Α44 – ΚΡΥΠΤΟΓΡΑΦΙΑ
ΣΗΜΕΙΩΣΕΙΣ #7

ΘΕΟΔΟΥΛΟΣ ΓΑΡΕΦΑΛΑΚΗΣ

1. Παραγοντοποιηση ακεραιων

Θα μελετήσουμε το πρόβλημα της ανάλυσης ακεραίων σε πρώτους παράγοντες. Μας δίνεται ένας ακέραιος $n > 0$. Η πρώτη μας δουλειά είναι να ελέγξουμε αν ο n είναι πρώτος.Αυτό μπορεί να γίνει εύκολα με ένα πιθανοθεωρητικό τέστ. Γνωρίζοντας ότι ο αριθμός μας είναι σύνθετος, προχωρούμε στην παραγοντοποίηση του. Μια πρώτη προσέγγιση είναι να δοκιμάσουμε να βρούμε τους πρώτους παράγοντες του n δοκιμάζοντας διαδοχικές διαιρέσεις με 2,3,5,7 κ.λ.π. Κάθε σύνθετος αριθμός n έχει πρώτο παράγοντα μικοτερο ή ίσο με $\sqrt{n}$. Άρα χρειάζεται να ελέγξουμε τους πρώτους έως το $\sqrt{n}$, για να ανακαλύψουμε κάποιο πρώτο παράγοντα του n. Το πρόβλημα είναι ότι μπορεί ο μικρότερος πρώτος διαιρέτης του n να είναι της τάξης του $\sqrt{n}$, οπότε η παραπάνω μέθοδος θα χρειαστεί να κάνει περίπου τόσες διαιρέσεις. Ο αριθμός $\sqrt{n} = e^{0.5 \log n}$ είναι εκθετικός στο μέγεθος της εισόδου, που είναι $\log n$. Πρακτικά, αν το $n \sim 2^{1000}$, τότε θα χρειαστούμε περίπου 2^{500} διαιρέσεις...

2. Η μεθοδος $p-1$

Θα δούμε τώρα μια μέθοδο που δουλεύει καλά για αριθμούς ειδικής μορφής. Για την απλούστευση της περιγραφής της μεθόδου, ας υποθέσουμε ότι $n = pq$, όπου p, q είναι πρώτοι. Τότε γνωρίζουμε ότι για a με $(a, n) = 1$, ισχύουν

$$\begin{aligned} a^{p-1} &\equiv 1 \pmod{p} \\ a^{q-1} &\equiv 1 \pmod{q}. \end{aligned}$$

Αν είχα ένα αριθμό E τέτοιον ώστε $p-1|E$, αλλά $q-1 \not| E$, τότε σίγουρα

$$a^E \equiv 1 \pmod{p},$$

και περιμένω ότι

$$a^E \not\equiv 1 \pmod{q},$$

εκτός αν η τάξη του a modulo q διαιρεί το E. Στην περίπτωση που οι δύο παραπάνω σχέσεις ισχύουν, τότε

$$(a^E - 1, n) = p$$

και κατάφερα να παραγοντοποιήσω. Προσέξτε ότι όλη η μέθοδος συνίσταται στην επιλογή του E, που είναι λίγο-πολύ αφθαίρετη, και του a, που είναι τυχαία, και στον υπολογισμό ενός μέγιστου κοινού διαιρέτη. Πότε περιμένουμε η μέθοδος να επιτύχει; Ας εξετάσουμε πότε η μέθοδος αποτυγχάνει. Αποτυχία σημαίνει ότι ο μ.κ.δ. $(a^E - 1, n)$ είναι τετριμμένος, δηλαδή ίσος με 1 ή με n. Η πρώτη περίπτωση σημαίνει ότι $p \not| a^E - 1$ και $q \not| a^E - 1$, δηλαδή

$$\begin{aligned} a^E &\not\equiv 1 \pmod{p} \\ a^E &\not\equiv 1 \pmod{q} \end{aligned}$$

το οποίο σημαίνει ότι το $p-1$ και το $q-1$ δεν διαιρούν το E.

Η άλλη περίπτωση αποτυχίας είναι $(a^E - 1, n) = n$ που σημαίνει ότι

$$\begin{aligned} a^E &\equiv 1 \pmod{p} \\ a^E &\equiv 1 \pmod{q} \end{aligned}$$

που σημαίνει (αν το a είναι γεννήτορας mod p και mod q) ότι και το $p-1$ και το $q-1$ διαιρούν το E.

Πώς μπορώ λοιπόν να επιλέξω το E; Επιλέγω ένα φράγμα B και θέτω $E = B!$. Αν οι πρώτοι παράγοντες του $p-1$ είναι μικροί ($\leq B$) και εμφανίζονται σε μικρές σχετικά δυνάμεις, τότε $p-1|B!$ και επομένως $a^{B!} \equiv 1 \pmod{p}$. Αν ο $q-1$ έχει κάποιο πρώτο παράγοντα μεγαλύτερο του B τότε ελπίζω ότι θα έχω $a^{B!} \not\equiv 1 \pmod{q}$ οπότε ο μ.κ.δ. $(a^{B!} - 1, n)$ είναι ίσος με p.

Προσέξτε ότι η επιτυχία του αλγόριθμου εξαρτάται από το μέγεθος των πρώτων παραγόντων του $p-1$ και *όχι* του ίδιου του n.

Παράδειγμα 2.1. Έστω ότι θέλουμε να παραγοντοποιήσουμε τον αριθμό $n = 1223917$. Επιλέγουμε $a = 2$, οπότε $(a, n) = 1$, και το φράγμα $B = 9$. Υπολογίζουμε $a^{B!} \mod n = 2^{9!} \mod n = 517467$, οπότε

$$(2^{9!} - 1, n) = (517467 - 1, 1223917) = 1009.$$

Με ένα πιθανοθεωρητικό τέστ βλέπουμε ότι με μεγάλη πιθανότητα το $p = 1009$ είναι πρώτος και ότι το $q = n/p = 1213$ είναι επίσης πρώτος. Έτσι έχουμε την ανάλυση $n = 1009 \cdot 1213$.

Κανείς μπορεί να ελέγξει ότι

$$p - 1 = 1008 = 2^4 \cdot 3^2 \cdot 7 \quad \text{και} \quad q - 1 = 2^2 \cdot 3 \cdot 101.$$

Έτσι φαίνεται ότι η επιλογή $B = 7$ ή 8 θα έδιναν το ίδιο αποτέλεσμα. Το ίδιο και τιμές του B στο διάστημα $[7, 100]$, καθώς η τάξη του a modulo q είναι $q-1$. Αν επιλέγαμε $B = 6$, τότε $p - 1 \not| 6!$ καθώς και $q - 1 \not| 6!$, οπότε όπως θα περιμέναμε $(2^{6!} - 1, n) = 1$. Οι τιμές $B \geq 101$ επίσεις οδηγούν σε αποτυχία, αφού τότε $(2^{B!} - 1, n) = n$.

3. Διαφορες τετραγωνων

Η επόμενη μέθοδος αποδίδεται στον Fermat και βασίζεται στη γνωστή ταυτότητα $x^2 - y^2 = (x+y)(x-y)$. Αν μου δοθεί ένας φυσικός n και καταφέρω να τον γράψω ως διαφορά δύο τετραγώνων, τότε μπορώ να τον γράψω σαν γινόμενο δύο αριθμών, όχι κατ' ανάγκη πρώτων, τους οποίους θα προσπαθήσω στη συνέχεια να παραγοντοποιήσω.

Η πρώτη παρατήρηση είναι ότι κάθε περιττός σύνθετος μπορεί να γραφεί ως διαφορά τετραγώνων. Πραγματικά, αν είναι $n = A \cdot B$, όπου A και B είναι περιττοί μεγαλύτεροι ή ίσοι του 3 τότε οι αριθμοί

$$x = \frac{A+B}{2}, \quad y = \frac{A-B}{2}$$

ικανοποιούν την ισότητα $x^2 - y^2 = A \cdot B = n$. Η γραφή αυτή του n ως διαφορά τετραγώνων δεν είναι κατ' ανάγκη μοναδική. Αυτό εξαρτάται από το πλήθος των πρώτων παραγόντων του n.

Η μέθοδος μου, λοιπόν, είναι η εξής: Υπολογίζω διαδοχικά τους αριθμούς $n + x^2$ για $x = 0, 1, 2, \ldots$ και ελέγχω αν είναι τέλεια τετράγωνα ή όχι. Όταν κάποιος από αυτούς τους αριθμούς είναι τέλειο τετράγωνο, ας πούμε $n + x^2 = y^2$ τότε έχω τη διαφορά τετραγώνων που ψάχνω και αναλύω το n στο γινόμενο $(x+y)(x-y)$. Αν κάποιος από τους $x+y$ και $x-y$ δεν είναι πρώτος συνεχίζω να αναλύσω αυτόν.

Παράδειγμα 3.1. Έστω $n = 8850609$. Υπολογίζουμε διαδοχικά

$$\begin{aligned} n + 1^2 &= 8850610 \text{ δεν είναι τετράγωνο} \\ n + 2^2 &= 8850613 \text{ δεν είναι τετράγωνο} \\ n + 3^2 &= 8850618 \text{ δεν είναι τετράγωνο} \\ n + 4^2 &= 8850625 = 2975^2 \end{aligned}$$

οπότε $8850609 = (2975-4)(2975+4) = 2971 \cdot 2979$. Κανείς μπορεί να ελέγξει ότι το 2971 είναι πρώτος, ενώ $2979 = 3^2 \cdot 331$.

Παράδειγμα 3.2. Έστω $n = 14987880589$. Υπολογίζουμε

$$\begin{aligned} n + 1^2 &= 14987880590 \text{ δεν είναι τετράγωνο} \\ n + 2^2 &= 14987880593 \text{ δεν είναι τετράγωνο} \\ \cdots &\quad \cdots \\ n + 6^2 &= 14987880625 = 122425^2 \end{aligned}$$

και έχουμε $n = (122425 - 6)(122425 + 6) = 122419 \cdot 122431$. Κανένας από τους δύο δεν είναι πρώτος. Συνεχίζουμε με την ανάλυση του 122419.

$$\begin{aligned} 122419 + 1^2 &= 122420 \text{ δεν είναι τετράγωνο} \\ 122419 + 2^2 &= 122423 \text{ δεν είναι τετράγωνο} \\ \cdots &\quad \cdots \\ 122419 + 9^2 &= 122500 = 350^2 \end{aligned}$$

οπότε $122419 = (350 - 9)(350 + 9) = 341 \cdot 359$. Διαπιστώνουμε ότι ο 359 είναι πρώτος. Βρίσκουμε, για παράδειγμα με δοκιμαστικές διαιρέσεις, ότι $341 = 11 \cdot 31$ και έτσι έχουμε την ανάλυση $122419 = 11 \cdot 31 \cdot 359$.

Συνεχίζουμε με την ανάλυση του 122431. Υπολογίζουμε το $122431 + k^2$ για μερικές διαδοχικές τιμές του k, όμως δε βρίσκουμε τέλειο τετράγωνο. Ο λόγος είναι ότι το 122431 είναι γινόμενο δύο πρώτων, άρα η γραφή του ως διαφορά τετραγώνων είναι μοναδική και δυστυχώς για εμάς, βρίσκουμε τετράγωνο για $k = 225$. Εδώ φαίνεται και η αδυναμία της μεθόδου: αν ο αριθμός μας δε γράφεται σαν γινόμενο δύο ίσων σχεδόν αριθμών, τότε πρέπει να κάνουμε πολλές δοκιμές προκειμένου να φτιάξουμε τη διαφορά τετραγώνων.