Algebra 1 (Schoof) $\qquad$ 2^o esonero $\qquad$ 30 gennaio 2017, ore 11:00–13:00.

COGNOME .... *NOME* ....

Accompagnare le risposte con spiegazioni *chiare ed essenziali*. Ogni esercizio vale 5 punti.

1. Sia A un anello (commutativo con 1) e siano I, J due ideali di A. Dimostrare che $(I+J)(I\cap J)\subset IJ$.
2. Scrivere $X^2Y^2+Y^2Z^2+Z^2X^2$ come polinomio nei polinomi simmetrici elementari $s_1, s_2, s_3 \in \mathbf{Z}[X,Y,Z]$.
3. Dimostrare che l'anello $\mathbf{Z}[\sqrt{-2}]=\{a+b\sqrt{-2} : a,b\in\mathbf{Z}\}\subset\mathbf{C}$ è un dominio Euclideo rispetto alla funzione $N(a+b\sqrt{-2})=a^2+2b^2$.
4. Sia p un primo. Determinare la cardinalità del gruppo degli elementi invertibili dell'anello $\mathbf{Z}_p[X]/(X^2-1)$.
5. Determinare la cardinalità dell'anello $\mathbf{Z}[X]/(X^2-2X, X+3)$.
6. Sia $p>2$ un numero primo. Dimostrare che per ogni $n\geq 1$ il polinomio X^2-1 ha esattamente due zeri in $\mathbf{Z}_{p^n}$.

Soluzioni.

1. Un elemento di $(I+J)(I\cap J)$ è una somma di prodotti xy con $x\in I+J$ e $y\in I\cap J$. Basta dimostrare che ogni prodotto xy appartiene a IJ. Scriviamo $x=u+v$ con $u\in I$ e $v\in J$. Allora $xy=uy+vy$. Poiché uy, vy stanno entrambi in IJ, ci sta anche xy.
2. Questo è l'esercizio 5 del foglio 12.
3. Questo è l'esercizio 4 del foglio 11.
4. Se $p\neq 2$, i polinomi $X-1$ e $X+1$ sono coprimi in $\mathbf{Z}_p[X]$. Per il teorema cinese del resto, l'anello $\mathbf{Z}_p[X]/(X^2-1)$ è isomorfo a $\mathbf{Z}_p[X]/(X+1)\times\mathbf{Z}_p[X]/(X-1)\cong\mathbf{Z}_p\times\mathbf{Z}_p$. Il gruppo degli elementi invertibili è quindi isomorfo a $\mathbf{Z}_p^*\times\mathbf{Z}_p^*$ ed ha $(p-1)^2$ elementi. Invece, se $p=2$, l'anello in questione è isomorfo a $\mathbf{Z}_2[X]/(X+1)^2\cong\mathbf{Z}_2[Y]/(Y^2)$ ed ha 4 elementi. Qua $Y=X+1$. Solo gli elementi $\overline{1}$ e $\overline{1+Y}$ sono invertibili.
5. Siano $I=(X^2-2X)$ e $J=(X+3)$. Allora $\mathbf{Z}[X]/(X^2-2X,X+3)=\mathbf{Z}[X]/(I+J)$ è isomorfo a $\mathbf{Z}[X]/J$ modulo $(I+J)/J$, vale a dire a $\mathbf{Z}[X]/(X+3)$ modulo $(X^2-2X,X+3)/(X+3)$. Applichiamo l'isomorfismo $\mathbf{Z}[X]/(X+3)\longrightarrow\mathbf{Z}$ dato da $f\mapsto f(-3)$. Troviamo che il nostro anello è isomorfo a $\mathbf{Z}/((-3)^2-2(-3),(-3)+3)$ ed ha quindi 15 elementi.
6. In $\mathbf{Z}_{p^n}$ ci sono gli zeri $+1$ e -1. Visto che $p\neq 2$, sono distinti. Va dimostrato che non ci sono altri zeri. Supponiamo che $a\in\mathbf{Z}$ sia un terzo zero modulo p^n. Allora p^n divide $a^2-1=(a+1)(a-1)$. Affermo che uno dei due fattori $a+1$ e $a-1$ non è divisibile per p. Quindi p^n divide l'altro fattore e si ha che $a\equiv\pm 1 \pmod{p^n}$ come richiesto.

   Per dimostrare l'affermazione, supponiamo per assurdo che $a+1$ e $a-1$ siano entrambi divisibili per il primo p. Ma, allora anche la differenza $2=(a+1)-(a-1)$ è divisibile per p. Contraddizione, perché $p\neq 2$.