Cairo University Faculty of Engineering		3rd Year Comp. MTH3251- Fall 2022 Number theory - Sheet 4

(1) Use Modular Exponentiation algorithm to find
- (a) 7^{644} **mod** 645.
- (b) 11^{644} **mod** 645.
- (c) 3^{2003} **mod** 99.
- (d) 123^{1001} **mod** 101.

lw m2lksh fermat ghalbn hyb2a 3auzk tstkhdm el binary zy dol kda...

El sheet shklo sahl,
fana ha7awl feh w hatfrg 3la el video
for verifications.

~~(2) Use Fermat's theorem to verify that 17 divides $11^{104} + 1$.~~

(3) From Fermat's theorem deduce that, for any integer n > 0, $13 \mid 11^{12n+6} + 1$.

(4) Derive each of the following congruences:
- (a) $a^{21} \equiv a \pmod{15}$ for all a.
  [Hint: By Fermat's theorem, $a^5 \equiv a \pmod 5$.]

mohemaaaaaaaaaas

- (b) $a^7 \equiv a \pmod{42}$ for all a.
- (c) $a^{13} \equiv a \pmod{3 \cdot 7 \cdot 13}$ for all a.
- (d) $a^9 \equiv a \pmod{30}$ for all a.

3 · 5 · 2

(5) Use Fermat's little theorem to find 7^{121} mod 13.

(6) Use Fermat's little theorem to find 23^{1002} mod 41.

(7) Use Fermat's little theorem to show that if p is prime and $p \nmid a$, then a^{p-2} is an inverse of a modulo p. Hence, find an inverse of 5 modulo 41.

(8) a) Show that $2^{340} \equiv 1 \pmod{11}$ by Fermat's little theorem and noting that $2^{340} = (2^{10})^{34}$.
b) Show that $2^{340} \equiv 1 \pmod{31}$ using the fact that $2^{340} = (2^5)^{68} = 32^{68}$.
c) Conclude from parts (a) and (b) that $2^{340} \equiv 1 \pmod{341}$.

Easy

(9) If $7 \nmid a$, prove that either a^3+1 or $a^3- 1$ is divisible by 7.

(10) a) Use Fermat's little theorem to compute 3^{302} mod 5, 3^{302} mod 7, and 3^{302} mod 11.
b) Use your results from part (a) and the Chinese remainder theorem to find 3^{302} mod 385.
(Note that $385 = 5 \cdot 7 \cdot 11$.)

(11) a) Use Fermat's little theorem to compute 5^{2003} mod 7, 5^{2003} mod 11, and 5^{2003} mod 13.
b) Use your results from part (a) and the Chinese remainder theorem to find 5^{2003} mod 1001.
(Note that $1001 = 7 \cdot 11 \cdot 13$.)