Una nota sulle congruenze quadratiche

Cristofer Villani

Durante il Tutorato di Aritmetica del 20 ottobre ho cercato, con scarso successo, di improvvisare la risoluzione di una generica congruenza quadratica. Per completezza, e per chi fosse curioso, riporto qui una versione pensata di quello che cercavo di dire.

Sia p un primo. Siamo interessati a risolvere una generica congruenza della forma

$$ax^2 + bx + c \equiv 0 \pmod{p},$$

dove a, b, c sono numeri interi.

1 Il caso reale

Come riscaldamento, ricordiamo come si ottiene la formula risolutiva di un'equazione di secondo grado

$$ax^2 + bx + c = 0$$

quando a, b, c sono numeri reali, con $a \neq 0$. L'idea è ricondursi a un'equazione senza il termine in x "completando il quadrato". Più precisamente, dividiamo per a e riscriviamo l'equazione come

$$x^2 + \frac{b}{a}x + \left(\frac{b}{2a}\right)^2 - \left(\frac{b}{2a}\right)^2 + \frac{c}{a} = 0,$$

e notiamo che i primi tre termini sono il quadrato di un binomio, per cui l'equazione equivale a

$$\left(x + \frac{b}{2a}\right)^2 = \left(\frac{b}{2a}\right)^2 - \frac{c}{a},$$

vale a dire a

$$(2ax + b)^2 = b^2 - 4ac \tag{1}$$

dopo aver moltiplicato per $4a^2$. A questo punto, chiamando $\Delta = b^2 - 4ac$ e notando che $4a^2$ è sempre un quadrato, otteniamo che

i) se Δ non è un quadrato in $\mathbb{R}$, cioè $\Delta < 0$, non ci sono soluzioni;

ii) se Δ è un quadrato in $\mathbb{R}$, cioè $\Delta \geqslant 0$, le soluzioni sono

$$x = -\frac{b}{2a} \pm \frac{\sqrt{\Delta}}{2a} = \frac{-b \pm \sqrt{\Delta}}{2a},$$

eventualmente coincidenti nel caso $\Delta = 0$.

2 Quadrati (mod p)

La ragione che motiva il completamento del quadrato nel caso reale è che, a differenza di un'equazione generica, un'equazione di secondo grado "pura" è immediatamente risolubile: $x^2 = a$ ha zero soluzioni se $a < 0$, un'unica soluzione se $a = 0$ e esattamente due, i.e. $\pm\sqrt{a}$, se $a > 0$.

Se vogliamo replicare il completamento del quadrato modulo p dobbiamo quindi prima saper risolvere le equazioni della forma $x^2 \equiv a \pmod{p}$, dove a è un intero. In altri termini, dobbiamo contare i quadrati (mod p). Per fortuna, la situazione risulta analoga al caso reale.

Diremo che un intero a è un *quadrato (mod p)* se l'equazione $x^2 \equiv a \pmod{p}$ ha soluzione.

Proposizione 1. *Sia p un primo diverso da 2. Se a è un intero, vale esattamente una delle seguenti:*

i) a *non è un quadrato (mod p);*

ii) $a \equiv 0$ *(mod p), e in tal caso $x^2 \equiv a$ (mod p) ha 0 come unica soluzione (mod p);*

iii) a *è un quadrato (mod p) e $a \not\equiv 0$ (mod p). In tal caso, $x^2 \equiv a$ (mod p) ha esattamente due soluzioni (mod p), della forma $\pm[n]_p$ per qualche $n \in \mathbb{Z}$.*

Dimostrazione. È evidente che ogni $a \in \mathbb{Z}$ o non è un quadrato (mod p), oppure è congruo a zero (mod p), oppure è un quadrato non cogruo a zero (mod p). Nel caso (ii), certamente 0 risolve $x^2 \equiv 0 \pmod{p}$; d'altra parte, $x^2 \equiv 0 \pmod{p}$ se e solo se $p \mid x^2$ ma, siccome p è primo, p divide x^2 se e solo se divide x, cioè $x^2 \equiv 0$ se e solo se $x \equiv 0$.

Resta il caso in cui $a \not\equiv 0 \pmod{p}$ è un quadrato (mod p): allora, esiste $n \in \mathbb{Z}$ tale che $n^2 \equiv a \pmod{p}$. Se $m \in \mathbb{Z}$ è un altro intero tale che $m^2 \equiv a \pmod{p}$, vale

$$n^2 - m^2 \equiv 0 \pmod{p},$$

che equivale a

$$(n-m)(n+m) \equiv 0 \pmod{p},$$

vale a dire

$$p \mid (n-m)(n+m).$$

Di nuovo, siccome p è primo, vale una tra $m \equiv n \pmod{p}$ e $m \equiv -n \pmod{p}$, pertanto le uniche "radici quadrate" di $[a]_p$ sono $[n]_p$ e $-[n]_p$. D'altra parte, sono anche distinte: $n \equiv -n \pmod{p}$ se e solo se $2n \equiv 0 \pmod{p}$ e, poiché $p \neq 2$ ed è primo, ciò implica $n \equiv 0 \pmod{p}$, che contraddice $[a]_p \neq [0]_p$. □

Incidentalmente, questo risultato equivale al punto (i) dell'Esercizio 3.7.38 delle dispense, che risolviamo per completezza.

Esercizio (3.7.38(i))**.** *Se* $p \neq 2$ *è un primo, i quadrati (mod* p*) sono esattamente* $(p+1)/2$*.*

Dimostrazione. Consideriamo la funzione $\varphi : \mathbb{Z}/p\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$ definita da $\varphi(x) = x^2$, e notiamo che il numero di quadrati (mod p) è esattamente $\#\operatorname{im}(\varphi)$, la cardinalità di dell'immagine di φ.

Se $y \in \operatorname{im}(\varphi)$, o $y = [0]_p$, e allora $\varphi^{-1}(y) = \{[0]_p\}$ ha 1 elemento per il punto (ii) della Proposizione 1, oppure $y \neq [0]_p$, nel qual caso $\varphi^{-1}(y)$ ha esattamente 2 elementi per il punto (iii). D'altra parte,

$$\begin{aligned}\mathbb{Z}/p\mathbb{Z} &= \bigsqcup_{y \in \operatorname{im}(\varphi)} \varphi^{-1}(y) \\ &= \varphi^{-1}([0]_p) \sqcup \bigsqcup_{y \in \operatorname{im}(\varphi) \setminus \{[0]_p\}} \varphi^{-1}(y).\end{aligned}$$

Passando alle cardinalità, otteniamo

$$p = 1 + 2 \cdot (\#\operatorname{im}(\varphi) - 1),$$

da cui $\#\operatorname{im}(\varphi) = (p+1)/2$. □

Un'osservazione: la mia dimostrazione della Proposizione 1 e la mia soluzione dell'Esercizio sono, per i miei gusti, profondamente ineleganti. Vi invito a migliorare l'esposizione degli argomenti usati

i) per l'Esercizio, quando avrete parlato di omomorfismi di gruppi;

ii) per la Proposizione, quando avrete dimostrato il Teorema di Ruffini per campi qualsiasi.

3 Il caso (mod p)

Forti del nostro risultato sulle equazioni pure, applichiamo ora la stessa strategia risolutiva del caso reale a una congruenza modulo un primo p, facendo tuttavia attenzione ad adattare correttamente i passaggi in modo coerente con l'aritmetica modulare.

Iniziamo notando che, nel caso reale, la supposizione $a \neq 0$ serve perché vogliamo dividere per a: se vogliamo farlo (mod p), dovremo allora supporre $a \not\equiv 0 (p)$, cioè che p non divida a; siccome, nel procedimento sopra esposto, vogliamo anche poter dividere per 2, dovremo anche supporre che 2 sia invertibile (mod p), cioè $p \neq 2$. In conclusione, **supponiamo nel seguito che** $p \nmid 2a$.

Con questa supposizione, ripetiamo i passaggi fino a (1). L'equazione

$$ax^2 + bx + c \equiv 0 \pmod{p}$$

si riscrive

$$x^2 + (ba^{-1})x + \left(b \cdot (2a)^{-1}\right)^2 - \left(b \cdot (2a)^{-1}\right)^2 + c \cdot a^{-1} \equiv 0 \pmod{p},$$

dove a^{-1} (risp. $(2a)^{-1}$) denota un inverso moltiplicativo di a (risp. $2a$) modulo p, che esiste perché abbiamo supposto $p \nmid 2a$. Raccogliendo e spostando otteniamo

$$\left(x + b \cdot (2a)^{-1}\right)^2 \equiv \left(b \cdot (2a)^{-1}\right)^2 - c \cdot a^{-1} \pmod{p},$$

e moltiplicando per $4a^2$, che è invertibile (mod p) perché p è primo e non divide $2a$, abbiamo finalmente

$$(2ax + b)^2 \equiv b^2 - 4ac \pmod{p}. \tag{2}$$

A questo punto, concludiamo come nel caso reale usando la Proposizione 1. Chiamiamo $\Delta = b^2 - 4ac$ e otteniamo che

i) se Δ *non* è un quadrato (mod p), l'equazione (2) *non* ha soluzioni;

ii) se $\Delta \equiv 0 \pmod{p}$, per il punto (ii) l'equazione (2) equivale a

$$2ax + b \equiv 0 \pmod{p},$$

e pertanto ha l'unica soluzione

$$x \equiv -(2a)^{-1} b \pmod{p};$$

iii) se Δ è un quadrato (mod p), chiamiamo $\sqrt{\Delta}$ *un qualsiasi numero intero* che risolva $x^2 \equiv \Delta \pmod{p}$ [a differenza del caso reale, non c'è nessun modo di scegliere canonicamente una delle due in generale!], e otteniamo che la (2) diventa

$$2ax + b \equiv \pm\sqrt{\Delta} \pmod{p},$$

per il punto (iii) della Proposizione, per cui la soluzione è

$$x \equiv (2a)^{-1}(-b \pm \sqrt{\Delta}) \pmod{p}.$$

Abbiamo ottenuto

Teorema 2. *Siano a, b, c numeri interi e sia p un primo tale che $p \nmid 2a$. L'equazione*

$$ax^2 + bx + c \equiv 0 \ (\textit{mod}\ p)$$

ha soluzione se e solo se $\Delta = b^2 - 4ac$ è un quadrato (mod p). In tal caso, indicando con $\sqrt{\Delta}$ un qualsiasi intero il cui quadrato è congruo a Δ (mod p), la soluzione dell'equazione è data da

$$x \equiv (2a)^{-1}(-b \pm \sqrt{\Delta}) \ (\textit{mod}\ p).$$

4 Qualche esempio

1. Risolviamo l'equazione $3x^2 + x + 1 \equiv 0 \pmod 5$. Vale $\Delta = 1 - 4 \cdot 3 = -11 \equiv -1 \pmod 5$. Siccome -1 è un quadrato (mod 5), e le sue radici quadrate sono ± 2, la soluzione è $x \equiv (2 \cdot 3)^{-1} \cdot (-1 \pm 2) \pmod 5$, vale a dire $x \equiv 1$ o $x \equiv 2 \pmod 5$. Potete verificare direttamente che queste sono le uniche soluzioni.

2. Consideriamo l'esercizio 2.64 delle dispense di Aritmetica 2022/2023. Per quanto la soluzione sia più semplice (la trovate negli appunti del Tutorato), proviamo a risolverlo via il Teorema 2. L'esercizio chiede di mostrare che, per ogni primo p, l'equazione

$$6n^2 + 5n + 1 \equiv 0 \pmod p$$

ha soluzione. Se $p = 2, 3$ non possiamo applicare il Teorema 2, ma è facile concludere a mano. Supponiamo quindi $p \neq 2, 3$: in tal caso, dobbiamo mostrare che Δ è un quadrato (mod p). D'altra parte, $\Delta = 25 - 4 \cdot 6 = 1$, che per fortuna è un quadrato (mod p) per ogni p, e l'esercizio è concluso!