Addenda et Corrigenda per la dispensa "Introduzione alla Crittografia"

Alessandro Zaccagnini

27 dicembre 2005

1 Addenda

1.1 Esercizi

Gli Esercizi qui proposti *non* sono ordinati per difficoltà crescente.

Esercizio 1. *Risolvere l'equazione* $3x \equiv 7 \bmod 20$ *e l'equazione* $2x \equiv 4 \bmod 20$.

Risposta: $x \equiv 9 \bmod 20$; $x \equiv 2 \bmod 10$.

Esercizio 2. *Determinare* $d = (135, 102)$ *mediante l'Algoritmo di Euclide descritto nel* §6.1, *e determinare* $\lambda, \mu \in \mathbb{Z}$ *tali che* $d = 135\lambda + 102\mu$.

Risposta: $d = 3 = -3 \cdot 135 + 4 \cdot 102$.

Esercizio 3. *Determinare* $31^{-1} \bmod 37$.

Risposta: $31^{-1} \equiv 6 \bmod 37$.

Esercizio 4. *Usando il Teorema di Fermat* 3.1.6 *ed il Teorema Cinese del Resto* 2.1.2, *dimostrare che* $n \cdot (n^{30} - 1)$ *è divisibile per* $2 \cdot 3 \cdot 7 \cdot 11 \cdot 31$ *qualunque sia* $n \in \mathbb{Z}$.

Risposta: Dato $p \in \{2, 3, 7, 11, 31\}$, si osservi che $p - 1 \mid 30$: dunque, se $p \nmid n$ allora $n^{p-1} \equiv 1 \bmod p$, e quindi $n^{30} \equiv 1 \bmod p$. Se invece $p \mid n$ non c'è niente da dimostrare. La tesi segue dal Teorema Cinese del Resto.

Esercizio 5. *Usando il Teorema di Eulero* 3.1.9 *ed il Teorema Cinese del Resto* 2.1.2, *dimostrare che* $5n^3 + 7n^5 \equiv 0 \bmod 12$ *per ogni* $n \in \mathbb{Z}$.

Risposta: Osserviamo che $5n^3 + 7n^5 \equiv 7n^3(n^2 - 1) \bmod 12$, e che è sufficiente dimostrare la tesi considerando separatamente le due congruenze modulo 3 e 4. Se $3 \nmid n$ allora $n^2 \equiv 1 \bmod 3$, ed in caso contrario $n^3 \equiv 0 \bmod 3$. Inoltre se $2 \nmid n$ allora $n^2 \equiv 1 \bmod 4$, ed in caso contrario $n^2 \equiv 0 \bmod 4$.

Esercizio 6. *Determinare il massimo comun divisore* D *degli elementi di* $\{n^{13} - n \colon n \in \mathbb{N}\}$.

Risposta: Naturalmente $D \mid 2^{13} - 2 = 2 \cdot 3^2 \cdot 5 \cdot 7 \cdot 13$. Per il Teorema di Fermat 3.1.6, D è divisibile per $d = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 13$, cioè per il prodotto dei primi p tali che $p - 1 \mid 13 - 1$. Inoltre, si osservi che $p^2 \nmid (p^{13} - p)$ e quindi $p^2 \nmid D$ per ciascuno dei primi considerati sopra, cioè $D = d$.

Esercizio 7. *Determinare tutti gli interi a e b tali che* $13a+17b=1$.

Risposta: $a=4+17k$, $b=-3-13k$, dove $k\in\mathbb{Z}$.

Esercizio 8. *Dimostrare che* 8 *non genera* $\mathbb{Z}_p^*$ *per* $p=7$, 13, 19, 31*; piú in generale, dimostrare che* 8 *non genera* $\mathbb{Z}_p^*$ *se* $p\equiv 1 \bmod 6$. *Suggerimento: dimostrare che l'ordine di* 8 *è* $\leq \frac{1}{3}(p-1)$.

Risposta: Se $p\equiv 1 \bmod 6$ allora esiste $k\in\mathbb{N}$ tale che $p=1+3k$. Per il Teorema di Lagrange 1.3.7 si ha $2^{p-1}=1$, e quindi $8^k=2^{3k}=1$, e l'ordine di 8 non supera $k=\frac{1}{3}(p-1)$.

Esercizio 9. *Dimostrare che se* $x\in\mathbb{Z}_n^*$*, allora l'ordine di* x^{-1} *è uguale all'ordine di* x.

Risposta: Siano d e δ rispettivamente l'ordine di x e l'ordine di x^{-1} in $\mathbb{Z}_n^*$: allora $\left(x^{-1}\right)^d = x^{-d} = \left(x^d\right)^{-1} = 1$. Dunque $\delta\leq d$. In modo del tutto analogo si dimostra che $d\leq\delta$, e quindi $d=\delta$.

Esercizio 10. *Determinare l'ordine di tutti gli elementi di* $\mathbb{Z}_{15}^*$ *e dedurne che il gruppo in questione non è ciclico.*

Risposta: Si ha $\mathbb{Z}_{15}^*=\{1,2,4,7,8,11,13,14\}$, i cui ordini sono rispettivamente 1, 4, 2, 4, 4, 2, 4, 2. Se $\mathbb{Z}_{15}^*$ fosse ciclico dovrebbe esserci almeno un elemento di ordine 8.

Esercizio 11. *Dimostrare che ogni elemento di* $\mathbb{Z}_{15}^*$ *può essere scritto nella forma* $2^m\cdot 11^n$*, con* $m\in\mathbb{Z}_4$, $n\in\mathbb{Z}_2$*; dedurne che il massimo ordine degli elementi di* $\mathbb{Z}_{15}^*$ *è* 4.

Risposta: Si tratta di una verifica.

Esercizio 12. *Determinare, se esistono, le “radici quadrate” di* 2 *in* $\mathbb{Z}_{15}^*$*, cioè le soluzioni dell'equazione* $x^2\equiv 2 \bmod 15$.

Risposta: Per quanto visto sopra, l'equazione non ha soluzioni.

Esercizio 13. *Dati due numeri primi dispari distinti* p *e* q*, dimostrare che l'equazione* $x^2\equiv 1 \bmod pq$ *ha* 4 *soluzioni distinte. Suggerimento: usare il Lemma* 2.2.8 *ed il Teorema Cinese del Resto* 2.1.2.

Risposta: L'equazione $x^2\equiv 1 \bmod p$ ha le soluzioni $x_p\equiv 1 \bmod p$ ed $y_p\equiv -1 \bmod p$. Analogamente, l'equazione $x^2\equiv 1 \bmod q$ ha le soluzioni $x_q\equiv 1 \bmod q$ ed $y_q\equiv -1 \bmod q$. Le quattro soluzioni dell'equazione proposta sono dunque le soluzioni dei sistemi di congruenze

$$\begin{cases} x\equiv x_p \bmod p \\ x\equiv x_q \bmod q \end{cases} \quad \begin{cases} x\equiv x_p \bmod p \\ x\equiv y_q \bmod q \end{cases} \quad \begin{cases} x\equiv y_p \bmod p \\ x\equiv x_q \bmod q \end{cases} \quad \begin{cases} x\equiv y_p \bmod p \\ x\equiv y_q \bmod q \end{cases}$$

Questi sistemi hanno soluzione per il Teorema Cinese del Resto, e queste soluzioni sono evidentemente tutte distinte. Non possono esserci altre soluzioni perché se x è soluzione di $x^2\equiv 1 \bmod pq$, allora $x^2\equiv 1 \bmod p$ ed $x^2\equiv 1 \bmod q$.

Esercizio 14. *Dedurre dall'Esercizio precedente che se* n *è divisibile per due primi dispari distinti allora* $\mathbb{Z}_n^*$ *non è ciclico. (Si veda il commento a pag. 24 alla fine del* §3.1*).*

Esercizio 15. *Determinare tutte le soluzioni di* $x^2\equiv 1 \bmod 16$. *In generale, mostrare che per* $\alpha\geq 1$ *l'equazione* $x^2\equiv 1 \bmod 2^{\alpha+2}$ *ha le* 4 *soluzioni distinte* ± 1, $2^{\alpha+1}\pm 1$ *e non ne ha altre.*

Risposta: La prima parte è una semplice verifica. Sia ora $x\not\equiv\pm 1$ una soluzione dell'equazione $x^2\equiv 1 \bmod 2^{\alpha+2}$. Dato che questa equivale a $2^{\alpha+2}\mid (x-1)(x+1)$, scriviamo $x-1=2^\beta n$ ed $x+1=2^\gamma m$ per opportuni β, $\gamma\in\mathbb{N}$, e per n, $m\in\mathbb{N}$ dispari. Osserviamo che uno fra β

e γ vale necessariamente 1, perché altrimenti sia $x-1$ che $x+1$ sarebbero divisibili per 4, e questo è impossibile (se $x+1 \equiv x-1 \equiv 0 \bmod 4$ allora $(x+1)-(x-1) \equiv 0 \bmod 4$, e cioè $2 \equiv 0 \bmod 4$). Inoltre, per l'ipotesi $x \not\equiv \pm 1 \bmod 2^{\alpha+2}$ abbiamo anche $0 < \beta, \gamma \leq \alpha+1$. Dunque, dato che $2^{\alpha+2} \mid (x-1)(x+1)$, abbiamo $\alpha+2 \leq \beta+\gamma$, ed esaminando i casi possibili troviamo $\beta = \alpha+1$ e $\gamma = 1$ oppure $\beta = 1$ e $\gamma = \alpha+1$.

Esercizio 16. *Sia $p = 2^8+1 = 257$. Dimostrare che 3 genera $\mathbb{Z}_p^*$. In generale, dimostrare che $g \in \mathbb{Z}_p^*$ è un generatore se e solo se l'equazione $x^2 \equiv g \bmod p$ non ha soluzione.*

Risposta: I divisori di $p-1$ sono della forma 2^j, con $j = 0, \ldots, 8$. Se l'equazione $x^2 \equiv g \bmod p$ ha soluzione, allora l'ordine di g è $\leq \frac{1}{2}(p-1)$ e g non genera $\mathbb{Z}_p^*$. Piú semplicemente, dato che 3 è un generatore, dall'Esempio in fondo a pag. 23 sappiamo che 3^h è a sua volta un generatore se e solo se $(h, p-1) = 1$, che equivale a $(h,2) = 1$, cioè h deve essere dispari.

Esercizio 17. *Utilizzando l'algoritmo di Gauss descritto nel* §6.6, *determinare un generatore di $\mathbb{Z}_{19}^*$. Determinare tutte le soluzioni dell'equazione $x^3 \equiv -1 \bmod 19$.*

Risposta: Preso $a_1 = 2$, si verifica che $o(2) = 18$. Le soluzioni dell'equazione proposta hanno ordine che divide 6: infatti $x^6 \equiv 1 \bmod 19$ e quindi l'ordine di x divide 6. Inoltre né x né x^3 valgono 1 e quindi x ha ordine 2 oppure 6. Nel primo caso $x \equiv -1 \bmod 19$. Nel secondo caso $2^{18/6} \equiv 8 \bmod 19$ e $2^{5\cdot 18/6} \equiv 12 \bmod 19$ sono le altre due soluzioni.

Esercizio 18. *Utilizzando l'algoritmo di Gauss descritto nel* §6.6, *determinare un generatore di $\mathbb{Z}_{43}^*$.*

Risposta: Preso $a_1 = 2$ si verifica che $o(2) = 14$ e che $3 \notin \langle 2 \rangle$. Con qualche calcolo si verifica anche che $o(3) = 42$.

Esercizio 19. *Determinare il logaritmo discreto di 5 rispetto al generatore 3 nel gruppo ciclico $\mathbb{Z}_{43}^*$, ed utilizzare il risultato per dimostrare che anche 5 è un generatore. Trovare la "formula di cambiamento di base" per i logaritmi: in altre parole, esprimere il logaritmo discreto di $x \in \mathbb{Z}_{43}^*$ rispetto al generatore 5 mediante il logaritmo discreto rispetto al generatore 3.*

Risposta: Il logaritmo discreto cercato vale 25. Sia y il logaritmo discreto di x rispetto al generatore 3 e sia t il logaritmo discreto di x rispetto al generatore 5: in altre parole, $3^y \equiv x \equiv 5^t \bmod 43$. Dato che $5 \equiv 3^{25} \bmod 43$, possiamo riscrivere l'ultima uguaglianza nella forma $3^{y-25t} \equiv 1 \bmod 43$. Poiché $1 = 3\cdot 42 - 5\cdot 25$, abbiamo che $t \equiv -5y \bmod 42$. Si osservi che la situazione è formalmente identica a quella che si presenta in $\mathbb{R}$ dove la formula è

$$\log_a(x) = \frac{\log_b(x)}{\log_b(a)}.$$

Qui $t = \log_5(x) = (\log_3(x)) \cdot (\log_3(5))^{-1} \equiv -5y \bmod 42$.

Nel risolvere gli esercizi che seguono conviene utilizzare il *minimo residuo* piuttosto che il *minimo residuo positivo*, come indicato nella Definizione 2.1.1. In altre parole, dato che si devono svolgere calcoli in $\mathbb{Z}_{61}$, si consiglia di osservare che $31 \equiv -30 \bmod 61$, $32 \equiv -29 \bmod 61$ e cosí via.

Esercizio 20. *Dimostrare con il minor numero di calcoli possibile che 2 genera il gruppo ciclico $\mathbb{Z}_{61}^*$.*

Risposta: I divisori di 60 sono 1, 2, 3, 4, 5, 6, 10, 12, 15, 20, 30, 60. Non è difficile vedere che $2^1 \equiv 2 \bmod 61$, $2^2 \equiv 4 \bmod 61$, $2^3 \equiv 8 \bmod 61$, $2^4 \equiv 16 \bmod 61$, $2^5 \equiv 32 \equiv -29 \bmod 61$, $2^6 \equiv$

$-58 \equiv 3 \bmod 61$, $2^{10} = 2^4 \cdot 2^6 \equiv 16 \cdot 3 = 48 \equiv -13 \bmod 61$, $2^{12} \equiv (2^6)^2 \equiv 9 \bmod 61$, $2^{15} = 2^{12} \cdot 2^3 \equiv 9 \cdot 8 \equiv 11 \bmod 61$, $2^{20} \equiv (2^{10})^2 \equiv 169 \equiv -14 \bmod 61$, $2^{30} \equiv (2^{15})^2 \equiv -1 \bmod 61$.

Esercizio 21. *Sapendo che* 2 *genera il gruppo ciclico* $\mathbb{Z}_{61}^*$, *determinare tutti gli altri generatori. Si sfrutti il fatto che* $\phi(60) = 16$.

Risposta: I generatori di $\mathbb{Z}_{61}^*$ hanno la forma 2^n, dove $n \in \mathbb{Z}_{60}^* = \{1, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 49, 53, 59\}$. I generatori sono dunque $2^1 = 1$, $2^7 \equiv 6 \bmod 61$, $2^{11} \equiv -26 \bmod 61$, $2^{13} \equiv 18 \bmod 61$, ...

Esercizio 22. *Determinare il logaritmo discreto di* 15 *e di* 24 *rispetto al generatore* $g = 2$ *nel gruppo* $\mathbb{Z}_{61}^*$ *usando l'algoritmo di Shanks detto “Baby steps, giant steps” descritto nel* §6.7.1.

Risposta: Sono rispettivamente 28 e 9.

1.2 Altro

Il racconto di E. A. Poe [2] in traduzione italiana è reperibile all'indirizzo
http://web.tiscali.it/no-redirect-tiscali/manuel_ger/ita/bug_ita.htm

Il testo [3] è servito da base per la parte iniziale della monografia “Introduzione alla crittografia” [1] di Alessandro Languasco e Alessandro Zaccagnini.

2 Corrigenda

Pag	riga	Errata	Corrige
10	10	definita	definite
15	−7	$(\pm 1, \pm 3, \pm 5, \pm 7)$	$(\pm 1, \pm 5, \pm 7, \pm 11)$
31	−4	$x^{r(p-1)/2}$	$x^{r(p-1)/4}$
34	22	vettorale	vettoriale
38	−10	$4a^2x^2 + 4ax + b^2$	$4a^2x^2 + 4abx + b^2$
40	7	gaurdia	guardia
40	−7	Rabin	Rivest
41	2	$d \in \mathbb{Z}_n^*$	$d \in \mathbb{Z}_{\phi(n)}^*$
42	6	$m = mb^k \cdot a^{-ky}$	$m = mb^k \cdot \alpha^{-ky}$
43	8	intizione	intuizione
43	−13	$e \in \mathbb{Z}_p^*$	$e \in \mathbb{Z}_{p-1}^*$
47	1	Figura 6.2	Vedi Figura 1
50	8	Lehmann	Lehman
50	−14	$p^{1/4}$	$p^{1/2}$
52	−8	a_1^r	$a_1^{r_1}$
52	−2	$a_2 = 2^4 \cdot 3 \bmod p = 7$	$a_2 = 2^8 \cdot 3^5 \bmod p = 11$
54	14	$g^m = 3^{11} \equiv 96 \bmod 101$	$g^m = 3^{11} \equiv 94 \bmod 101$
56	−1	algorimo	algoritmo

Se il numero della riga è negativo si intende che deve essere contata dal basso.

Tra la fine della pagina 58 e l'inizio della successiva si sostituisca (3 volte) “Lagrange” con “Legendre.”

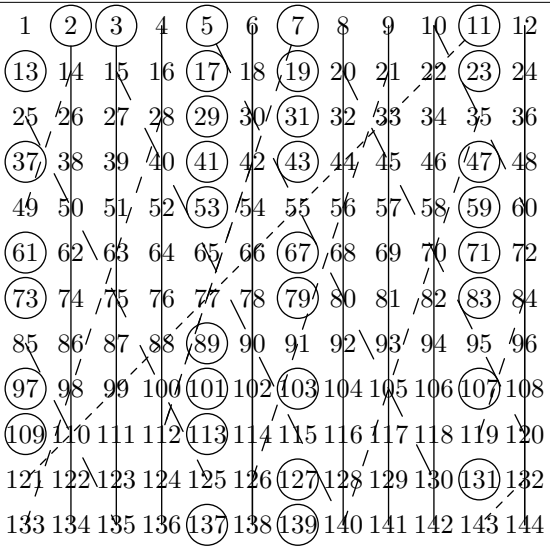

Figura 1: La versione corretta della Figura 6.2

Desidero ringraziare l'amico Alessandro Languasco per avermi segnalato alcuni fra gli errori piú gravi.

3 Prove scritte

3.1 Prova A, 15 maggio 2003

1. Determinare λ, $\mu \in \mathbb{Z}$ tali che $25\lambda + 32\mu = 1$ ed utilizzare il risultato ottenuto per risolvere l'equazione $25x \equiv 4 \bmod 32$.

Soluzione. Dato che $9 \cdot 25 - 7 \cdot 32 = 1$, l'equazione ha soluzione $x \equiv 4 \bmod 32$.

2. Usando il fatto che 3 genera $\mathbb{Z}_{31}^*$, determinare nel modo piú semplice possibile le soluzioni dell'equazione $x^6 \equiv 1 \bmod 31$.

Soluzione. Le soluzioni dell'equazione proposta hanno ordine che divide 6, e quindi sono 1, 3^5, 3^{10}, 3^{15}, 3^{20}, 3^{25}.

3. Dimostrare che 11 è un generatore di $\mathbb{Z}_{18}^*$, e determinarli tutti sapendo che $\phi(18) = 6$.

Soluzione. È una verifica: l'altro generatore è 5.

4. Sapendo che 3 genera $\mathbb{Z}_{31}^*$, determinare il logaritmo discreto di 29 usando il metodo di Shanks.

Soluzione. Prima calcoliamo $m = 6$, e quindi $3^0 \equiv 1 \bmod 31$, $3^6 \equiv 16 \bmod 31$, $3^{12} \equiv 8 \bmod 31$, $3^{18} \equiv 4 \bmod 31$, $3^{24} \equiv 2 \bmod 31$, $3^{30} \equiv 1 \bmod 31$. Dato che 29 non compare in questa lista, calcoliamo in successione $3 \cdot 29 \equiv 25 \bmod 31$, poi $3^2 \cdot 29 \equiv 13 \bmod 31$, e infine $3^3 \cdot 29 \equiv 8 \bmod 31$, da cui ricaviamo $29 \equiv 3^{12-3} \equiv 3^9 \bmod 31$.

5. Dimostrare (senza fare tutti i calcoli) che le soluzioni dell'equazione $x^6 \equiv 1 \bmod 47$ sono $x \equiv \pm 1 \bmod 47$. Suggerimento: per il Teorema di Fermat si ha $x^{46} \equiv 1 \bmod 47$ se $x \not\equiv 0 \bmod 47$ (ma $x \equiv 0 \bmod 47$ non è soluzione dell'equazione data). Dunque $x^{6\lambda+46\mu} \equiv 1 \bmod 47$ per ogni λ, $\mu \in \mathbb{Z}$. Si scelgano λ e μ in modo opportuno con l'Algoritmo di Euclide esteso.

Soluzione. Scelto $\lambda = 8$ e $\mu = -1$ si trova che $x^2 \equiv 1 \bmod 47$.

3.2 Prova B, 15 maggio 2003

1. Determinare λ, $\mu \in \mathbb{Z}$ tali che $24\lambda + 35\mu = 1$ ed utilizzare il risultato ottenuto per risolvere l’equazione $24x \equiv 5 \bmod 35$.

Soluzione. Dato che $-16 \cdot 24 + 11 \cdot 35 = 1$, l’equazione ha soluzione $x \equiv 25 \bmod 35$.

2. Usando il fatto che 3 genera $\mathbb{Z}_{31}^*$, determinare nel modo piú semplice possibile le soluzioni dell’equazione $x^5 \equiv 1 \bmod 31$.

Soluzione. Le soluzioni dell’equazione proposta hanno ordine che divide 5, e quindi sono 1, 3^6, 3^{12}, 3^{18}, 3^{24}.

3. Dimostrare che 5 è un generatore di $\mathbb{Z}_{18}^*$, e determinarli tutti sapendo che $\phi(18) = 6$.

Soluzione. È una verifica: l’altro generatore è 11.

4. Sapendo che 3 genera $\mathbb{Z}_{31}^*$, determinare il logaritmo discreto di 15 usando il metodo di Shanks.

Soluzione. Prima calcoliamo $m = 6$, e quindi $3^0 \equiv 1 \bmod 31$, $3^6 \equiv 16 \bmod 31$, $3^{12} \equiv 8 \bmod 31$, $3^{18} \equiv 4 \bmod 31$, $3^{24} \equiv 2 \bmod 31$, $3^{30} \equiv 1 \bmod 31$. Dato che 15 non compare in questa lista, calcoliamo in successione $3 \cdot 15 \equiv 14 \bmod 31$, poi $3^2 \cdot 15 \equiv 11 \bmod 31$, e infine $3^3 \cdot 15 \equiv 2 \bmod 31$, da cui ricaviamo $15 \equiv 3^{24-3} \equiv 3^{21} \bmod 31$.

5. Dimostrare (senza fare tutti i calcoli) che le soluzioni dell’equazione $x^8 \equiv 1 \bmod 47$ sono $x \equiv \pm 1 \bmod 47$. Suggerimento: per il Teorema di Fermat si ha $x^{46} \equiv 1 \bmod 47$ se $x \not\equiv 0 \bmod 47$ (ma $x \equiv 0 \bmod 47$ non è soluzione dell’equazione data). Dunque $x^{8\lambda+46\mu} \equiv 1 \bmod 47$ per ogni λ, $\mu \in \mathbb{Z}$. Si scelgano λ e μ in modo opportuno con l’Algoritmo di Euclide esteso.

Soluzione. Scelto $\lambda = 6$ e $\mu = -1$ si trova che $x^2 \equiv 1 \bmod 47$.

Riferimenti bibliografici

[1] A. Languasco, A. Zaccagnini. *Introduzione alla crittografia*. Ulrico Hoepli Editore, Milano, 2004.

[2] E. A. Poe. The Gold Bug. In *The complete tales and poems of Edgar Allan Poe*, pagine 42–70, New York, 1975. Random House. Trad. it. *Lo scarabeo d’oro*, in *Racconti*, L’Unità–Einaudi. Si veda `http://web.tiscali.it/no-redirect-tiscali/manuel_ger/ita/bug_ita.htm`.

[3] A. Zaccagnini. Introduzione alla Crittografia, 2003. Dispensa per il corso omonimo, tenuto per il “Master in Gestione della Sicurezza Informatica e delle Reti nelle Aziende e nella Pubblica Amministrazione.” Facoltà di Ingegneria. A. A. 2002–2003. Disponibili all’indirizzo `http://www.math.unipr.it/~zaccagni/psfiles/didattica/Master.pdf`.