Teoria elementare dei numeri. 2. Radici primitive; algoritmo Pollard ϱ. Roma, 16 ottobre 2005.

1. Sia p un numero primo. Una *radice primitiva* modulo p è un numero $g \in \mathbf{Z}$ tale che la classe $\overline{g}$ modulo p ha ordine $p-1$. Calcolare tutte le radice primitive in $\mathbf{Z}_{23}^*$. Stessa domanda per $\mathbf{Z}_{31}^*$.
2. Sia n un numero naturale e sia $x \in \mathbf{Z}$ con $\mathrm{mcd}(x,n) = 1$. Sia $a = \mathrm{ord}_n(x)$ e sia $k \in \mathbf{Z}$. Dimostrare che $\mathrm{ord}_n(x^k) = a/\mathrm{mcd}(a,k)$.
3. Sia $n = 10001$.
   (a) Fattorizzare $\varphi(n)$.
   (b) Esibire, se esiste, un $\overline{x} \in \mathbf{Z}_n^*$ di ordine 17.
   (c) Esibire, se esiste, un $\overline{x} \in \mathbf{Z}_n^*$ di ordine 8.
4. Siano $n = 56492375429317645$ e $m = 986764526573$.
   (a) Far vedere che $\mathrm{mcd}(n,m) = 1$;
   (b) Calcolare $\lambda, \mu \in \mathbf{Z}$ tali che $\lambda n + \mu m = 1$.
   (c) Calcolare $\lambda, \mu \in \mathbf{Z}$ tali che $\lambda n + \mu m = 2$.
5. (Numeri di Fermat) Per ogni numero naturale n, si definisce l'ennesimo numero di Fermat come $F_n = 2^{2^n} + 1$. Sia p un divisore primo di F_n;
   (a) Dimostrare che la classe $\overline{2} \in \mathbf{Z}_p^*$ ha ordine 2^{n+1}.
   (b) Dimostrare che $p \equiv 1 \pmod{2^{n+1}}$.

   (si veda http://mathworld.wolfram.com/FermatNumber.html)
6. Si p un numero primo dispari.
   (a) Dimostrare che per ogni $\overline{x} \in \mathbf{Z}_p^*$ la classe $\overline{x}^{(p-1)/2}$ è uguale a $\pm\overline{1}$.
   (b) Far vedere che $\overline{x} \in \mathbf{Z}_p^*$ è un *quadrato* se e solo se $\overline{x}^{(p-1)/2} = \overline{1}$.
   (c) Quanti quadrati ci sono in $\mathbf{Z}_p^*$?
7. Si p un numero primo e sia d un divisore di $p-1$.
   (a) Sia $W = \{\overline{x} \in \mathbf{Z}_p^* : \overline{x}^d = \overline{1}\}$. Quanti elementi ci sono in W?
   (b) Dimostrare che per ogni $\overline{x} \in \mathbf{Z}_p^*$ la classe $\overline{x}^{(p-1)/d}$ è un elemento di W.
   (c) Far vedere che $\overline{x} \in \mathbf{Z}_p^*$ è una *d-esima potenza* se e solo se $\overline{x}^{(p-1)/d} = \overline{1}$.
   (d) Quante d-esime potenze ci sono in $\mathbf{Z}_p^*$?
8. (Pollard ρ) Sia p un numero primo e $f : \mathbf{Z}_p \longrightarrow \mathbf{Z}_p$ la funzione data da $\overline{x} \mapsto \overline{x^2+1}$. Scegliere p fra 30 e 60 e disegnare il seguente grafo diretto: i vertici sono le classi $\overline{x} \in \mathbf{Z}_p$. Esiste una freccia da $\overline{x}$ verso $\overline{y}$ se e soltanto se $f(\overline{x}) = \overline{y}$.
9. (Logaritmo discreto) Sia p un numero primo.
   (a) Sia $p = 41$. Determinare una radice primitiva $\overline{g}$ in $\mathbf{Z}_p^*$.
   (b) Ogni classe $\overline{x}$ di $\mathbf{Z}_p^*$ è potenza di $\overline{g}$. Per $p = 41$, determinare $i \in \mathbf{Z}$ tale che $\overline{2} = \overline{g}^i$.
   (c) Stesse domande per $p = 1009$.
   (d) Per $\overline{a} \in \mathbf{Z}_p^*$, l'esponente j tale che $\overline{a} = \overline{g}^j$ in $\mathbf{Z}_p^*$, si dice *il logaritmo discreto* di a (mod 41) rispetto alla radice primitiva $\overline{g}$. Far vedere che il logaritmo discreto è ben definito modulo $p-1$ e che il logaritmo di un prodotto è uguale alla somma dei logaritmi dei fattori (mod $p-1$).
10. Siano dati i seguenti due numeri n e m.

$$n = 1174305121654314261470648822244 1321,$$
$$m = 1174305121654314266417599496279 5097.$$

    (a) Far vedere che non sono numeri primi.
    (b) Fattorizzare n e m. (Uno di n, m è abbastaza facilmente fattorizzabile con il metodo ρ di Pollard, ma *non* con il metodo $p-1$. Per l'altro numero vale il viceversa.)