ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ

Σημειώσεις Διαλέξεων

Στοιχεία Θεωρίας Αριθμών
&
Εφαρμογές στην Κρυπτογραφία

Επιμέλεια σημειώσεων:
Διονύσης ΖΗΝΔΡΟΣ
Αντώνης ΑΝΑΣΤΑΣΟΠΟΥΛΟΣ

Διδάσκοντες:
Στάθης ΖΑΧΟΣ
Άρης ΠΑΓΟΥΡΤΖΗΣ

2 Δεκεμβρίου 2011

Επίλυση γραμμικής ισοτιμίας

Ζητείται να λυθεί η ισοτιμία ως προς x:

$$ax \equiv b \pmod{n}$$

Για παράδειγμα:

$$4x \equiv 6 \pmod{7}$$

Καθώς βρισκόμαστε σε αριθμητική modulo, μπορούμε να δοκιμάσουμε εξαντλητικά τις πιθανές λύσεις:

$$4\mathbb{Z}_7 = \{0, 4, 1, 5, 2, 6, 3\}$$

Πράγματι η μοναδική λύση της ισοτιμίας είναι:

$$x \equiv 5 \pmod{7}$$

Λήμμα. *Η ισοτιμία* $ax \equiv b \pmod{n}$ *έχει μοναδική λύση όταν* $\gcd(a, n) = 1$.

Απόδειξη. Πράγματι, υπάρχει η λύση $x \equiv a^{-1}b \pmod{n}$. Έστω τώρα ότι υπάρχουν λύσεις x, x'. Τότε έχουμε:

$$\begin{aligned}
\begin{cases} ax & \equiv b \pmod{n} \\ ax' & \equiv b \pmod{n} \end{cases} & \Rightarrow ax \equiv ax' \pmod{n} \\
& \Leftrightarrow n | a(x - x') \\
& \Leftrightarrow n | (x - x') \\
& \Leftrightarrow x \equiv x' \pmod{n}
\end{aligned}$$

$\square$

Το αποτέλεσμα αυτό δεν ισχύει απαραίτητα όταν $\gcd(a, n) \neq 1$. Για παράδειγμα η εξής ισοτιμία δεν έχει λύση:

$$10x \equiv 6 \pmod{35}$$

Πράγματι, θα είναι:

$$10\mathbb{Z}_{35} = \{0, 10, 20, 30, 5, 15, 25, 0, 10, 20, 30, \dots\}$$

Ενώ για παράδειγμα η εξής ισοτιμία έχει πολλές λύσεις:

$$10x \equiv 30 \pmod{35}$$

Λήμμα. *Έστω* $d = \gcd(a, n) > 1$. *Η ισοτιμία* $ax \equiv b \pmod{n}$ *έχει ακριβώς* d *λύσεις ανν* $d|b$. *Διαφορετικά δεν έχει λύσεις.*

Απόδειξη. Θα δείξουμε ότι $\exists x \Rightarrow d|b$. Πράγματι:

$$\begin{aligned} & ax \equiv b \pmod{n} \\ \Leftrightarrow & n|(ax-b) \\ \Rightarrow & d|(ax-b) \\ \Rightarrow & d|b \end{aligned}$$

Αντίστροφα έχουμε:

$$\begin{aligned} & ax \equiv b \pmod{n} \\ \Leftrightarrow & n|(ax-b) \\ \Leftrightarrow & \exists \lambda \in \mathbb{Z} : ax - b = \lambda n \\ \Leftrightarrow & \exists \lambda \in \mathbb{Z} : \frac{a}{d}x - \frac{b}{d} = \lambda \frac{n}{d} \\ \Leftrightarrow & \frac{n}{d}|(\frac{a}{d}x - \frac{b}{a}) \\ \Leftrightarrow & \frac{a}{d}x \equiv \frac{a}{d}x \equiv \frac{b}{d} \pmod{\frac{n}{d}} \end{aligned}$$

Άρα η μοναδική λύση στο $\mathbb{Z}_{\frac{n}{d}}$ θα είναι η:

$$x_0 \equiv (\frac{a}{d})^{-1}_{\pmod{\frac{n}{d}}} \frac{b}{d} \pmod{\frac{n}{d}}$$

Συνεπώς οι λύσεις στο $\mathbb{Z}_n$ θα είναι οι εξής d:

$$\{x_0 + i\frac{n}{d} : 0 \leq i < d\}$$

$\square$

Λήμμα. *Απαλοιφής*

$$ax \equiv ax' \pmod{n} \Leftrightarrow x \equiv x' \pmod{\frac{n}{\gcd(a,n)}}$$

Επίλυση τετραγωνικής ισοτιμίας

Ζητείται να λυθεί η ισοτιμία ως προς x:

$$ax^2 \equiv b \pmod{n}$$

Θα εξετάσουμε την περιπτωση:

$$x^2 \equiv b \pmod{n}$$

Λήμμα. *Έστω ότι $n = p$ πρώτος. Τότε αν η ισοτιμία $x^2 \equiv b \pmod{n}$ έχει λύσεις, τότε αυτές είναι ακριβώς 2 και μεταξύ τους αντίθετες.*

Απόδειξη. Έστω x και y δύο διαφορετικές λύσεις της ισοτιμίας.

$$\begin{aligned} & x^2 \equiv y^2 \pmod p \\ \Leftrightarrow & p|(x-y)(x+y) \\ \Leftrightarrow & p|(x-y) \lor p|(x+y) \\ \Leftrightarrow & x \equiv y \pmod p \lor x \equiv -y \pmod p \end{aligned}$$

□

Λήμμα. *Έστω ότι n γινόμενο δύο πρώτων $n = pq$. Τότε αν η ισοτιμία $x^2 \equiv b \pmod n$ έχει λύσεις, τότε αυτές είναι ακριβώς 2 ή 4 και θα είναι μεταξύ τους ανά 2 αντίθετες.*

Απόδειξη. Έστω λύσεις της ισοτιμίας x και y. Τότε παρόμοια με παραπάνω θα έχουμε:

$$\begin{cases} & p|(x-y) \land q|(x+y) \\ \lor & p|(x-y) \land q|(x-y) \\ \lor & p|(x+y) \land q|(x+y) \\ \lor & p|(x+y) \land q|(x-y) \end{cases}$$

$$\Leftrightarrow \begin{cases} x \equiv \pm y \pmod p \\ \land x \equiv \pm y \pmod q \end{cases}$$

□

Για παραδειγμα:

$$\begin{aligned} & x^2 \equiv 29 \pmod{35} \\ \Rightarrow & \begin{cases} x^2 \equiv 29 \pmod 5 \\ x^2 \equiv 29 \pmod 7 \end{cases} \\ \Rightarrow & \begin{cases} x^2 \equiv 4 \pmod 5 \\ x^2 \equiv 1 \pmod 7 \end{cases} \\ \Rightarrow & \begin{cases} x \equiv \pm 2 \pmod 5 \\ x \equiv \pm 1 \pmod 7 \end{cases} \\ \Rightarrow & x \equiv \begin{cases} 22 \\ 27 \\ 8 \\ 13 \end{cases} \pmod{35} \end{aligned}$$

Στα παραπάνω θεωρήματα η λύση 0 θεωρείται διπλή.

Ασκήσεις

1. Να αποδειχθεί το Λήμμα Απαλοιφής.