

(a) Se $p \equiv 3 \pmod{4}$, allora $X^2 + 1$ è irriducibile su $\mathbf{Z}_p$ (siccome è di grado due, se fosse riducibile, sarebbe scomponibile in fattori di primo grado, quindi avrebbe almeno una radice in $\mathbf{Z}_p$, ma questo è falso per l'ipotesi che $p \equiv 3 \pmod{4}$), quindi R è un campo (per l'esercizio 6 precedente), e $\#R^* = \#R - 1 = p^2 - 1$.

Se $p \equiv 1 \pmod{4}$, allora $X^2 + 1$ è riducibile su $\mathbf{Z}_p$, e si fattorizza, diciamo, come $X^2 + 1 = (X+m)(X+n)$ (qui e in seguito, se non specificato diversamente, i coefficienti sono tutti modulo p . Non si perde in generalità supponendo che i fattori siano monici; notare che per forza $m \neq n$, siccome $p > 2$ è dispari). Siccome $\overline{a+bX}$ è invertibile se e solo se $\gcd(a+bX, X^2+1) = 1$ ($\mathbf{Z}_p[X]$ è un anello euclideo, quindi possiamo usare Bezout), allora gli elementi invertibili di R sono esattamente le classi dei polinomi di grado ≤ 1 che non sono multipli né di $X+m$ né di $X+n$, quindi ci sono esattamente $p^2 - (2p-1) = (p-1)^2$ elementi invertibili in R .

(b) Innanzitutto, ϕ è ben definita: se $\overline{a+bX} \in R^*$, allora $a^2+b^2 \neq 0$. Infatti, se $a^2+b^2 = 0$, allora $(a+bX)(a-bX) = \overline{a^2-b^2X^2} = \overline{a^2+b^2} = 0$, quindi $\overline{a+bX}$ non sarebbe invertibile.

Si può verificare direttamente che ϕ è un omomorfismo. Altrimenti, si osservi che $R \cong \mathbf{Z}[i]/(p)$, mediante un isomorfismo (di anelli) che manda $\overline{a+bX}$ in $a+bi$. Usando questa identificazione, e siccome $N(xy) = N(x)N(y)$ in $\mathbf{Z}[i]$, si ottiene che ϕ è un omomorfismo passando alle classi modulo p , siccome per $a, a' \in \mathbf{Z}$ si ha che $a \equiv a' \pmod{p}$ implica $a^2 \equiv a'^2 \pmod{p}$.

(c) Sia $c \in \mathbf{Z}_p^*$. Gli insiemi $A = \{c - a^2 \mid a \in \mathbf{Z}_p\}$ e $B = \{b^2 \mid b \in \mathbf{Z}_p\}$ hanno entrambi cardinalità $\frac{p+1}{2}$. Questo, ad esempio, usando l'esercizio 5(b), oppure notando che da $x^2 = y^2$ segue $0 = x^2 - y^2 = (x-y)(x+y)$, quindi $x = y$ oppure $x = -y$. Dunque $A \cap B \neq \emptyset$, quindi $c - a^2 = b^2$, per certi a e b , cioè $c = a^2 + b^2 = \phi(\overline{a+bX})$. Notiamo che $\overline{a+bX}$ è invertibile, poiché $(\overline{a+bX})(\overline{a-bX})c^{-1} = (a^2+b^2)c^{-1} = 1$.

(d) Poiché ϕ è suriettiva, $R^*/\ker\phi \cong \mathbf{Z}_p^*$. Quindi $\#\ker\phi = \#R^*/\#\mathbf{Z}_p^*$, cioè $\#\ker\phi = \frac{p^2-1}{p-1} = p+1$, se $p \equiv 3 \pmod{4}$, e $\#\ker\phi = \frac{(p-1)^2}{p-1} = p-1$, se $p \equiv 1 \pmod{4}$.

Per ogni $t \in \mathbf{Z}_p^*$, $\{\overline{f(X)} \mid \phi(\overline{f(X)}) = t\}$ è un laterale di $\ker\phi$, quindi ha esattamente $\#\ker\phi$ elementi. Siccome $\phi(\overline{a+bX}) = a^2+b^2$, il numero delle coppie è esattamente $\#\ker\phi$, cioè $p+1$, se $p \equiv 3 \pmod{4}$, e $p-1$, se $p \equiv 1 \pmod{4}$.