IL GRUPPO $\mathbb{Z}_{p^a}^*$ per $p \neq 2$.
Il gruppo $\mathbb{Z}_{p^a}^*$ ha ordine $\phi(p^a) = (p-1)p^{a-1}$. Mostriamo che il gruppo e' ciclico facendo vedere che esiste un elemento il cui ordine e' l'ordine del gruppo. Dato che $(p-1)$ e' coprimo con p^{a-1} e' sufficiente esibire un elemento di ordine $(p-1)$ ed un elemento di ordine p^{a-1} (il prodotto di questi due elementi avra' infatti l'ordine desiderato). Per il primo elemento dobbiamo intanto mostrare che esiste una radice primitiva modulo p (si vedano le dispense del professore "Nota sulle radici primitive modulo p"; dalla dimostrazione si sa che esiste un elemento di ordine $p-1$ ma non viene determinato chi sia). Sia z intero tale che $z(\bmod p)$ ha ordine $p-1$. Allora l'ordine di $z(\mathrm{mod}p^a)$ e' un multiplo di $p-1$ quindi l'elemento cercato e' una opportuna potenza di z.
Un elemento di ordine p^{a-1} e' la classe di $1+p$ (si deve svolgere il binomio):

$$(1+p)^{p^{a-2}} = 1 + p^{a-1} + p^a(....) \neq 1(\mathrm{mod}p^a)$$

$$(1+p)^{p^{a-1}} = 1 + p^a(....) = 1(\mathrm{mod}p^a).$$

IL GRUPPO $\mathbb{Z}_2^*$ ha un solo elemento.
IL GRUPPO $\mathbb{Z}_{2^2}^*$ ha due elementi quindi e' isomorfo a $\mathbb{Z}_2$.
IL GRUPPO $\mathbb{Z}_{2^a}^*$ per $a \geq 3$.
Tale gruppo ha ordine 2^{a-1}. Dimostriamo che e' isomorfo a $\mathbb{Z}_{2^{a-2}} \times \mathbb{Z}_2$.
Dimostriamo che la classe di -1 non sta in $\langle 5 \rangle$: $5 = 1(\bmod 4)$ quindi anche le sue potenze. Invece $-1 \neq 1(\mathrm{mod}4)$. Se $5^m = -1(\mathrm{mod}2^a)$ allora in particolare si avrebbe $5^m = -1(\mathrm{mod}4)$.
Dimostriamo che la classe di 5 ha ordine 2^{a-2}: il suo ordine non puo' essere 2^{a-1} dato che non genera il gruppo. Quindi basta calcolare che $5^{2^{a-3}} \neq 1(\mathrm{mod}2^a)$. Si ha (si deve svolgere il binomio):

$$(5)^{2^{a-3}} = (1+2^2)^{2^{a-3}} = 1 + 2^{a-1} + 2^a(....) \neq 1(\mathrm{mod}2^a).$$

La classe di 5 ha ordine 2^{a-2} quindi un sottogruppo che contiene strettamente $\langle 5 \rangle$ e' l'intero gruppo. La classe di -1 non sta in $\langle 5 \rangle$ allora 5 e -1 generano. Dato che $\mathbb{Z}_{2^a}^*$ contiene un elemento di ordine 2^{a-2} ci sono solo due possibilita' per la sua scrittura come prodotto di gruppi ciclici: $\mathbb{Z}_{2^{a-2}} \times \mathbb{Z}_2$ e $\mathbb{Z}_{2^{a-1}}$. L'esponente di un gruppo con ordine potenza di un primo e' il massimo degli ordini dei suoi elementi ed in questo caso e' allora 2^{a-2}. Dobbiamo allora scartare il caso in cui $\mathbb{Z}_{2^a}^*$ sia ciclico (avrebbe esponente 2^{a-1}) e concludiamo.
Notare che possiamo scrivere gli elementi come $\pm 1 \cdot 5^t(2^a)$ per un qualche t compreso tra $0 \leq t \leq 2^{a-2}$ (nota: questo fatto puo' essere utile per svolgere l'esercizio 3 del foglio 5).

IL GRUPPO $\mathbb{Z}_n^*$. Il gruppo $\mathbb{Z}_n^*$ ha ordine $\phi(n)$. Se la fattorizzazione di n e' $\prod p^a$ allora il gruppo $\mathbb{Z}_n^*$ e' il prodotto dei gruppi $\mathbb{Z}_{p^a}^*$.

Alcuni esercizi svolti

ESERCIZIO 3 FOGLIO 4 La curva data e' della forma $Y^2 = X^3 + AX + B$ ed il campo su cui e' definita ha caratteristica diversa da 2 e da 3. La curva data e' una curva ellittica se $4A^3 + 27B^2$ (un elemento di $\mathbb{Z}_5$ in questo caso) e' diverso da zero. Dobbiamo trovare tutte le coppie (ordinate!) di elementi di $\mathbb{Z}_5$ che soddisfano l'equazione. Puo' essere conveniente calcolare chi sono i quadrati in $\mathbb{Z}_5$ (mandando ogni elemento nel suo quadrato si ottengono solo le classi di $0, 1, -1$). Poi si assegna un valore alla x e si calcola $x^3 + x + 1$. Se questo e' un quadrato le sue due radici (una si ottiene dall'altra moltiplicando per -1) e solo 0 nel caso dello zero saranno i valori della y da considerare per il dato valore della x. Quanti punti potranno esserci? Ci sono alpiu' 25 coppie ordinate di elementi di $\mathbb{Z}_5$ piu' il punto all'infinito quindi avremo un numero di punti compreso tra 1 (il punto all'infinito c'e' sempre) e 26. E' poi possibile calcolare l'ordine degli

elementi trovati. Se si trova un punto che ha ordine la cardinalita' del gruppo si deduce che il gruppo e' ciclico e tale elemento e' un generatore.

ESERCIZIO 4 FOGLIO 4 Per $a \neq 3$ si calcola che $4A^3 + 27B^2$ e' diverso da zero. Per il punto b) si ragiona come nell'esercizio precedente. Per $a = 1(5)$ si trovano 8 soluzioni (x, y) quindi con il punto all'infinito abbiamo 9 punti. Per $a = 2$ similmente 7 punti. Per $a = -1$ similmente 8 punti. Un gruppo abeliano di ordine (i.e. cardinalita') un numero primo e' ciclico ed e' generato da ogni elemento che non sia l'identita'. Quindi per $a = 2$ abbiamo $\mathbb{Z}_7$. Per $a = 1$ abbiamo $\mathbb{Z}_9$ se esiste un elemento di ordine 9, altrimenti abbiamo $\mathbb{Z}_3 \times \mathbb{Z}_3$. Quindi prendiamo 3 volte un elemento: se non fa zero esso ha ordine 9 e abbiamo finito. Prendiamone un altro e facciamo lo stesso. Nota: se troviamo almeno 3 elementi di ordine esattamente 3 (cioe' diversi dall'identita' e tali che 3 volte loro sono l'identita') sappiamo che siamo nel caso $\mathbb{Z}_3 \times \mathbb{Z}_3$. Infatti $\mathbb{Z}_9$ ha solo 2 elementi di ordine 3. Per vedere se un punto ha ordine 3 si puo' usare il criterio dell'esercizio 8 (si trovano solo due punti di ordine 3 quindi si esclude il caso $\mathbb{Z}_3 \times \mathbb{Z}_3$ in cui ci sarebbero 4 tali punti). Facciamo il caso $a = -1$. Le possibilita' per un gruppo abeliano di ordine 8 sono $\mathbb{Z}_8$, $\mathbb{Z}_2 \times \mathbb{Z}_{2^2}$ e $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$. L'ultima possibilita' possiamo scartarla perche' dalla teoria delle curve ellittiche sappiamo che il gruppo di punti e' un sottogruppo di $\mathbb{Z}_n \times \mathbb{Z}_n$ per un qualche n (che in particolare non puo' avere 3 elementi di ordine 2 come invece ha $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$). Troviamo un solo punto di ordine 2 (usare il criterio $y = 0$ dell'esercizio 7 per trovare tali punti) quindi il gruppo cercato e' $\mathbb{Z}_8$.

ESERCIZIO 5 FOGLIO 4 In un qualsiasi gruppo il sottoinsieme degli elementi con ordine che divide n e' un sottogruppo (verificare che si ha l'identita', la chiusura rispetto alla somma e l'esistenza dell'inverso: notare che l'esistenza dell'inverso segue dalla chiusura rispetto alla somma per un gruppo finito dato che l'inverso e' un multiplo/potenza dell'elemento dato!).

ESERCIZIO 7 FOGLIO 4 Dalle formule vediamo che se P non e' l'identita' e $y \neq 0$ nessun denominatore si annulla nella formula per $P+P$ quindi $2P$ ha coordinate nel campo (in particolare non e' il punto all'infinito che e' l'identita'). Viceversa se $y = 0$ le coordinate del punto $P + P$ non sono in K e quindi $2P$ e' l'identita'. Inoltre dato che siamo in un campo $y = 0$ se e solo se $y^2 = 0$ e quindi si trova l'equazione $x^3 + Ax + B = 0$. Una equazione a coefficienti in un campo ha alpiu' tante radici quante il suo grado. Dato che $y = 0$ e ci sono massimo 3 possibilita' per la x il punto b) e' immediato. Quindi ci sono alpiu' 3 punti di ordine esattamente 2 e allora ci sono alpiu' 4 punti di ordine che divide 2.
Il sottogruppo dei punti con ordine che divide 2 e' un gruppo di esponente 2 (nota: e' il piu' grande sottogruppo con esponente 2) ed ha alpiu' 4 elementi. Nota: l'esponente di un gruppo divide l'ordine del gruppo (perche' l'ordine degli elementi divide l'ordine del gruppo e cosi' il loro m.c.m.). Il gruppo puo' essere il gruppo banale, $\mathbb{Z}_2$, $\mathbb{Z}_2 \times \mathbb{Z}_2$ (abbiamo scartato $\mathbb{Z}_4$ che ha esponente 4).

ESERCIZIO 8 FOGLIO 4 Se P ha ordine 3 allora ne' P ne' $2P$ sono il punto all'infinito. Usando allora le formule per $P + 2P$ deve aversi $x_P = x_{2P}$ oppure $3P$ avra' le coordinate nel campo. Sviluppando $x_P = x_{2P}$ si ottiene il polinomio cercato (sostituire y_P^2 con $x_P^3 + Ax_P + B$). Viceversa se P (si sottointende che non sia l'infinito) e' tale che x_P soddisfa tale polinomio e non ha ordine 2 allora si avra' $x_P = x_{2P}$ da cui segue $3P = 0$ e quindi l'ordine del punto sara' 3. Ma se P avesse ordine 2 allora x_P sarebbe soluzione comune di $x^3 + Ax + B = 0$ e di $3x^4 + 6Ax^2 + 12Bx - A^2 = 0$. Ma dato che il risultante di questi polinomi non e' nullo non ci sono soluzioni comuni (Il risultante e' $(4A^3 + 27B^2)^2 = disc^2$ quindi non e' nullo).