Μάνος Λυδάκης Ολοκλήρωση της απόδειξης του Θεωρήματος Ύπαρξης Πρωταρχικών Ριζών $\bmod N$

Στην αίθουσα αποδείξαμε το παραπάνω θεώρημα, με μια εξαίρεση: Ισχυριστήκαμε ότι για $N = p^s$, με p περιττό πρώτο και s θετικό ακέραιο, υπάρχει πρωταρχική ρίζα $\bmod N$, αλλά το αποδείξαμε μόνο για $s = 1$. Άρα τα παρακάτω δύο λήμματα ολοκληρώνουν την απόδειξη:

Λήμμα 1: Αν το γ είναι πρωταρχική ρίζα $\bmod p$, τότε ή το γ ή το $\delta = \gamma + p$ είναι πρωταρχική ρίζα $\bmod p^2$. (Ειδικότερα, αφού υπάρχει πρωταρχική ρίζα $\bmod p$, υπάρχει και πρωταρχική ρίζα $\bmod p^2$.)

Λήμμα 2: Αν το γ είναι πρωταρχική ρίζα $\bmod p^2$, τότε είναι και πρωταρχική ρίζα $\bmod p^s$ για κάθε ακέραιο $s \geq 3$. (Ειδικότερα, υπάρχει πρωταρχική ρίζα $\bmod p^s$.)

Δείτε παρακάτω τις αποδείξεις.

Σας θυμίζω σύντομα τους δυωνυμικούς συντελεστές $\binom{n}{m}$ για $n = 0, 1, 2, \ldots$ και $m = 0, 1, 2, \ldots, n$. Για παράδειγμα,

$$\binom{7}{2} = \frac{7 \cdot 6}{1 \cdot 2} = 21 \quad \text{και} \quad \binom{7}{3} = \frac{7 \cdot 6 \cdot 5}{1 \cdot 2 \cdot 3} = 35$$

και, γενικότερα,

$$\binom{n}{m} = \frac{n \cdot (n-1) \cdots (n-m+1)}{1 \cdot 2 \cdots m}$$

ειδικότερα $\binom{n}{1} = n$, $\binom{n}{n} = 1$, και συμφωνούμε ότι $\binom{n}{0} = 1$.

Μόνο τρία πράγματα θα χρειαστούμε για τους δυωνυμικούς συντελεστές, και το πρώτο είναι πολύ εύκολο, είναι ότι ο $\binom{p}{2}$ είναι ακέραιο πολλαπλάσιο του p (εννοείται, p περιττός πρώτος). Πράγματι, ο p είναι περιττός, άρα ο $p-1$ είναι άρτιος, άρα το $\frac{p-1}{2}$ είναι ακέραιος. Τέλος, $\binom{p}{2} = p\frac{p-1}{2}$.

Τα άλλα δύο θεωρήματα για τους δυωνυμικούς συντελεστές είναι πιο ενδιαφέροντα αλλά δεν θα τα αποδείξουμε. Το ένα είναι ότι αυτοί είναι ακέραιοι. Το άλλο είναι το Θεώρημα του Δυωνύμου, που λέει

$$(x+y)^n = \sum_{m=0}^{n} \binom{n}{m} x^{n-m} y^m$$

που ισχύει για $x, y \in \mathbb{R}$ (ισχύει πολύ γενικότερα, όμως εμάς και μόνο το $x, y \in \mathbb{Z}$ μας αρκεί).

Απόδειξη του Λήμματος 1: Στην περίπτωση που το γ είναι πρωταρχική ρίζα $\bmod p^2$, δεν απομένει τίποτα άλλο να δείξω. Αρκεί λοιπόν να εξετάσω την περίπτωση που το γ δεν είναι πρωταρχική ρίζα $\bmod p^2$.

Έστω n η τάξη του $\gamma \bmod p^2$. Αφού το γ είναι πρωταρχική ρίζα $\bmod p$, η τάξη του $\gamma \bmod p$ είναι $\phi(p) = p-1$ που σημαίνει ότι από τα $\gamma, \gamma^2, \ldots, \gamma^{p-2}$ κανένα δεν είναι ισότιμο με άσσο $\bmod p$, άρα και $\bmod p^2$. Αυτό λέει ότι $n \geq p-1$.

Ισχυρίζομαι ότι $p \not| n$ και εξηγώ: Με άτοπο, υποθέστε λοιπόν $p|n$, δηλαδή ότι το n είναι πολλαπλάσιο του p. Ξέρω ότι $\gamma^n \equiv 1 \bmod p^2$, άρα και $\bmod p$. Άρα το n είναι και πολλαπλάσιο της τάξης του $\gamma \bmod p$, δηλαδή του $p-1$. Περίληψη: το n είναι κοινό πολλαπλάσιο των $p, p-1$. Άρα διαιρείται με το ΕΚΠ$(p, p-1)$ που είναι το $p(p-1)$ αφού ΜΚΔ$(p, p-1) = 1$. Αλλά και η «αντίστροφη διαιρετότητα» ισχύει, αφου η τάξη $\bmod N$ διαιρεί το $\phi(N)$. Το τελικό συμπερασμα είναι ότι $n = p(p-1)$, δηλαδή $n = \phi(p^2)$, δηλαδή το γ είναι πρωταρχική ρίζα $\bmod p^2$, άτοπο. Τέλος εξήγησης.

Ξέρω λοιπόν ότι ΜΚΔ$(n, p) = 1$ και ότι $n|p(p-1)$, άρα $n|p-1$ που, μαζί με το $n \geq p-1$, λέει ότι $n = p-1$. Ειδικότερα $\gamma^{p-1} \equiv 1 \bmod p^2$.

Παρατηρήστε ότι, αν υποθέσω ότι το δ δεν είναι πρωταρχική ρίζα $\bmod p^2$, και ότι τώρα το n συμβολίζει την τάξη του $\delta \bmod p^2$, τότε οι προηγούμενες δύο παράγραφοι ισχύουν και για το δ στη θέση του γ και δείχνουν ότι $\delta^{p-1} \equiv 1 \bmod p^2$. (Ο λόγος είναι ότι $\delta \equiv \gamma \bmod p$ άρα και από τα $\delta, \delta^2, \ldots, \delta^{p-2}$ κανένα δεν είναι ισότιμο με άσσο $\bmod p$, άρα και $\bmod p^2$, άρα εξακολουθεί να ισχύει ότι $n \geq p-1$.) Εγώ θέλω να αποδείξω ότι το δ είναι πρωταρχική ρίζα $\bmod p^2$. Αρκεί λοιπόν να δείξω ότι $\delta^{p-1} \not\equiv 1 \bmod p^2$. Με άτοπο, υποθέστε λοιπόν ότι $\delta^{p-1} \equiv 1 \bmod p^2$.

Εφαρμόζω το Θεώρημα του Δυωνύμου:

$$\delta^{p-1} = (\gamma + p)^{p-1} = \gamma^{p-1} + (p-1)\gamma^{p-2}p + \text{ άθροισμα όρων της μορφής «ακέραιος επί } p^2\text{»}$$

Το συμπέρασμα είναι ότι το p^2 διαιρεί το $\delta^{p-1} - \gamma^{p-1} - p(p-1)\gamma^{p-2}$, δηλαδή ότι

$$0 = 1 - 1 \equiv \delta^{p-1} - \gamma^{p-1} \equiv p(p-1)\gamma^{p-2} \mod p^2,$$

δηλαδή ότι το p^2 διαιρεί το $p(p-1)\gamma^{p-2}$, δηλαδή ότι το p διαιρεί το $(p-1)\gamma^{p-2}$, άρα (αφού το p είναι πρώτος που δεν διαιρεί το $p-1$) το p διαιρεί το γ^{p-2}, που είναι άτοπο, αφού το γ είναι πρωταρχική ρίζα $\mod p$, ειδικότερα $\gamma \in U_p$ δηλαδή $\text{ΜΚΔ}(\gamma, p) = 1$.

Απόδειξη του Λήμματος 2: Μια εύκολη επαγωγή στο $s \geq 2$ δείχνει: αρκεί να δείξω ότι το γ είναι πρωταρχική ρίζα $\mod p^{s+1}$, υποθέτοντας ότι το γ είναι πρωταρχική ρίζα $\mod p^s$.

Θέτω $n = p^{s-1}$, $N = p^2 n$, $m = \phi(n)$, και $M = \phi(N)$. Επειδή $\phi(p^t) = p^{t-1}(p-1)$ για κάθε θετικό ακέραιο t, συμπεραίνω ότι $\phi(pn) = pm$ και ότι $M = p^2 m$.

Ξέρω ότι το γ είναι πρωταρχική ρίζα $\mod pn$, δηλαδή ότι η τάξη του $\gamma \mod pn$ είναι $\phi(pn)$, δηλαδή pm, άρα, αφού $m < pm$, $\gamma^m \not\equiv 1 \mod pn$. Από την άλλη, από το ΘΕΦ, $\gamma^m \equiv 1 \mod n$. Το τελικό συμπέρασμα είναι ότι το γ^m γράφεται $\gamma^m = 1 + kn$ για κάποιο k που δε διαιρείται με το p.

Θεωρήστε τώρα την τάξη l του $\gamma \mod N$. Ισχύει $\gamma^l \equiv 1 \mod N$, άρα και $\mod pn$ (επειδή $pn \mid N$), άρα $pm \mid l$ (επειδή η τάξη του $\gamma \mod pn$ είναι pm). Επίσης $l \mid \phi(N) = p^2 m$. Περίληψη: $p^{s-1}(p-1) \mid l \mid p^s(p-1)$. Εξετάζοντας τις πιθανές παραγοντοποιήσεις του l σε πρώτους, βλέπω ότι υπάρχουν ακριβώς δύο τέτοιες παραγοντοποιήσεις, η πρώτη δίνει $l = p^{s-1}(p-1)$ (αυτή την περίπτωση θα τη λέω περίπτωση 1), και η δεύτερη δίνει $l = p^s(p-1)$ (αυτή την περίπτωση θα τη λέω περίπτωση 2).

Θυμηθείτε εγώ θέλω να δείξω ότι το γ είναι πρωταρχική ρίζα $\mod N$, δηλαδή ότι η τάξη του $\gamma \mod N$ είναι $\phi(N)$, δηλαδή ότι βρίσκομαι στην περίπτωση 2. Δηλαδή θέλω να δείξω ότι η περίπτωση 1 είναι αδύνατη.

Αρκεί λοιπόν να καταλήξω σε άτοπο, υποθέτοντας ότι $\gamma^{pm} \equiv 1 \mod N$. Εφαρμόζω το Θεώρημα του Δυωνύμου:

$$\gamma^{pm} = (1+kn)^p = 1 + pkn + \binom{p}{2} k^2 n^2 + \text{ άθροισμα όρων της μορφής «ακέραιος επί } n^3\text{»}$$

Επειδή $s \geq 2$, το p διαιρεί το n, άρα το $N = p^2 n$ διαιρεί το n^3. Επειδή το p διαιρεί το $\binom{p}{2}$, το N διαιρεί το $\binom{p}{2} k^2 n^2$. Άρα, $\mod N$, το γ^{pm} είναι ισότιμο με το $1 + pkn$, δηλαδή το 1 είναι ισότιμο με το $1 + pkn$, δηλαδή το N διαιρεί το pkn, δηλαδή το p διαιρεί το k, άτοπο.