Number Theory - Exercises 1

Lea Terracini

1. Find $\gcd(272, 1479)$, $\text{lcm}(272, 1479)$ and compute Bézout identity.

2. Prove that, if a and b are relatively prime, then

$$\gcd(a+b, a-b) = 1 \text{ or } 2;$$
$$\gcd(2a+b, a+2b) = 1 \text{ or } 3,$$
$$\gcd(a+b, a^2+b^2) = 1 \text{ or } 2.$$

3. Write 100 as a sum of two positive integers which are multiple of 7 and 11 respectively.

4. Compute

$$75 + 22 \mod 87$$
$$56 \cdot 12 \mod 87$$
$$160^{-1} \mod 841$$

5. Solve the following system of congruences

$$\begin{cases} x \equiv 4 & \mod 11 \\ x \equiv 5 & \mod 13 \\ x \equiv 1 & \mod 15 \end{cases}$$

6. Compute $\varphi(1000)$.

7. Prove that for any odd integer a

$$a^{33} \equiv a \mod 4080$$

(Notice that $4080 = 15 \cdot 16 \cdot 17$).

8. Show that if $\gcd(m, n) = 1$ then

$$m^{\varphi(n)} + n^{\varphi(m)} \equiv 1 \mod mn.$$

9. Say if the congruences

$$34x \equiv 6 \mod 38; \quad 34x \equiv 7 \mod 38$$

admit solutions; if they are, solve them.

10. Say if $\overline{7}$ lies in $\mathbb{Z}_{32}^{\times}$; in this case determine its order[1].

11. Let $N = 7919$ and let it be known that N is prime. Compute

$$2^{15839} + N^{11} \mod 3N$$

[1] Recall that the *order* of an element g in a finite group G is the smallest $n > 0$ such that $g^n = e$, where e is the identity element in G

12. Let

$$N = 1147, \qquad M = 5$$

a) Compute the greatest common divisor of N and 1000 and write the Bézout identity.

b) Find the canonical representatives of the following remainder classes:

$$[N-1]_M, \quad [1000]_N^{-1}, \quad [M^{10}-7]_M$$

c) Let it be known that M is the order[2] of $[1000]_N$ in $\mathbb{Z}_N^\times$.
Is it true that $1000^{N-1} \equiv 1 \pmod{N}$?
Deduce from your answer that N is not prime (<u>without</u> factoring N).

[2]Recall that the *order* of an element g in a finite group G is the smallest $n > 0$ such that $g^n = e$, where e is the identity element in G