Διακριτά Μαθηματικά ΙΙ

Χρήστος Νομικός

Τμήμα Μηχανικών Η/Υ και Πληροφορικής
Πανεπιστήμιο Ιωαννίνων

MMXXIII

Περιεχόμενα

1 Θεωρία Αριθμών

Περιεχόμενα

1 Θεωρία Αριθμών

Θα ασχοληθούμε με την επίλυση ισοτιμιών της μορφής:

$$a \cdot x \equiv b \ (mod \ m)$$

όπου a, b, m είναι ακέραιοι αριθμοί, με $a \neq 0$ και $m > 1$.

Όταν έχουμε την αντίστοιχη εξίσωση στους πραγματικούς αριθμούς:

$$a \cdot x = b$$

όπου $a \neq 0$, τότε η λύση προκύπτει πολλαπλασιάζοντας τα δύο μέλη της ισότητας με τον αντίστροφο του a.

$$a^{-1} \cdot a \cdot x = a^{-1} \cdot b \Leftrightarrow x = a^{-1} \cdot b$$

Στην περίπτωση των ισοτιμιών, τα πράγματα είναι λίγο διαφορετικά, καθώς ενδέχεται να μην υπάρχει ο αντίστροφος του a modulo m και η ισοτιμία $a \cdot x \equiv b \ (mod \ m)$ να μην έχει λύση.

Παράδειγμα

Η ισοτιμία $2 \cdot x \equiv 3 \ (mod\ 4)$ δεν έχει λύση.

Πράγματι

- αν $x \bmod 4 = 0$, τότε
  $(2 \cdot x) \bmod 4 = (2 \cdot (x \bmod 4)) \bmod 4 = (2 \cdot 0) \bmod 4 = 0$
- αν $x \bmod 4 = 1$, τότε
  $(2 \cdot x) \bmod 4 = (2 \cdot (x \bmod 4)) \bmod 4 = (2 \cdot 1) \bmod 4 = 2$
- αν $x \bmod 4 = 2$, τότε
  $(2 \cdot x) \bmod 4 = (2 \cdot (x \bmod 4)) \bmod 4 = (2 \cdot 2) \bmod 4 = 0$
- αν $x \bmod 4 = 3$, τότε
  $(2 \cdot x) \bmod 4 = (2 \cdot (x \bmod 4)) \bmod 4 = (2 \cdot 3) \bmod 4 = 2$

Παράδειγμα (συνέχεια)

Συνεπώς για κάθε ακέραιο x ισχύει $(2 \cdot x) \bmod m \neq 3$ και άρα $2 \cdot x \not\equiv 3 \ (mod\ 4)$.

Αυτό οφείλεται στο ότι δεν υπάρχει ακέραιος $\bar{a}$ τέτοιος ώστε $\bar{a} \cdot 2 = 1 \ (mod\ 4)$.

Το παρακάτω θεώρημα μας εξασφαλίζει ότι αν οι αριθμοί a και m είναι σχετικά πρώτοι, τότε η ισοτιμία $a \cdot x \equiv b \ (mod \ m)$ έχει πάντα μοναδική λύση modulo m.

Θεώρημα

Έστω δύο ακέραιοι αριθμοί $a \neq 0$ και $m > 1$, τέτοιοι ώστε $gcd(a, m) = 1$. Τότε υπάρχει ένας μοναδικός θετικός ακέραιος $\bar{a}$ μικρότερος του m τέτοιος ώστε $(\bar{a} \cdot a) \bmod m = 1$. Ο $\bar{a}$ ονομάζεται αντίστροφος του a modulo m. Επιπλέον για κάθε ακέραιο x τέτοιον ώστε $\bar{a} \equiv x \ (mod\ m)$ ισχύει $(x \cdot a) \bmod m = 1$.

Απόδειξη

Γνωρίζουμε ότι υπάρχουν ακέραιοι s και t τέτοιοι ώστε $s \cdot a + t \cdot m = gcd(a, m) = 1$.

Άρα $(s \cdot a + t \cdot m) \bmod m = 1$

Όμως $(s \cdot a + t \cdot m) \bmod m = ((s \cdot a) \bmod m + (t \cdot m) \bmod m) \bmod m = ((s \cdot a) \bmod m + 0) \bmod m = (s \cdot a) \bmod m$.

Από τα παραπάνω προκύπτει ότι $(s \cdot a) \bmod m = 1$.

Άρα $((s \bmod m) \cdot a) \bmod m = 1$.

Απόδειξη (συνέχεια)

Ο αντίστροφος του a modulo m είναι ο αριθμός $\bar{a} = (s \bmod m)$.

Επειδή $0 \cdot a \bmod m = 0 \neq 1$, ισχύει $\bar{a} \neq 0$ και άρα ο $\bar{a}$ πράγματι θετικός αριθμός μικρότερος του m.

Απόδειξη (συνέχεια)

Για να δείξουμε ότι ο $\bar{a}$ είναι μοναδικός, ας θεωρήσουμε έναν θετικό ακέραιο $b < m$ τέτοιο ώστε $(b \cdot a) \bmod m = 1$.

Τότε ισχύει $\bar{a} \cdot a \equiv b \cdot a \ (mod\ m)$ που συνεπάγεται $m \mid (\bar{a} \cdot a) - (b \cdot a)$ ή ισοδύναμα $m \mid (\bar{a} - b) \cdot a$.

Επειδή $gcd(a, m) = 1$, η τελευταία σχέση συνεπάγεται ότι $m \mid \bar{a} - b$. Αυτό όμως συνεπάγεται $\bar{a} = b$, επειδή $0 \leq \bar{a}, b < m$.

Απόδειξη (συνέχεια)

Τέλος έστω ακέραιος x τέτοιος ώστε $\bar{a} \equiv x \ (mod \ m)$.

Τότε, $(x \cdot a) \bmod m = ((x \bmod m) \cdot a) \bmod m = (\bar{a} \cdot a) \bmod m = 1$. □

Για να επιλύσουμε την ισοτιμια $a \cdot x \equiv b \ (mod \ m)$ όπου $a \neq 0, b, m > 1$ είναι ακέραιοι αριθμοί, τέτοιοι ώστε $gcd(a, m) = 1$, αρκεί να βρούμε τον αντίστροφο $\bar{a}$ του a modulo m.

Έχουμε

$$\begin{aligned} a \cdot x \equiv b \ (mod \ m) &\Leftrightarrow \bar{a} \cdot a \cdot x \equiv \bar{a} \cdot b \ (mod \ m) \\ &\Leftrightarrow x \equiv \bar{a} \cdot b \ (mod \ m) \\ &\Leftrightarrow x \bmod m = (\bar{a} \cdot b) \bmod m \\ &\Leftrightarrow x = (\bar{a} \cdot b) \bmod m + q \cdot m \text{ για κάποιο } q \in \mathbb{Z} \end{aligned}$$

Για μικρές τιμές του m, η εύρεση του $\overline{a}$ μπορεί να γίνει με εξαντλητική αναζήτηση.

Για μεγαλύτερες τιμές του m, μπορούμε να υπολογίσουμε τους συντελεστές Bézout s και t εκτελώντας τον αλγόριθμο του Ευκλείδη και να θέσουμε $\overline{a} = s \bmod m$.

Παράδειγμα

Θα λύσουμε την ισοτιμία $5 \cdot x \equiv 2 \ (mod\ 7)$.

Έχουμε $(1 \cdot 5) \bmod 7 = 5$, $(2 \cdot 5) \bmod 7 = 3$ και $(3 \cdot 5) \bmod 7 = 1$. Άρα ο αντίστροφος του 5 modulo 7 είναι το 3.

Συνεπώς η δεδομένη ισοτιμία είναι ισοδύναμη με
$x \equiv 3 \cdot 2 \ (mod\ 7) \Leftrightarrow x \equiv 6 \ (mod\ 7)$.

Οι ακέραιοι που ικανοποιούν την παραπάνω ισοτιμία είναι οι ακέραιοι της μορφής $x = 6 + q \cdot 7$, όπου $q \in \mathbb{Z}$.

Παράδειγμα

Θα λύσουμε την ισοτιμία $203 \cdot x \equiv 64 \ (mod\ 507)$.

Επειδή το 507 είναι αρκετά μεγάλο, θα υπολογίσουμε το αντίστροφο του 203 modulo 507, βρίσκοντας τους συντελεστές Bézout s και t με τον αλγόριθμο του Ευκλείδη.

Παράδειγμα (συνέχεια)

Υπολογίζουμε τις τιμές a_i και b_i από πάνω προς τα κάτω και στη συνέχεια τις τιμές s_i και t_i από κάτω προς τα πάνω.

i	a_i	b_i	s_i	t_i
0	203	507	$1-(507 \text{ div } 203)\cdot(-2)=5$	-2
1	203	$507 \bmod 203 = 101$	1	$0-(203 \text{ div } 101)\cdot 1=-2$
2	$203 \bmod 101 = 1$	101	$1-(101 \text{ div } 1)\cdot 0=1$	0
3	1	$101 \bmod 1 = 0$	1	0

Συνεπώς για τις τιμές $s=5$ και $t=-2$ ισχύει $s\cdot 203+t\cdot 507=1$.

Παράδειγμα

Έχουμε $5 \cdot 203 - 2 \cdot 507 = 1$ που συνεπάγεται $5 \cdot 203 \bmod 507 = 1$. Άρα ο αντίστροφος του 203 modulo 507 είναι το 5.

Συνεπώς η δεδομένη ισοτιμία είναι ισοδύναμη με
$x \equiv 5 \cdot 64 \ (mod\ 507) \Leftrightarrow x \equiv 320 \ (mod\ 507)$.

Οι ακέραιοι που ικανοποιούν την παραπάνω ισοτιμία είναι οι ακέραιοι της μορφής $x = 320 + q \cdot 507$, όπου $q \in \mathbb{Z}$.

Στη συνέχεια θα δούμε πώς μπορούμε να επιλύσουμε συστήματα ισοτιμιών της μορφής

$$\begin{aligned} x &\equiv a_1 \ (mod \ m_1) \\ x &\equiv a_2 \ (mod \ m_2) \\ &\dots \\ x &\equiv a_k \ (mod \ m_k) \end{aligned}$$

Λήμμα

Έστω $m_1, m_2, \ldots, m_k$ ακέραιοι αριθμοί μεγαλύτεροι από το 1, οι οποίοι είναι ανά δύο σχετικά πρώτοι, και $a_1, a_2, \ldots, a_k$ οποιοιδήποτε ακέραιοι αριθμοί. Αν το σύστημα ισοτιμιών

$$\begin{aligned} x &\equiv a_1 \ (mod\ m_1) \\ x &\equiv a_2 \ (mod\ m_2) \\ &\ldots \\ x &\equiv a_k \ (mod\ m_k) \end{aligned}$$

ικανοποιείται από μία ακέραια τιμή $x = r$, τότε ικανοποιείται και για κάθε ακέραια τιμή $x = s$ με $r \equiv s \ (mod\ m)$, όπου $m = m_1 \cdot m_2 \cdot \cdots \cdot m_k$.

Απόδειξη

Έστω ότι η τιμή $x = r$ ικανοποιεί το σύστημα ισοτιμιών, δηλαδή για κάθε i, ισχύει $r \equiv a_i \ (mod \ m_i)$.

Αν $s \equiv r \ (mod \ m)$, τότε ισχύει $m \mid (s - r)$ και επειδή $m_i \mid m$, προκύπτει ότι $m_i \mid (s - r)$.

Η τελευταία σχέση συνεπάγεται ότι $s \equiv r \ (mod \ m_i)$ και άρα $s \equiv a_i \ (mod \ m_i)$.

Συνεπώς αν $s \equiv r \ (mod \ m)$, τότε το s ικανοποιεί επίσης το σύστημα ισοτιμιών. □

Κινέζικο Θεώρημα Υπολοίπων

Έστω $m_1, m_2, \ldots, m_k$ ακέραιοι αριθμοί μεγαλύτεροι από το 1, οι οποίοι είναι ανά δύο σχετικά πρώτοι, και $a_1, a_2, \ldots, a_k$ οποιοιδήποτε ακέραιοι αριθμοί. Τότε το σύστημα ισοτιμιών

$$\begin{aligned} x &\equiv a_1 \ (mod\ m_1) \\ x &\equiv a_2 \ (mod\ m_2) \\ &\ldots \\ x &\equiv a_k \ (mod\ m_k) \end{aligned}$$

έχει μοναδική λύση n στο σύνολο $\mathbb{Z}_m = \{0, 1, \ldots, m-1\}$, όπου $m = m_1 \cdot m_2 \cdot \cdots \cdot m_k$. Επιπλέον για κάθε ακέραιο αριθμό z ισχύει ότι το z ικανοποιεί το σύστημα ισοτιμιών αν και μόνο αν $z \equiv n \ (mod\ m)$.

Απόδειξη

Έστω $M_j = m \text{ div } m_j$, για κάθε j, $1 \leq j \leq k$.

Ισχύει $M_j = m_1 \cdot m_2 \cdot \cdots \cdot m_{j-1} \cdot m_{j+1} \cdot \cdots \cdot m_k$ και άρα $M_j \bmod m_i = 0$, αν $i \neq j$.

Επίσης $gcd(m_j, M_j) = 1$. Πράγματι, αν οι m_j και M_j έχουν έναν κοινό διαιρέτη $d > 1$ τότε διαιρούνται και από κάποιον πρώτο αριθμό p. Αυτό όμως συνεπάγεται ότι ο p θα πρέπει να διαιρεί κάποιο m_i, με $i \neq j$. Τότε όμως ο p είναι κοινός διαιρέτης των m_j και m_i, το οποίο αντίκειται στην υπόθεση ότι οι m_j και m_i είναι σχετικά πρώτοι.

Επειδή $gcd(m_j, M_j) = 1$, υπάρχει ο αντίστροφος y_j του M_j modulo m_j.

Απόδειξη (συνέχεια)

Θέτουμε $r = a_1 \cdot y_1 \cdot M_1 + a_2 \cdot y_2 \cdot M_2 + \cdots + a_k \cdot y_k \cdot M_k$

Για $i \neq j$ ισχύει $M_j \bmod m_i = 0$, που συνεπάγεται
$a_j \cdot y_j \cdot M_j \bmod m_i = 0$.

Άρα για κάθε i, $1 \leq i \leq n$

$$\begin{aligned}
r \bmod m_i &= (a_1 \cdot y_1 \cdot M_1 + a_2 \cdot y_2 \cdot M_2 + \cdots + a_k \cdot y_k \cdot M_k) \bmod m_i \\
&= ((a_1 \cdot y_1 \cdot M_1) \bmod m_i + (a_2 \cdot y_2 \cdot M_2) \bmod m_i + \ldots \\
&\quad + (a_k \cdot y_k \cdot M_k) \bmod m_i) \bmod m_i \\
&= (a_i \cdot y_i \cdot M_i) \bmod m_i \\
&= ((a_i \bmod m_i) \cdot ((y_i \cdot M_i) \bmod m_i)) \bmod m_i \\
&= ((a_i \bmod m_i) \cdot 1) \bmod m_i \\
&= a_i \bmod m_i
\end{aligned}$$

Απόδειξη (συνέχεια)

Άρα για κάθε i, ισχύει $r \equiv a_i \ (mod \ m_i)$. Συνεπώς το r ικανοποιεί το σύστημα των ισοτιμιών.

Από το προηγούμενο λήμμα, προκύπτει ότι ο αριθμός $n = r \bmod m$ ικανοποιεί το σύστημα ισοτιμιών. Επιπλέον $n \in \mathbb{Z}_m$.

Απόδειξη (συνέχεια)

Για να δείξουμε ότι ο αριθμός n είναι η μοναδική λύση του συστήματος ισοτιμιών η οποία ανήκει στο σύνολο $\mathbb{Z}_m$, παρατηρούμε ότι για δεδομένες τιμές των $m_1, m_2, \ldots, m_k$ υπάρχουν m_i διαφορετικές τιμές του a_i, τέτοιες ώστε $0 \leq a_i < m_i$.

Το συνολικό πλήθος συστημάτων ισοτιμιών που μπορούμε να κατασκευάσουμε για τις δεδομένες τιμές των $m_1, m_2, \ldots, m_k$ έτσι ώστε $0 \leq a_i < m_i$ για όλα τα i είναι $m_1 \cdot m_2 \cdot \cdots \cdot m_k = m$.

Απόδειξη (συνέχεια)

Κάθε ένα από τα παραπάνω συστήματα όπως δείξαμε έχει μία λύση που ανήκει στο σύνολο $\mathbb{Z}_m$.

Επιπλέον, κάθε ακέραιος x μπορεί να αποτελεί λύση μόνο για ένα από τα παραπάνω συστήματα ισοτιμιών, καθώς αν ικανοποιεί ένα σύστημα ισοτιμιών, τότε τα υπόλοιπα της διαίρεσής του με τους αριθμούς $m_1, m_2, \ldots, m_k$ θα πρέπει να ταυτίζονται μετα $a_1, a_2, \ldots, a_k$ του συστήματος αυτού.

Αν κάποιο από τα παραπάνω m συστήματα είχε περισσότερες από μία λύσεις στο σύνολο $\mathbb{Z}_m$, επειδή κανένας αριθμός του συνόλου δεν αποτελεί λύση δύο διαφορετικών συστημάτων, το πλήθος των στοιχείων του $\mathbb{Z}_m$ θα έπρεπε να είναι μεγαλύτερο του m, το οποίο είναι άτοπο.

Απόδειξη (συνέχεια)

Συνεπώς το n είναι η μοναδική λύση του συστήματος ισοτιμιών η οποία ανήκει στο σύνολο $\mathbb{Z}_m$.

Επιπλέον κάθε αριθμός στο σύνολο $\mathbb{Z}_m$ ικανοποιεί κάποιο από τα παραπάνω m συστήματα ισοτιμιών.

Απόδειξη (συνέχεια)

Τέλος, έστω ένας οποιοσδήποτε ακέραιος αριθμός z.

Αν $z \equiv n \ (mod \ m)$, τότε από το προηγούμενο λήμμα προκύπτει ότι ο z ικανοποιεί το σύστημα ισοτιμιών.

Αν $z \not\equiv n \ (mod \ m)$, ο αριθμός $z \bmod m$ ικανοποιεί ένα διαφορετικό σύστημα ισοτιμών από τα m που περιγράψαμε παραπάνω, το οποίο από το προηγούμενο λήμμα ικανοποιεί και ο z. Επειδή όπως δείξαμε κάθε ακέραιος μπορεί να ικανοποιεί μόνο ένα από τα m συστήματα ισοτιμιών, συμπεραίρουμε ότι ο z δεν ικανοποιεί το δεδομένο σύστημα ισοτιμιών. □

Παράδειγμα

Θα λύσουμε το παρακάτω σύστημα ισοτιμιών:

$$x \equiv 1 \ (mod\ 4)$$
$$x \equiv 4 \ (mod\ 5)$$
$$x \equiv 2 \ (mod\ 9)$$

Έχουμε $a_1 = 1$, $a_2 = 4$, $a_3 = 2$, $m_1 = 4$, $m_2 = 5$, $m_3 = 9$ και $m = 4 \cdot 5 \cdot 9 = 180$.

Παράδειγμα (συνέχεια)

Υπολογίζουμε τα $M_1 = 5 \cdot 9 = 45$, $M_2 = 4 \cdot 9 = 36$ και $M_3 = 4 \cdot 5 = 20$.

Βρίσκουμε το αντίστροφο y_1 του $M_1 = 45$ modulo 4. Έχουμε $(1 \cdot 45) \bmod 4 = 1$, άρα $y_1 = 1$.

Βρίσκουμε το αντίστροφο y_2 του $M_2 = 36$ modulo 5. Έχουμε $(1 \cdot 36) \bmod 5 = 1$, άρα $y_2 = 1$.

Βρίσκουμε το αντίστροφο y_3 του $M_3 = 20$ modulo 9. Έχουμε $(5 \cdot 20) \bmod 9 = 1$, άρα $y_3 = 5$.

Παράδειγμα (συνέχεια)

Η μοναδική λύση του συστήματος ισοτιμιών η οποία ανήκει στο σύνολο $\mathbb{Z}_{180}$ είναι ο αριθμός

$$\begin{aligned} n &= (a_1 \cdot y_1 \cdot M_1 + a_2 \cdot y_2 \cdot M_2 + a_3 \cdot y_3 \cdot M_3) \bmod 180 \\ &= (1 \cdot 1 \cdot 45 + 4 \cdot 1 \cdot 36 + 2 \cdot 5 \cdot 20) \bmod 180 \\ &= (45 + 144 + 200) \bmod 180 \\ &= 389 \bmod 180 \\ &= 29 \end{aligned}$$

Συνεπώς ακέραιοι που ικανοποιούν το δεδομένο σύστημα ισοτιμιών είναι οι ακέραιοι z για τους οποίους ισχύει $x \equiv 29 \ (mod\ 180)$.

Οι ακέραιοι που ικανοποιούν την παραπάνω ισοτιμία είναι οι ακέραιοι της μορφής $z = 29 + q \cdot 180$, όπου $q \in \mathbb{Z}$.

Το επόμενο θεώρημα, το οποίο δίνεται χωρίς απόδειξη, μπορεί να χρησιμοποιηθεί για να υπολογίσουμε δυνάμεις με μεγάλους εκθέτες ενός αριθμού a modulo έναν πρώτο αριθμό p στην περίπτωση που ο p δεν διαιρεί το a

Μικρό Θεώρημα του Fermat

Έστω p ένας πρώτος αριθμός και a ένας ακέραιος αριθμός. Ισχύουν οι τα παρακάτω:

- Αν ο p δεν διαιρεί τον a τότε $a^{p-1} \bmod p = 1$.
- $a^p \bmod p = a \bmod p$.

Παράδειγμα

Θα υπολογίσουμε το $8^{12569} \bmod 13$, με τη βοήθεια του παραπάνω θεωρήματος.

Έχουμε $12569 \text{ div } 12 = 1047$ και $12575 \bmod 12 = 5$.

Παράδειγμα

Άρα

$$\begin{aligned} 8^{12569} &= 8^{1047\cdot 12+5} \\ &= 8^{1047\cdot 12} \cdot 8^5 \\ &= (8^{12})^{1047} \cdot 8^5 \\ &\equiv 1^{1047} \cdot 8^5 \\ &\equiv 8^5 \ (mod\ 13) \end{aligned}$$

λαμβάνοντας υπόψη ότι $8^{12} \equiv 1\ (mod\ 13)$, όπως προκύπτει από το μικρό θεώρημα του Fermat.

Παράδειγμα (συνέχεια)

Έχουμε

$8^2 \bmod 13 = 64 \bmod 13 = 12.$

$8^3 \bmod 13 = (8 \cdot 8^2) \bmod 13 = ((8 \bmod 13) \cdot (8^2 \bmod 13)) \bmod 13 = (8 \cdot 12) \bmod 13 = 96 \bmod 13 = 5.$

$8^5 \bmod 13 = (8^3 \cdot 8^2) \bmod 13 = ((8^3 \bmod 13) \cdot (8^2 \bmod 13)) \bmod 13 = (5 \cdot 12) \bmod 13 = 60 \bmod 13 = 8.$

Άρα $8^{12569} \bmod 13 = 8^5 \bmod 13 = 8.$

Η ιδεα που εφαρμόστηκε στο προηγούμενο παράδειγμα γενικεύεται στο επόμενο πόρισμα.

Πόρισμα

Έστω p ένας πρώτος αριθμός, a ένας ακέραιος αριθμός και n ένας μη αρνητικός ακέραιος αριθμός. Αν ο p δεν διαιρεί το a τότε $a^n \equiv a^{n \bmod (p-1)} \ (mod\ p)$.

Απόδειξη

Έχουμε

$$\begin{aligned} a^n &= a^{(n \text{ div } (p-1))\cdot(p-1)+n \bmod (p-1)} \\ &= a^{(n \text{ div } (p-1))\cdot(p-1)} \cdot a^{n \bmod (p-1)} \\ &= (a^{p-1})^{n \text{ div } (p-1)} \cdot a^{n \bmod (p-1)} \\ &\equiv 1^{n \text{ div } (p-1)} \cdot a^{n \bmod (p-1)} \\ &\equiv a^{n \bmod (p-1)} \ (mod\ p) \end{aligned}$$

λαμβάνοντας υπόψη ότι $a^{p-1} \equiv 1\ (mod\ p)$, όπως προκύπτει από το μικρό θεώρημα του Fermat. □

Από το Μικρό Θεώρημα του Fermat προκύπτει ότι για κάθε πρώτο αριθμό $p > 2$ ισχύει $2^{p-1} \equiv 1 \ (mod \ p)$.

Αν ίσχυε η αντίστροφη πρόταση της παραπάνω, δηλαδή αν κάθε αριθμός n για τον οποίο ισχύει $2^{n-1} \equiv 1 \ (mod \ n)$ ήταν πρώτος αριθμός, θα είχαμε βρει έναν πολύ αποδοτικό αλγόριθμο για να αποφασίζουμε αν ένας αριθμός είναι πρώτος.

Ωστόσο υπάρχουν σύνθετοι αριθμοί n τέτοιοι ώστε $2^{n-1} \equiv 1 \ (mod \ n)$, όπως για παράδειγμα ο αριθμός $341 = 11 \cdot 31$.

Ορισμός

Έστω $b \geq 2$ ένας ακέραιος και n ένας σύνθετος ακέραιος. Ο n ονομάζεται ψευδοπρώτος στη βαση b αν $b^{n-1} \equiv 1 \ (mod \ n)$.

Ορισμός

Ένας σύνθετος αριθμός n ονομάζεται αριθμός Carmichael, αν για κάθε θετικό ακέραιο b τέτοιο ώστε $\gcd(n, b) = 1$, ισχύει $b^{n-1} \equiv 1 \ (mod \ n)$.

Ο αριθμός 561 είναι αριθμός Carmichael. Υπάρχει άπειρο πλήθος από αριθμούς Carmichael.

Λόγω της ύπαρξης των αριθμών Carmichael δεν μπορούμε να εφαρμόσουμε το Μικρό Θεώρημα του Fermat για να αποφασίσουμε αν ένας αριθμός είναι πρώτος, ανεξάρτητα από το πλήθος των βάσεων που θα χρησιμοποιήσουμε.

Ωστόσο το θεώρημα αυτό μπορεί να μας βοηθήσει να διαπιστώσουμε γρήγορα ότι ένας αριθμός n δεν είναι πρώτος: Αρκεί να βρούμε κάποια βάση b τέτοια ώστε $\gcd(n, b) = 1$ και $b^{n-1} \not\equiv 1 \ (mod \ n)$.

Παράδειγμα

Επειδή $2^{510} \bmod 511 = 64$, συμπεραίνουμε ότι ο αριθμός 511 δεν είναι πρώτος.

Πράγματι $511 = 7 \cdot 73$.

Ορισμός

Έστω p ένας πρώτος αριθμός. Ο αριθμός $r \in \mathbb{Z}_p = \{0, 1, \ldots, p-1\}$ ονομάζεται πρωταρχική (ή αρχέτυπη) ρίζα modulo p αν για κάθε $a \in \mathbb{Z}_p$ με $a \neq 0$, υπάρχει $k \in \mathbb{Z}_{p-1}$ τέτοιο ώστε $a \equiv r^k \ (mod \ p)$.

Παράδειγμα

Έχουμε

$$\begin{aligned} 3^0 &\equiv 1 \ (mod\ 7) \\ 3^1 &\equiv 3 \ (mod\ 7) \\ 3^2 &\equiv 2 \ (mod\ 7) \\ 3^3 &\equiv 6 \ (mod\ 7) \\ 3^4 &\equiv 4 \ (mod\ 7) \\ 3^5 &\equiv 5 \ (mod\ 7) \end{aligned}$$

Άρα το 3 είναι πρωταρχική ρίζα modulo 7.

Παράδειγμα

Έπίσης

$$\begin{aligned} 5^0 &\equiv 1 \ (mod\ 7) \\ 5^1 &\equiv 5 \ (mod\ 7) \\ 5^2 &\equiv 4 \ (mod\ 7) \\ 5^3 &\equiv 6 \ (mod\ 7) \\ 5^4 &\equiv 2 \ (mod\ 7) \\ 5^5 &\equiv 3 \ (mod\ 7) \end{aligned}$$

Άρα και το 5 είναι πρωταρχική ρίζα modulo 7.

Παράδειγμα

Ωστόσο

$$
\begin{aligned}
2^0 &\equiv 1 \,(mod\ 7)\\
2^1 &\equiv 2 \,(mod\ 7)\\
2^2 &\equiv 4 \,(mod\ 7)\\
2^3 &\equiv 1 \,(mod\ 7)\\
2^4 &\equiv 2 \,(mod\ 7)\\
2^5 &\equiv 4 \,(mod\ 7)
\end{aligned}
$$

Άρα το 2 δεν είναι πρωταρχική ρίζα modulo 7.

Το επόμενο θεώρημα δίνεται χωρίς απόδειξη.

Θεώρημα

Για κάθε πρώτο αριθμό p υπάρχει μία πρωταρχική ρίζα modulo p.

Ορισμός

Έστω p ένας πρώτος αριθμός, r μία πρωταρχική ρίζα modulo p και a ένας ακέραιος αριθμός όπου $1 \leq a \leq p-1$. Ονομάζουμε διακριτό λογάριθμο του a modulo p με βάση r τον μοναδικό αριθμό k με $0 \leq k \leq p-2$, για τον οποίο ισχύει $a \equiv r^k \ (mod\ p)$.

Παράδειγμα

Στο προηγούμενο παράδειγμα είδαμε ότι το 5 είναι μία πρωταρχική ρίζα modulo 7 και ότι $5^4 \equiv 2 \ (mod \ 7)$.

Άρα ο διακριτός λογάριθμος του 2 modulo 7 με βάση 5 είναι το 4.

Δεν υπάρχει γνωστός αποδοτικός αλγόριθμος, ο οποίος με δεδομένο έναν πρώτο αριθμό p, μία πρωταρχική ρίζα r modulo p και έναν ακέραιο αριθμό a με $1 \leq a \leq p-1$, υπολογίζει το διακριτό λογάριθμο του a modulo p με βάση r.

Στην υπολογίστική δυσκολία του παραπάνω προβλήματος βασίζονται διάφορες μέθοδοι κρυπτογράφησης.