Το κλειδί του Παύλου και το σώμα του Galois

N. Lygeros

Ο δράκος δεν είχε εμφανιστεί.
Τουλάχιστον αυτό πίστευαν.
Θα χρειαζόταν εβδομάδες για να συνειδητοποιήσουν ότι ήταν πλέον μαζί τους.
Ο Paul Zimmermann εργαζόταν στη Nancy, στη Βόρεια Γαλλία. Είχε έρθει με το τρένο. Τον είχε καλέσει για το έργο του πάνω στα σώματα του Galois. Είχε τελειώσει το Πολυτεχνείο Παρισιού κι ήταν δάσκαλος από τους σπάνιους στο τομέα της πληροφορικής. Τότε δεν είχαν μιλήσει για τις ελλειπτικές καμπύλες αλλά θα γινόταν στο μέλλον ένα άλλο πεδίο συνεργασίας.
Ήταν πολύ δυναμικός κι ανοιχτός σε κάθε πρόβλημα που αφορούσε μαθηματικά και πληροφορική. Ήταν μάλλον πολύ τεχνικός για τον René Ouzilou, ο οποίος άνηκε στην παλιά σχολή της Γεωμετρίας. Αλλά γενικά είχε κάνει καλή εντύπωση στο σεμινάριο.
Η πραγματική συζήτηση έγινε στο γραφείο.
Και το τέρας περίμενε τη συνάντηση.
Ο Paul Zimmermann δεν ήταν του πίνακα αλλά της οθόνης.
Η εξήγηση του προβλήματος του Vavoda έγινε με διαφορετικό τρόπο. Του έδειξαν τα προγράμματα που είχαν γράψει για να τον βάλουν στο πλαίσιο.
Βέβαια, ποσοτικά, το τέρας έκανε τη μεγαλύτερη δουλειά.

* Είναι γρήγορος!
* Και μαθαίνει γρήγορα.
* Ενεργοποίησε το δίκτυο.
* Άνοιξε την ασφάλεια.
* Καλώς. Και τα προγράμματα;
* Άνοιξε τα κι αυτά.
* Έγινε

Maple, MuPAD
GP-Pari.
Πεδίο μάχης έτοιμο.
Οι αριθμοί έγιναν κώδικες κι οι πρώτοι αριθμοί κλειδιά.

* Εκτέλεση.
* Πολλαπλή.

– Όλα λειτουργούν περίφημα. Ας κάνουμε μερικά πειράματα.

Ο Michel Mizony το χάρηκε. Κρατούσε την πίπα του στην τσέπη του. Ήθελε να νιώθει τη ζεστασιά της. Δεν μιλούσε, χαμογελούσε. Ο Paul Zimmermann ήταν ριζικά διαφορετικός αλλά είχε το πνεύμα που έπρεπε. Το τέρας υπολόγιζε μ' όλα τα συστήματα που διέθετε. Έκανε ό,τι μπορούσε για να μην απογοητεύσει το διάσημο χειριστή.

* Φωτονεική επαφή.
* Όχι, ακόμα.
* Το ηλεκτρομαγνητικό πεδίο πάλευε με τους πρώτους αριθμούς.

– Νομίζω ότι είμαστε σε θέση να κάνουμε υπολογισμούς και με άλλα a.
– Ποιοι είναι οι υποψήφιοι;
– Θα τους πάρουμε όλους στη σειρά μέσω της ισοδυναμίας που βρήκαμε.

– Ας εξετάσουμε τους πρώτους κάθε ακτής.
– Ακτής;
– Ακτής του Vavoda… Έτσι ονομάσαμε τα παράθυρα των λύσεων.
– Ωραία.
– a = 6.
– n = 194.
– a = 12.
– n = 40123.
– a = 18.
– n = 10553419.
– a = 24.
– n = 3140422032.
– a = 30.
– n = 1003652348061.
– Υπάρχουν λύσεις σε κάθε ισοδυναμία.
– Είναι απίστευτο.
– Κι όμως.
– Επιπλέον, υπάρχουν τετραπλές λύσεις για a == 6,12,18, 24, 30.
– Και πενταπλές λύσεις για a = 30.
– Το αποτέλεσμά μας φαίνεται να είναι βέλτιστο για τις πρώτες τιμές.
– Ας εξετάσουμε τώρα τη σταθερότητα του a.
– Με ανισότητες…
– Αρκεί.
– Μπορεί.
– Θυμάμαι και κάποια νέα αποτελέσματα.
– Λοιπόν το θεώρημα των Rosser-Schoenfeld του 1975 λέει:

Για $k \geq 6$, $p_k \leq k (\log k + \log \log k)$

– Υπάρχει όμως και το νέο αποτέλεσμα του Dusart:

Για $k \geq 2$, $p_k \geq k (\log k + \log \log k - 1)$.

– Τότε μπορούμε να κλειδώσουμε το συμπέρασμά μας με το άλλο θεώρημα του Dusart:

Το διάστημα $\left[x, x + \frac{x}{2\log^2 x}\right]$ εμπεριέχει τουλάχιστον ένα πρώτο αριθμό για $x \geq 3275$.

* Για τα προηγούμενα είναι όλα εντάξει.
* Καλώς.
* Τώρα μπορούμε να γράψουμε το νέο μας θεώρημα.
* Σωστά.
* Θα είχε ενδιαφέρον να δούμε τι γίνεται με 7 πρώτους αριθμούς.
* Απλώς χρειαζόμαστε περισσότερο χρόνο.
* Ο χρόνος είναι μαζί μας.