

Hodnocení							$\Sigma$	

Jméno: .....

Na každý příklad získáte nezáporný počet bodů.

Na práci máte 90 minut.

- (10krát  $\pm 2$  body — správně 2 body, chybně  $-2$ , bez odpovědi 0)  
Odpovězte (škrtnutím nehodícího se **ano** nebo **ne** na patřičném řádku), zda jsou pravdivá následující tvrzení (čtěte **velmi** pozorně!):
  - ano** — **ne** Mají-li celá čísla  $x$ , resp.  $y$  řád  $a$ , resp.  $b$  modulo  $m \in \mathbb{N}$ , pak má číslo  $x \cdot y$  řád  $a \cdot b$  modulo  $m$ .
  - ano** — **ne** Pro každé reálné číslo  $x$  platí, že  $\langle x \rangle$  (tj. necelá část  $x$ ) je menší než  $x$ .
  - ano** — **ne** Existuje nekonečně mnoho prvočísel tvaru  $10k + 1$ .
  - ano** — **ne** Libovolná binomická kongruence  $x^n \equiv -1 \pmod{m}$ , kde  $n$  je liché, má řešení.
  - ano** — **ne** Pro každé přirozené číslo  $m$  je  $\varphi(m)$  sudé číslo.
  - ano** — **ne** Je-li řešitelná kongruence  $f(x) \equiv 0 \pmod{m}$ , pro  $m \in \mathbb{N}$  a  $f(x) \in \mathbb{Z}[x]$ , pak je tato kongruence řešitelná modulo libovolné přirozené číslo  $d$ , splňující  $d \mid m$ .
  - ano** — **ne** Relace dělitelnosti na množině celých čísel je antisymetrická.
  - ano** — **ne** Je-li celé číslo  $g$  primitivním kořenem modulo  $m \in \mathbb{N}$ , pak je také primitivním kořenem modulo libovolné  $d \in \mathbb{N}$ , které je dělitelem  $m$ .
  - ano** — **ne** Diofantická rovnice  $x^n + y^n = z^n$  s neznámými  $x, y, z \in \mathbb{N}$  nemá pro parametr  $n \in \mathbb{N}, n > 1$  žádné řešení.
  - ano** — **ne** Pro libovolné  $m \in \mathbb{N}$  je grupa  $(\mathbb{Z}_m^\times, \cdot)$  cyklická.

- (10 bodů) V oboru celých čísel řešte soustavu rovnic:

$$\begin{aligned}x^2 + 5y^2 &= z^2 \\5x^2 + y^2 &= u^2\end{aligned}$$

- (15 bodů) Zjistěte, pro která prvočísla  $p$  je řešitelná kongruence

$$x^2 - 10 \equiv 0 \pmod{p}.$$

- (10 bodů) Řešte v  $\mathbb{N}$  rovnici  $\varphi(m) = \frac{m}{3}$ .
- (15 bodů) Určete primitivní kořen modulo  $23^2$ . Řešte kongruenci  $x^5 \equiv 534 \pmod{23^2}$
- (10 bodů) Definujte *Möbiovu funkci* a uveďte Möbiovu inverzní formuli.