ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ
ATHENS UNIVERSITY OF ECONOMICS AND BUSINESS

ΣΧΟΛΗ ΕΠΙΣΤΗΜΩΝ & ΤΕΧΝΟΛΟΓΙΑΣ ΤΗΣ ΠΛΗΡΟΦΟΡΙΑΣ
SCHOOL OF INFORMATION SCIENCES & TECHNOLOGY
ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ
DEPARTMENT OF INFORMATICS

Ειδικά Θέματα Αλγορίθμων

Ασκήσεις Φροντιστηρίου #3

Algorithms on Numbers

1. (a) Να δειχθεί ότι εάν $ar =_m as$ δεν ισχύει απαραίτητα $r =_m s$.
(b) Να δειχθεί ότι η παραπάνω συνεπαγωγή ισχύει εάν a, m είναι μεταξύ τους πρώτοι.
(c) Να δειχθεί ότι εάν a, m είναι μεταξύ τους πρώτοι τότε υπάρχει φυσικός αριθμός $n \leq m$ τέτοιος ώστε $a^n =_m 1$.

2. Εάν $gcd(a, m) = 1$, ορίζουμε ως τάξη d ενός αριθμού a mod m, τον μικρότερο φυσικό αριθμό για τον οποίον ισχύει $a^d =_m 1$.
(a) Να δειχθεί ότι η τάξη του 3 mod 80 είναι 4.
(β) Να δειχθεί ότι εάν $gcd(a, m) = 1$ και d είναι η τάξη του a mod m, τότε $a^n =_m 1 \Leftrightarrow d|n$.
(c) Να υπολογιστεί η τάξη του 2 mod 33.

3. Χρησιμοποιώντας το Chinese Remainder Theorem, να δειχθεί ότι εάν οι 5,7,11 δεν διαιρούν έναν δεδομένο αριθμό n, τότε $385|(n^{60} - 1)$.

4. Δίνεται ότι $2^{40} =_{527} 1$ και $526 = 40 \cdot 13 + 6$. Να ελεγθεί εάν ο 527 είναι πρώτος αριθμός.