Κρυπτογραφία και Πολυπλοκότητα

Απόδειξη του Αλγορίθμου Tonelli - Shanks

Κωστής Γκιώνης

Σχολή Εφαρμοσμένων και Φυσικών Επιστημών

Δευτέρα 13 Φεβρουαρίου 2011

Το Πρόβλημα

Να βρούμε $x_1, x_2 \in \mathbb{Z}_p$ τέτοια ώστε:

$$x_i^2 \equiv a \pmod{p} \quad i \in 1, 2 \tag{1}$$

για κάποιο $a \in \mathbb{Z}_p$.

Το Πρόβλημα

Να βρούμε $x_1, x_2 \in \mathbb{Z}_p$ τέτοια ώστε:

$$x_i^2 \equiv a \pmod{p} \quad i \in 1, 2 \tag{1}$$

για κάποιο $a \in \mathbb{Z}_p$.

- Ύπαρξη Λύσης $\rightarrow$ Κριτήριο Euler.

Το Πρόβλημα

Να βρούμε $x_1, x_2 \in \mathbb{Z}_p$ τέτοια ώστε:

$$x_i^2 \equiv a \pmod{p} \quad i \in 1, 2 \tag{1}$$

για κάποιο $a \in \mathbb{Z}_p$.

- Ύπαρξη Λύσης $\rightarrow$ Κριτήριο Euler.
- Εύρεση Λύσης $\rightarrow$ Αλγόριθμος Tonelli - Shanks.

Το Πρόβλημα

Να βρούμε $x_1, x_2 \in \mathbb{Z}_p$ τέτοια ώστε:

$$x_i^2 \equiv a \pmod{p} \quad i \in 1, 2 \tag{1}$$

για κάποιο $a \in \mathbb{Z}_p$.

- Ύπαρξη Λύσης $\rightarrow$ Κριτήριο Euler.
- Εύρεση Λύσης $\rightarrow$ Αλγόριθμος Tonelli - Shanks.
- Αρκεί να βρούμε μία λύση, διότι $x_2 = -x_1 + p$.

Κριτήριο Euler

Πρόταση

Έστω p πρώτος αριθμός. Η εξίσωση

$$x^2 \equiv a \pmod{p} \tag{2}$$

έχει λύση αν και μόνο άν $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$.

Μικρό Θεώρημα Fermat

Πρόταση

Έστω π πρώτος και $a \in \mathbb{Z}$ *τέτοιο ώστε* $\gcd(a, p) = 1$*, τότε:*

$$a^{p-1} \equiv 1 \pmod{p}$$

Με άλλα λόγια η τάξη του a *στο* $\mathbb{Z}_p$ *διαιρεί το* $p - 1$*, δηλαδή* $ord_p(a) | (p - 1)$*.*

Σημαντικό Λήμμα

Lemma

Αν p περιττός πρώτος και $y^2 \equiv 1 \pmod{p}$, τότε $y \equiv \pm 1 \pmod{p}$.

Σημαντικό Λήμμα

Lemma

Αν p περιττός πρώτος και $y^2 \equiv 1 \pmod{p}$, τότε $y \equiv \pm 1 \pmod{p}$.

Απόδειξη.

Από υπόθεση $p|y^2 - 1 \Rightarrow p|(y-1)(y+1)$.

Σημαντικό Λήμμα

Lemma

Αν p περιττός πρώτος και $y^2 \equiv 1 \pmod{p}$, τότε $y \equiv \pm 1 \pmod{p}$.

Απόδειξη.

Από υπόθεση $p|y^2 - 1 \Rightarrow p|(y-1)(y+1)$. Επειδή ο p πρώτος $\Rightarrow$ $p|(y-1)$ ή $p|(y+1)$.

Σημαντικό Λήμμα

Lemma

Αν p περιττός πρώτος και $y^2 \equiv 1 \pmod{p}$, τότε $y \equiv \pm 1 \pmod{p}$.

Απόδειξη.

Από υπόθεση $p|y^2 - 1 \Rightarrow p|(y-1)(y+1)$. Επειδή ο p πρώτος $\Rightarrow$ $p|(y-1)$ ή $p|(y+1)$. Διότι αν διαιρούσε και τους δύο, θα $\exists \lambda_1, \lambda_2 \in \mathbb{R}$ ώστε $(y-1) = \lambda_1 p$ και $(y+1) = \lambda_2 p$.

Σημαντικό Λήμμα

Lemma

Αν p περιττός πρώτος και $y^2 \equiv 1 \pmod{p}$, τότε $y \equiv \pm 1 \pmod{p}$.

Απόδειξη.

Από υπόθεση $p|y^2 - 1 \Rightarrow p|(y-1)(y+1)$. Επειδή ο p πρώτος $\Rightarrow$ $p|(y-1)$ ή $p|(y+1)$. Διότι αν διαιρούσε και τους δύο, θα $\exists \lambda_1, \lambda_2 \in \mathbb{R}$ ώστε $(y-1) = \lambda_1 p$ και $(y+1) = \lambda_2 p$. Προσθέτοντας κατά μέλη: $(\lambda_1 + \lambda_2)p = y - 1 + y + 1 = 2y$.

Σημαντικό Λήμμα

Lemma

Αν p περιττός πρώτος και $y^2 \equiv 1 \pmod{p}$, τότε $y \equiv \pm 1 \pmod{p}$.

Απόδειξη.

Από υπόθεση $p|y^2 - 1 \Rightarrow p|(y-1)(y+1)$. Επειδή ο p πρώτος $\Rightarrow$ $p|(y-1)$ ή $p|(y+1)$. Διότι αν διαιρούσε και τους δύο, θα $\exists \lambda_1, \lambda_2 \in \mathbb{R}$ ώστε $(y-1) = \lambda_1 p$ και $(y+1) = \lambda_2 p$. Προσθέτοντας κατά μέλη: $(\lambda_1 + \lambda_2)p = y - 1 + y + 1 = 2y$. Συεπώς
$p|2y \Rightarrow p|y \Rightarrow p|y^2 \Rightarrow y^2 \equiv 0 \pmod{p}$.

Σημαντικό Λήμμα

Lemma

Αν p περιττός πρώτος και $y^2 \equiv 1 \pmod{p}$, τότε $y \equiv \pm 1 \pmod{p}$.

Απόδειξη.

Από υπόθεση $p|y^2 - 1 \Rightarrow p|(y-1)(y+1)$. Επειδή ο p πρώτος $\Rightarrow$ $p|(y-1)$ ή $p|(y+1)$. Διότι αν διαιρούσε και τους δύο, θα $\exists \lambda_1, \lambda_2 \in \mathbb{R}$ ώστε $(y-1) = \lambda_1 p$ και $(y+1) = \lambda_2 p$. Προσθέτοντας κατά μέλη: $(\lambda_1 + \lambda_2)p = y - 1 + y + 1 = 2y$. Συεπώς
$p|2y \Rightarrow p|y \Rightarrow p|y^2 \Rightarrow y^2 \equiv 0 \pmod{p}$. Άτοπο!

■

Παρατήρηση Gauss

Παρατήρησε πως την (2) τη λύνουμε αν βρούμε περιπό ακέραιο S τέτοιον ώστε:

$$a^S \equiv 1 \pmod{p}$$

διότι τότε η μία λύση είναι η:

$$x = a^{\frac{S+1}{2}} \mod p$$

αφού:

$$\begin{aligned} x^2 &\equiv \left(a^{\frac{S+1}{2}}\right)^2 \pmod{p} \\ &\equiv a^S a \pmod{p} \\ &\equiv a \pmod{p} \end{aligned}$$

Λύση Gauss

Παρατήρηση

Αν επιλέξουμε τύχαια έναν p πρώτο θα ισχύει:

$$p \equiv 3 \pmod 4 \quad \text{με 50\% πιθανότητα, ή} \tag{3}$$

$$p \equiv 1 \pmod 4 \tag{4}$$

Λύση Gauss

Παρατήρηση

Αν επιλέξουμε τύχαια έναν p πρώτο θα ισχύει:

$$p \equiv 3 \pmod 4 \qquad \text{με 50\% πιθανότητα, ή} \tag{3}$$

$$p \equiv 1 \pmod 4 \tag{4}$$

Συνεπώς για $S = \frac{p-1}{2}$ είμαστε εντάξει για τη περίπτωση 3 αφού:

$$a^S \equiv a^{\frac{p-1}{2}} \equiv 1 \pmod p$$

Λύση Gauss

Παρατήρηση

Αν επιλέξουμε τύχαια έναν p πρώτο θα ισχύει:

$$p \equiv 3 \pmod 4 \quad \text{με 50\% πιθανότητα, ή} \tag{3}$$

$$p \equiv 1 \pmod 4 \tag{4}$$

Συνεπώς για $S = \frac{p-1}{2}$ είμαστε εντάξει για τη περίπτωση 3 αφού:

$$a^S \equiv a^{\frac{p-1}{2}} \equiv 1 \pmod p$$

και υπάρχει $x \equiv a^{\frac{S+1}{2}} \pmod p \equiv a^{\frac{p+1}{4}} \pmod p$, αφού το $4|p+1$.

Αλγόριθμος Tonelli - Shanks

1. Είσοδος: $a, p \in \mathbb{Z}$, με p πρώτο
2. Έξοδος: $x_1, x_2 \in \mathbb{Z}$ τέτοια ώστε $x_1^2 \equiv a \pmod{p}$ και $x_2^2 \equiv a \pmod{p}$.
3. Έλεγχος: Αν $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$ συνέχισε κανονικά αλλιώς διέκοψε. Ο a είναι τετραγωνικό μη υπόλοιπο modulo p.
4. Βρες S, e: Με διαδοχικούς υποδιπλασιασμούς βρες s, e τέτοια ώστε $p - 1 = S \cdot 2^e$.
5. Βρες n: Θέσε $n = 2$. Αν $n^{\frac{p-1}{2}} \equiv -1 \pmod{p}$ τότε συνέχισε αλλιώς επανάλαβε για $n = n + 1$.

6. Initial Guess: Αρχικοποίησε τις παρακάτω παραμέτρους
   1. $x = a^{\frac{S+1}{2}} \mod p$
   2. $b = a^S \mod p$
   3. $g = n^S \mod p$
   4. $r = e$
7. Βρες m: Θέσε $m = 0$. Αν $b^{2^m} \equiv 1 \pmod p$ τότε συνέχισε αλλιώς επανάλαβε για $m = m + 1$.
8. Τερματισμός: Αν $m = 0$ τότε επέστρεψε x και $(-x \mod p)$ και τερμάτισε.
9. Ανανέωση: Κάνε τα παρακάτω:
   1. $x = x \cdot g^{2^{r-m-1}} \mod p$
   2. $b = b \cdot g^{2^{r-m}} \mod p$
   3. $g = g^{2^{r-m}} \mod p$
   4. $r = m$

Η $\sqrt{8}$ στο $\mathbb{Z}_{40961}$

Αρχικοποιούμε:

1. $a = 5, p = 40961$ και επειδή $5^{20480} \equiv 1 \pmod{p}$ είμαστε εντάξει.
2. $p - 1 = 40960 = 20480 \cdot 2 = 10240 \cdot 2^2 = \ldots = 5 \cdot 2^{13}$, άρα $S = 5$ και $e = 13$.
3. $x = a^{\frac{S+1}{2}} \mod p = 8^3 \mod 40961 \Rightarrow x = 512$.
4. $b = a^S \mod p = 5^5 \mod 40961 \Rightarrow b = 32768$
5. Ξεκινωντας από $n = 2$ βρίσκουμε πως $n = 3$.
6. $g = n^S = 3^5 = 243$

i	m	$x = x \cdot g^{2^{r-m-1}}$	$b = b \cdot g^{2^{r-m}}$	$g = g^{2^{r-m}}$	r
		512	32768	243	13
1	11	3870	8387	20237	11
2	9	17966	21040	8603	9
3	6	23589	39178	14529	6
4	5	23589	31679	19808	5
5	3	10952	14541	31679	3
6	2	10952	40960	14541	2
7	1	10952	1	40960	1

Πίνακας: Αφού $b \not\equiv 1 \pmod{p}$ ξεκινάμε τις επαναλήψεις. Χρειαζόμαστε 7 επαναλήψεις για να υπολογίσουμε το $\sqrt{8}$

Επιλογή Λύσης

Επιλέγουμε S τέτοιο ώστε:

$$p - 1 = S \cdot 2^e$$

Επιλογή Λύσης

Επιλέγουμε S τέτοιο ώστε:

$$p - 1 = S \cdot 2^e$$

Επιλέγουμε ως λύση (Initial Guess) τη:

$$x = a^{\frac{S+1}{2}} \mod p$$

Επιλογή Λύσης

Επιλέγουμε S τέτοιο ώστε:

$$p - 1 = S \cdot 2^e$$

Επιλέγουμε ως λύση (Initial Guess) τη:

$$x = a^{\frac{S+1}{2}} \mod p$$

Παρατηρούμε πως:

$$x^2 \equiv \left(a^{\frac{S+1}{2}}\right)^2 \pmod p \equiv a^{S+1} \pmod p \equiv a^S \cdot a \pmod p$$

Βελτιώσεις

Η $x = a^{\frac{S+1}{2}} \mod p$ είναι λύση αν και μόνο αν:

$$a^S \equiv 1 \pmod{p}$$

Αυτό συμβαίνει στα $2/3$ των περιπτώσεων. Συνεπώς οι βελτιώσεις:

1. Μεγαλύτερη πιθανότητα να βρούμε τη λύση με ένα βήμα.
2. Λύση ακόμη και αν τύχουμε στο $1/3$ των περιπτώσεων.

Τάξη του Fudge Factor

Fudge Factor

Στην έκφραση:

$$x^2 \equiv a^S \cdot a \pmod{p}$$

τον αριθμό $b = a^S$ τον καλούμε Fudge Factor (FF).

Τάξη του Fudge Factor

Fudge Factor

Στην έκφραση:

$$x^2 \equiv a^S \cdot a \pmod{p}$$

τον αριθμό $b = a^S$ τον καλούμε Fudge Factor (FF).

Αν τύχουμε στο $1/3$ των περιπτώσεων, τότε:

$$a^S \not\equiv 1 \pmod{p}$$

Τάξη του Fudge Factor

Fudge Factor

Στην έκφραση:

$$x^2 \equiv a^S \cdot a \pmod{p}$$

τον αριθμό $b = a^S$ τον καλούμε Fudge Factor (FF).

Αν τύχουμε στο $1/3$ των περιπτώσεων, τότε:

$$a^S \not\equiv 1 \pmod{p}$$

Δηλαδή $ord(b) > 1$.

Στόχος

Αφού $ord(a^S) > 1$, θέλουμε να βρούμε πολ/κό παράγοντα για την:

$$x^2 \equiv a^S \cdot a \pmod{p}$$

ώστε με επαναλήψεις να καταλήξουμε σε μια έκφραση της οποίας ο Fudge Factor να έχει τάξη ίση με 1.

Τάξη FF

Θυμίζουμε πως στο Βήμα 7 βρίσκουμε **m** τέτοιο ώστε:

$$\left(a^s\right)^{2^m} \equiv 1 \pmod{p}$$

Τάξη FF

Θυμίζουμε πως στο Βήμα 7 βρίσκουμε **m** τέτοιο ώστε:

$$\left(a^S\right)^{2^m} \equiv 1 \pmod{p}$$

Επειδή:

$$\left(a^S\right)^{2^{e-1}} = a^{\frac{S\cdot 2^e}{2}} = a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$$

Τάξη FF

Θυμίζουμε πως στο Βήμα 7 βρίσκουμε **m** τέτοιο ώστε:

$$\left(a^S\right)^{2^m} \equiv 1 \pmod{p}$$

Επειδή:

$$\left(a^S\right)^{2^{e-1}} = a^{\frac{S\cdot 2^e}{2}} = a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$$

Παρατηρούμε πως:

$$ord\left(a^S\right) | 2^{e-1}$$

Τάξη FF

Θυμίζουμε πως στο Βήμα 7 βρίσκουμε **m** τέτοιο ώστε:

$$\left(a^S\right)^{2^m} \equiv 1 \pmod{p}$$

Επειδή:

$$\left(a^S\right)^{2^{e-1}} = a^{\frac{S\cdot 2^e}{2}} = a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$$

Παρατηρούμε πως:

$$ord(a^S) | 2^{e-1}$$

Οπότε μπορούμε να βρούμε $0 \leq m \leq e-1$ τέτοιο ώστε:

$$ord(b) = 2^m$$

Πολ/κός Παράγοντας

Θυμίζουμε (Βήμα 5 του αλγορίθμου) πως έχουμε βρει **n** τέτοιο ώστε:

$$n^{\frac{p-1}{2}} \equiv -1 \pmod{p}$$

Πολ/κός Παράγοντας

Θυμίζουμε (Βήμα 5 του αλγορίθμου) πως έχουμε βρει **n** τέτοιο ώστε:

$$n^{\frac{p-1}{2}} \equiv -1 \pmod{p}$$

Πολ/κός Παράγοντας

Είναι ο αριθμός $\left(n^s\right)^{2^{e-m}}$.

Πολ/κός Παράγοντας

Θυμίζουμε (Βήμα 5 του αλγορίθμου) πως έχουμε βρει **n** τέτοιο ώστε:

$$n^{\frac{p-1}{2}} \equiv -1 \pmod{p}$$

Πολ/κός Παράγοντας

Είναι ο αριθμός $\left(n^S\right)^{2^{e-m}}$.

Τον εφαρμόζουμε στην εξίσωση:

$$x^2 \equiv a^S \cdot a \pmod{p}$$

Πολ/κός Παράγοντας

Θυμίζουμε (Βήμα 5 του αλγορίθμου) πως έχουμε βρει **n** τέτοιο ώστε:

$$n^{\frac{p-1}{2}} \equiv -1 \pmod{p}$$

Πολ/κός Παράγοντας

Είναι ο αριθμός $\left(n^S\right)^{2^{e-m}}$.

Τον εφαρμόζουμε στην εξίσωση:

$$x^2 \equiv a^S \cdot a \pmod{p}$$

και λαμβάνουμε:

$$x^2 \cdot \left(n^S\right)^{2^{e-m}} \equiv a^S \cdot \left(n^S\right)^{2^{e-m}} \cdot a \pmod{p}$$

Νέα Λύση

Έτσι:

$$\text{Νέα Λύση: } x' = \left(x \cdot \left(n^S\right)^{2^{e-m-1}}\right)^2 \mod p$$

$$\text{Νέος FF: } b' = a^S \cdot \left(n^S\right)^{2^{e-m}} \mod p$$

Νέα Λύση

Έτσι:

$$\text{Νέα Λύση: } x' = \left(x \cdot \left(n^S\right)^{2^{e-m-1}}\right)^2 \mod p$$

$$\text{Νέος FF: } b' = a^S \cdot \left(n^S\right)^{2^{e-m}} \mod p$$

Για να αποδείξουμε την ορθότητα του αλγορίθμου μένει να δείξουμε πως η τάξη του νέου FF είναι μικρότερη από του προηγούμενου.

Νέα Λύση

Έτσι:

$$\text{Νέα Λύση: } x' = \left(x \cdot \left(n^S\right)^{2^{e-m-1}}\right)^2 \mod p$$

$$\text{Νέος FF: } b' = a^S \cdot \left(n^S\right)^{2^{e-m}} \mod p$$

Για να αποδείξουμε την ορθότητα του αλγορίθμου μένει να δείξουμε πως η τάξη του νέου FF είναι μικρότερη από του προηγούμενου.

Θυμίζουμε πως $ord(b) = 2^m$. Συνεπώς αρκεί ν.δ.ο:

$$ord(b') \leq 2^{m-1} \Leftrightarrow (b')^{2^{m-1}} \equiv 1 \pmod p$$

Παρατήρηση 1

Ισχύει πως:

$$a^{S\cdot 2^{m-1}} \equiv -1 \pmod{p}$$

Θέτουμε:

$$y = a^{S\cdot 2^{m-1}} = \left(a^S\right)^{2^{m-1}}$$

Παρατηρούμε πως:

$$\begin{aligned} y^2 &= \left(a^{S\cdot 2^{m-1}}\right)^2 = \left(a^{S\cdot 2^m}\right) \\ &= \left(a^S\right)^{2^m} = 1 \end{aligned}$$

Συνεπώς από Ἰσημαντικό Λήμμα': $y = -1 \pmod{p}$.

Απόδειξη

$$
\begin{aligned}
b'^{2^{m-1}} &\equiv a^{s\cdot 2^{m-1}} \cdot n^{s\cdot 2^{e-m+m-1}} \pmod{p} \\
&\equiv a^{s\cdot 2^{m-1}} \cdot n^{s\cdot 2^{e-1}} \pmod{p} \\
&\equiv a^{s\cdot 2^{m-1}} \cdot n^{s\cdot 2^{e-1}} \pmod{p} \\
&\equiv a^{s\cdot 2^{m-1}} \cdot n^{\frac{p-1}{2}} \pmod{p} \\
&\equiv -1 \cdot -1 \pmod{p} \\
&\equiv 1 \pmod{p}
\end{aligned}
$$

■


Ζάχος, Ε. *Σημειώσεις στη Θεωρία Αριθμών και την Κρυπτογραφία*. Εκδόσεις ΕΜΠ, 2007.


Turner, S.M. *Square roots mod p*, American Mathematical Monthly 101, 1994, 443-449.


Wikipedia contributors, *Tonelli -- Shanks algorithm*, Wikipedia, The Free Encyclopedia (accessed February 6, 2010).