Πρότυπο Πειραματικό Γενικό Λύκειο Εταγγελικής Σχολής Σμύρνης

Όμιλος

Μαθηματικών

Α΄ Λυκείου

21 Σεπτεμβρίου 2015 | Φύλλο 3 | Στοιχειοθετείται με το LaTeX

Καθηγητές: Ν.Σ. Μαυρογιάννης, www.nsmavrogiannis.gr , Σωτήριος Χασάπης, http://users.sch.gr/shasapis

Η αριθμητική mod m. 

1 Η αριθμητική mod m

Όλα τα προηγούμενα χρόνια δουλεύουμε με την συνηθισμένη αριθμητική των φυσικών, των ακεραίων, των ρητών και των πραγματικών αριθμών. Και θα συνεχίσουμε να δουλεύουμε με αυτήν. Υπάρχουν όμως και άλλες αριθμητικές που έχουν την δική τους θεωρητική αξία και τις δικές τους εφαρμογές. Στη σημερινή συνάντηση θα συζητήσουμε μία από αυτές. Μελετήθηκε συστηματικά από τον Carl Friedrich Gauss[1] στο έργο του *Disquisitiones Arithmeticae* (Αριθμητικές Έρευνες).

Ονομάζεται *γνωμονική αριθμητική* (modular arithmetic). Στην αριθμητική αυτή επιλέγουμε ένα ακέραιο $m > 1$ και εκτελούμε τις πράξεις μεταξύ ακεραίων με *γνώμονα* αυτόν τον ακέραιο ως εξής: προσθέτουμε αφαιρούμε ή πολλαπλασιάζουμε τους δύο ακεραίους και μετά ότι βρούμε το διαιρούμε δια m. Σαν αποτέλεσμα βάζουμε όχι τον αριθμό που βρήκαμε αλλά το υπόλοιπο της διαίρεσης του αριθμού που βρήκαμε δια m. Αν για παράδειγμα θέλουμε να προσθέσουμε τους 7 και 13 mod 8 τότε

Carl Friedrich Gauss
1777-1855

- Θα προσθέσουμε τους 7 και 13 με τον συνηθισμένο τρόπο και θα βρούμε 20.
- Θα διαιρέσουμε το 20 δια του 8 και θα βρούμε πηλίκο 2 (που δεν μας ενδιαφέρει) και υπόλοιπο 4,
- το αποτέλεσμα της πρόσθεσης των 7 και 13 όχι με τον συνηθισμένο τρόπο αλλά mod 8 είναι 4. Γράφουμε $7 + 13 \equiv 4(\mod 8)$.

Καθώς αντιλαμβάνεσθε στην αριθμητική mod 8 τα αποτελέσματα που μπορούμε να βρούμε είναι υπόλοιπα διαίρεσης δια 8. Και αυτά είναι τα 0, 1, 2, 3, 4, 5, 6, 7. Γενικά αν δουλεύουμε mod m τα αναμενόμενα αποτελέσματα είναι 0, 1, 2, ..., $m-1$. Είδαμε ότι

$$7 + 13 \equiv 4(\mod 8)$$

Αλλά και

$$15 + 13 \equiv 4(\mod 8)$$

$$15 + 21 \equiv 4(\mod 8)$$

$$(-1) + 13 \equiv 4(\mod 8)$$

$$(-1) + 5 \equiv 4(\mod 8)$$

$$(-1) + 21 \equiv 4(\mod 8)$$

Δεν είναι δύσκολο να δείτε ότι οποιοσδήποτε από τους αριθμούς 7, 15, -1 προστεθεί mod 8 με οποιονδήποτε από τους αριθμούς 13, 21, 5 θα δώσει αποτέλεσμα 4. Αν προσέξουμε θα δούμε ότι όλοι οι αριθμοί 7, 15, -1 είναι ισοϋπόλοιποι mod 8 (διαιρούμενοι με το 8 αφήνουν υπόλοιπο 7). Αλλά και οι 13, 21, 5 είναι ισοϋπόλοιποι mod 8. Αυτός είναι και ο λόγος που παίρνουμε το ίδιο αποτέλεσμα. Πράγματι ας υποθέσουμε ότι $\alpha + \beta = \gamma(\mod 8)$. Ας υποθέσουμε ότι έχουμε δύο άλλους αριθμούς α', β' που είναι ισότιμοι με τους α, β mod 8. Τότε $\alpha - \alpha' = 8k$ αλλά και $\beta - \beta' = 8k'$. Αυτό σημαίνει ότι $\alpha - \alpha' + \beta - \beta' = 8k + 8k'$ και επομένως $(\alpha + \beta) - (\alpha' + \beta') = 8(k + k')$. Άρα οι αριθμοί $\alpha + \beta$ και $\alpha' + \beta'$ είναι ισοϋπόλοιποι mod 8. και αφού το υπόλοιπο της διαίρεσης $\alpha+\beta : 8$ είναι γ και το υπόλοιπο της $\alpha'+\beta' : 8$ θα είναι γ. Επομένως θα είναι και $\alpha' + \beta' = \gamma(\mod 8)$. Αν κάνουμε τον ίδιο συλλογισμό αλλά αντί στην θέση του 8 φαντασθούμε τον m θα έχουμε το:

Θεώρημα 1.1 Αν $\alpha \equiv \alpha'(\mod m)$ και $\beta \equiv \beta'(\mod m)$ τότε $\alpha + \beta \equiv \alpha' + \beta'(\mod m)$.

Οι αριθμοί που είναι μεταξύ τους ισότιμοι (ισοϋπόλοιποι) mod 8 είναι «οργανωμένοι» σε σύνολα (λέγονται και κλάσεις):

- Εκείνοι που αφήνουν υπόλοιπο 0:
  $\ldots -16, -8, 0, 8, 16, 24, \ldots$
- Εκείνοι που αφήνουν υπόλοιπο 1:
  $\ldots -15, -7, 1, 9, 17, 25, \ldots$
- Εκείνοι που αφήνουν υπόλοιπο 2:
  $\ldots -14, -6, 2, 10, 18, 26, \ldots$
- Εκείνοι που αφήνουν υπόλοιπο 3:
  $\ldots -13, -5, 3, 11, 19, 27, \ldots$

[1] Στα Ελληνικά υπάρχει η μυθιστορηματική βιογραφία του: *Καρλ Φρίντριχ Γκάους. Ο Πρίγκιπας των Μαθηματικών* της M. B. W. Tent σε μετάφραση Στάμου Τσιτσώνη από τις εκδόσεις ΤΡΑΥΛΟΣ, 2007

- Εκείνοι που αφήνουν υπόλοιπο 4:
  $... -12, -4, 4, 12, 20, 28, ...$

- Εκείνοι που αφήνουν υπόλοιπο 5:
  $... -11, -3, 5, 13, 21, 29, ...$

- Εκείνοι που αφήνουν υπόλοιπο 6:
  $... -10, -2, 6, 14, 22, 30, ...$

- Εκείνοι που αφήνουν υπόλοιπο 7:
  $... -9, -1, 7, 15, 23, 31, ...$

Αν προσθέτουμε $\mod 8$ όποιον αριθμό και αν πάρουμε από μία κλάση και όποιον αριθμό πάρουμε από μία άλλη το αποτέλεσμα που θα βρούμε θα είναι το ίδιο. Στην πρόσθεση $\mod 8$ όλες οι κλάσεις «εκπροσωπούνται» εξ' ίσου καλά όποιον αριθμό και αν διαλέξουμε να τις «εκπροσωπήσει». Ας συμβολίσουμε την πρώτη κλάση με **0** την δεύτερη με **1** κ.οκ. φθάνοντας στην όγδοη που θα συμβολίσουμε με **7**.Η σχέση $7 + 13 \equiv 4 (\mod 8)$ που είδαμε πιο πριν ουσιαστικά μας λέει ότι όποιο αριθμό και αν προσθέσουμε από την κλάση **7** με όποιον αριθμό από την κλάση **5** (σε αυτήν ανήκει ο 13) θα πάρουμε αριθμό από την κλάση **4**. Γράφουμε συμβολικά $\mathbf{7 + 5 = 4}$. Ουσιαστικά η νέα αριθμητική μας έχει 8 στοιχεία (:τις κλάσεις). Σε αυτήν $\mathbf{6 + 5 = 3}$ και $\mathbf{4 + 4 = 0}$!

Άσκηση 1 Να συμπληρώσετε τον παρακάτω πίνακα «προπαίδειας» για την πρόσθεση $\mod 8$.

+	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**
0								
1								
2								
3								
4								
5								
6								
7								

Με εντελώς ανάλογο τρόπο ορίζεται και ο πολλαπλασιασμός $\mod m$: Πολλαπλασιάζουμε τους αριθμούς και ότι βρούμε το διαιρούμε δια m. Το υπόλοιπο που προκύπτει είναι το γινόμενο τους $\mod m$. Ισχύει το ακόλουθο:

Θεώρημα 1.2 Αν $\alpha \equiv \alpha' (\mod m)$ και $\beta \equiv \beta' (\mod m)$ τότε $\alpha \cdot \beta \equiv \alpha' \cdot \beta' (\mod m)$.

Άσκηση 2 Να αποδείξετε το θεώρημα **;;**

Άσκηση 3 Να συμπληρώσετε τον παρακάτω πίνακα «προπαίδειας» για τον πολλαπλασιασμό $\mod 8$.

×	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**
0								
1								
2								
3								
4								
5								
6								
7								

Άσκηση 4 Να συμπληρώσετε τον παρακάτω πίνακα «προπαίδειας» για τον πολλαπλασιασμό $\mod 5$.

×	**0**	**1**	**2**	**3**	**4**
0					
1					
2					
3					
4					
5					

2 Η αριθμητική $\mathbb{Z}_m$

Με $\mathbb{Z}_m$ συμβολίζουμε το σύνολο των κλάσεων $\mod m$ που τις συμβολίζουμε με **0**, **1**, **2**,..., $\mathbf{m-1}$. Προστίθενται και πολλαπλασιάζονται με τον τρόπο που περιγράψαμε πριν. Στο $\mathbb{Z}_m$ μπορούμε να κάνουμε διάφορους υπολογισμούς, να λύνουμε εξισώσεις συστήματα κ.α. Ας δούμε μερικούς:

Άσκηση 5 *Να υπολογίσετε την τιμή της παράστασης*

$$(\mathbf{2+3})(\mathbf{5+4}) + \mathbf{2}$$

στο $\mathbb{Z}_8$.
Κατόπιν να κάνετε το ίδιο στο $\mathbb{Z}_{12}$.

Άσκηση 6 Να βρείτε τον αντίθετο (: που έχει με αυτόν άθροισμα μηδέν) του **4**:

1. Στο $\mathbb{Z}_{12}$
2. Στο $\mathbb{Z}_5$

Άσκηση 7 Να βρείτε τον αντίστροφο (: που έχει με αυτόν γινόμενο ένα) του **4**:

1. Στο $\mathbb{Z}_5$
2. Στο $\mathbb{Z}_{12}$

Άσκηση 8 Να λύσετε στο $\mathbb{Z}_5$ την εξίσωση

$$\mathbf{2x + 3 = 1}$$

.

Άσκηση 9 Να λύσετε στο $\mathbb{Z}_7$ το σύστημα:

$$\left.\begin{array}{l} \mathbf{2x + y = 1} \\ \mathbf{x - 2y = 3} \end{array}\right\}$$

ΤΟ ΠΡΟΒΛΗΜΑ ΤΗΣ ΕΒΔΟΜΑΔΑΣ

Στο σχήμα τα τρίγωνα ΑΒΔ και ΑΓΕ είναι ισόπλευρα. Να αποδείξετε ότι ΒΕ = ΓΔ.