COLUMBIA UNIVERSITY
IN THE CITY OF NEW YORK

Number Theory and Cryptography
Math UN3020
New York, 2023/03/22

Exercise Sheet 9

Binomial Congruences

Exercise 1 (8 points)**.** Compute 3^{25} modulo 45.

Exercise 2 (8 points)**.** Find the last two digits of $3^{3^{97}}$.
(Definition: a^{b^c} is defined as a^k, where $k = b^c$.)

Exercise 3 (8 points)**.** Verify that [2] is a primitive element in $\mathbb{Z}_{13}$. Then compute the other primitive elements and compute the orders of all the elements of $\mathbb{Z}_{13}$

Exercise 4 (8 points)**.** Solve the following congruences.

(a) $x^3 \equiv 2 \pmod{15}$.

(b) $4x^5 \equiv 5 \pmod{21}$.

(c) $10x^5 \equiv 14 \pmod{18}$.

(d) $14x^3 \equiv 10 \pmod{24}$.

Exercise 5 (10 points)**.** Solve the following congruences. Consider using a try-and-error method, if necessary.

(a) $x^3 \equiv 3 \pmod 5$.

(b) $x^3 \equiv 6 \pmod{10}$.

(c) $x^3 \equiv 6 \pmod 7$.

(d) $x^3 \equiv 1 \pmod 7$.

(e) $x^3 \equiv 2 \pmod 7$.

Exercise 6 (8 points)**.** Solve the following system of congruences.

$$\begin{cases} x^5 \equiv 2 & \pmod{35} \\ x^7 \equiv 11 & \pmod{63} \end{cases}$$

Exercise 7 (10 points)**.** Solve the following binomial congruences.

(a) $x^6 \equiv 1 \pmod{31}$.

(b) $x^{25} \equiv 1 \pmod{31}$.

(c) $x^7 \equiv 1 \pmod{31}$.

(d) $x^3 \equiv 8 \pmod{31}$.

(e) $x^6 \equiv 64 \pmod{31}$.

(Hint:) use that $[3]$ is a primitive element in $\mathbb{Z}_{31}$.