

Author: Ν Τζανάκης

Title: Μια περιδιάβαση στη Θεωρία Αριθμών.

Abstract: Το άρθρο αυτό αποτελεί το περιεχόμενο ομιλίας, που δόθηκε στα πλαίσια του διημέρου, το οποίο οργάνωσε το Παράρτημα Ηρακλείου στις 27 και 28 Νοεμβρίου 1998, με την ευκαιρία του εορτασμού των 80 χρόνων της Ε.Μ.Ε.

Creator: HDML

## Μία περιδιάβαση στη Θεωρία Αριθμών

Ν.Γ. Τζανάκης \*

Το άρθρο αυτό αποτελεί το περιεχόμενο ομιλίας, που δόθηκε στα πλαίσια του διημέρου, το οποίο οργάνωσε το Παράρτημα Ηρακλείου στις 27 και 28 Νοεμβρίου 1998, με την ευκαιρία του εορτασμού των 80 χρόνων της Ε.Μ.Ε.

Ο G.H. Hardy στην « Απολογία ενός μαθηματικού »<sup>1</sup> δίνει ως υπόδειγμα απλών και κομψών Μαθηματικών την απόδειξη για το άρρητο του  $\sqrt{2}$  καθώς και εκείνη του Ευκλείδη (300 π.Χ) για την απειρία των πρώτων αριθμών. Υπενθυμίζω τις αποδείξεις :

- Αν  $\sqrt{2} \in \mathbb{Q}$ , τότε ας γράψουμε  $\sqrt{2} = a/b$ ,  $a, b \in \mathbb{Z}$ ,  $\text{ΜΚΔ}(a, b) = 1$ . Υψώνοντας στο τετράγωνο,  $a^2 = 2b^2$ . Βλέπουμε ότι ο  $a^2$  είναι άρτιος, άρα και ο  $a$ . Έτσι, ας θέσουμε  $a = 2a_1$ ,  $a_1 \in \mathbb{Z}$ . Αντικαθιστώντας στην προηγούμενη ισότητα και απλοποιώντας δια 2, παίρνουμε  $2a_1^2 = b^2$ . Συμπεραίνουμε ότι ο  $b^2$ , άρα και ο  $b$ , είναι άρτιος. Αλλά προηγουμένως συμπεράναμε ότι και ο  $a$  είναι άρτιος, οπότε ερχόμαστε σε αντίφαση με την υπόθεση  $\text{ΜΚΔ}(a, b) = 1$ .
- Αν το σύνολο όλων των πρώτων ήταν πεπερασμένο, έστω  $\mathcal{P} = \{p_1, p_2, \dots, p_n\}$ , τότε θα σχηματίζαμε τον ακέραιο  $P = p_1 p_2 \dots p_n + 1$ , ο οποίος, καθώς είναι  $> 1$ , έχει τουλάχιστον ένα πρώτο διαιρέτη. Αυτός, αναγκαστικά, ανήκει στο  $\mathcal{P}$ , άρα κάποιο  $p_i$  διαιρεί τον  $P$ . Διαιρεί, προφανώς, και το γινόμενο  $p_1 p_2 \dots p_n$ , άρα και τη διαφορά τους, που είναι 1, άτοπο.

Αυτά είναι δύο μικρά κομψοτεχνήματα των λεγομένων *καθαρών Μαθηματικών*.

Περίπου 500 χρόνια μετά τον Ευκλείδη, ο Διόφαντος ασχολείται με υπολογιστικά προβλήματα της Θεωρίας Αριθμών: Αναζήτηση ρητών λύσεων εξισώσεων με ρητούς συντελεστές. Η επικρατούσα άποψη για το έργο του Διοφάντου, ως συνοθυλεύματος τυχαίων τεχνασμάτων έχει αναθεωρηθεί χάρη στο έργο της Isabella Bashmakova, η οποία έδειξε ότι πίσω από τα τεχνάσματα υποκρύπτονται - συνειδητά ή ασυνειδητά - γεωμετρικές ιδέες. Τυπικό παράδειγμα,

$$x^2 + y^2 = a^2 + b^2$$

με τους  $a, b$  δεδομένους ρητούς. Η ουσία της μεθόδου του Διοφάντου για την επίλυση της συγκεκριμένης εξίσωσης συνίσταται στο εξής: Η εξίσωση παριστάνει κύκλο κέντρου  $(0, 0)$  και ακτίνας  $\sqrt{a^2 + b^2}$ , του οποίου ένα ρητό σημείο (δηλ. σημείο με ρητές συντεταγμένες) είναι το  $(a, -b)$ . Άρα, αν μία ευθεία με ρητή κλίση

\*Τμήμα Μαθηματικών, Πανεπιστήμιο Κρήτης

<sup>1</sup> Συστήνω θερμά την πολύ επιμελημένη ελληνική έκδοση αυτού του βιβλίου από τις ΠΑΝΕΠΙΣΤΗΜΙΑΚΕΣ ΕΚΔΟΣΕΙΣ ΚΡΗΤΗΣ.

διέρχεται από το  $(a, -b)$ , το δεύτερο σημείο τομής της με τον κύκλο είναι επίσης ρητό· και αντίστροφα, κάθε ρητό σημείο  $(x, y)$  πάνω στον κύκλο, ορίζει με το  $(a, -b)$  μία ευθεία, της οποίας η κλίση είναι ρητή. Συνεπώς, οι λύσεις παραμετρικοποιούνται από την τομή του κύκλου με την ευθεία  $\epsilon_\lambda$ , η οποία διέρχεται δια του σημείου  $(a, -b)$  και έχει κλίση  $\lambda$ , καθώς το  $\lambda$  διατρέχει όλες τις ρητές τιμές:

$$\epsilon_\lambda: x = a + t, y = -b + \lambda t, \lambda \in \mathbb{Q}.$$

Τα σημεία τα διάφορα του  $(a, -b)$  αντιστοιχούν σε  $t \neq 0$ , οπότε, αντικαθιστώντας τα  $x, y$  στην εξίσωση και λύνοντας ως προς  $t$ , το οποίο υποθέτουμε  $\neq 0$ , παίρνουμε  $t = 2 \frac{\lambda b - a}{1 + \lambda^2}$  και, στη συνέχεια,

$$x = \frac{a\lambda^2 + 2b\lambda - a}{1 + \lambda^2}, y = \frac{b\lambda^2 - 2a\lambda - b}{1 + \lambda^2}, \lambda \in \mathbb{Q}.$$

Ανάλογη μέθοδος εφαρμόζεται σε εξισώσεις

$$Ax^2 + By^2 = C,$$

οι οποίες έχουν μία τουλάχιστον λύση, όπως λ.χ. οι

$$2x^2 + 3y^2 = 5, 2x^2 + 3y^2 = 173 \quad (173 = 2 \cdot 7^2 + 3 \cdot 5^2)$$

Ας θεωρήσουμε τώρα τις εξισώσεις,

$$x(6 - x) = y^3 - y \quad (1)$$

$$x^3 - 3x^2 + 3x + 1 = y^2 \quad (2)$$

από τα βιβλία δ' και ε', αντιστοίχως, του Διοφάντου. Η μέθοδος του Διοφάντου περιέχει σε λανθάνουσα μορφή την εξής ιδέα:

Αν  $P, Q$  είναι δύο ρητά σημεία επί μιας κυβικής καμπύλης, η οποία ορίζεται από εξίσωση με ρητούς συντελεστές, το τρίτο σημείο τομής της καμπύλης με την ευθεία  $PQ$  - ως το συμβολίσουμε  $P * Q$  - είναι, επίσης, ρητό<sup>2</sup>. Εννοείται ότι, στην περίπτωση που τα δύο σημεία  $P, Q$  ταυτίζονται, η ευθεία  $PQ$  είναι η εφαπτομένη της καμπύλης στο σημείο  $P = Q$ , δηλαδή το σημείο  $P * P$  είναι το σημείο της καμπύλης, στο οποίο η εφαπτομένη στο  $P$  την τέμνει.

Σήμερα προτιμούμε να κάνουμε ένα ακόμη βήμα: Φέρνουμε την ευθεία, η οποία ενώνει το σημείο  $P * Q$ , με το επ' άπειρο σημείο της καμπύλης, και παίρνουμε ένα τρίτο σημείο τομής της με την καμπύλη, συμβολιζόμενο  $P + Q$ . Το να ενώσεις ένα σημείο με το επ' άπειρο σημείο σημαίνει, στην περίπτωση της (1), να φέρεις την παράλληλο προς τον άξονα των  $x$ , ενώ στην περίπτωση της (2), να φέρεις την παράλληλο προς τον άξονα των  $y$ . (Βλ. το σχήμα, παρακάτω, για την περίπτωση

<sup>2</sup> Αποδεικνύεται απλά, με στοιχειώδη μαθηματικά, ότι αν μία καμπύλη τρίτου βαθμού έχει ρητούς συντελεστές και δύο σημεία της είναι ρητά, τότε η ευθεία, που αυτά ορίζουν, τέμνει την καμπύλη σε ένα τρίτο σημείο, επίσης ρητό.

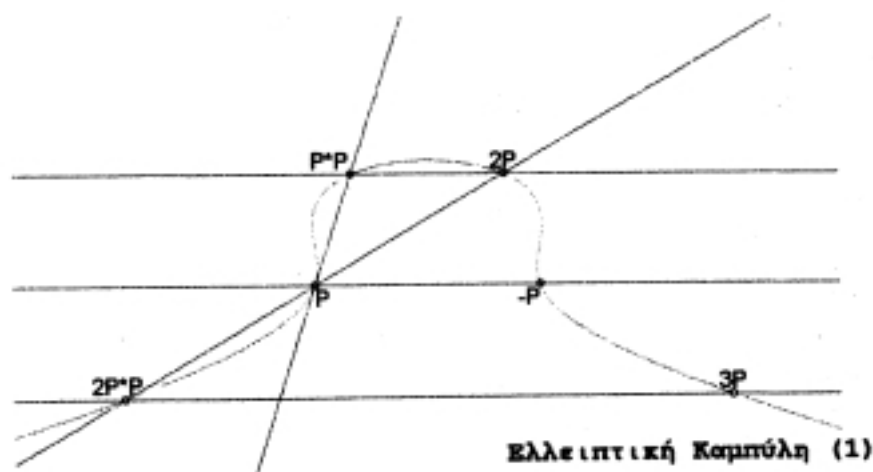
της καμπύλης (1).) Ο λόγος που επιλέγομε το  $P+Q$  αντι του  $P*Q$ , όπως επίσης και η χρήση του συμβόλου  $+$ , είναι ότι η διαδικασία

$$(P, Q) \rightarrow P + Q$$

ορίζει μία πράξη στο σύνολο των ρητών σημείων της κυβικής καμπύλης, η οποία το καθιστά αβελιανή ομάδα, που λέγεται ομάδα Mordell-Weil της καμπύλης. Παρατηρήστε ότι ουδέτερο στοιχείο της ομάδας είναι το επ' άπειρο σημείο της καμπύλης, ενώ το αντίθετο ενός σημείου  $P$  είναι το τρίτο σημείο τομής της καμπύλης και της ευθείας, η οποία ενώνει το επ' άπειρο σημείο της καμπύλης με το  $P$ . Αρκετά δυσκολώτερο είναι να αποδείξομε την προσεταιριστικότητα της πράξης  $+$ .

Στο παράδειγμα της (1), ξεκινώντας από το  $P = (0, -1)$ , βρίσκομε

$$2P = P + P = \left(\frac{136}{27}, \frac{17}{9}\right), \quad 3P = 2P + P = \left(\frac{24402}{2197}, -\frac{664}{169}\right).$$



Στις αρχές του αιώνα, ο H. Poincaré διατύπωσε την εικασία ότι η ομάδα αυτή είναι πεπερασμένα παραγόμενη, κάτι που αποδείχθηκε από τον L.J. Mordell στα 1922. Αυτό σημαίνει ότι, για κάθε καμπύλη όπως η (1) είτε η (2), υπάρχουν πεπερασμένα το πλήθος σημεία  $P_1, \dots, P_n$ , ονομαζόμενα γεννήτορες, έτσι ώστε κάθε ρητό σημείο πάνω στην αντίστοιχη καμπύλη να εκφράζεται ως  $m_1P_1 + \dots + m_nP_n$  για κατάλληλους ακέραιους  $m_1, \dots, m_n$ . Αν, για παράδειγμα, το σύνολο των γεννητόρων της ομάδος Mordell-Weil είναι μονοσύνολο, όπως στην περίπτωση της (2), που αποτελείται μόνο από το  $P = (0, 1)$ , βρίσκομε διαδοχικά,

$$2P = \left(\frac{21}{4}, -\frac{71}{8}\right), \quad 3P = \left(\frac{568}{441}, \frac{13175}{9261}\right),$$

$$4P = \left(\frac{146769}{80656}, -\frac{36583777}{22906304}\right), \quad 5P = \left(\frac{157151400}{48846121}, \frac{1226178094681}{341385539669}\right),$$

κλπ, απ' όπου βρίσκονται αμέσως και τα  $-P, -2P, -3P, \dots$  : Το  $-mP$  έχει την ίδια τετμημένη με το  $mP$  και αντίθετη τεταγμένη. Η διαδικασία αυτή δίνει τον

αλγόριθμο για την εύρεση όλων των ρητών σημείων της (2). Αν οι γεννήτορες είναι περισσότεροι, ο αλγόριθμος είναι κάπως πολυπλοκώτερος.

Οι καμπύλες (1) και (2) ανήκουν στην κατηγορία των λεγομένων **ελλειπτικών**, οι οποίες παίζουν σημαντικώτατο ρόλο στη σύγχρονη θεωρία των Αριθμών και τα Μαθηματικά, εν γένει. Χαρακτηριστικό παράδειγμα εντυπωσιακής εφαρμογής των ελλειπτικών καμπύλων είναι η απόδειξη του **Μεγάλου Θεωρήματος του Fermat**, το οποίο διατυπώθηκε γύρω στα 1637 και αποδείχθηκε περίπου 360 χρόνια αργότερα, στα 1995, από τον A. Wiles. Η μεγαλειώδης αυτή απόδειξη ξεκινά από την παρατήρηση του G. Frey ότι, αν  $a^n + b^n = c^n$  είναι μία λύση με  $abc \neq 0$ , τότε η ελλειπτική καμπύλη  $y^2 = x(x - a^n)(x + b^n)$  έχει ορισμένες αξιοσημείωτες ιδιότητες από την άποψη της Θεωρίας των Ελλειπτικών Καμπύλων. Ο Wiles θέτει τον μηχανισμό αυτής της Θεωρίας σε πλήρη λειτουργία, εν συνδυασμό με την αλγεβρική **Θεωρία Αναπαραστάσεων Ομάδων**, επιτυγχάνοντας την απόδειξη. Το έδαφος είχε προετοιμασθεί, ήδη από ετών, λόγω του σημαντικού έργου και άλλων πρώτου μεγέθους μαθηματικών. Ας τονισθεί με έμφαση το εξής:

Δεν πρόκειται για απόδειξη, που έγινε με αυθαίρετα, ουρανοκατέβατα, πανέξυπνα τεχνάσματα, των οποίων η εμβέλεια περιορίζεται στο συγκεκριμένο θεώρημα. Η απόδειξη ανοίγει σημαντικούς δρόμους στα Μαθηματικά.

Εδώ αξίζει να τονισθεί ότι, μερικές φορές, κατά τη διάρκεια αποτυχημένων προσπαθειών, όταν αυτές προέρχονται από εμπνευσμένους μαθηματικούς, οι μέθοδοι που αναπτύσσονται και τα επινοούμενα μαθηματικά εργαλεία μπορεί να φέρουν, κυριολεκτικά, επανάσταση. Χαρακτηριστική η περίπτωση του E.E. Kummer. Η απόδειξη που έδωσε, περί τα μέσα του περασμένου αιώνα, για το Τελευταίο Θεώρημα του Fermat αποδείχθηκε λανθασμένη, αλλά έβαλε τις ουσιαστικές βάσεις της **Αλγεβρικής Θεωρίας Αριθμών**, βασικός ρόλος της οποίας είναι να επεκτείνει την Αριθμητική των συνήθων ακεραίων σε ακεραίους αλγεβρικών αριθμών.<sup>3</sup> Δύο προβλήματα, εντελώς στοιχειώδη, στα οποία δεν θα μπορούσαμε να απαντήσουμε χωρίς την Αλγεβρική Θεωρία Αριθμών :

- Εκτός από το 25, υπάρχει άλλο τέλειω τετράγωνο, που αυξημένο κατά 2 να δίνει τέλειω κύβο ; (Fermat). Δηλαδή, έχει άλλες θετικές ακέραιες λύσεις η  $x^2 + 2 = y^3$ , πλην της  $(x, y) = (5, 3)$  ;
- Για  $x = 1, 3, 5, 11, 181$  ο αριθμός  $x^2 + 7$  είναι δύναμη του 2 :  $2^3, 2^4, 2^5, 2^7, 2^{15}$ , αντιστοίχως. Συμβαίνει αυτό για άλλα  $x$ ; (S. Ramanujan, 1913). Δηλαδή, υπάρχουν κι άλλες θετικές ακέραιες λύσεις της  $x^2 + 7 = 2^n$ , πλην των  $(x, n) = (1, 2), (3, 4), (5, 5), (11, 7), (181, 15)$  ;

Το πρώτο πρόβλημα είναι προκλητικό στην απλότητά του και γίνεται ακόμη προκλητικώτερο όταν διαπιστώνει κανείς ότι η Στοιχειώδης Θεωρία Αριθμών δεν αρκεί για τη λύση του. Το δεύτερο έχει αρκετά δυσκολώτερη λύση και είναι αξιοσημείωτο ότι βρίσκει εφαρμογή στη **Θεωρία των Κωδίκων**. Η απάντηση και στα δύο είναι αρνητική.

<sup>3</sup>Ένας μιγαδικός αριθμός λέγεται αλγεβρικός αν είναι ρίζα πολυωνόμου με ρητούς συντελεστές.

Τσως νομίζει κανείς ότι οι Ελλειπτικές Καμπύλες είναι θέμα που αφορά αποκλειστικά τα λεγόμενα «καθαρά» Μαθηματικά. Καθόλου, αφού έχει λ.χ. στενή σχέση με την Κρυπτογραφία! Στα 1987, ο H.W. Lenstra επινόησε μία μέθοδο για την παραγοντοποίηση ακεραίων αριθμών βασισμένη στις Ελλειπτικές Καμπύλες. Αν και, στα πλαίσια αυτής της διάλεξης, είναι αδύνατον να δοθούν έστω και λίγες λεπτομέρειες γι' αυτή τη μέθοδο, μπορούμε όμως να δώσουμε μία σαφή ιδέα της σχέσης, που έχει η ανάλυση ενός ακεραίου σε πρώτους παράγοντες, με την Κρυπτογραφία.

Το πρόβλημα της παραγοντοποίησης των ακεραίων αριθμών είναι, από θεωρητική άποψη, τετριμμένο. Από άποψη υπολογιστική, είναι εξαιρετικά δυσχερές, ένα από τα πιο δύσκολα, όταν επιχειρήσει κανείς την παραγοντοποίηση ακεραίων με πολλά ψηφία. Έστω ο ακεραίος  $n = pq$ , όπου οι  $p, q$  είναι διαφορετικοί πρώτοι. Αν σας δοθεί ο  $n$ , καθώς και η πληροφορία ότι είναι γινόμενο δύο διαφορετικών πρώτων και σας ζητηθεί να βρείτε αυτούς τους πρώτους, τι θα κάνετε, στην περίπτωση που ο  $n$  έχει 20 με 22 ψηφία; Γύρω στα 1970, ένα τέτοιο εγχείρημα ήταν περίπου αδύνατο. Σήμερα, χάρη στην επινόηση νέων έξυπνων μεθόδων παραγοντοποίησης και στις σύγχρονες υπολογιστικές δυνατότητες, μπορούμε να δώσουμε εύκολα την απάντηση, αν ο προσωπικός μας υπολογιστής διαθέτει το κατάλληλο πρόγραμμα (π.χ. ένα πρόγραμμα βασισμένο στη μέθοδο των Ελλειπτικών Καμπύλων, που προαναφέραμε). Αν ο  $n$  έχει περί τα 130 ψηφία, η κατάσταση γίνεται οριακή, υπό τις σημερινές συνθήκες. Αν τα ψηφία του  $n$  είναι 150, η απάντηση, με τις σημερινές υπολογιστικές μας δυνατότητες, θα έλθει ύστερα από 2 με 3 αιώνες! Γιατί όμως είναι σημαντικό να μπορούμε να παραγοντοποιούμε τόσο μεγάλους ακεραίους;

Μία από τις σημαντικότερες σύγχρονες μεθόδους κρυπτογραφίας – η μέθοδος **RSA** – που αναπτύχθηκε στη δεκαετία του '80, βασίζεται στο πρακτικώς ανέφικτο της παραγοντοποίησης ενός πολύ μεγάλου ακεραίου. Η βασική ιδέα της μεθόδου θα γίνει κατανοητή με ένα παράδειγμα, στο οποίο, για ευνοήτους λόγους, δεν θα κάνουμε χρήση μεγάλων αριθμών. Πρώτ' απ' όλα, στα γράμματα του αλφαβήτου A, B, ..., Ω, αντιστοιχούμε τους αριθμούς 01, 02, ..., 24. Στην αρχή ή και στο τέλος του μηνύματος μπορεί να προσθέσουμε κάποιο «κενό γράμμα», στο οποίο αντιστοιχεί ο αριθμός 25, όταν θέλουμε το συνολικό πλήθος των μονοψηφίων αριθμών του μηνύματος να είναι πολλαπλάσιο ενός συγκεκριμένου αριθμού (στο παρακάτω παράδειγμα, ο αριθμός αυτός είναι το 3). Η φράση

#### ΘΕΩΡΙΑ ΤΩΝ ΑΡΙΘΜΩΝ

γίνεται

$$25\ 08\ 05\ 24\ 17\ 09\ 01\ 19\ 24\ 13\ 01\ 17\ 09\ 08\ 12\ 24\ 13\ 25\ . \quad (3)$$

Κολλώ τους αριθμούς και τους ξαναχωρίζω ανά τρεις:

$$250\ 805\ 241\ 709\ 011\ 924\ 130\ 117\ 090\ 812\ 241\ 325\ . \quad (4)$$

Θέλω να στείλω αυτό το μήνυμα στον Δημήτρη. Σε κάποιο ειδικό κατάλογο βρίσκω το κλειδί του Δημήτρη. Είναι το

$$(N, e) = (90113, 3631) .$$

Εδώ πρέπει να φαντασθείτε ότι, σε πραγματικές συνθήκες, ο  $N$  είναι ένας τεράστιος ακέραιος και ο  $e$  είναι αναλόγου μεγέθους. Ακολουθώ την εξής διαδικασία: Υπολογίζω  $\text{mod } N$  τις δυνάμεις με εκθέτη  $e$  των αριθμών της λίστας (4). Αυτή η διαδικασία μου δίνει 12 5-ψήφιους ακεραίους (αν έχουν λιγώτερα από 5 ψηφία προσθέτω μηδενικά στην αρχή), τους οποίους κολλώ μεταξύ τους. Ο Δημήτρης λαμβάνει το μήνυμα

300336359482611039225347951332344851015133276381578261143145 .

και ακολουθεί την εξής διαδικασία αποκρυπτογράφησης: Το χωρίζει σε 5-ψήφιους αριθμούς, 30033, 63594, ... και ξέρει ότι, αν  $a$  είναι ένας από αυτούς, αυτός προήλθε από κάποιον τριψήφιο  $x$ , τέτοιοι ώστε

$$x^e \equiv a \pmod{N} . \quad (5)$$

Για την εύρεση του  $x$  γίνεται χρήση της συναρτήσεως  $\phi$  του Euler: Αν  $n$  είναι ένας θετικός ακέραιος, ο αριθμός  $\phi(n)$  δείχνει το πλήθος των θετικών ακεραίων, οι οποίοι είναι  $\leq n$  και πρώτοι προς τον  $n$ . Για τον υπολογισμό του  $\phi(n)$  μας χρειάζεται η ανάλυση του  $n$  σε πρώτους παράγοντες. Συγκεκριμένα,

αν όλοι οι διαφορετικοί πρώτοι διαιρέτες του  $n$  είναι  $p_1, \dots, p_k$ , τότε

$$\phi(n) = n \left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_k}\right) .$$

Στην περίπτωσή μας, επειδή  $N = 97 \cdot 929$ ,  $\phi(N) = 96 \cdot 928 = 89088$ . Επίσης, γίνεται χρήση του **Θεωρήματος του Euler**, που λέει ότι, για κάθε θετικό ακέραιο  $n$  και για κάθε  $x$  πρώτο προς τον  $n$ ,

$$x^{\phi(n)} \equiv 1 \pmod{n} .$$

Ειδικότερα, αν  $k \equiv 1 \pmod{\phi(N)}$ , οπότε  $k = 1 + m \cdot \phi(N)$  για κάποιον ακέραιο  $m$ , τότε το Θεώρημα του Euler συνεπάγεται ότι  $x^k = x(x^{\phi(N)})^m \equiv x \cdot 1 \equiv x \pmod{N}$ . Άρα, αν βρούμε  $f$  τέτοιο ώστε

$$e \cdot f \equiv 1 \pmod{\phi(N)} ,$$

τότε  $x^{ef} \equiv x \pmod{N}$ , άρα, από την (5),  $x \equiv a^f \pmod{N}$ , επιλύοντας έτσι την (5). Στο συγκεκριμένο παράδειγμα, οι συνήθεις στοιχειώδεις τεχνικές για την επίλυση γραμμικών ισοδυναμιών δίνουν  $f = 13519$ , άρα,  $x \equiv a^{13519} \pmod{90113}$ . Σημειώστε ότι, η ύψωση σε τεράστιο εκθέτη, επειδή γίνεται  $\text{mod } N$ , δεν δημιουργεί κανένα υπολογιστικό πρόβλημα. Ακολουθώντας ο Δημήτρης αυτή τη διαδικασία, διαδοχικά για  $a = 30033, 63594, \dots, 43145$  θα ξαναβρεί τους αριθμούς της λίστας (4), θα τους κολλήσει και, τέλος, θα τους χωρίσει σε διψήφια τμήματα για να πάρει τους αριθμούς της λίστας 3 και, συνεπώς, το μήνυμα που του έστειλα.

Φυσικά, την ίδια διαδικασία θα μπορούσε να ακολουθήσει και οποιοσδήποτε άλλος ανεπιθύμητος υπέκλεπτε το κρυπτογραφημένο μήνυμα. Αν όμως, αντί του συγκεκριμένου  $N$  είχαμε κάποιον ακέραιο με 150 ψηφία, γινόμενο δύο πρώτων, κανείς άλλος, πλην του Δημήτρη - ο οποίος έφτιαξε τον  $N$  - δεν θα μπορούσε να υπολογίσει το  $\phi(N)$ , άρα δεν θα μπορούσε να ακολουθήσει τη διαδικασία της

αποκρυπτογράφησης, εκτός κι αν είχε την υπομονή να διαβάσει το μήνυμά μου ύστερα από 200 ή περισσότερα χρόνια! Σημειώστε, τέλος, ότι, αν εγώ που έστειλα το μήνυμα ξεχάσω το περιεχόμενό του, δεν έχω ελπίδα να το ξαναμάθω – αφού ξέρω μεν τον  $N$ , όχι όμως και την ανάλυσή του σε πρώτους παράγοντες – εκτός αν και εγώ έχω ανάλογη υπομονή!

Με αυτό το παράδειγμα εφαρμογής της Θεωρίας των Αριθμών στον λεγόμενο «πραγματικό κόσμο» κλείνω τη διάλεξή μου, ευχαριστώντας σας για την προσοχή σας.