Κρυφές πληροφορίες

Ή, πώς δύο μυστικά μάς δίνουν μια βεβαιότητα

S. Artyomov, Y. Gimatov και V. Fyodorov

ΘΑ ΘΕΛΑΜΕ ΝΑ ΣΑΣ ΜΙΛΗΣΟΥμε για ένα πρόβλημα που η λύση του απαιτεί ιδιαίτερα πολύπλοκη λογική.

Ένας μαθηματικός M είπε στους μαθηματικούς Π και Σ: «Έχω σκεφτεί δύο φυσικούς αριθμούς. Και οι δύο είναι μεγαλύτεροι από τη μονάδα, ενώ το άθροισμά τους είναι μικρότερο του εκατό. Θα αποκαλύψω τώρα στον Π, κρυφά από την Σ, το γινόμενο αυτών των αριθμών. Και μετά θα πω στην Σ, κρυφά από τον Π, το άθροισμά τους». Έτσι έγινε, και στη συνέχεια ο M ζήτησε από τους συναδέλφους του να μαντέψουν τους αριθμούς. Τότε, ο Π και η Σ έκαναν την επόμενη συζήτηση (οι δηλώσεις του Π συμβολίζονται με το γράμμα π και της Σ με το γράμμα σ):

«Απ' ό,τι φαίνεται, δεν μπορώ να πω ποιοι είναι οι αριθμοί». (π_1)

«Ήξερα από πριν ότι δεν θα μπορούσες». (σ_1)

«Αφού είναι έτσι, τους γνωρίζω!» (π_2)

«Τότε τους γνωρίζω κι εγώ!» (σ_1)

Προσπαθήστε τώρα να μαντέψετε εσείς τους αριθμούς!

1. Είναι πράγματι δυνατόν;

Εκ πρώτης όψεως, φαίνεται ότι είναι αδύνατον να λυθεί το πρόβλημα: πώς μπορούμε να μαντέψουμε τους αριθμούς όταν δεν έχει δοθεί καμία πληροφορία γι' αυτούς;

Ας δοκιμάσουμε ένα συγκεκριμένο παράδειγμα. Έστω ότι ο M σκέφτηκε τους αριθμούς 7 και 42. Επομένως, οι αριθμοί που ανέφερε στον Π και την Σ ήταν 294 και 49, αντίστοιχα. Τι θα συμβεί λοιπόν; Ο Π δεν μπορεί να μαντέψει τους αριθμούς —καθόλου περίεργο, αφού γνωρίζει μόνο το γινόμενό τους. Ή μάλλον, όχι μόνο το γινόμενο. Γνωρίζει επίσης ότι είναι φυσικοί αριθμοί, μεγαλύτεροι από το 1, και ότι το άθροισμά τους είναι μικρότερο από το 100. Σε τι βοηθούν όλα αυτά;

Συμβολίζουμε τους άγνωστους αριθμούς με k_0 και ℓ_0 και υποθέτουμε, χωρίς να βλάπτεται η γενικότητα, ότι $k_0 \leq \ell_0$. Συμβολίζουμε το γινόμενο $k_0 \cdot \ell_0$ με p_0 και το άθροισμα $k_0 + \ell_0$ με s_0.

Μπορούμε τώρα να πούμε πως ο Π πληροφορήθηκε ότι $p_0 = 294$. Τότε, οι πιθανές τιμές του k_0 είναι 2, 3, 6, 7 και 14. Το ℓ_0 σ' αυτή την περίπτωση είναι, αντίστοιχα, 147, 98, 49, 42, ή 21. Οι δύο πρώτες τιμές του k_0 δεν μας ικανοποιούν, διότι το άθροισμα γίνεται πολύ μεγάλο: $s_0 > 100$. Μένουν ακόμη τρεις πιθανότητες, οπότε πραγματικά ο P δεν μπορεί να μαντέψει τους αριθμούς.

Ας συνεχίσουμε. Η μαθηματικός Σ ισχυρίζεται πως γνώριζε προκαταβολικά ότι ο Π αδυνατούσε να μαντέψει τους αριθμούς. Πώς μπορούσε να το γνωρίζει αυτό; Πρέπει να είχε ελέγξει όλες τις δυνατές αναπαραστάσεις του αριθμού της s_0 ως αθροίσματος δύο επιτρεπτών αριθμών:

$$49 = 2 + 47 = 3 + 46 = ... = 24 + 25.$$

Ο R μπορεί να σκέφτηκε ένα οποιοδήποτε από αυτά τα ζεύγη αριθμών. Είπε στον Π ένα από τα γινόμενα $n \cdot (49 - n)$, και η Σ υποστηρίζει ότι ο Π, όποιο και αν ήταν το γινόμενο που του είπε, δεν θα μπορούσε να ανακαλύψει τους αριθμούς.

Τι θα συνέβαινε, όμως, αν για κάποιο n και οι δύο αριθμοί, n και $49 - n$, είναι πρώτοι; Αν, για παράδειγμα, ο M είχε σκεφτεί το 2 και το 47, θα έδινε στον Π το αριθμό 94, και ο τελευταίος θα μπορούσε εύκολα να μαντέψει τους μυστικούς αριθμούς.

Έτσι, αν ο M είχε σκεφτεί το 7 και το 42, τότε η S, μαθαίνοντας το άθροισμα $s_0 = 49$, δεν θα είχε δικαίωμα να κάνει τη δήλωση (σ_1). Αυτό σημαίνει ότι ο M δεν σκέφτηκε τους αριθμούς 7 και 42.

Επομένως, αποδεικνύεται ότι *μπορούμε* να πούμε κάτι για τους άγνωστους αριθμούς.

Και τώρα που διασκεδάσαμε τις αρχικές μας αμφιβολίες, ας δούμε πώς μπορούμε να προχωρήσουμε. Μια μέθοδος επίλυσης είναι ήδη φανερή: μπορούμε απλώς να ακολουθήσουμε το δρόμο της πλήρους απαρίθμησης —της δοκιμής και του λάθους— και να ελέγξουμε όλα τα ζεύγη που ικανοποιούν τις συνθήκες

$$2 \leq k_0 \leq \ell_0 \leq 97, \qquad (1)$$
$$4 \leq k_0 + \ell_0 \leq 99, \qquad (2)$$

για να δούμε ποια από αυτά «επιβιώνουν» από το διάλογο (π_1)-(σ_2).

Αφού το πλήθος των δυνατοτήτων είναι σε κάθε περίπτωση πεπερασμένο, θα μπορούσαμε πραγματικά να

Εικονογράφηση: Vera Khlebnikova

συνεχίσουμε με αυτό τον άτεχνο τρόπο, και κάποια στιγμή να βρούμε την απάντηση. Αλλά κάτι τέτοιο δεν θα ήταν βαρετό; Ας προσπαθήσουμε λοιπόν να περιορίσουμε την έρευνα.

Πρώτα απ' όλα, αντί των τιμών των k_0, ℓ_0, θα ερευνήσουμε τις τιμές του s_0, αφού υπάρχουν περισσότερα από 2.000 δυνατά ζεύγη (k_0, ℓ_0), ενώ οι δυνατότητες για το s_0 είναι λιγότερες από εκατό. Πάντως, ακόμη και σ' αυτή την περίπτωση, η άμεση έρευνα είναι μακρά και επίπονη.

2. Η εικασία των Goldbach-Euler

Τι πληροφορίες μπορούμε να εξαγάγουμε από τις (π_1) και (σ_1); Ποιο είναι το νόημα αυτών των προτάσεων; Η πρώτη πρόταση, η (π_1), μας λέει προφανώς ότι

το p_0 δεν παραγοντοποιείται μονοσήμαντα σε γινόμενο δύο αριθμών που ικανοποιούν τις ανισότητες (1) και (2). (π_1')

Η δεύτερη πρόταση σημαίνει ότι

με όποιον τρόπο κι αν αναλύσουμε τους αριθμούς s_0 σε άθροισμα δύο αριθμών που ικανοποιούν την ανισότητα (1), το γινόμενο των προσθετέων θα έχει την ιδιότητα (π_1'). (σ_1')

Η πρώτη συνθήκη εξαιρεί μερικά γινόμενα· η δεύτερη αποκλείει ορισμένα αθροίσματα.

Ειδικά, από την (σ_1') έπεται ότι είναι αδύνατον να παρασταθεί το s_0 ως άθροισμα δύο πρώτων. (Διαφορετικά, το γινόμενο αυτών των πρώτων έχει μία και μοναδική παραγοντοποίηση σε δύο παράγοντες που ικανοποιούν τις ανισότητες (1) και (2), και επομένως δεν ικανοποιεί την (π_1').)

Κάθε άρτιος αριθμός, όμως, που ικανοποιεί την ανισότητα (2) παριστάται ως άθροισμα δύο πρώτων (αυτό μπορούμε να το πιστοποιήσουμε άμεσα για όλους τους αριθμούς 4, 6, 8, ..., 98). Άρα, το s_0 είναι *περιττό*. Επιπλέον, το $s_0 - 2$ είναι σύνθετος αριθμός —διαφορετικά το $s_0 = 2 + (s_0 - 2)$ είναι μια παράσταση του s_0 ως αθροίσματος δύο πρώτων. Αν απορρίψουμε τους αριθμούς που δεν ικανοποιούν αυτές τις δύο συνθήκες, καταλήγουμε σε 24 δυνατές τιμές του s_0.

Το γεγονός που χρησιμοποιήσαμε στην προηγούμενη παράγραφο —ότι όλοι οι άρτιοι αριθμοί από το 4 έως το 98 μπορούν να γραφτούν ως άθροισμα δύο πρώτων— συνδέεται με ένα συναρπαστικό μαθηματικό πρόβλημα. Το 1742, ένα μέλος της Ακαδημίας Επιστημών της Αγίας Πετρούπολης, ο Christian Goldbach (Γερμανός που προσέφερε τις υπηρεσίες του στο ρωσικό κράτος) έστειλε μια επιστολή στον Leonard Euler στην οποία διατύπωνε την εικασία ότι κάθε περιττός αριθμός μεγαλύτερος του 5 μπορεί να παρασταθεί ως άθροισμα τριών πρώτων. Ο Euler στην απάντησή του πρότεινε την εικασία ότι κάθε άρτιος αριθμός μεγαλύτερος του 2 είναι άθροισμα δύο πρώτων. (Δεν είναι δύσκολο να συναγάγουμε την εικασία του Goldbach από την υπόθεση του Euler —δοκιμάστε το μόνοι σας!)

Και οι δύο εικασίες, για δύο σχεδόν αιώνες, φαινόταν αδύνατον να αποδειχτούν, παρότι είχαν επαληθευτεί με άμεση έρευνα για όλους τους αριθμούς έως το 9.000.000.

Το 1930, ο σπουδαίος ρώσος μαθηματικός L.G. Shnirelman απέδειξε ότι υπάρχει ένας αριθμός k τέτοιος ώστε κάθε ακέραιος $n > 1$ να παριστάται ως άθροισμα k το πολύ πρώτων αριθμών. Στην απόδειξη του Shnirelman, ο αριθμός k ήταν μάλλον μεγάλος· αργότερα αποδείχτηκε ότι το θεώρημα αληθεύει για $k = 20$.

Το 1934, ένας άλλος διάσημος ρώσος μαθηματικός, ο I.M. Vinogradov, απέδειξε ότι κάθε αριθμός $n > n_0$, για κάποιο συγκεκριμένο n_0, γράφεται ως άθροισμα τριών πρώτων. Σήμερα, στην εποχή των υπολογιστών, θα φαινόταν λογική η υπόθεση ότι μπορούμε να στηριχτούμε στη «μηχανή» για να ελέγξουμε όλους τους υπόλοιπους αριθμούς (από το 7 έως το n_0). Ωστόσο, η σταθερά n_0 του Vinogradov είναι τόσο μεγάλη ($n_0 > 2^{2^{16}}$), ώστε η επαλήθευση υπερβαίνει ακόμη τις δυνατότητες των υπολογιστών.[1]

Όσον αφορά την εικασία του Euler, δεν έχει ακόμη επιτευχθεί κάποια σημαντική πρόοδος προς την κατεύθυνση της απόδειξής της.

3. Δεύτερος γύρος

Μπορούμε να μειώσουμε κι άλλο το πλήθος των υποψηφίων για το s_0: μπορούμε να συμπεράνουμε από την (σ_1') ότι

$$s_0 < 55. \tag{3}$$

Για να δούμε γιατί ισχύει αυτό, ας υποθέσουμε ότι, αντίθετα, $s_0 \geq 55$. Τότε, το s_0 δεν ικανοποιεί τη (σ_1'): μπορούμε να το αναλύσουμε στο άθροισμα δύο όρων που ικανοποιούν την ανισότητα (1), το γινόμενο των οποίων δεν ικανοποιεί τη συνθήκη (π_1'). Η ανάλυση είναι η $s_0 = 53 + (s_0 - 53)$. Πραγματικά, το γινόμενο $53 \cdot (s_0 - 53)$ παραγοντοποιείται μόνο με έναν τρόπο σε γινόμενο δύο παραγόντων που το άθροισμά τους δεν υπερβαίνει το 100, διότι ο ένας από τους δύο έχει αναγκαστικά τη μορφή $53d$ —αφού το 53 είναι πρώτος—, και είναι μεγαλύτερος από το 100 αν $d > 1$. Άρα, $d = 1$, και η παραγοντοποίηση είναι μοναδική. Αυτό όμως έρχεται σε αντίθεση με την ιδιότητα (σ_1') του s_0!

Μετά την απόδειξη της ανισότητας (3), το πλήθος των δυνατών τιμών του s_0 μειώνεται σε έντεκα:

$$11, 17, 23, 27, 29, 35, 37,$$
$$41, 47, 51, 53. \tag{4}$$

Ας προσπαθήσουμε να ανακαλύψουμε ποιοι από αυτούς τους αριθμούς συμφωνούν με τη συνθήκη (σ_1') χωρίς άμεση έρευνα. Έστω s ένας από τους αριθμούς (4). Το s είναι περιττό, συνεπώς όταν δύο αριθμοί αθροιζόμενοι μας δίνουν το s, ο ένας τους είναι άρτιος και ο άλλος περιττός. Επομένως, μπορούμε να γράψουμε $s = 2a + m$. Αν το s δεν ικανοποιεί τη συνθήκη (σ_1'), τότε για κάποιο συγκεκριμένο a υπάρχει μία και μοναδική παραγοντοποίηση του γινομένου $2am$.

Αυτό το a δεν μπορεί να ισούται με τη μονάδα, διότι υπάρχουν τουλάχιστον δύο παραγοντοποιήσεις του $2m$. Πράγματι, ας υποθέσουμε ότι $a = 1$. Τότε, ο αριθμός m είναι σύνθετος, οπότε μπορούμε να γράψουμε $m = uv$, όπου $u > 2$ και $v > 2$, ενώ και οι

1. Αυτή η εκτίμηση μπορεί να μην αληθεύει πλέον σήμερα (το άρθρο δημοσιεύτηκε αρχικά στο *Kvant* το 1977).

δύο παραγοντοποιήσεις

$$2m = 2u \cdot v = 2 \cdot uv$$

μας ικανοποιούν:

$$2 + uv = 2 + m = s \leq 100$$

και

$$2u + v = 2 + uv - (u-1)(v-2) < 2 + uv \leq 100.$$

Έπεται ότι $a \geq 2$.

Τώρα, είτε $a = m$ είτε $a \neq m$, και μπορούμε να εξετάσουμε τις δύο περιπτώσεις ξεχωριστά. Αν $a \neq m$, τότε η $p = 2a \cdot m$ και η $p = 2m \cdot a$ είναι δύο διαφορετικές παραγοντοποιήσεις. Αφού $2a + m = s < 100$ και η παραγοντοποίηση του p είναι μοναδική, πρέπει να έχουμε $2m + a \geq 100$. Ταυτόχρονα, από την $s = 2a + m < 53$, έπεται ότι $m \leq 53 - 2a$, και επομένως $2m + a \leq 106 - 3a$. Συνεπώς, $100 \leq 2m + a \leq 106 - 3a$, άρα $a \leq 2$. Σ' αυτή την περίπτωση, λοιπόν, έχουμε $a = 2$, $2m + a = 100$ και $m = 49$, οπότε οδηγούμαστε στη μοναδική «ύποπτη» τιμή $s = 53$ και στην ανάλυσή της $53 = 4 + 49$.

Στην περίπτωση $a = m$, ο αριθμός $s = 3a$ διαιρείται με το 3. Δύο μόνο από τους αριθμούς (4) είναι πολλαπλάσια του 3: το 27 και το 51. Οι «ύποπτες» αναλύσεις τους είναι $27 = 18 + 9$ και $51 = 34 + 17$.

Ο αριθμός 51 δεν ικανοποιεί την (σ_1') —πράγματι, το γινόμενο $17 \cdot 34$ παραγοντοποιείται μόνο με έναν τρόπο σε δύο παράγοντες με άθροισμα μικρότερο του 100, και επομένως μπορούμε να το εξαιρέσουμε από τη λίστα των «υποψηφίων για το s_0».

Οι αριθμοί 27 και 53 εξακολουθούν να είναι στη λίστα: ικανοποιούν την (σ_1'), διότι για το 27 έχουμε $9 \cdot 18 = 2 \cdot 81$ και $2 + 81 < 100$, και για το 53 έχουμε $4 \cdot 49 = 7 \cdot 28$ και $7 + 28 < 100$.

Επομένως, απομένουν δέκα «υποψήφιοι»: 11, 17, 23, 27, 29, 35, 37, 41, 47 και 53. Όλοι τους ικανοποιούν την (σ_1').

4. «Τότε τους γνωρίζω κι εγώ»

Τέλος, ας χρησιμοποιήσουμε τις προτάσεις (π_2) και (σ_2). Θα μπορούσαμε να τις ερμηνεύσουμε όπως τις δύο προηγούμενες. Υπάρχει όμως ένας συντομότερος τρόπος.

Από την (σ_2) και την ανισότητα (3) συμπεραίνουμε ότι

$$s_0 < 33. \qquad (5)$$

Ας υποθέσουμε ότι αυτό δεν αληθεύει. Τότε, $s_0 \geq 33$, και η μαθηματικός Σ, αναλύοντας το s_0 σε άθροισμα δύο όρων με κάθε δυνατό τρόπο, θα εύρισκε τις εξής παραλλαγές: $s_0 = (s_0 - 31) + 31 = (s_0 - 29) + 29$. Η πορεία των σκέψεών της θα ήταν τότε η εξής: αν είχε δοθεί στον Π το γινόμενο $(s_0 - 31) \cdot 31$, τότε, αν χρησιμοποιούσε την εκτίμηση (3) και το γεγονός ότι το 31 είναι πρώτος, θα είχε καταλάβει ότι το $(s_0 - 31) \cdot 31$ έχει μία μόνο παραγοντοποίηση τέτοια ώστε το άθροισμα των δύο όρων της να ικανοποιεί την ανισότητα (3). Τότε, ο Π θα μάντευε τους άγνωστους αριθμούς. Το ίδιο επιχείρημα, όμως, εφαρμόζεται και στο γινόμενο $(s_0 - 29) \cdot 29$.

Επομένως, στην περίπτωση $s_0 \geq 33$, η μαθηματικός Σ δεν θα μπορούσε να προσδιορίσει ακριβώς τα k_0, ℓ_0 ακόμη και μετά τη δήλωση (π_2) του Π, αντίθετα απ' ό,τι συνέβη στην ιστορία μας.

Άρα, η ανισότητα (5) είναι πραγματικά αληθής, και έτσι απομένουν μόνο πέντε αριθμοί: 11, 17, 23, 27, 29.

Επιπλέον, αν $p_0 = 2^n \cdot p$, όπου p περιττός πρώτος και $n > 1$, τότε ο Π μπορεί να προσδιορίσει με βεβαιότητα τους μυστικούς αριθμούς, διότι υπάρχει μόνο ένα περιττό άθροισμα της μορφής $2^{n-t} + 2^t p$ —συγκεκριμένα, το $2^n + p$. Έτσι, αν το s_0 έχει δύο αναπαραστάσεις της μορφής $2^n + p$, τότε η Σ δεν μπορεί να βρει την απάντηση και να κάνει τη δήλωση (σ_2). Αυτή η παρατήρηση εξαιρεί τρεις ακόμη αριθμούς, τους $11 = 4 + 7 = 8 + 3$, 23 και 27, και αφήνει μόνο δύο υποψήφιους στη λίστα: το 17 και το 29.

5. Τότε τους γνωρίζουμε κι εμείς!

Στην περίπτωση του αριθμού $s_0 = 29$, το τελευταίο επιχείρημα δεν ισχύει, διότι υπάρχει μόνο μία αναπαράσταση της μορφής $2^n + p$ με p περιττό πρώτο $(29 = 16 + 13)$. Μπορούμε, όμως, να το χρησιμοποιήσουμε ελαφρά τροποποιημένο για την ανάλυση: $29 = 4 + 25$. Στην περίπτωση $p_0 = 4 \cdot 25$ έχουμε μόνο ένα ακόμη δυνατό περιττό άθροισμα εκτός από το 29, το $25 = 20 + 5$ (προφανώς $4 \cdot 25 = 5 \cdot 20$), αλλά τότε το $25 - 2$ είναι πρώτος, ενώ το $s_0 - 2$ πρέπει να είναι σύνθετος. Έτσι, σ' αυτή την περίπτωση είναι και πάλι αδύνατον να μαντέψει η Σ τους αριθμούς, συνεπώς η λίστα των υποψηφίων περιορίζεται σε έναν αριθμό, τον 17 —δηλαδή, είτε $s_0 = 17$ είτε το πρόβλημα δεν έχει λύση.

Λοιπόν, ποιο γινόμενο p_0 δόθηκε στον Π αν $s_0 = 17$; Ας ερευνήσουμε όλες τις δυνατές αναλύσεις του s_0 σε άθροισμα δύο όρων:

$$17 = 2 + 15 = 3 + 14 = \ldots = 8 + 9.$$

Για καθένα από τα αντίστοιχα γινόμενα, εκτός από το $4 \cdot 13$, ο Π θα ήταν αδύνατον να μαντέψει την απάντηση και να κάνει τη δήλωση (π_2). Για παράδειγμα, στην περίπτωση της ανάλυσης $17 = 2 + 15$, έχουμε $p_0 = 2 \cdot 15 = 30 = 5 \cdot 6$, αλλά και το 17 και το $11 = 5 + 6$ ικανοποιούν την ιδιότητα (σ_1').

Επομένως, η μοναδική δυνατή τιμή του p_0 είναι $4 \cdot 13 = 52$. Με αυτή την τιμή, ο μαθηματικός Π έχει τη δυνατότητα να μαντέψει τους αριθμούς, διότι απ' όλες τις δυνατές αναλύσεις του 52 σε δύο παράγοντες μόνο μία, η $52 = 4 \cdot 13$, δίνει περιττό άθροισμα παραγόντων. Συνεπώς, $s_0 = 17$, $p_0 = 52$, και οι αριθμοί που σκέφτηκε ο μαθηματικός M ήταν το 4 και το 13.

Προβλήματα

1. Είναι δυνατόν να παραστήσουμε κάθε περιττό αριθμό μεγαλύτερο του 3 ως άθροισμα της μορφής $2^n + p$, όπου p πρώτος; Αν όχι, δώστε το μικρότερο δυνατό αντιπαράδειγμα.

2. Ας υποθέσουμε ότι η ιστορία μας τροποποιείται ως εξής. Μέχρι την πρόταση (σ_1) παραμένει ίδια, αλλά μετά συνεχίζεται με τις επόμενες προτάσεις:

«Και γνώριζα εκ των προτέρων ότι αυτό το ήξερες από πριν». (π_2)

«Δεν γνωρίζω ποιοι είναι οι αριθμοί». (σ_2)

«Τότε τους γνωρίζω εγώ». (π_3)

Βρείτε τους ζητούμενους αριθμούς.

(B. Kukushkin)

ΑΠΑΝΤΗΣΕΙΣ, ΥΠΟΔΕΙΞΕΙΣ ΚΑΙ ΛΥΣΕΙΣ ΣΤΗ ΣΕΛ. 62