
Στην (προαιρετική) αυτή διάλεξη δεν πρόλαβα να αποδείξω το Θεώρημα 2 του Μέρους Ε, δηλαδή την πολλαπλασιαστικότητα του συμβόλου του Legendre. Δείτε παρακάτω την απόδειξη που σκόπευα να κάνω:

Απόδειξη του Θεωρήματος 2: Δεδομένου περιττού πρώτου p και ακεραίων a και b που δε διαιρούνται με το p, θέτω $c = ab$. Ζητώ:

$$\left(\tfrac{a}{p}\right)\left(\tfrac{b}{p}\right) = \left(\tfrac{c}{p}\right) \quad ?$$

Θέτω $a' = [a]_p$, $b' = [b]_p$, και $c' = [c]_p$. Ξέρω:

$$\left(\tfrac{a}{p}\right) = \left(\tfrac{a'}{p}\right)$$

και παρόμοια για τα b και c. Άρα αρκεί:

$$\left(\tfrac{a'}{p}\right)\left(\tfrac{b'}{p}\right) = \left(\tfrac{c'}{p}\right) \quad ?$$

Ξέρω ότι μπορώ να βρω (και βρίσκω) γ που είναι Πρωταρχική Ρίζα $\bmod p$. Όπως συνήθως στην αίθουσα, γράφω απλώς «log» αντί «$\log_\gamma$».

Θέτω $t = \log a'$, $s = \log b'$, και $n = \phi(p)$. Δηλαδή το πεδίο τιμών του log είναι το $\mathbb{Z}_n$. Όπως συνήθως στην αίθουσα, το χρώμα «•» συμβολίζει «κλάσεις και πράξεις $\bmod n$».

Θυμηθείτε $\log c' = \log(a'b') = \log(\gamma^t\gamma^s) = \log(\gamma^{t+s}) = \log(\gamma^{t+s}) = t + s = [t+s]_n$.

Παρατηρήστε τώρα ένα χρήσιμο τύπο:

$$(-1)^k = \begin{cases} (-1)^0, & k \text{ άρτιος} \\ (-1)^1, & k \text{ περιττός} \end{cases} = (-1)^{[k]_2} \qquad (1)$$

Άρα $\left(\tfrac{a'}{p}\right)\left(\tfrac{b'}{p}\right) \overset{\Theta 5}{=} (-1)^t(-1)^s = (-1)^{t+s} \overset{(1)}{=} (-1)^{[t+s]_2} \overset{\Theta 3}{=} (-1)^{[[t+s]_n]_2} \overset{(1)}{=} (-1)^{[t+s]_n} = (-1)^{\log c'} \overset{\Theta 5}{=} \left(\tfrac{c'}{p}\right)$, που είναι αυτό ακριβώς που ήθελα να αποδείξω.