Εργασία Θεωρία Αριθμών

Κωνσταντίνος Ζουριδάκης 1115202000254

1 Άσκηση 1

Θα εφαρμόσουμε τον αλγόριθμο του Ευκλείδη.

Αρχικά εφαρμόζουμε στους αριθμούς 2200, 1210:

$$\begin{aligned}
2200 &= 1210 \cdot 1 + 990 \\
1210 &= 990 \cdot 1 + 220 \\
990 &= 220 \cdot 4 + 110 \\
220 &= 110 \cdot 2
\end{aligned}$$

Άρα, $(2200, 1210) = 110$.

Τώρα εφαρμόζουμε τον αλγόριθμο στους αριθμούς 110 και 1078

$$\begin{aligned}
1078 &= 110 \cdot 9 + 88 \\
110 &= 88 \cdot 1 + 22 \\
88 &= 22 \cdot 4
\end{aligned}$$

Οπότε, $(1078, 1210, 2200) = 22$.

Έχουμε:

$$\begin{aligned}
22 &= 110 - 88 \\
&= 110 - (1078 - 110 \cdot 9) \\
&= 10 \cdot 110 - 1078 \\
&= 10 \cdot (990 - 220 \cdot 4) - 1078 \\
&= 10 \cdot ((1210 - 220) - 220 \cdot 4) - 1078 \\
&= 10 \cdot (1210 - 220 \cdot 5) - 1078 \\
&= -5 \cdot 2200 + 10 \cdot 1210 - 1078
\end{aligned}$$

Τελικά, $x = -5, y = 10, z = -1$

2 Άσκηση 2

2.1 Περίπτωση $n \mod 2 = 0$

Αν ο n είναι περιττός, τότε $(-1)^{n+1} = 1$. Η έκφραση $2^n + (-1)^{n+1} > 3$, οπότε από κριτήριο σύνθετων αριθμών η έκφραση θα έχει ως αποτέλεσμα πάντα σύνθετο αριθμό $\forall n > 2$.

2.2 Περίπτωση $n \mod 2 = 1$

Αν ο n είναι άρτιος, τότε $(-1)^{n+1} = -1$. Η έκφραση πάλι θα είναι $2^n + (-1)^{n+1} > 3$, οπότε από κριτήριο σύνθετων αριθμών η έκφραση θα έχει ως αποτέλεσμα πάντα σύνθετο αριθμό $\forall n > 2$.

3 Άσκηση 3

$$478^{534} + 534^{478} \mod 23$$

Το Μικρό Θεώρημα του Φερμάτ μας λέει ότι για έναν πρώτο αριθμό p και οποιονδήποτε ακέραιο a που δεν διαιρείται από το p:

$$a^{p-1} \equiv 1 \mod p$$

Στην περίπτωσή μας $p = 23$, οπότε:

$$a^{22} \equiv 1 \mod 23$$

Υπολογίζουμε τα υπόλοιπα των 478 και 534 mod 23.

$$478 \div 23 = 20 \text{ (υπόλοιπο 18)}, \quad 534 \div 23 = 23 \text{ (υπόλοιπο 5)}$$

Άρα:

$$478 \equiv 18 \mod 23, \quad 534 \equiv 5 \pmod{23}$$

Τώρα η αρχική έκφραση γίνεται:

$$478^{534} + 534^{478} \equiv 18^{534} + 5^{478} \mod 23$$

Με το Μικρό Θεώρημα του Φερμά, μπορούμε να μειώσουμε τους εκθέτες mod 22:

$$534 \mod 22 = 6, \quad 478 \mod 22 = 18$$

Άρα:

$$18^{534} + 5^{478} \equiv 18^6 + 5^{18} \mod 23$$

$$18^2 \equiv 18 \times 18 = 324 \equiv 2 \mod 23$$
$$18^4 = (18^2)^2 \equiv 2^2 = 4 \mod 23$$
$$18^6 = 18^4 \times 18^2 \equiv 4 \times 2 = 8 \mod 23$$

$$5^2 = 25 \equiv 2 \mod 23$$
$$5^4 = (5^2)^2 = 2^2 = 4 \mod 23$$
$$5^8 = (5^4)^2 = 4^2 = 16 \mod 23$$
$$5^{16} = (5^8)^2 = 16^2 = 256 \equiv 3 \mod 23$$
$$5^{18} = 5^{16} \times 5^2 \equiv 3 \times 2 = 6 \mod 23$$

Προσθέτουμε τα αποτελέσματα mod 23:

$$18^6 + 5^{18} \equiv 8 + 6 = 14 \mod 23$$

Αφού $18^6 + 5^{18} \equiv 14 \pmod{23}$, ο αριθμός $478^{534} + 534^{478}$ δεν διαιρείται με το 23.

4 Άσκηση 4

4.1 α'

$$x \equiv 3 \mod 42$$
$$x \equiv 24 \mod 63$$

Έχουμε:

$$(42, 63) = (21, 42) = (21, 21) = 21$$

Όμως, το σύστημα γραμμικών ισοδυναμιών έχει μοναδική λύση $\mod 42 \cdot 63 = \mod 2646$, αφού:

$$(42, 63) | (24 - 3) = 21 | 21$$

Οπότε, έχουμε:

$$x \equiv 3 \mod 42 \Rightarrow x = 42\lambda + 3 \tag{1}$$

Συνεπώς:

$$\begin{aligned} x \equiv 24 \mod 63 \overset{(1)}{\Rightarrow} 42\lambda + 3 &\equiv 24 \mod 63 \\ 42\lambda &\equiv 21 \mod 63 \\ 2\lambda &\equiv 1 \mod 3 \end{aligned}$$

Όμως, $(2,3) = (1,2) = (1,1) = 1$ Άρα η ισοδυναμία έχει μοναδική λύση:

$$\begin{aligned} \lambda &\equiv 1 \cdot 2^{\phi(3)-1} \mod 3 \\ \lambda &\equiv 1 \cdot 2 \mod 3 \\ \lambda &\equiv 2 \mod 3 \end{aligned}$$

Οπότε καταλήγουμε:

$$\lambda \equiv 3\mu + 2 \tag{2}$$

$$(1) \overset{(2)}{\Rightarrow} x = 42 \cdot (3\mu + 2) + 3 \Rightarrow x = 126\mu + 87$$

Άρα

$$x \equiv 87 \mod 126$$

4.2 β'

$$\begin{aligned} 4x &\equiv 3 \mod 5 \\ 2x &\equiv 6 \mod 12 \end{aligned}$$

Έχουμε:

$$\begin{aligned} (5,12) &= (5,7) = (2,5) = (2,3) = (1,2) = (1,1) = 1 \\ (4,5) &= (1,4) = (1,1) = 1 \\ (2,12) &= (2,10) = (2,8) = \cdots = (1,1) = 1 \end{aligned}$$

Άρα το σύστημα έχει μία λύση $\mod 60$.
Οπότε έχουμε:

$$4x \equiv 3 \mod 5 \Rightarrow 4x = 5\lambda + 3 \tag{3}$$

Συνεπώς:

$$\begin{aligned} 2x \equiv 6 \mod 12 \Rightarrow 4x \equiv 12 \mod 24 \overset{(1)}{\Rightarrow} 5\lambda + 3 \equiv 12 \mod 24 \\ 5\lambda \equiv 9 \mod 24 \end{aligned}$$

Όμως, $(5,24) = (5,19) = (5,14) = (5,9) = (4,5) = (1,4) = (1,1) = 1$. Άρα η ισοδυναμία έχει μοναδική λύση:

$$\begin{aligned} &\lambda \equiv 9 \cdot 5^{\phi(24)-1} \mod 24 \\ &\lambda \equiv 9 \cdot 5^{7} \mod 24 \\ &\lambda \equiv 703125 \mod 24 \end{aligned}$$

Οπότε καταλήγουμε:

$$\lambda = 24\mu + 703125 \tag{4}$$

$$\begin{aligned} (3) \overset{(4)}{\Rightarrow} 4x = 120\mu + 3515628 \\ x = 30\mu + 878907 \Rightarrow x \equiv 878907 \mod 30 \end{aligned}$$

5 Άσκηση 5

$$f(x) = 2x^4 - x^2 + 6 \equiv 0 \mod 49$$

Η πολυωνυμική ισοδυναμία έχει 2 λύσεις οι οποίες είναι:

$$\begin{aligned} r \equiv 1 \mod 7 \\ r \equiv 6 \mod 7 \end{aligned}$$

Έχουμε:

$$
\begin{aligned}
f'(x) &= 8x^3 - 2x \\
f'(1) &= 6 \not\equiv 0 \mod 7 \\
f'(6) &= 1716 \not\equiv 0 \mod 7
\end{aligned}
$$

Έχουμε:

$$
\begin{aligned}
f(1) = 7 = 7w &\Rightarrow w = 1 \\
kf'(1) + w \equiv 0 \mod 7 &\Rightarrow 6k + 1 \equiv 0 \mod 7 \\
&\Rightarrow k \equiv 6 \mod 7
\end{aligned}
$$

Άρα η μοναδική λύση που αντιστοιχεί στη λύση $r \equiv 1 \mod 7$ είναι:

$$y = r + kp = 1 + 6 \cdot 7 \equiv 43 \mod 7^2$$

Επίσης, έχουμε:

$$
\begin{aligned}
f(6) = 2562 = 7w &\Rightarrow w = 366 \\
kf'(6) + w \equiv 0 \mod 7 &\Rightarrow 1716k + 366 \equiv 0 \mod 7 \\
&k \equiv 2 \mod 7
\end{aligned}
$$

Άρα η μοναδική λύση που αντιστοιχεί στη λύση $r \equiv 6 \mod 7$ είναι:

$$y = r + kp = 6 + 366 \cdot 7 \equiv 2568 \mod 7$$

6 Άσκηση 6

6.1 α

$$x^2 \equiv -270 \mod 773$$

Έχουμε:

$$
\begin{aligned}
\left(\frac{-270}{773}\right) &= -\left(\frac{2}{773}\right)\left(\frac{3}{773}\right)\left(\frac{3}{773}\right)\left(\frac{3}{773}\right)\left(\frac{5}{773}\right) \\
&\Rightarrow -(-1 \cdot (-1) \cdot (-1) \cdot (-1) \cdot (-1)) = 1
\end{aligned}
$$

Άρα η τετραγωνική ισοδυναμία έχει λύση.

6.2 β

$$\left(\frac{88}{175}\right) = \left(\frac{2}{175}\right)\left(\frac{2}{175}\right)\left(\frac{2}{175}\right)\left(\frac{11}{175}\right)$$
$$\Rightarrow 1 \cdot 1 \cdot 1 \cdot 1 = 1$$

7 Άσκηση 7

Πρέπει να βρούμε $p : \left(\frac{-3}{p}\right) = -\left(\frac{3}{p}\right) = 1$

Οπότε θα πρέπει:

$$\left(\frac{3}{p}\right)\left(\frac{-1}{p}\right) = 1$$

Αν $p = 1 \mod 4$ από το οποίο συνεπάγεται ότι $\left(\frac{-1}{p}\right) = 1$ θα πρέπει $\left(\frac{3}{p}\right) = 1$ το οποίο ισχύει για $p = 1 \mod 3$.

Αν $p = 3 \mod 4$ από το οποίο συνεπάγεται ότι $\left(\frac{-1}{p}\right) = -1$, τότε θα πρέπει $\left(\frac{3}{p}\right) = -1$ το οποίο ισχύει για $p = 2 \mod 3$.

Οπότε έτσι ψάχνουμε και βρίσκουμε τους αριθμούς που ικανοποιούν αυτές τις δύο συνθήκες.

8 Άσκηση 8

Για να βρούμε αν υπάρχουν λύσεις της εξίσωσης:

$$\begin{aligned} 158 &= 81 + 77 \\ 81 &= 77 + 4 \\ 77 &= 4 \cdot 19 + 1 \\ 4 &= 1 \cdot 4 \end{aligned}$$

Οπότε η εξίσωση έχει λύσεις.

Πρέπει να βρούμε $x_0, y_0 : 81x_0 + 158y_0 = 1$

Κάνοντας αντίστροφα τις πράξεις του Ευκλείδιου αλγόριθμου και έπειτα από αντικαταστάσεις καταλήγουμε:

$$x_0 = -39, y_0 = 20$$

Πολλαπλασιάζοντας με το 5870 για να καταλήξουμε στην αρχική εξίσωση παίρνουμε τις λύσεις:

$$x_0 = -228930, y_0 = 117400$$