příjmení: **11ALG – závěrečný test – varianta VZOR**

jméno: **8.1.2013**

skupina:

Stvrzuji svým podpisem, že jsem test vypracovala/vypracoval samostatně a použila/použil jsem pouze povolené zdroje informací. Beru na vědomí, že v případě jakéhokoliv porušení pravidel z mé strany bude můj test klasifikován známkou F a *stejně tak budou klasifikovány testy kolegyň a kolegů v mém bezprostředním okolí* (na sousedním místě po mé levici, pravici, přede mnou a za mnou).

podpis: .....

1. Jaká záporná čísla náleží do třídy kongruence $[3]_5$? [1 bod]

2. Za jakých podmínek lze kongruenci $k \cdot a \equiv k \cdot b \pmod{n}$ redukovat na $a \equiv b \pmod{n}$? [2 body] • Jak se zbavíte k na levé straně výše uvedené kongruence, pokud ji nemůžete přímo redukovat? [1 bod]

3. Co nám udává Eulerův totient? Jak jej spočítáme? [2 body]

4. Na jakém výpočetně složitém *principu* je založen Diffieho-Helmannův mechanismus výměny šifrovacího klíče? [2 body]

5. Uveďte obě podmínky *korektnosti* numerické úlohy. [2 body]

6. Pravda / nepravda: Podmíněnost numerické úlohy nezávisí na kvalitě algoritmu, jímž úlohu řešíme. [1 bod] • Své tvrzení demonstrujte na příkladu pomocí čísla podmíněnosti úlohy. [1 bod]

7. Jaká podmínka zaručí, že metoda půlení intervalu nalezne nulu spojité nelineární funkce na omezujícím intervalu $\langle a, b \rangle$? [2 body]

8. Jaký tvar má rovnice řešená metodou prosté iterace (této metodě se někdy také říká iterace v pevném bodě, anglicky *fixed point iteration*)? [2 body]

9. Nakreslete příklad situace, kdy metoda tečen při hledání kořene nelineární rovnice diverguje. [2 body]

10. Pravda / nepravda: Simpsonovo kvadraturní pravidlo je založeno na kvadratické interpolaci a má proto algebraický řád 2. [2 body]

11. Na jakém principu spočívá *aproximace* funkce zadané tabulkou hodnot? [2 body] • Jaký je rozdíl mezi aproximací a *interpolací*? [1 bod]