Richiami di teoria

ORDINE - ESPONENTE DI UN GRUPPO. L'ordine di un gruppo e' la cardinalita' del gruppo. L'esponente di un gruppo e' il m.c.m. degli ordini dei suoi elementi oppure equivalentemente e' il piu' piccolo intero positivo che annulla tutti gli elementi (i.e. il piu' piccolo intero positivo che e' multiplo dell'ordine di ciascun elemento).
L'ordine di un gruppo prodotto e' il prodotto degli ordini dei fattori. L'esponente del gruppo prodotto e' il m.c.m. degli ordini degli elementi.
Esiste sempre un elemento che ha ordine l'esponente del gruppo. Invece esiste un elemento che ha come ordine l'ordine del gruppo se e solo se il gruppo e' ciclico.
Esempio: $\mathbb{Z}_6 \times \mathbb{Z}_{14}$ ha ordine 84 ed esponente 42.

NOTA SULL"ORDINE DI UN ELEMENTO Se a ha ordine α e b ha ordine β allora a+b ha ordine $\alpha\beta$? oppure il m.c.m. di α e β? VERI entrambi SE a e b sono coprimi FALSI in generale (prendere b l'inverso di a, notare che l'inverso di un elemento ha lo stesso ordine dell'elemento).

Mostriamo allora che esiste un elemento che ha ordine l'esponente del gruppo. Per la nota basta far vedere che per ogn primo p che divide l'esponente esiste un elemento di ordine p^t (la massima potenza di p che divide l'esponente del gruppo). Basta vedere che per ogni p esiste un elemento con ordine multiplo di p^t poi un opportuno multiplo dell'elemento avra' l'ordine voluto. Ma se tutti gli ordini degli elementi dividono p^{t-1} moltiplicato un numero coprimo con p questo accade per l'm.c.m. quindi facilmente concludiamo.

NOTA SULLA TAVOLA PITAGORICA $\mathbb{Z}_p^*$ e' isomorfo a $\mathbb{Z}_{p-1}$: scelta una radice primitiva modulo p un isomorfismo si ottiene mandando un elemento nel suo logaritmo discreto (e se moltiplico gli elementi gli esponenti si sommano!) Cosi' confrontiamo le tavole pitagoriche dei due gruppi.

RICHIAMI SUL LOGARITMO DISCRETO IN $\mathbb{Z}_p^*$: Sia $p \neq 2$ e sia g una radice primitiva.
-Il logaritmo discreto e' ben definito a meno di $p-1$ perche' $g^{p-1} = 1$;
-$\log_g(ab) = \log_g a + \log_g b$; $\log_g(a^-1) = -\log_g a$; $\log_g 1 = 0$ (scrivere $a = g^\alpha$, $b = g^\beta$, $1 = g^{p-1} = g^0$, $a^{-1} = g^{-\alpha}$);
- Cambiare radice primitiva g fa cambiare il logaritmo discreto di ogni elemento per una stessa costante c (che si puo' scegliere tra 1 e $p-1$, infatti $g_1 = g_2^c$ implica $\log_{g_2} x = c \log_{g_1} x$);
-Un elemento e' un quadrato se e solo se $\log_g$ e' pari (concetto ben definito dato che $p-1$ e' pari). In particolare il prodotto di due quadrati o di due non-quadrati e' un quadrato e il prodotto di un quadrato e di un non-quadrato e' un non-quadrato.

Alcuni esercizi svolti

ESERCIZIO 1 FOGLIO 3: Se p divide F_n allora $p \neq 2$ e si ha $2^{2^n} + 1 = 0 (\mathrm{mod} p)$. Quindi si ha $2^{2^n} = -1 (\mathrm{mod} p)$ da cui si deduce che l'ordine di 2 in $\mathbb{Z}_p^*$ e' 2^{n+1}. Questo numero allora divide $\phi(p) = p - 1$ per cui $p = 1 (\mathrm{mod} 2^{n+1})$.

ESERCIZIO 7 FOGLIO 3: Il logaritmo di -1 e' $\frac{p-1}{2}$ quindi esso e' pari se e solo se $p = 1 (\mathrm{mod}\, 4)$ (dato che $p > 3$ l'unica altra possibilita' era $p = 3 (\mathrm{mod} 4)$). Commentiamo il suggerimento: come accade in $\mathbb{C}$ le soluzioni di $T^2 + 3$ si ottengono dalle soluzioni di $T^2 + T + 1$ ($a = \sqrt{3}$; $b_{1,2} = \frac{-1 \pm \sqrt{3}}{2}$). In $\mathbb{Z}_p^*$ analogamente $b_{1,2} = (-1 \pm a)(2^{-1})$ ed $a = b_1 - b_2$. Accettato il sug-

gerimento bisogna mostrare che $p-1=0(\text{mod}3)$ se e solo se T^2+T+1 ha soluzione in $\mathbb{Z}_p$ (notare che se ha una soluzione le ha entrambe e $b_2=1-b_1$). Il polinomio T^2+T+1 moltiplicato per $T-1$ da' il polinomio T^3-1 e le soluzioni sono dunque le radici dell'unita' di ordine esattamente 3. Ma se $\mathbb{Z}_p^*$ contiene un elemento di ordine 3 allora 3 divide $\phi(p)=p-1$ dunque $p-1=0(\text{mod}3)$. Viceversa in un gruppo ciclico di ordine un multiplo di 3 esiste un elemento di ordine 3 che quindi e' una radice dell'unita' di ordine 3. Il punto c) segue facilmente dai precedenti dato che $-3=3(-1)$ e le congruenze date sono equivalenti allora al fatto che 3 e -1 sono entrambi quadrati oppure entrambi non-quadrati.

ESERCIZIO 8 FOGLIO 3: Il testo corretto dell'esercizio e' il seguente: Sia $n\in\mathbb{Z}_{>0}$ e non divisibile per 3. Il numero di classi x in $\mathbb{Z}_n$ tali che $x^3=1(\text{mod}n)$ e' uguale a 3^t dove t e' il numero di divisori primi di n congrui ad 1 modulo 3. Sia a_p l'esponente di p nella fattorizzazione di n. Per il teorema cinese del resto e' sufficiente mostrare che $x^3=1(\text{mod}p^{a_p})$ ha 3 soluzioni se $p=1(\text{mod}3)$ ed una sola soluzione (la classe di 1) se $p=2(\text{mod}3)$ (notare che per ipotesi $p\neq 0(\text{mod}3)$). Le soluzioni devono essere cercate nel gruppo ciclico $\mathbb{Z}_{p^a}^*$ (dato che 0 non e' soluzione) e sono tante quante gli elementi di tale gruppo con ordine che divide 3. Tale gruppo ha ordine $\phi(p^a)=p^{a-1}(p-1)$. Nel caso $p=1(\text{mod}3)$ un gruppo ciclico di ordine multiplo di 3 ha esattamente 3 tali elementi, nel caso $p=2(\text{mod}3)$ dato che 3 non divide l'ordine del gruppo solo l'identita' ha ordine che divide 3.

ESERCIZIO 7 FOGLIO 5: Fissato m bisogna determinare il massimo n tale che l'esponente (m.c.m degli ordini degli elementi) del gruppo $\mathbb{Z}_n^*$ divide m. L'esponente di un prodotto di gruppi e' il m.c.m. degli esponenti dei fattori (l'operazione si fa coordinata per coordinata). L'esponente di $\mathbb{Z}_n^*$ e' il m.c.m. degli esponenti di $\mathbb{Z}_{p^a}^*$ (scrivendo la fattorizzazione $n=\prod p^a$). Notare che p^a sara' allora la massima potenza di p tale che l'esponente di $\mathbb{Z}_{p^a}^*$ divide m. Quindi bisogna massimizzare p^a. L'esponente di $\mathbb{Z}_{p^a}^*$ per p dispari e' $(p-1)p^{a-1}$; per 2 esso e' 1, per 4 esso e' 2, per 2^a con $a\geq 3$ esso e' 2^{a-2}. Facciamo il caso $m=6$. Se p e' dispari $p-1$ divide 6 cioe' $p=3,7$. Inoltre 3^{a_3-1} divide 6, 7^{a_7-1} divide 6. Per $p=2$ dato che 2 divide 6 allora possiamo prendere $a_2\geq 3$. Si deve avere 2^{a_2-2} divide 6. Quindi ricaviamo $n=8\cdot 9\cdot 7=504$.