UNITELMA SAPIENZA

SAPIENZA
Università di Roma
Dipartimento di Informatica

Algebra

Alessandro D'Andrea

10. Congruenze quadratiche

Richiami

- $(\mathbb{Z}/n)^{\times}$ è un gruppo rispetto alla moltiplicazione
- Calcolo di potenze modulo n
- Crittografia RSA
- Oggi: **Risolubilità di congruenze quadratiche**
  - Simbolo di Legendre e reciprocità quadratica
  - Algoritmo probabilistico di Solovay-Strassen per stabilire la primalità di un numero (grande)

Congruenze quadratiche

Se vogliamo risolvere una congruenza di secondo grado

$$Ax^2 + Bx + C \equiv 0 \mod n,$$

possiamo sicuramente utilizzare il teorema cinese dei resti e affrontare il problema (potenza di) primo per (potenza di) primo.

Limitiamoci al caso più semplice:

$$x^2 \equiv a \mod p,$$

dove p è un numero primo.

Per quanti e quali valori di a posso aspettarmi di avere soluzioni?

0 è sempre un quadrato

Nella risoluzione di

$$x^2 \equiv a \mod p$$

è rilevante solo la classe di congruenza di a modulo p.

Il caso $\overline{a} = \overline{0}$ è banale. Se $x \not\equiv 0 \mod p$, allora $\overline{x}$, e quindi anche $\overline{x^2}$, è invertibile in $\mathbb{Z}/p$; in particolare, $x^2 \not\equiv 0 \mod p$.

Solo $\overline{0}$ può avere quadrato $\overline{0}$ e quindi la congruenza

$$x^2 \equiv 0 \mod p$$

è equivalente a

$$x \equiv 0 \mod p.$$

Caso invertibile

Nella risoluzione di

$$x^2 \equiv a \mod p$$

possiamo allora supporre che $\overline{a}$ sia invertibile in $\mathbb{Z}/p$; di conseguenza, cerchiamo soluzioni x che siano invertibili modulo p.

Se $\overline{a}$ non è un quadrato in $\mathbb{Z}/p$, allora la congruenza non ha soluzione; viceversa, se $\overline{a} = \overline{b}^2$, allora

$$\begin{aligned} x^2 &\equiv b^2 \mod p \\ x^2 - b^2 &\equiv 0 \mod p \\ (x-b)(x+b) &\equiv 0 \mod p \end{aligned}$$

Sappiamo già che se un prodotto è nullo in $\mathbb{Z}/p$, allora almeno uno dei fattori è nullo. Di conseguenza, la soluzione della congruenza iniziale è

$$x \equiv \pm b \mod p.$$

Residui quadratici mod 7

Rimane il problema di stabilire — possibilmente in modo semplice e veloce — quali classi di congruenza invertibili siano quadrati (gergo: residui quadratici) e quali non lo siano (gergo: non residui) modulo un primo p.

Vediamo, ad esempio, cosa accade modulo 7

$$
\begin{aligned}
1^2 &= 1 \mod 7 \\
2^2 &= 4 \mod 7 \\
3^2 &= 2 \mod 7 \\
4^2 &= 2 \mod 7 \\
5^2 &= 4 \mod 7 \\
6^2 &= 1 \mod 7.
\end{aligned}
$$

Le classi $1, 2, 4$ sono residui quadratici, mentre $3, 5, 6$ non lo sono.

Residui quadratici $\mod p$

Se $p > 2$ è un numero primo, il gruppo $(\mathbb{Z}/p)^\times$ possiede $p - 1$ elementi. Tali elementi, a coppie $\pm b$, forniscono lo stesso quadrato b^2. Coppie distinte forniscono quadrati distinti.

In conclusione, si ottengono $(p - 1)/2$ residui quadratici. Le restanti $(p - 1)/2$ classi sono non residui. Ad esempio, se $p = 7$, ci saranno $3 = (7 - 1)/2$ residui quadratici.

Modulo 11, ci sono 10 classi invertibili. I residui quadratici $1, 3, 4, 5, 9$ sono esattamente $5 = (11 - 1)/2$, così come i non residui $2, 6, 7, 8, 10$.

Simbolo di Legendre - I

Uno strumento utile nello studio di residui e non residui è il simbolo di Legendre:

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{se } a \text{ è un quadrato} \mod p; \\ -1 & \text{se } a \text{ non è un quadrato} \mod p; \\ 0 & \text{se } p \text{ divide } a. \end{cases}$$

Teorema

Si ha

$$\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \mod p.$$

In particolare

$$\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right).$$

Simbolo di Legendre - II

$$\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \mod p.$$

Dimostrazione: se $a \not\equiv 0 \mod p$, sappiamo che

$$a^{p-1} \equiv 1 \mod p.$$

Pertanto $(a^{(p-1)/2})^2 \equiv 1 \mod p$; ma le soluzioni di $x^2 \equiv 1 \mod p$ sono $x = \pm 1$, quindi $a^{(p-1)/2}$ può assumere solo i valori ± 1.

Se $a = b^2$, allora $a^{(p-1)/2} = b^{p-1} \equiv 1 \mod p$, quindi l'espressione assume il valore 1 su tutti i residui quadratici.

Tuttavia l'equazione $x^{(p-1)/2} = 1$ ha al più $(p-1)/2$ soluzioni in $\mathbb{Z}/p$. Sappiamo già che ogni quadrato è soluzione, e i quadrati sono esattamente $(p-1)/2$. Per ogni altro valore di x l'espressione non potrà valere 1, e dovrà quindi valere -1.

Simbolo di Legendre - III

Verifichiamo tutto nel caso $p = 7$. In questo caso $(p-1)/2 = 3$. Allora

$$\begin{aligned}
1^3 \quad\quad\; &= 1 \mod 7 \\
2^3 = 8 \quad &\equiv 1 \mod 7 \\
3^3 = 27 \; &\equiv -1 \mod 7 \\
4^3 = 64 \; &\equiv 1 \mod 7 \\
5^3 = 125 &\equiv -1 \mod 7 \\
6^3 = 216 &\equiv -1 \mod 7.
\end{aligned}$$

Per quali p è un quadrato -1?

La congruenza $x^2 \equiv -1 \mod p$ ammette soluzione esattamente quando

$$\left(\frac{-1}{p}\right) \equiv (-1)^{(p-1)/2} \equiv 1 \mod p.$$

Questo accade quando $(p-1)/2$ è pari, cioè quando $p \equiv 1 \mod 4$.

Fatto: $(p-1)! \equiv -1 \mod p$.

$$\begin{aligned} -1 &\equiv 1 \cdot 2 \cdot \ldots \left(\frac{p-1}{2}\right) \cdot \left(\frac{p+1}{2}\right) \cdot \ldots \cdot (p-2) \cdot (p-1) \\ &\equiv \left(\frac{p-1}{2}\right)! \cdot (-1)^{(p-1)/2} \cdot \left(\frac{p-1}{2}\right)! \end{aligned}$$

Quando $p \equiv 1 \mod 4$,

$$\left(\left(\frac{p-1}{2}\right)!\right)^2 \equiv -1 \mod p.$$

Per quali p è un quadrato 2? - I

Cerchiamo di capire se 2 è un quadrato modulo $p = 103$. NB: $(p-1)/2 = 51$.

$$\begin{aligned}
2^{51} \cdot 51! &= 2 \cdot 4 \cdot 6 \cdot \ldots \cdot 50 \cdot 52 \cdot \ldots \cdot 98 \cdot 100 \cdot 102 \\
&\equiv 2 \cdot 4 \cdot 6 \cdot \ldots \cdot 50 \cdot (-51) \cdot \ldots \cdot (-5) \cdot (-3) \cdot (-1) \\
&\equiv (-1)^{26} 51! \mod 103
\end{aligned}$$

Semplificando,

$$\left(\frac{2}{103}\right) \equiv 2^{(103-1)/2} = 2^{51} \equiv (-1)^{26} = 1 \quad \mod 103,$$

e quindi 2 è un quadrato modulo 103.

Per quali p è un quadrato 2? - II

In generale, si ottiene

$$
\begin{aligned}
2^{(p-1)/2} \cdot \left(\frac{p-1}{2}\right)! &= 2 \cdot 4 \cdot \ldots \cdot (p-3) \cdot (p-1) \\
&\equiv 2 \cdot 4 \cdot \ldots \cdot (-3) \cdot (-1) \\
&\equiv (-1)^{?} \left(\frac{p-1}{2}\right)! \mod p
\end{aligned}
$$

$$
\left(\frac{2}{p}\right) \equiv 2^{(p-1)/2} \equiv (-1)^{\frac{p-1}{2} - \lfloor \frac{p-1}{4} \rfloor} \mod p.
$$

Per quali p è un quadrato 2? - III

$$\left(\frac{2}{p}\right) \equiv 2^{(p-1)/2} \equiv (-1)^{\frac{p-1}{2}-\lfloor\frac{p-1}{4}\rfloor} \mod p$$

sembra complicato.

$$(-1)^{\frac{p-1}{2}-\lfloor\frac{p-1}{4}\rfloor} = \begin{cases} 1 \text{ se } p \equiv \pm 1 \mod 8 \\ -1 \text{ se } p \equiv \pm 3 \mod 8. \end{cases}$$

Si scrive anche

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}.$$

Dal momento che $103 \equiv -1 \mod 8$, allora

$$\left(\frac{2}{103}\right) = 1$$

e quindi 2 è un quadrato modulo 103. ($38^2 = 1444 \equiv 2 \mod 103$)

Reciprocità quadratica

Teorema (di reciprocità quadratica, Gauss)

Se $p \neq q$ sono primi dispari, allora

$$\left(\frac{p}{q}\right) \cdot \left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}} = \begin{cases} -1 \text{ se } p \equiv q \equiv 3 \mod 4 \\ 1 \text{ altrimenti.} \end{cases}$$

37 è un quadrato modulo 107?

$$\left(\frac{37}{107}\right) = \left(\frac{107}{37}\right) = \left(\frac{33}{37}\right) = \left(\frac{3}{37}\right) \cdot \left(\frac{11}{37}\right) = 1,$$

dal momento che

$$\left(\frac{3}{37}\right) = \left(\frac{37}{3}\right) = \left(\frac{1}{3}\right) = 1, \quad \left(\frac{11}{37}\right) = \left(\frac{37}{11}\right) = \left(\frac{4}{11}\right) = \left(\frac{2^2}{11}\right) = 1.$$

$(12^2 = 144 \equiv 37 \mod 107)$