = 3 \; mod 25$$

   Po vynásobení dostaneme:

   $$4^{k-1} \cdot 3^k \equiv 1 \cdot 3 = 3 \; mod \, 25$$

   a po vynásobení 4 dostaneme

   $$12^k \equiv 12 \; mod \, 100$$

   Poslední dvě číslice čísla 2012^k jsou tedy 12.

2. **Najděte všechna $n \in \mathbb{N}$, pro která platí $13 \mid 4(n^2 + 1)$.**

Rešení. Řešení je ekvivalentní řešení rovnice

$$4(n^2+1) \equiv 0 \; mod \, 13$$

Protože $NSD(4, 13) = 1$, můžeme vydělit 4 a dostaneme

$$\begin{aligned} n^2+1 &\equiv 0 \; mod \, 13 \\ n^2+1 &\equiv 26 \; mod \, 13 \\ n^2-25 &\equiv 0 \; mod \, 13 \\ (n-5)(n+5) &\equiv 0 \; mod \, 13 \end{aligned}$$

Tedy množina čísel splňujících danou podmínku je rovna

$$\{5+13k,\ 8+13k \ : \ k \in \mathbb{N}_0\}$$

3. **Dokažte, že pro každé $a \in \mathbb{Z}$ a dvě různá prvočísla p, q platí**

$$pq \mid a^{p+q} - a^{p+1} - a^{q+1} + a^{1+1}$$

Rešení. Nejprve výraz upravíme do následující podoby:

$$a^{p+q} - a^{p+1} - a^{q+1} + a^{1+1} = a^p(a^q - a) - a(a^q - a) = (a^p - a)(a^q - a)$$

Protože p, q jsou různá prvočísla, jsou jistě nesoudělná a pro $\forall c$ tedy platí

$$pq \mid c \ \Leftrightarrow p \mid c \ \wedge \ q \mid c$$

Stačí tedy, když ověříme, že $p \mid a(a^{p-1} - 1)$ (pro q bychom ověřili analogicky). Pokud $p|a$, jsme hotovi. V opačném případě, podle Malé Fermatovy věty platí $a^{p-1} \equiv 1 \; mod \, p$ a tedy $p \mid (a^{p-1} - 1)$.

4. **Dokažte, že je-li p prvočíslo různé od 2, potom**

$$p \mid 1^p + 2^p + 3^p + \ldots + (p-1)^p$$

Rešení. Pro $\forall a \in \{1,\ 2, \ldots,\ p-1\}$ jistě platí $NSD(a, p) = 1$, tedy podle Malé Fermatovy věty platí

$$a^{p-1} \equiv 1 \; mod \, p \; \forall a \in \{1,\ 2, \ldots,\ p-1\}$$

Tedy platí

$$1^p+2^p+3^p+\ldots+(p-1)^p \equiv 1+2+3+\ldots+(p-1) = p \cdot \frac{(p-1)}{2} \equiv 0 \pmod{p}$$

Předpokládáme, že p je liché prvočíslo, tedy skutečně $\frac{p-1}{2} \in \mathbb{N}$.

5. **Najděte všechna $n \in \mathbb{N}$ taková, že $\varphi(n) = 18$.**

Rešení. Nejprve si všimneme, že platí následující pozorování: Pokud $NSD(2, n) = 1$, potom $\varphi(2n) = \varphi(2) \cdot \varphi(n) = 1 \cdot \varphi(n)$. Tedy pokud najdeme n liché takové, že $\varphi(n) = 18$, potom i $\varphi(2n) = 18$.
Pokud bychom uvažovali čísla n dělitelná 4 (vyšší mocnina 2 nemůže dělit n, protože 4 nedělí 18), zbyde nám v rozkladu 9, což nedá žádný rozklad ve tvaru "'vhodném"' pro $\varphi(n)$. Podle předchozího pozorování můžeme uvažovat pouze lichá n, a tedy ignorovat 1 v prvočíselném rozkladu. Dále postupujeme rozborem možností.

$$18 = 2 \cdot 3 \cdot 3$$

- $\varphi(p) = p - 1$, tedy určitě $\varphi(19) = 18$ a tedy i $\varphi(38) = 18$
- $18 = 2 \cdot 3 \cdot 3 = 2 \cdot 3^2 = \varphi(3^3)$, tedy i $\varphi(2 \cdot 3^3) = 18$
- pro $18 = 3 \cdot 6$ nenajdeme žádné vhodné n
- pro $18 = 2 \cdot 9$ nenajdeme žádné vhodné n

Tím jsme vyčerpali všechny možnosti, řešením je tedy množina

$$\{18,\ 39,\ 27,\ 54\}$$