Modern Cryptography
Bachelor Computer Science, University of Amsterdam, 2022/23
TEACHER: Christian Schaffner, TA: Léo Colisson, Llorenc Escolà Farràs, Jaròn Has

Practice problem set : Computational Number Theory

As during the written exam, all these problems should be solved by hand, without the help of electronic devices (except for double-checking your solutions).

Problem 1: generating elements

(a) Show that 5 is a generator of $\mathbb{Z}_7^*$.

(b) Show that 4 generates a subgroup of size 3 of $\mathbb{Z}_7^*$.

(c) Show that 3 is a generator of $\mathbb{Z}_{17}^*$.

Hint: In these problems, it can save you some computation power, if you work with negative numbers. For example observe that when computing modulo 17, it holds that $15 = (-2)$. Hence, rather than computing $15 \cdot 3 = 45 = 2 \cdot 17 + 11 = 11 \mod 17$, it is quicker to compute $(-2) \cdot 3 = (-6) = 11 \mod 17$.

Problem 2: square-and-multiply

Use square-and-multiply to compute the following. Don't forget to reduce all numbers $\mod N$ on the way to simplify the calculations!

(a) $[3^{65} \mod 7]$

(b) $[7^3 \mod 10]$

(c) $[7^{131} \mod 10]$

(d) $[5^{65} \mod 21]$

Hint: For this type of problems, Fermat's little theorem often provides you some nice shortcuts.

Problem 3: greates common divisors

Use the Euclidean algorithm to compute

(a) $\gcd(14, 91)$

(b) $\gcd(126, 399)$

(c) $\gcd(126, 400)$

Problem 4: multiplicative inverses

Use the extended Euclidean algorithm to compute

(a) integers $a, b \in \mathbb{Z}$ such that $a \cdot 91 + b \cdot 14 = \gcd(91, 14)$

(b) integers $a, b \in \mathbb{Z}$ such that $a \cdot 45 + b \cdot 16 = 1$

(c) $[16^{-1} \mod 45]$

(d) $[13^{-1} \mod 16]$

(e) $[7^{-1} \mod 9]$