ΟΙ ΜΙΓΑΔΙΚΟΙ ΑΡΙΘΜΟΙ

1. Ιστορικό των μιγαδικών αριθμών. Φαίνεται ότι, οι μιγαδικοί αριθμοί εισήχθησαν στα Μαθηματικά, από τον John Wallis (1673). Όμως, πολύ πριν απ' αυτόν, το πρόβλημα του υπολογισμού τετραγωνικής ρίζας αρνητικού αριθμού είχε τεθεί σε μιά σειρά μαθηματικών (π.χ. Ήρων (50 μ.Χ.), Διόφαντος (275 μ.Χ.), Mahavira (850 μ.Χ.), Bhaskara (1150 μ.Χ.) κλπ.). Ο Wallis στο "Algebra", (cap. LXVI, Vol. II, p. 286, έκδοση στα Λατινικά), ισχυρίζεται ότι, η τετραγωνική ρίζα ενός αρνητικού αριθμού αν και αδύνατος, δεν είναι ωστόσο πιο ακατανόητη από έναν αρνητικό αριθμό. Ονομάζει τις ποσότητες αυτές "φανταστικές ποσότητες" και φθάνει μέχρι το σημείο να θεωρήσει έναν άξονα κάθετο προς τον άξονα των πραγματικών αριθμών και να πει ότι αυτός θα έπρεπε να λέγεται άξων των φανταστικών ποσοτήτων. Πέραν του σημείου αυτού όμως, δεν προχωρά.
Την συνέχεια της μελέτης των φανταστικών ποσοτήτων, την ανέλαβε ο Leibnitz (1676) και ο Jean Bernoulli (1702).
Για περισσότερες λεπτομέρειες, παραπέμπουμε στο "History of Mathematics" Vol II, σελ. 261, του D.E. Smith, έκδοση Dover, απ' όπου έχουμε πάρει τις παραπάνω πληροφορίες.

Ορισμός των μιγαδικών αριθμών. Έστω $\mathbb{R}$ το σώμα των πραγματικών αριθμών. Θεωρούμε το $\mathbb{R}\times\mathbb{R}=\{(x,y),\ \text{με}\ x\in\mathbb{R}\ \text{και}\ y\in\mathbb{R}\}$ και μέσα σ' αυτό ορίζουμε την ισότητα $(x_1,y_1)=(x_2,y_2)$ αν και μόνον αν $x_1=x_2$, $y_1=y_2$ και τις εσωτερικές πράξεις "+", $+:\mathbb{R}\times\mathbb{R}\to\mathbb{R}\times\mathbb{R}$ (που θα καλούμε πρόσθεση) και "$\circ$", $\circ:\mathbb{R}\times\mathbb{R}\to\mathbb{R}\times\mathbb{R}$, (που θα καλούμε πολλαπλασιασμό και θα παραλείπουμε το σύμβολο "$\circ$"), ως εξής:

Την πρόσθεση, από την σχέση, $(x_1,y_1)+(x_2,y_2)=(x_1+x_2,y_1+y_2)$.

Τον πολλαπλασιασμό από την σχέση, $(x_1,y_1)\circ(x_2,y_2)=(x_1x_2-y_1y_2,x_1y_2+x_2y_1)$.

Η δομή που έτσι ορίστηκε, παρίσταται με το $\mathbb{C}$ και τα στοιχεία της με τα γράμματα, (συνήθως) z, w, κλπ. Με 1 παριστάνουμε το στοιχείο $(1,0)$, με i παριστάνουμε το στοιχείο $(0,1)$, και με 0 το στοιχείο $(0,0)$ της δομής $\mathbb{C}$. Το $\mathbb{C}$, με τις πράξεις αυτές, αποκτά την δομή αντιμεταθετικού σώματος. Φανερά, $(0,1)\circ(0,1)=(-1,0)$, ή $i^2=-1$. Γράφουμε, $\mathbb{C}\ni z=(x,y)=x+iy$. Εισάγουμε και έναν μονόμετρο πολλαπλασιασμό $\cdot:\mathbb{R}\times\mathbb{C}\to\mathbb{C}$, θέτοντας, $\lambda z=\lambda(x,y)=(\lambda x,\lambda y)$.
Η δομή $(\mathbb{C},+,\cdot)$ είναι δομή διανυσματικού χώρου. Τα στοιχεία $(1,0)$ και $(0,1)$ αποτελούν μιά βάση του χώρου αυτού. Τον υπόχωρο $\mathbb{R}_{\mathbb{C}}=<(1,0)>$ τον ταυτίζουμε με το $\mathbb{R}$, και γράφουμε απλά 1, αντί του $(1,0)$, ως επίσης x αντί του $(x,0)=x(1,0)$. Η ταύτιση αυτή γίνεται μέσω του προφανούς ισομορφισμού $\mathbb{R}\ni x\mapsto(x,0)\in\mathbb{R}_{\mathbb{C}}$ των δομών $(\mathbb{R}_{\mathbb{C}},+,\circ)$ και $(\mathbb{R},+,\cdot)$

Θεώρημα. Η δομή $\mathbb{C}$ των μιγαδικών αριθμών, είναι ένα αντιμεταθετικό σώμα, που περιέχει ένα υπόσωμα, ισόμορφο του σώματος $\mathbb{R}$ των πραγματικών αριθμών, και μέσα στο οποίο, ισχύει η ισότητα $1^2+i^2=0$. Η ισότητα αυτή, απαγορεύει την εισαγωγή

διατάξεως "$\leq$" εν αυτώ, συμβατής με τις πράξεις του $\mathbb{C}$. (Θεώρημα των E. Artin και Otto Schreier, βλέπε Σ.Π. Ζερβού, Π. Κρικέλη, «Πως Μεταβαίνουμε από τα Κλασικά Μαθηματικά στα Νεώτερα».

Το x καλείται πραγματικό μέρος του $z = x + iy$, και το y φανταστικό μέρος του z.. Γράφουμε και $x = \mathrm{Re}z$, $y = \mathrm{Im}z$ Θέτουμε, $\mathrm{Re} = \{x \mid x \in \mathbb{R}\}$ και $\mathrm{Im} = \{y \mid y \in \mathbb{R}\}$.
Με κάθε μιγαδικό $z = x + iy$, θεωρούμε και τον συζυγή του $\bar{z} = x - iy$. Είναι, $z\bar{z} = x^2 + y^2$, δηλαδή, $z\bar{z} = \in \mathbb{R}^+$. Η απεικόνιση $\mathbb{C} \ni z \mapsto +\sqrt{x^2 + y^2} = z\bar{z} = \bar{z}z \in \mathbb{R}^+$ καλείται απόλυτος τιμή $|z|$ του z.

Τους μιγαδικούς αριθμούς, θα μπορούσαμε να τους εισάγουμε, χρησιμοποιώντας τον ισομορφισμό που δίδεται από την σχέση $\mathbb{C} \ni z = x + iy \mapsto \begin{pmatrix} x & y \\ -y & x \end{pmatrix} \in \mathbb{R}^{2\times 2}$.
Ο ισομορφισμός αυτός είναι χρήσιμος στον λογισμό των μιγαδικών αριθμών. Π.χ., αν θέλουμε να βρούμε τον z^{-1}, απλά, λαβαίνουμε τον αντίστροφο πίνακα

$$\begin{pmatrix} \frac{x}{x^2+y^2} & \frac{-y}{x^2+y^2} \\ \frac{y}{x^2+y^2} & \frac{x}{x^2+y^2} \end{pmatrix}$$ του πίνακα $$\begin{pmatrix} x & y \\ -y & x \end{pmatrix}$$ που αντιστοιχεί μέσω του ισομορφισμού μας, στον z. Στην συνέχεια, γράφουμε, $z^{-1} = \frac{x}{x^2+y^2} - \frac{y}{x^2+y^2}i$.

Απ' ότι είπαμε παραπάνω, συμπεραίνουμε ότι, αν $z_1 = x_1 + iy_1$ και $z_2 = x_2 + iy_2$ έχουμε, τότε, και ότι

α) $z_1 + z_2 = (x_1 + x_2) + i(y_1 + y_2)$ και $z_1 z_2 = (x_1 x_2 - y_1 y_2) + i(x_1 y_2 + x_2 y_1)$

β) $\overline{z_1 + z_2} = \overline{z_1} + \overline{z_2}$ και $\overline{z_1 z_2} = \overline{z_1}\,\overline{z_2}$

γ) $\bar{\bar{z}} = z$. δ) $|z|^2 = z\bar{z}$ ε) $\frac{1}{z} = \frac{\bar{z}}{|z|^2}$

δ) $|z_1 + z_2| \leq |z_1| + |z_2|$ και $|z_1 - z_2| \geq \| z_1| - |z_2 \|$. Επαγωγικά, $\left|\sum_{i=1}^{n} z_i\right| \leq \sum_{i=1}^{n} |z_i|$.

ε) $|z_1 z_2| = |z_1|\,|z_2|$.

στ) Η διαίρεση του πολυωνύμου $z^{n+1} - 1$ με το $z - 1$, δίδει την ταυτότητα

$$1 + z + z^2 + \ldots + z^n = \frac{1 - z^{n+1}}{1 - z}.$$

2. Το μιγαδικό επίπεδο. Το μιγαδικό επίπεδο λαβαίνετε, αν σε κάθε σημείο $(x, y) \in \mathbb{R}^2$, αντιστοιχίσουμε τον μιγαδικό αριθμό $z = x + iy$. Ο άξων Ox ταυτίζεται, τότε, με το σύνολο Re και ο Oy με το Im. Στον μιγαδικό αριθμό z αντιστοιχεί το ακτινικό διάνυσμα $\overrightarrow{OZ}$, όπου $Z = (x, y)$. Το μέτρο ή η απόλυτος τιμή του $|z|$ συμπίπτει με την απόσταση

του σημείου Z από την αρχή O του συστήματος αναφοράς του Oxy επιπέδου, και ισούται με $+\sqrt{x^2+y^2}$.

Χρήσιμη είναι και η παράσταση του z μέσω των πολικών συντεταγμένων του. Επειδή είναι $x = r\cos\theta$, $y = r\sin\theta$ όπου $r = |z|$, είναι και $z = r(\cos\theta + i\sin\theta)$, $0 \le \theta < 2\pi$, $r, \theta \in \mathbb{R}$. Παρατηρούμε ότι, γωνίες θ, που είναι πολλαπλάσια του 2π, παριστούν στο μιγαδικό επίπεδο, το ίδιο σημείο. Η γωνία θ καλείται και Argument (Argz) του z, όταν είναι $0 \le \theta < 2\pi$, και argument του z (argz), όταν θ = 2kπ, $k \in \mathbb{Z}$. Μετράται πάντα με φορά αντίθετη της φοράς των δεικτών του ωρολογίου.

Το άθροισμα των μιγαδικών αριθμών, αναπαρίσταται από το άθροισμα των ακτινικών διανυσμάτων τους.

Για να βρούμε σε τι αντιστοιχεί το γινόμενο δύο μιγαδικών $z_1 = x_1 + iy_1$ και $z_2 = x_2 + iy_2$, χρησιμοποιούμε τις πολικές τους συντεταγμένες (r_1, θ_1) και (r_2, θ_2), οπότε είναι,

$$z_1 z_2 = r_1 r_2 (\cos(\theta_1 + 2k\pi) + i\sin(\theta_1 + 2k\pi))(\cos(\theta_2 + 2k\pi) + i\sin(\theta_2 + 2k\pi))$$
$$= r_1 r_2 [(\cos(\theta_1 + \theta_2 + 2k\pi) + i\sin(\theta_1 + \theta_2 + 2k\pi)].$$

Η ισότητα αυτή δείχνει ότι, το γινόμενο του z_1 επί τον z_2, αντιστοιχεί σε εκείνο το σημείο του μιγαδικού επιπέδου, που απέχει από την αρχή απόσταση r ίση προς $|z_1||z_2| = |z_1 z_2|$, και έχει πολική γωνία $\arg z = \theta_1 + \theta_2$. Ο πολλαπλασιασμός ενός μιγαδικού αριθμού z επί τον i, αντιστοιχεί σε περιστροφή του σημείου Z δεξιόστροφα, κατά γωνία π/2. Τούτο είναι βέβαια σύμφωνο με την δράση του πίνακα, που αντιστοιχεί στον i, πάνω στο διάνυσμα $\overrightarrow{OZ}$.

Πράγματι, είναι, $\begin{pmatrix} x & y \\ -y & x \end{pmatrix}\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} -y & x \\ -x & -y \end{pmatrix}$, και το σημείο $z' = -y + xi$ έχει ακτινικό διάνυσμα $\overrightarrow{OZ'}$ κάθετο στο $\overrightarrow{OZ}$, μιά και $\overrightarrow{OZ} \cdot \overrightarrow{OZ'} = (x, y) \cdot (-y, x) = -xy + xy = 0$.

Αν $z_1 = x_1 + iy_1 = r_1(\cos\theta_1 + i\sin\theta_1)$ και $z_2 = x_2 + iy_2 = r_2(\cos\theta_2 + i\sin\theta_2)$ τότε έχουμε και τις σχέσεις:

α) $\arg(z_1 z_2) = \arg z_1 + \arg z_2$

β) $z^n = (r(\cos\theta + i\sin\theta))^n = r^n(\cos n\theta + i\sin n\theta)$ όπου το n ρητός αριθμός (κανόνας του de Moivre). Η ισότητα αυτή, μας επιτρέπει να υπολογίζουμε δυνάμεις και ρίζες μιγαδικών αριθμών. Π.χ. αν θέλουμε να βρούμε την $\sqrt{z}$, γράφουμε,

$$\sqrt{z} = z^{1/2} = \sqrt{r}\left(\cos\frac{\theta + 2k\pi}{2} + i\sin\frac{\theta + 2k\pi}{2}\right), \; k = 1, 2.$$

γ) Από την ταυτότητα στ) της προηγούμενης παραγράφου, λαβαίνουμε και τις σχέσεις

$$1 + \cos\theta + \cos 2\theta + \ldots + \cos n\theta = \frac{1}{2} + \frac{\sin[(n + 1/2)\theta]}{2\sin(\theta/2)} \qquad \text{και}$$

$$\sin\theta + \sin 2\theta + \ldots + \sin n\theta = \frac{1}{2}\cot(\theta/2) - \frac{\cos[(n + 1/2)\theta]}{2\sin(\theta/2)}, \text{ όπου } 0 < \theta < 2\pi.$$

Βιβλιογραφία. 1) Complex variables and applications, Ruel V. Churchill, McGraw-Hill.
2) Complex Variables, George Polya – Gordon Latta, Wiley.

Ασκήσεις. 1. Έστω $\alpha,\beta \in \mathbb{R}$. Να βρεθούν $x, y \in \mathbb{R}$, έτσι ώστε $(x+iy)^2 = \alpha + i\beta$.

2. Να δείξετε ότι $|1+iz| = |1-iz|$, αν και μόνον αν $z \in \mathbb{R}$.

3. Έστω $p(t)$ πολυώνυμο με πραγματικούς συντελεστές. Να δείξετε ότι, για $w \in \mathbb{C}$, $p(\overline{w}) = \overline{p(w)}$. Άρα, αν w ρίζα του $p(t)$, και ο $\overline{w}$ ρίζα του.

4. Για ποιά σημεία του επιπέδου $\Re z = \Im z$;

5. Να δείξετε ότι, $r^n \cos n\theta = x^n - \binom{n}{2} x^{n-2} y^2 + \binom{n}{4} x^{n-4} y^4 - \ldots$

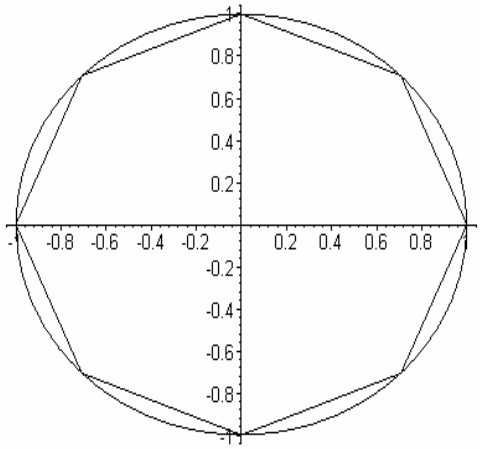
$$r^n \sin n\theta = \binom{n}{1} x^{n-1} y - \binom{n}{3} x^{n-3} y^3 + \ldots$$

όπου $x+iy = r(\cos\theta + i\sin\theta)$.

6. Να δείξετε ότι, $\dfrac{z_1}{z_2} = \dfrac{r_1}{r_2}\big(\cos(\theta_1-\theta_2) + i\sin(\theta_1-\theta_2)\big)$, όπου

$z_1 = r_1(\cos\theta_1 + i\sin\theta_1)$ και $z_2 = r_2(\cos\theta_2 + i\sin\theta_2)$.

3. Αρχικές ρίζες της μονάδος. Αν θέλουμε να βρούμε τις ***n ρίζες τις μονάδος,*** γράφουμε $1 = \cos 0 + i\sin 0$, οπότε και, $\sqrt[n]{1} = 1^{1/n} = \cos\dfrac{2k\pi}{n} + i\sin\dfrac{2k\pi}{n}$, k = 1, 2, . . . , n–1, n. Τα σημεία του μιγαδικού επιπέδου, που αντιστοιχούν στις n ρίζες της μονάδος, για τις διαφορετικές τιμές του k, βρίσκονται όλα επί περιφερείας κύκλου κέντρου την αρχή Ο και ακτίνας r = 1 (ο μοναδιαίος κύκλος) και αυτά, αποτελούν τις κορυφές κανονικού n-γώνου, με πρώτη κορυφή το σημείο $P_0 = (1,0)$, το οποίο το λαβαίνουμε για k = n, ή $k = 0$. Ας καλέσουμε αυτή την κορυφή P_0, μηδενική κορυφή. Γράφουμε και $\omega_k = \omega_1^k$, όπου $\omega_1 = \cos\dfrac{2\pi}{n} + i\sin\dfrac{2\pi}{n}$.



Παρατηρούμε ότι, όλες οι n διαφορετικές ρίζες της μονάδος δίδονται από τις δυνάμεις ω_n, ω_{n-1}, … ,ω_1, μιά και ισχύει, από τον κανόνα de Moivre, ότι $\omega_l\omega_m = \omega_{l+m}$ (γενικότερα, έχουμε, $\omega_k\omega_m = \omega_{k+m}$). Το γινόμενο δύο ριζών της μονάδος, είναι, λοιπόν, ρίζα της μονάδος. Το σύνολο συνεπώς $\Omega = \{\omega_n, \omega_{n-1}, \ldots, \omega_1\}$ με πράξη τον πολλαπλασιασμό του $\mathbb{C}$, αποτελεί κυκλική ομάδα, τάξεως n, παραγόμενη από την ω_1. Η γεωμετρική ερμηνεία του πολλαπλασιασμού της ω_k επί ω_1, είναι η περιστροφή

της κορυφής k κατά γωνία $2\pi/n$ και η μεταφορά της στην κορυφή $k+1$. Ισχύει, λοιπόν, ότι $\sum_{i=1}^{n}\omega_i = 0$.

Ορισμός. Ένας μιγαδικός αριθμός ω_k που είναι ρίζα της μονάδος, καλείται ***n-αρχική ρίζα της μονάδος,*** αν και μόνον αν, $\omega_k^n = \omega_k$, αλλά $\omega_k^m \neq \omega_k \ \ \forall m$ με $1 \le m \le n$.
Ο n είναι λοιπόν, ο ελάχιστος εκθέτης, για τον οποίο $\omega_k^n = \omega_k$.

Μία αρχική ρίζα της μονάδος, πολλαπλασιαζομένη επί τον εαυτό της όσες φορές χρειάζεται, θα μας δώσει και τις n ρίζες της μονάδος. Κάτι, που δεν ισχύει για τις μη αρχικές ρίζες. Πράγματι, αν οι ρίζες μου είναι π.χ. στις κορυφές κανονικού οκταγώνου, για την κορυφή 2, που αντιστοιχεί στην ρίζα ω_2, είναι, $\omega_2\omega_2 = \omega_4$, $\omega_4\omega_2 = \omega_6$, $\omega_6\omega_2 = \omega_0$, κ.ο.κ.

Αν n τυχόν φυσικός, με $\varphi(n)$ συμβολίσαμε το πλήθος των φυσικών $1 \le k \le n$, οι οποίοι είναι πρώτοι προς τον n (συνάρτηση φ του Euler). Θα δείξουμε ότι, για κάθε n, έχουμε ακριβώς φ(n) n-αρχικές ρίζες της μονάδος. Θα δείξουμε δηλαδή ότι, αν $1 \le k \le n$, τότε οι παρακάτω προτάσεις είναι ισοδύναμες:
1) $(\omega_k)^n = \omega_k$.
2) Το ω_k παράγει την ομάδα Ω.
3) για κάποιον εκθέτη h, $(\omega_k)^h = \omega_1$ και, τέλος,
4) Οι k και n είναι πρώτοι μεταξύ τους, δηλαδή, ότι $(k,n) = 1$ [ή ισοδύναμα, ότι υπάρχουν ακέραιοι α και β, τέτοιοι ώστε, $\eta k + \lambda n = 1$ (Ταυτότητα του Bezout)].
Ότι το 1) $\rightarrow$ 2) και ότι 2) $\rightarrow$ 3) το δείξαμε πιο πάνω.
για την 3) $\rightarrow$ 4), παρατηρούμε ότι, για τον φυσικό η = n – k, $\omega_k^h = \omega_1$. Άρα και $\cos\frac{2(\eta k)\pi}{n} + i\sin\frac{2(\eta k)\pi}{n} = \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n}$, δηλαδή, $\frac{2(\eta k)\pi}{n} + 2\lambda\pi = \frac{2\pi}{n}$, ή λn+ηk = 1.
για την 4) $\rightarrow$ 1), έχουμε την λn+ηk = 1, απ' όπου την $\frac{2(\eta k)\pi}{n} + 2\lambda\pi = \frac{2\pi}{n}$, δηλαδή την $\omega_k^h = \omega_1$. Άρα $\left(\omega_k^h\right)^n = \omega_1{}^n = \omega_1 = \omega_k^h$ ή $(\omega_k)^n = \omega_k$.

Παράδειγμα. για κάθε $n \ge 1$, η $\omega_1 = \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n}$ είναι n-αρχική ρίζα της μονάδος.
Έχουμε, λοιπόν, τον παρακάτω πίνακα:

n	**n-αρχικές ρίζες της μονάδος**	**φ(n)**
1	$\omega_1 = 1$	1
2	$\omega_1 = -1$	1
3	$\omega_1 = -\frac{1}{2} + i\frac{\sqrt{3}}{2}, \quad \omega_2 = \omega_1^2 = -\frac{1}{2} - i\frac{\sqrt{3}}{2}$	2
4	$\omega_1 = i, \ \omega_3 = -i$	2
5	$\omega_k = \cos\frac{2k\pi}{5} + i\sin\frac{2k\pi}{5}, \ k = 1, 2, 3, 4$	4
6	$\omega_1 = \frac{1}{2} - i\frac{\sqrt{3}}{2}, \qquad \omega_5 = \omega_1^5 = \frac{1}{2} + i\frac{\sqrt{3}}{2}$	2

Έστω, τώρα, ότι έχουμε να υπολογίσουμε την n-στη ρίζα ενός αριθμού $z \in \mathbb{C}$. Αν, με κάποιο τρόπο, έχουμε υπολογίσει μία ρίζα, και έστω αυτή η u, τότε, και οι $u\omega, \ \ldots \ , u\omega^{n-1}$, είναι ρίζες του z. Όλες, λοιπόν, οι διαφορετικές n ρίζες του z είναι οι $u\omega^0, u\omega^1, \ \ldots \ , u\omega^{n-1}$.

Κυκλοτομικό πολυώνυμο $Q_n(z)$ λέγεται εκείνο το πολυώνυμο $\varphi(n)$ βαθμού, του οποίου οι ρίζες είναι οι n-αρχικές ρίζες της μονάδος. Έχοντας υπ' όψη τον παραπάνω πίνακα, υπολογίζουμε τα κυκλοτομικά πολυώνυμα: $Q_2 = z + 1$

$$Q_3 = \left(z + \frac{1}{2} - i\frac{\sqrt{3}}{2}\right)\left(z + \frac{1}{2} + i\frac{\sqrt{3}}{2}\right) = z^2 + z + 1$$

$$Q_4 = (z + i)(z - i) = z^2 + 1$$

$$Q_6 = \left(z - \frac{1}{2} + i\frac{\sqrt{3}}{2}\right)\left(z - \frac{1}{2} - i\frac{\sqrt{3}}{2}\right) = z^2 - z + 1$$

για p πρώτο αριθμό, είναι, $Q_p = z^{p-1} + z^{p-2} + \ \ldots \ + z + 1$.

Θεώρημα. Αν το $f(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_0$, με ακεραίους συντελεστές είναι τέτοιο ώστε ο πρώτος p δεν διαιρεί τον a_n, τότε η ισοδυναμία $f(x) \equiv 0 (\mathrm{mod}\, p)$ έχει το πολύ n ακέραιες διαφορετικές (mod p) λύσεις.

Απόδειξη. Με επαγωγή επί του n. Γιά $n = 0$ δεν έχουμε καμία λύση μιά και $f(x) = a_0 \neq 0 (\mathrm{mod}\, p)$. Υποθέτουμε ότι το θεώρημα ισχύει γιά κάθε πολυώνυμο βαθμού $n - 1$. Θα δείξουμε ότι ισχύει και γιά πολυώνυμο βαθμού n.

Εάν η ισοδυναμία $f(x) \equiv 0 (\mathrm{mod}\, p)$ δεν έχει καμία λύση, δεν έχουμε τίποτα να δείξουμε. Σε περίπτωση όμως που έχουμε κάποια λύση r, τότε έχουμε και

$$f(x) - f(r) = \sum_{k=1}^{n} a_k (x^k - r^k) = (x - r) \sum_{k=1}^{n} a_k (x^{k-1} + x^{k-2} r + \ldots + r^{k-1}) = (x - r) g(x)$$

όπου $\deg g(x) = n - 1$. Εξ άλλου, επειδή ο r ρίζα της $f(x) \equiv 0 (\mathrm{mod}\, p)$, είναι και

$$0 \equiv f(x) \equiv (x - r) g(x) (\mathrm{mod}\, p)$$

Αν $x - r \neq 0 (\mathrm{mod}\, p)$, είναι, και, $g(x) \equiv 0 (\mathrm{mod}\, p)$, που σύμφωνα με την υπόθεση έχει $n - 1$ διαφορετικές (mod p) ρίζες. Άρα το $f(x)$ έχει το πολύ n ακέραιες διαφορετικές

(mod p) λύσεις.

Πόρισμα. Αν p πρώτος, τότε υπάρχουν ακριβώς $\varphi(p-1)$ διαφορετικές αρχικές ρίζες της μονάδος (mod p).

Παράδειγμα. Αν $p=11$, θα πρέπει να έχουμε $\varphi(10)=4$ διαφορετικές αρχικές ρίζες της $x^p-1=(x-1)(x^{p-1}+...+1)=0$. Πράγματι, αν ω^i είναι μία ρίζα της μονάδας, για να βρούμε τις αρχικές ρίζες, θα πρέπει να βρούμε ποιός εκθέτης δίδει με πράξη την $(\omega^i)^j=\omega^{ij}$ (mod 11) όλους τους εκθέτες από τον 1 μέχρι τον 10. Καταρτίζουμε, λοιπόν, τον παρακάτω πίνακα, όπου έχουμε υπολογίσει τους εκθέτες mod 11:

	1	2	3	4	5	6	7	8	9	10
1	**1**									
2	**2**	**4**	**8**	$16\equiv$ **5**	$32\equiv$ **10**	$64\equiv$ **9**	**7**	**3**	**6**	**1**
3	**3**	**9**	$27\equiv$ **5**	$81\equiv$ **4**	**1**					
4	**4**	**5**	**9**	**3**	**1**					
5	**5**	**3**	**4**	**9**	**1**					
6	**6**	**3**	**7**	**9**	**10**	**5**	**8**	**4**	**2**	**1**
7	**7**	**5**	**2**	**3**	**10**	**4**	**6**	**9**	**8**	**1**
8	**8**	**9**	**6**	**4**	**10**	**3**	**2**	**5**	**7**	**1**
9	**9**	**4**	**3**	**5**	**1**					
10	**10**	**1**								

Σύμφωνα με τον πίνακα αυτόν, αρχικές ρίζες είναι οι $\omega^2,\ \omega^6,\ \omega^7,\ \omega^8$.

Βιβλιογραφία. 1) "Το τελευταίο θεώρημα του Fermat". Ιωάννα Φερεντίνου Νικολακοπούλου. ΟΕΔΒ, 1984.

2) "Polynomials". E.J. Barbeau, Springer-Verlag, 1989.