Note su alcuni argomenti di Teoria dei Numeri

M.B.S.Laporta[1]

[1]Indirizzo: Dipartimento di Matematica e Appl., Università degli Studi di Napoli, Via Cinthia, 80126 Napoli (Italia), email: laporta@matna2.dma.unina.it

Indice.

Guida per il lettore.

Le presenti note sono state scritte a completamento del quinto capitolo, "Radici primitive dell'unità e congruenze del tipo $X^m \equiv a \pmod{n}$", della dispensa del corso TN1 presso la Terza Università di Roma. Esse contengono alcuni argomenti trattati ed altri che sono stati omessi nelle lezioni tenute dal sottoscritto dal 23 marzo al 4 aprile 2004 presso la stessa Università (per esempio, a lezione sono stati studiati i casi piú semplici della dimostrazione del Teorema di Gauss, quelli di non esistenza delle radici). Le notazioni sono quelle della dispensa. In particolare, la lettera p, con o senza indici e apici, è riservata per denotare un numero primo.

M.B.S.Laporta

1.Algoritmo di Gauss per il calcolo di una radice primitiva modulo un numero primo p dispari.

Tale algoritmo si basa sulla seguente proprietà che dimostriamo:

Proposizione 1.1. *Sia* $S_p^* := \{1, 2, \ldots, p-1\}$ *e sia* $a \in S_p^* \setminus \{1\}$ *tale che* $\mathrm{ord}_p a < p-1$. *Per ogni* $b \in \{x \in S_p^* \setminus \{1\} : \ x \not\equiv a^i \pmod p,\ \forall i = 1, \ldots, \mathrm{ord}_p a\}$ *esiste* $a_1 \in S_p^* \setminus \{1, a\}$ *tale che* $\mathrm{ord}_p a_1 = \mathrm{m.c.m}(\mathrm{ord}_p a, \mathrm{ord}_p b) > \mathrm{ord}_p a$.

Dimostrazione. Siccome $\mathrm{ord}_p a < p-1$, si noti che

$$T_{a,p} := \{x \in S_p^* \setminus \{1\} : \ x \not\equiv a^i \pmod p,\ \forall i = 1, \ldots, \mathrm{ord}_p a\} \neq \emptyset\ .$$

Mostriamo che, per ogni $b \in S_p^* \setminus \{1\}$, esiste $a_1 \in S_p^* \setminus \{1\}$ tale che

1) $\mathrm{ord}_p a_1 = \mathrm{m.c.m}(\mathrm{ord}_p a, \mathrm{ord}_p b)$,

2) se, in piú, $b \in T_{a,p}$, allora $\mathrm{ord}_p a_1 > \mathrm{ord}_p a$ (da cui segue che $a_1 \neq a$).

Non è difficile rendersi conto che[2] esistono due interi coprimi d' e t', divisori rispettivamente di d e t, tali che $\mathrm{m.c.m}(\mathrm{ord}_p a, \mathrm{ord}_p b) = d't'$. Inoltre, risulta che $\mathrm{ord}_p a^{d/d'} = d'$ e $\mathrm{ord}_p b^{t/t'} = t'$. Dunque, posto $a_1 := a^{d/d'} b^{t/t'}$, dalla Proposizione 5.4 (5) segue che $\mathrm{ord}_p a_1 = d't' = \mathrm{m.c.m}(\mathrm{ord}_p a, \mathrm{ord}_p b)$, e questo prova la 1). Se fosse $\mathrm{ord}_p a_1 = \mathrm{ord}_p a$, allora $\mathrm{ord}_p b$ dividerebbe $\mathrm{ord}_p a$, da cui $b^{\mathrm{ord}_p a} \equiv 1 \pmod p$. In altri termini, b sarebbe una soluzione dell'equazione congruenziale $X^{\mathrm{ord}_p a} \equiv 1 \pmod p$, la quale evidentemente ammette come soluzioni anche a^i per ogni $i = 1, \ldots, \mathrm{ord}_p a$. Siccome $a^i \not\equiv a^j \pmod p$ per ogni $i, j = 1, \ldots, \mathrm{ord}_p a$ con $i \neq j$, per il Teorema di Lagrange (ved. Teorema 4.19) si dedurrebbe che $b \equiv a^i \pmod p$ per qualche $i = 1, \ldots, \mathrm{ord}_p a$, poiché l'equazione suddetta ha al piú $\mathrm{ord}_p a$ soluzioni. Ma ciò è contro l'ipotesi che $b \in T_{a,p}$. Questo dimostra la 2) e completa la dimostrazione della proposizione. □

Descrizione dell'algoritmo.

Passo 1. Scegliere un intero $a \in S_p^* \setminus \{1\}$ e calcolare $\mathrm{ord}_p a$. Se $\mathrm{ord}_p a = p-1$, allora l'algoritmo termina perché a è una radice primitiva (mod p). Altrimenti risulta $T_{a,p} \neq \emptyset$ e si può procedere con il passo seguente.

Passo 2. Scegliere $b \in T_{a,p}$ e calcolare $\mathrm{ord}_p b$. Se $\mathrm{ord}_p b = p-1$, allora l'algoritmo termina e b è una radice primitiva (mod p). Altrimenti si procede con il passo seguente.

[2]Si osservi che $|xy| = \mathrm{m.c.m}(x, y)\mathrm{MCD}(x, y)$, per interi non nulli x e y qualunque.

Passo 3. Dalla Proposizione 1.1 segue che è possibile determinare un intero a_1 tale che $\mathrm{ord}_p a_1 = \mathrm{m.c.m}(\mathrm{ord}_p a, \mathrm{ord}_p b) > \mathrm{ord}_p a$. Se $\mathrm{ord}_p a_1 = p-1$, allora l'algoritmo termina con esito positivo. Altrimenti si procede tornando al Passo 1, dove si sostituisce a con a_1.

Osservazioni.

1.Non è difficile rendersi conto che l'algoritmo termina con esito positivo dopo un numero finito di passi che ricalcano i tre descritti sopra. Infatti, si verrà a determinare una sequenza finita, $a, a_1, a_2, \ldots, a_s \in S_p^* \setminus \{1\}$, tale che $\mathrm{ord}_p a < \mathrm{ord}_p a_1 < \mathrm{ord}_p a_2 < \ldots < \mathrm{ord}_p a_s = p-1$. Si osservi che la scelta di b nel secondo passo si giustifica con il fatto che vanno evitate le potenze di interi giá testati: se a^i è una radice primitiva, allora lo è anche a, come discende facilmente dalla Proposizione 5.4 (3).

2.Pur essendo molto semplice, in generale l'algoritmo di Gauss si applica efficacemente solo per moduli p tali che $p-1$ abbia fattori primi "sufficientemente piccoli" (e quindi facilmente si determina la fattorizzazione nei primi di $p-1$). Infatti, vanno calcolati ordini di elementi di $S_p^* \setminus \{1\}$ e tali ordini sono divisori di $p-1$. Il problema di determinare la fattorizzazione di un intero è attualmente considerato il problema fondamentale in Teoria Computazionale dei Numeri (ved. [K] e www.crypto-world.com/FactorWorld.html per un costante aggiornamento sui progressi in materia).

3.Il calcolo dell'ordine di un elemento di $S_p^* \setminus \{1\}$ è un caso particolare dello stesso problema in un gruppo finito qualunque. Si veda per questo [C, §1.4] anche per una descrizione alternativa dell'algoritmo per il calcolo di una radice primitiva, anche nel caso in cui il modulo non sia primo. In proposito nel paragrafo successivo riportiamo la dimostrazione del teorema di Gauss (ved. Teorema 5.17) in cui si stabilisce che esiste una radice primitiva modulo $n > 1$ se, e solo se, n è di tipo speciale.

2.Il Teorema di Gauss sull'esistenza di una radice primitiva (mod n)**.**

Diamo la dimostrazione completa del Teorema 5.17 seguendo lo schema degli Esercizi 5.15, 5.16, 5.17 e 5.18 della dispensa (ved. anche [A],[H],[HW]):

Teorema di Gauss. *Esiste una radice primitiva modulo $n > 1$ se, e solo se, $n \in \{2, 4\} \cup \{p^k, 2p^k\}$, dove $k \geq 1$ e p è un primo dispari.*

Dimostrazione.

Non esiste una radice primitiva (mod $n = 2^k$)*, se $k \geq 3$* (ved. Esercizio 5.15).

Basta provare che $a^{\varphi(2^k)/2} \equiv 1 \pmod{2^k}$, per ogni a dispari e per ogni $k \geq 3$. Se $k = 3$, si osservi che $\varphi(2^3)/2 = 2$ e che $(2h+1)^2 = 4h(h+1) + 1 \equiv 1 \pmod 8$. Se si suppone vero l'asserto per $k \geq 3$, allora si ha che $a^{\varphi(2^k)/2} = 1 + 2^k t$ per qualche intero t. Ne segue che $a^{\varphi(2^{k+1})/2} = a^{\varphi(2^k)} = (1 + 2^k t)^2 = 1 + 2^{k+1}t + 2^{2k}t^2 \equiv 1 \pmod{2^{k+1}}$, perché $2k \geq k + 1$. Dunque l'asserto resta provato per induzione.

Non esiste una radice primitiva (mod mn)*, se $m, n \geq 3$ sono coprimi* (ved. Esercizio 5.17).

Basta provare che $a^{\varphi(mn)/2} \equiv 1 \pmod{mn}$, per ogni a coprimo con mn, cioè $(a, m) = (a, n) = 1$. Ricordando che $\varphi(mn) = \varphi(m)\varphi(n)$ ed essendo $\varphi(m) \equiv \varphi(n) \equiv 0 \pmod 2$ per $m, n \geq 3$, dal Teorema di Euler-Fermat (ved. Teorema 3.7) segue

$$a^{\varphi(mn)/2} = (a^{\varphi(m)/2})^{\varphi(n)} \equiv 1 \pmod n\,,\ a^{\varphi(mn)/2} = (a^{\varphi(n)/2})^{\varphi(m)} \equiv 1 \pmod m\,,$$

da cui l'asserto poiché m ed n sono coprimi.

In particolare, da quanto provato sinora, deduciamo che non esiste una radice primitiva modulo n sia quando n ha almeno due fattori primi dispari, sia quando n ha un solo fattore primo dispari ed è divisibile per 4 e sia quando, pur essendo privo di fattori primi dispari, n è divisibile per 8. In altri termini, non esiste una radice primitiva modulo $n > 1$ se $n \notin \{2, 4\} \cup \{p^k, 2p^k\}$, dove $k \geq 1$ e p è un primo dispari.

Se $n \in \{2, 4\}$, allora è facile verificare che 1 e 3 sono radici primitive rispettivamente modulo 2 e modulo 4. Per i casi rimanenti, $n = p^k$ e $n = 2p^k$, osserviamo che essi sono correlati dalla seguente notevole proprietà:

Ogni radice primitiva $r \pmod{p^k}$ *dispari*[3] *è radice primitiva* $\pmod{2p^k}$ (ved. Esercizio 5.18).

Infatti, $\mathrm{ord}_{2p^k} r$ divide $\varphi(2p^k) = \varphi(p^k)$ (ved. Proposizione 5.4 (2)); d'altra parte, per definizione $r^{\mathrm{ord}_{2p^k} r} \equiv 1 \pmod{2p^k}$, da cui $r^{\mathrm{ord}_{2p^k} r} \equiv 1 \pmod{p^k}$. Siccome r è radice primitiva $\pmod{p^k}$, allora $\varphi(p^k) = \varphi(2p^k)$ divide $\mathrm{ord}_{2p^k} r$, cioè $\varphi(2p^k) = \mathrm{ord}_{2p^k} r$.

Se ne deduce che il Teorema di Gauss resta dimostrato non appena si prova l'esistenza di una radice primitiva $\pmod{p^k}$, poichè in tal caso risulta che ne esiste almeno una dispari (se una radice primitiva $r \pmod{p^k}$ non è dispari allora evidentemente lo è $r + p^k$). Il caso $k = 1$ è stato giá dimostrato nel Teorema 5.10 della dispensa. Quindi consideriamo una radice primitiva $r \pmod{p}$. Siccome $\varphi(p^2) = p(p-1) > \varphi(p) = p-1$, una condizione necessaria affinché essa sia una radice primitiva $\pmod{p^2}$ è che

$$r^{p-1} \not\equiv 1 \pmod{p^2} \; . \tag{1}$$

Esiste una radice primitiva $\pmod{p}$ *che soddisfa la* (1) (ved. Esercizio 5.17 (a)).

Infatti, se r non verificasse la (1), allora per qualche intero t si avrebbe[4] $(r+p)^{p-1} = r^{p-1} + (p-1)r^{p-2}p + tp^2 \equiv 1 - pr^{p-2} \pmod{p^2}$. Non potendo essere $r^{p-2} \equiv 0 \pmod{p}$, se ne deduce che $r + p$ soddisfa la (1) (ed è una radice primitiva $\pmod{p}$).

Il passo cruciale della dimostrazione del Teorema è mostrare che la (1) è anche condizione sufficiente affinché una radice primitiva $\pmod{p}$ sia una radice primitiva $\pmod{p^k}$ per ogni $k \geq 1$. Dopodiché, per quanto provato prima, una almeno delle radici primitive r oppure $r + p \pmod{p}$ è una radice primitiva anche $\pmod{2p^k}$ (ved. Esercizio 5.17 (b)) e il Teorema resta completamente dimostrato. Questo ultimo passo viene suddiviso ulteriormente in due. Proviamo che (ved. Esercizio 5.17 (c)):

Se r *è una radice primitiva* $\pmod{p}$ *che soddisfa la* (1), *allora per ogni* $k \geq 2$

$$r^{(p-1)p^{k-2}} \not\equiv 1 \pmod{p^k} \; . \tag{2}$$

Si osservi innanzitutto che la (2) coincide con la (1) per $k = 2$. Se assumiamo soddisfatta la (2) dalla radice primitiva $r \pmod{p}$, per il Teorema di Euler-

[3]Il fatto che r sia dispari assicura che r sia coprimo con $2p^k$, che è una condizione necessaria perché sia una radice primitiva rispetto a tale modulo.

[4]Si applichi la formula del binomio di Newton.

Fermat si ha che esiste un intero t tale che $r^{(p-1)p^{k-2}} = 1 + tp^{k-1}$ e la (2) implica che t non è divisibile per p. Dunque, per qualche intero s si ha che

$$r^{(p-1)p^{k-1}} = (1 + tp^{k-1})^p =$$

$$1 + tp^k + t^2\frac{(p-1)p}{2}p^{2(k-1)} + sp^{3(k-1)} \equiv 1 + tp^k \pmod{p^{k+1}} ,$$

essendo $2k-1, 3(k-1) \geq k+1$. Ricordando che $p \not| t$, si conclude che l'asserto vale anche per $k+1$ e dunque resta completamente provato per induzione.

La dimostrazione si conclude provando che (ved. Esercizio 5.17 (d)):

Se r è una radice primitiva (mod p) *che soddisfa la* (2), *allora r è una radice primitiva* (mod p^k).

Si osservi che $p-1$ divide $\mathrm{ord}_{p^k} r$, poiché $r^{\mathrm{ord}_{p^k} r} \equiv 1 \pmod{p^k}$ implica che $r^{\mathrm{ord}_{p^k} r} \equiv 1 \pmod{p}$. Posto $t(p-1) = \mathrm{ord}_{p^k} r$, si ha che $t(p-1)$ divide $\varphi(p^k) = (p-1)p^{k-1}$ (ved. Proposizione 5.4 (2)), cioè $t = p^s$ con $s \leq k-1$. Se fosse $s \leq k-2$, allora $(p-1)p^{k-2}$ sarebbe un multiplo di $\mathrm{ord}_{p^k} r$ e la (2) non sarebbe verificata. Dunque deve essere $s = k-1$, cioè $\mathrm{ord}_{p^k} r = \varphi(p^k)$. L'asserto, e quindi il Teorema, è dimostrato. □

Corollario 1.2 *Se $n \notin \{2, 4\} \cup \{p^k, 2p^k\}$, dove $k \geq 1$ e p è un primo dispari, allora $a^{\varphi(n)/2} \equiv 1 \pmod{n}$, per ogni a coprimo con n.*

Dimostrazione. Discende immediatamente dal Teorema di Gauss. □

Corollario 1.3 *Se a è coprimo con $n > 2$ e l'equazione $X^2 \equiv a \pmod{n}$ è risolvibile*[5]*, allora esiste una radice primitiva* (mod n) *se, e soltanto se, tale equazione ammette esattamente due soluzioni.*

Dimostrazione. Se esiste una radice primitiva (mod n), allora l'asserto discende immediatamente dal Teorema di Gauss e dal Teorema 5.23 della dispensa. Viceversa, se l'equazione $X^2 \equiv a \pmod{n}$ ammette esattamente due soluzioni, allora esse sono *le* soluzioni anche di $X^2 \equiv a \pmod{p}$, per ogni divisore primo p di n. Alla luce dell'Osservazione 4.2 della dispensa, non è difficile rendersi conto che n deve essere del tipo prescritto dal Teorema di Gauss e quindi deve ammettere una radice primitiva. □

[5]In altri termini, se a è un residuo quadratico (mod n).

3. Somma di potenze (mod n)**.**

Proposizione 3.1. *Sia p primo dispari.*
1) $a \not\equiv 1 \pmod{p} \Rightarrow 1 + a + a^2 + \ldots + a^{\mathrm{ord}_p a - 1} \equiv 0 \pmod{p}$.
2)

$$1^n + 2^n + \ldots + (p-1)^n \equiv \begin{cases} 0 \pmod{p}, & \text{se } (p-1) \not| n, \\ -1 \pmod{p}, & \text{se } (p-1) | n. \end{cases}$$

3) se r è una radice primitiva (mod n)*, con $n > 2$, allora*

$$1 + r + r^2 + \ldots + r^{\varphi(n)-1} \equiv 0 \pmod{n}.$$

Dimostrazione.

1) Posto $S := 1 + a + a^2 + \ldots + a^{\mathrm{ord}_p a - 1}$, osserviamo che $aS \equiv S \pmod{p}$, cioè p divide $(a-1)S$. Siccome $a \not\equiv 1 \pmod{p}$, allora deve essere $S \equiv 0 \pmod{p}$.

2) (ved. Esercizio 5.3) Sia r una radice primitiva (mod p). Posto $S := 1^n + 2^n + \ldots + (p-1)^n$, si ha che $S \equiv 1 + r^n + r^{2n} + \ldots + r^{(p-2)n} \equiv 0 \pmod{p}$. Se $(p-1)|n$, allora $r^n \equiv r^{2n} \equiv \ldots \equiv r^{(p-2)n} \equiv 1 \pmod{p}$, da cui segue che $S \equiv p - 1 \equiv -1 \pmod{p}$. Se $(p-1) \not| n$, allora $r^n \not\equiv 1 \pmod{p}$. Da qui segue l'asserto perché $(1 + r^n + r^{2n} + \ldots + r^{(p-2)n})(r^n - 1) = r^{(p-1)n} - 1 \equiv 0 \pmod{p}$.

3) (ved. Esercizio 5.8) Se $n = p$ allora l'asserto discende dalla 1) della presente proposizione. Se $n = 4$, la verifica è immediata. In accordo con il Teorema di Gauss, restano i casi $n = p^k$, $n = 2p^s$, con p primo dispari, $k \geq 2$ e $s \geq 1$. Se $n = p^k$, notiamo che (ved. Esercizio 5.4):

se r è una radice primitiva (mod p^k)*, con $k \geq 2$, allora r è una radice primitiva* (mod p)*.*

Infatti, posto $h := \mathrm{ord}_p r$, si ha che p divide $r^h - 1$ e quindi anche $1 + r^h + \ldots + r^{h(p-2)} + r^{h(p-1)}$ (tutti i p addendi sono congrui ad 1 (mod p)). Ne segue che $r^{hp} - 1 = (r^h - 1)(1 + r + \ldots + r^{h(p-2)} + r^{h(p-1)}) \equiv 0 \pmod{p^2}$. Procedendo per induzione su k, si conclude che $r^{hp^{k-1}} \equiv 1 \pmod{p^k}$, cioè $\varphi(p^k) = p^{k-1}(p-1)$ divide hp^{k-1}, da cui segue che $h = \mathrm{ord}_p r = p - 1$. Questo prova l'asserto.

Posto $S := 1 + r + r^2 + \ldots + r^{\varphi(n)-1}$, si ha che $(r-1)S = r^{\varphi(n)} - 1 \equiv 0 \pmod{n}$. Nel caso $n = p^k$, abbiamo che p non divide $r - 1$ (perché r è anche una radice primitiva (mod p)). Dunque necessariamente $S \equiv 0 \pmod{p^k}$.

Resta da dimostrare la 3) per $n = 2p^s$, con p primo dispari e $s \geq 1$. Qui notiamo che:

Se r è una radice primitiva (mod $2p^s$)*, allora r è una radice primitiva* (mod p^s).

Infatti, siccome $r \equiv 1 \pmod 2$, allora si ha anche $r^{\mathrm{ord}_{p^s} r} \equiv 1 \pmod 2$; inoltre, per definizione $r^{\mathrm{ord}_{p^s} r} \equiv 1 \pmod{p^s}$, da cui $\mathrm{ord}_{p^s} r$ divide $\varphi(p^s) = \varphi(2p^s)$ (ved. Proposizione 5.4 (2)). Quindi $r^{\mathrm{ord}_{p^s} r} \equiv 1 \pmod{2p^s}$, perché p^s è coprimo con 2. Siccome r è radice primitiva (mod $2p^s$), allora $\varphi(2p^s) = \varphi(p^s)$ divide $\mathrm{ord}_{p^s} r$. In conclusione, $\mathrm{ord}_{p^s} r = \varphi(2p^s) = \varphi(p^s)$, cioè r è anche una radice primitiva (mod p^s).

Tenuto conto che $\varphi(2p^s) = \varphi(p^s) \equiv 0 \pmod 2$ e che $r^i \equiv 1 \pmod 2$ per ogni $i \geq 0$, si ha che S è somma di un numero pari di addendi dispari, cioè $S \equiv 0 \pmod 2$; inoltre, come prima concludiamo che $S \equiv 0 \pmod{p^s}$ (perché r è una radice primitiva (mod p)). Ne segue che $S \equiv 0 \pmod{2p^s}$, perché p^s è coprimo con 2. Questo completa la dimostrazione di 3) e della Proposizione. □

Osservazione. Una piú breve dimostrazione della 3) della Proposizione 3.1 è la seguente. Per $n > 2$, si consideri l'insieme di interi $S_n^* := \{x : \ 1 \leq x \leq n\,,\ (x, n) = 1\}$ (la cui cardinalità è $\varphi(n)$) e si osservi che $a \in S_n^* \Leftrightarrow n - a \in S_n^*$. Quindi

$$\sum_{a \in S_n^*} a = \sum_{a \in S_n^*} (n - a) = n\varphi(n) - \sum_{a \in S_n^*} a \Rightarrow 2 \sum_{a \in S_n^*} a = n\varphi(n)\ .$$

Siccome $\varphi(n) \equiv 0 \pmod 2$ per ogni $n > 2$, allora si ha che

$$\sum_{a \in S_n^*} a \equiv 0 \pmod n\ .$$

Se r è una radice primitiva (mod n), allora (ved. Lemma 5.6)

$$1 + r + r^2 + \ldots + r^{\varphi(n)-1} \equiv \sum_{a \in S_n^*} a \equiv 0 \pmod n.$$

Bibliografia.

[A] T.Apostol, *Introduction to Analytic Number Theory*, 3rd Ed., Springer-Verlag, 1986.

[C] H.Cohen, *A Course in Computational Algebraic Number Theory*, Springer-Verlag, 1993.

[HW] G.H.Hardy, E.M.Wright, *An Introduction to the Theory of Numbers*, 5th. edition, Oxford University Press, 1979.

[H] L.-K.Hua, *Introduction to Number Theory* , Springer-Verlag, 1982.

[K] N.Koblitz, *A Course in Number Theory and Cryptography*, Springer-Verlag, 1987.

Letture consigliate.

R.Crandall, C.Pomerance, *Prime numbers: a computational perspective*, Springer-Verlag, New York, 2001.

H.Davenport, *Aritmetica superiore*, Zanichelli Ed.,Bologna, 1994.

P.Ribenboim, *The New Book of Prime Number Records*, Springer-Verlag, 1996.