Řešení 1. příkladu. Řešíme kongruenci $3745x \equiv 686 \pmod{1456}$, která je ekvivalentní kongruenci $833x \equiv 686 \pmod{1456}$. Věta o řešení lineárních kongruencí nám říká, že tato bude řešitelná právě když $(833, 1456) \mid 686$. Největší společný dělitel je 7, o tom se gambleři buď mohou přesvědčit Euklidovým algoritmem nebo můžeme takto malá čísla rozložit na součin prvočísel - rozklady se budou hodit i později.

$$833 = 7 \cdot 119 = 7^2 \cdot 17$$

$$1456 = 7 \cdot 208 = 7 \cdot 13 \cdot 16$$

$$686 = 7 \cdot 98$$

Ta stejná věta říká, že modulo 1456 je těch řešení právě 7. Najděme je. Budeme řešit kongruenci

$$119x \equiv 98 \pmod{208}. \tag{1}$$

Z ní pak získáme veškerá řešení původního zadání. Mohli bychom hledat inverzi 119 (mod 208) Euklidovým algoritmem a zešílet u toho. Budeme postupovat chytřeji. Hledáme y, že platí

$$119y \equiv 1 \pmod{208},$$

to je ale podle *čínské zbytkové věty* to samé jako řešit soustavu

$$119y \equiv 1 \pmod{13}, \quad 119y \equiv 1 \pmod{16}.$$

Protože známe rozklady vystupujících čísel, je toto extrémně jednoduché:

$$119y \equiv 7 \cdot 17y \equiv 7 \cdot 4y \equiv 28y \equiv 2y \equiv 1 \pmod{13}$$

Vynásobíme-li obě strany sedmičkou (inverze 2 (mod 13)) získáváme $y \equiv 7 \pmod{13}$. Obdobně řešme druhou kongruenci:

$$7 \cdot 17y \equiv 7 \cdot y \equiv 1 \pmod{16} \;\Rightarrow\; y \equiv 7 \pmod{16}$$

Máme tedy $119 \cdot 7 \equiv 1 \pmod{208}$. Můžeme se vrátit k řešení samotné kongruence (1).

$$7 \cdot 119x \equiv x \equiv 7 \cdot 98 \equiv 62 \pmod{208}$$

Nyní už získáme řešení původní kongruence jako $62 + 208k \pmod{1456}$ pro $k = 0, 1, \ldots, 6$.

Řešení 2. příkladu. Přepišme si dokazované tvrzení do formy kongruence: Máme ukázat, že pro libovolné přirozené n platí

$$111 + 2^{2^{2^{2n-1}}} \equiv 0 \pmod{127},$$

což je to samé jako

$$2^{2^{2^{2n-1}}} \equiv 16 = 2^4 \pmod{127}.$$

Nejdůležitější je si všimnout, že $127 + 1 = 128 = 2^7$, tj. $2^7 \equiv 1 \pmod{127}$! Díky tomuto by nám stačilo zjistit, že mocnina dvojky na levé straně kongruence ($2^{2^{2n-1}}$) dává po dělení 7 zbytek 4, vskutku:

$$2^{2^{2^{2n-1}}} = 2^{7k+4} = (2^7)^k \cdot 2^4 \equiv 1^k \cdot 16 \equiv 16 \pmod{127}.$$

Potřebujeme nyní ověřit

$$2^{2^{2n-1}} \equiv 4 \pmod 7.$$

Můžeme zopakovat předešlé úvahy, teď pouze v jiném kontextu. Platí $2^3 \equiv 1$ (7) a tedy by stačilo ukázat, že exponent dvojky v kongruenci splňuje $2^{2n-1} \equiv 2$ (3). Nyní si zase všimněme $2^2 \equiv 1$ (3). Můžeme zpětně řešit kongruence, které jsme zmínili:

$$2^{2n-1} \equiv (2^2)^n \cdot 2^{-1} \equiv 1^n \cdot 2 \equiv 2 \pmod 3 \Rightarrow$$
$$\Rightarrow 2^{2^{2n-1}} \equiv 2^{3k+2} \equiv (2^3)^k \cdot 2^2 \equiv 4 \pmod 7$$

Tento přístup je přirozený; v podstatě jsme v exponentech *šplhali nahoru* a opakovali stejnou myšlenku - vždy jsme si uvědomili řád dvojky. Kdyby nás ale toto nenapadlo, můžeme postupovat jednoduchou *matematickou indukcí*:

Že platí $2^{2^{2n-1}} \equiv 4$ (7) se pro $n = 1$ lehce ověří spočítáním na prstech. V indukci předpokládejme, že fakt platí pro n a snažme se ověřit pravdivost i pro $n+1$:

$$2^{2^{2(n+1)-1}} = 2^{2^{2n+1}} = 2^{2^{2n-1+2}} = 2^{2^{2n-1}\cdot 2^2} = (2^{2^{2n-1}})^4 \overset{\text{IP}}{\equiv} 4^4 = 256 \equiv 4 \pmod 7$$

Řešení 3. příkladu. Srdceryvný příběh o útrapách cvičenců můžeme chladnokrevně přepsat do tvaru soustavy lineárních kongruencí. Neznámá x značí počet cvičenců.

$$x \equiv 5 \pmod 8$$
$$x \equiv 2 \pmod 9$$
$$x \equiv 7 \pmod{14} \Rightarrow x \equiv 0 \pmod 7$$
$$1000 < x < 1500$$

Poslední kongruence (neboli údaj o lidských pyramidách na sletu) nám také říká, že $x \equiv 1 \pmod 2$, ale že je x liché již víme z první kongruence.

Na řešení takové soustavy známe nepoužitelný vzoreček; budeme proto postupovat opět ekvivalentními úpravami a nějakými *ad hoc* úvahami. Nicméně moduly jsou již nesoudělné, o této situaci nám *čínská zbytková věta* říká, že existuje jednoznačné řešení modulo $8\cdot 9\cdot 7 = 504$, což nám *těsně* zaručuje jednoznačnost počtu cvičenců v mezích 1000 až 1500.
Poslední kongruence nám říká, že $x = 7k$, dosaďme do prostřední, tj. $7k \equiv 2 \pmod 9$, vynásobením čtyřmi dostáváme $k \equiv 8 \pmod 9$, tedy $k = 8 + 9l$. Konečně dosaďme do prvního vztahu, dostáváme $7(8+9l) = 56+63l \equiv 7l \equiv -l \equiv 5 \pmod 8$. Dosazujme zpětně do vztahů, které jsme postupně získali: $l = 3 + 8m$, pak $k = 8 + 9(3 + 8m) = 35 + 8 \cdot 9m$ a nakonec $x = 7(35 + 8 \cdot 9m) = 245 + 7 \cdot 8 \cdot 9m = 245 + 504m$. Do hledaného rozmezí se vejde pouze $x = 245 + 504 \cdot 2 = 1253$. *Na slet se slétlo 1253 cvičenců z celé naší Československé socialistické vlasti*

Řešení 4. příkladu. Počítejme $\varphi(71 \cdot 79) = (71-1)(79-1) = 3 \cdot 4 \cdot 5 \cdot 7 \cdot 13 = 5460$. Z prvočíselného rozkladu vidíme, že $e = 11$ má modulo n inverzi d - tu má totiž právě když $(e, \varphi(n)) = 1$. Toto d můžeme spočítat buď Euklidovým algoritmem nebo převodem na soustavu lineárních rovnic jako v předchozích příkladech. Oběma postupy se dostaneme k číslu $d = 3971$, které z definice splňuje $11 \cdot 3971 = ed = 1 + m\varphi n \equiv 1 \ (n)$ Nyní nám *Eulerova věta*(ev) pro všechna a nesoudělná s n zaručuje, že platí

$$(a^e)^d \equiv a^{ed} \equiv a^{1+m\varphi(n)} \equiv a \cdot (a^{\varphi(n)})^m \equiv a \pmod n \tag{2}$$

Poznámka (Toto je diskuze nad rámec úlohy). Platí dokazovaná kongruence i pro čísla a, pro která je $(a, n) > 1$? Ano: Nechť je tedy a soudělné s $n = pq$, součinu dvou prvočísel, v našem případě je $p = 71$ a $q = 79$. (a, n) může nabývat hodnot p, q nebo n. $(a, n) = n$ odpovídá situaci $a = kn$, tedy (2) platí triviálně. Nechť tedy $(a, n) = p$ (případ pro q se dokáže stejně), to znamená $a = kp$ a $(k, n) = 1$. Dosaďme do (2):

$$(kp)^{ed} \equiv k^{ed} p^{ed} \overset{\text{(ev)}}{\equiv} kp^{ed} \pmod n$$

Připomínáme, že Eulerovu větu jsme mohli použít vzhledem k definici d. Stačí nám tedy ukázat, že $p^{ed} \equiv p \ (n)$. Všimněme si, že platí

$$\begin{aligned} p^{1+k(q-1)} &\equiv 0 \pmod p, \\ p^{1+k(q-1)} &\equiv p \pmod q. \end{aligned} \tag{3}$$

První kongruence je bezobsažná a druhá je jednoduché použití *malé Fermatovy věty.* Čínská zbytková věta nám radí, že modulo pq existuje pouze jedno číslo x, které tyto kongruence splňuje a hned se vidí, že takovým je $x = p$. Volbou $k = p - 1$ dostáváme přesně $p^{ed} \equiv p$ (n), protože $ed = 1 + m\varphi(n) = 1 + (p - 1)(q - 1)$ Poznamenejme ještě, že tento fakt platí i pro obecnější n - konkrétně pro libovolné *square-free* n. Vyzýváme čtenáře si zkusit toto dokázat. Postup bude obdobný, trochu se obmění soustava kongruencí (3), speciálně v exponentech.

Řešení 5. příkladu. Pro výpočet budeme používat větu o kvadratické reciprocitě (qr), faktu že Legendrův symbol je multiplikativní funkce a také si nebudeme příliš dělat starosti, zda náhodou nepracujeme s Jacobiho symbolem - jejich kalkulus a hodnoty jsou stejné; liší se pouze interpretací výsledku. Ale o to nám nyní nejde. Počítejme:

$$\begin{aligned} \left(\frac{2013}{4049}\right) &\overset{\text{qr}}{=} \left(\frac{4049}{2013}\right) = \left(\frac{23}{2013}\right) \overset{\text{qr}}{=} \left(\frac{2013}{23}\right) = \left(\frac{12}{23}\right) = \\ &= \left(\frac{2 \cdot 2 \cdot 3}{23}\right) = \left(\frac{2}{23}\right)^2 \cdot \left(\frac{3}{23}\right) \overset{\text{qr}}{=} -(\pm 1)^2 \left(\frac{23}{3}\right) = -\left(\frac{2}{3}\right) = 1 \end{aligned}$$

Poslední rovnost platí, protože 2 není kvadratický zbytek modulo 3. Počítat s Legendrovým symbolem, jako by byl Jacobiho, nám ušetřilo dost práce, jinak bychom totiž museli zohledňovat fakt $2013 = 3 \cdot 11 \cdot 61$.