Il gruppo moltiplicativo di $\mathbb{Z}/n\mathbb{Z}$

Maurizio Cornalba

31 marzo 2010

Ci proponiamo di studiare $(\mathbb{Z}/n\mathbb{Z})^\times$, dove n è un intero maggiore di 1. Scriviamo $n = p_1^{\ell_1} \cdots p_k^{\ell_k}$, dove $p_1, \ldots, p_k$ sono primi distinti e $\ell_i \geq 1$ per ogni i. Il teorema cinese del resto dice che $\mathbb{Z}/n\mathbb{Z}$ è isomorfo, come anello, al prodotto diretto degli anelli $\mathbb{Z}/p_i^{\ell_i}\mathbb{Z}$, $i = 1, \ldots, k$. Da qui un isomorfismo di gruppi

$$(\mathbb{Z}/n\mathbb{Z})^\times \cong \prod_{i=1}^{k} (\mathbb{Z}/p_i^{\ell_i}\mathbb{Z})^\times$$

Sarà quindi sufficiente determinare la struttura di $(\mathbb{Z}/p^\ell\mathbb{Z})^\times$, dove p è un numero primo e ℓ è un intero ≥ 1. Gli elementi di $(\mathbb{Z}/p^\ell\mathbb{Z})^\times$ sono le classi modulo p^ℓ degli interi primi con p. Ne segue in particolare che l'omomorfismo naturale

$$\rho\colon (\mathbb{Z}/p^\ell\mathbb{Z})^\times \to (\mathbb{Z}/p\mathbb{Z})^\times \tag{1}$$

è suriettivo. Il nucleo di questo omomorfismo è costituito dalle classi modulo p^ℓ degli interi congrui a 1 modulo p, e consta quindi di $p^{\ell-1}$ elementi. Una conseguenza è che

$$\#\,(\mathbb{Z}/p^\ell\mathbb{Z})^\times = (p-1)p^{\ell-1} = p^\ell - p^{\ell-1}$$

Il gruppo $(\mathbb{Z}/2\mathbb{Z})^\times$ è ovviamente il gruppo banale. In tutti gli altri casi la struttura di $(\mathbb{Z}/p^\ell\mathbb{Z})^\times$ è descritta dal seguente risultato.

Teorema 1. a. *Se p è un primo dispari, $(\mathbb{Z}/p^\ell\mathbb{Z})^\times$ è ciclico di ordine $(p-1)p^{\ell-1}$;*

b. *se $\ell \geq 2$, il gruppo $(\mathbb{Z}/2^\ell\mathbb{Z})^\times$ è prodotto diretto di un gruppo ciclico di ordine $2^{\ell-2}$ e di uno di ordine 2.*

Supponiamo che $\ell = 1$. In questo caso $(\mathbb{Z}/p\mathbb{Z})^\times$ è il gruppo moltiplicativo del campo $\mathbb{Z}/p\mathbb{Z}$, e che sia ciclico segue dal seguente risultato più generale.

Proposizione 1. *Se F è un campo, ogni sottogruppo finito di $F^\times$ è ciclico.*

Dato che in un campo l'equazione $X^n = 1$ ha al più n soluzioni, questa proposizione è a sua volta conseguenza immediata del seguente lemma.

Lemma 1. *Sia G un gruppo finito. Supponiamo che, per ogni intero n, vi siano al più n elementi g di G tali che $g^n = 1$. Allora G è ciclico.*

Dimostrazione. Sia G un gruppo finito, non necessariamente soddisfacente l'ipotesi del lemma, e sia m il suo ordine. Sia d un intero positivo. Se vi è un elemento $g \in G$ di ordine d, allora d divide m e g genera un sottogruppo ciclico C di G di ordine d; Inoltre gli elementi di C che hanno ordine d sono i generatori e il loro numero è $\varphi(d)$, dove φ indica la funzione di Eulero. Per ogni divisore d di m indichiamo con $\chi(d)$ il numero degli elementi di G di ordine d. Per quanto osservato $\chi(d) = 0$ oppure $\chi(d) \geq \varphi(d)$. Inoltre, naturalmente,

$$m = \sum_{d \mid m} \chi(d) \tag{2}$$

Nel caso particolare in cui G è ciclico, G contiene un unico sottogruppo di ordine d per ogni divisore d di m, e quindi $\chi(d) = \varphi(d)$ per ogni d. Dunque

$$m = \sum_{d \mid m} \varphi(d) \tag{3}$$

Supponiamo ora che G soddisfi le ipotesi del lemma. Se G contiene un elemento di ordine d, quest'ultimo genera un sottogruppo L di ordine d, tutti i cui elementi x hanno la proprietà che $x^d = 1$. L'ipotesi fatta su G implica quindi che ogni elemento di G di ordine d deve appartenere a L. Ne segue che $\chi(d) = \varphi(d)$. Paragonando la (2) e la (3) se ne deduce che $\chi(d) = \varphi(d)$ per ogni divisore d di $m = \#G$. In particolare $\chi(m) > 0$ e quindi G contiene un elemento di ordine $m = \#G$. □

Passiamo ora alla dimostrazione del teorema 1 per ℓ arbitrario. Indichiamo con G_{p^ℓ} il nucleo della mappa ρ in (1). Per $p \neq 2$, il teorema segue dal seguente risultato intermedio.

Lemma 2. *Se p è un primo dispari, G_{p^ℓ} è ciclico.*

Per dedurre dal lemma la parte a) del teorema 1 possiamo ragionare così. Sia g un elemento di $(\mathbb{Z}/p^\ell\mathbb{Z})^\times$ tale che $\rho(g)$ sia un generatore di $(\mathbb{Z}/p\mathbb{Z})^\times$. L'ordine di g è della forma $(p-1)p^i$, dato che $\rho(g)$ ha ordine $p-1$. Se $i = \ell - 1$, g genera $(\mathbb{Z}/p^\ell\mathbb{Z})^\times$. Se invece $i < \ell - 1$, un generatore di $(\mathbb{Z}/p^\ell\mathbb{Z})^\times$ è $g\gamma$, dove γ è un generatore di G_{p^ℓ}. Infatti, da un lato $\rho(g\gamma) = \rho(g)$ ha ordine $p-1$, e quindi l'ordine di $g\gamma$ è della forma $(p-1)p^j$, dall'altro

$$(g\gamma)^{(p-1)p^{\ell-2}} = g^{(p-1)p^{\ell-2}}\gamma^{(p-1)p^{\ell-2}} = \gamma^{(p-1)p^{\ell-2}} \neq 1$$

Passiamo alla dimostrazione del lemma 2, che si basa su alcuni risultati elementari riguardanti le congruenze tra interi. Il primo di questi è ben noto e ne omettiamo la dimostrazione.

Lemma 3. *Se p è primo e $1 \leq h < p$, il cooefficiente binomiale $\binom{p}{h}$ è un intero divisibile per p.*

Lemma 4. *Siano a, b, ℓ e p interi, con $\ell \geq 1$ e p primo. Se $a \equiv b \mod p^\ell$, allora $a^p \equiv b^p \mod p^{\ell+1}$.*

Dimostrazione. L'ipotesi è che $b = a + kp^\ell$ per qualche intero k. Elevando i due lati alla p-esima potenza si ottiene

$$b^p = a^p + \sum_{i=1}^{p-1} \binom{p}{i} a^{p-i}k^i p^{i\ell} + k^p p^{p\ell}$$

Per il lemma 3, il termine i-esimo della sommatoria è divisibile per $p^{i\ell+1}$, e quindi per $p^{\ell+1}$. Inoltre $p\ell \geq 2\ell \geq \ell + 1$, e quindi anche $k^p p^{p\ell}$ è divisibile per $p^{\ell+1}$. □

Lemma 5. *Siano a, ℓ e p interi. Supponiamo che $\ell \geq 2$ e che p sia un primo dispari. Allora*

$$(1 + ap)^{p^{\ell-2}} \equiv 1 + ap^{\ell-1} \mod p^\ell \tag{4}$$

Dimostrazione. Ragioniamo per induzione su ℓ. Per $\ell = 2$ l'enunciato è ovviamente vero. Supponiamo vera la (4). Elevando alla p-esima potenza i suoi due lati e usando il lemma 4 si ottiene

$$(1 + ap)^{p^{\ell-1}} \equiv (1 + ap^{\ell-1})^p \mod p^{\ell+1} \tag{5}$$

D'altra parte

$$(1+ap^{\ell-1})^p = 1+ap^\ell + \sum_{i=2}^{p-1}\binom{p}{i}a^i p^{i(\ell-1)} + a^p p^{p(\ell-1)}$$

Tutti i termini della sommatoria sono divisibili per $p^{i(\ell-1)+1}$, e quindi per $p^{\ell+1}$; infatti $i(\ell-1)+1 \geq \ell+1$, dato che $i \geq 2$ e $\ell \geq 2$. Anche l'ultimo addendo del lato destro è divisibile per $p^{\ell+1}$, visto che $p(\ell-1) \geq 3\ell-3 = \ell+2\ell-3 \geq \ell+4-3$. In conclusione

$$(1+ap^{\ell-1})^p \equiv 1+ap^\ell \mod p^{\ell+1}$$

Questa congruenza, combinata con la (5), completa il passo induttivo. □

Siamo ora in grado di dimostrare il lemma 2, e quindi la parte a) del teorema 1. Infatti il lemma 5 implica che, se a non è divisibile per p, $(1+ap)^{p^{\ell-2}}$ non è congruo a 1 modulo p^ℓ, e quindi la classe di $1+ap$ in G_{p^ℓ} ha ordine $p^{\ell-1}$.

Resta da dimostrare la parte b) del teorema 1. Chiaramente, il gruppo $(\mathbb{Z}/4\mathbb{Z})^\times$ è ciclico di ordine 2. Possiamo dunque supporre che $\ell \geq 3$. In questo caso useremo il seguente lemma.

Lemma 6. *Per ogni intero $\ell \geq 3$,*

$$5^{2^{\ell-3}} \equiv 1+2^{\ell-1} \mod 2^\ell \tag{6}$$

Dimostrazione. Ragioniamo per induzione. Se $\ell = 3$ non c'è nulla da dimostrare. Elevando al quadrato la (6) si ottiene

$$5^{2^{\ell-2}} \equiv (1+2^{\ell-1})^2 \mod 2^{\ell+1}$$

Inoltre

$$(1+2^{\ell-1})^2 = 1+2^\ell+2^{2\ell-2} \equiv 1+2^\ell \mod 2^{\ell+1}$$

dato che $2\ell-2 \geq \ell+3-2$. Questo completa il passo induttivo. □

La dimostrazione del teorema 1 è completata dal seguente risultato.

Corollario 1. *Se $\ell \geq 3$, il gruppo $(\mathbb{Z}/2^\ell\mathbb{Z})^\times$ è il prodotto diretto del sottogruppo $\{\pm 1\}$ e del sottogruppo generato dalla classe di 5. Quest'ultimo sottogruppo ha ordine $2^{\ell-2}$.*

Dimostrazione. Il lemma 6 mostra che $5^{2^{\ell-2}} \equiv 1 \mod 2^\ell$ ma $5^{2^{\ell-3}} \not\equiv 1 \mod 2^\ell$, cioè che la classe di 5 ha ordine $2^{\ell-2}$. Dato che $(\mathbb{Z}/2^\ell\mathbb{Z})^\times$ ha esattamente $2^{\ell-1}$ elementi, per completare la dimostrazione basta mostrare che l'intersezione tra $\{\pm 1\}$ e il sottogruppo generato dalla classe di 5 è ridotta al solo elemento neutro. In effetti, se la classe di -1 appartenesse al sottogruppo generato dalla classe di 5, si avrebbe che $-1 \equiv 5^b \mod 2^\ell$, e riducendo questa congruenza modulo 4 se ne dedurrebbe che $-1 \equiv 1 \mod 4$, un assurdo. □