Exercise sheet 1

Arithmetics in $\mathbb{Z}$ and $\mathbb{Z}/n\mathbb{Z}$

Exercice 1. Find all the Bézout relation between 650 and 66.

Exercice 2. Prove that 429 is invertible modulo $\mathbb{Z}/700\mathbb{Z}$ and compute its inverse.

Exercice 3. Compute the gcd $(n^3+n^2+1)\wedge(n^2+2n-1)$ in terms of $n \in \mathbb{N}$. Similarly, compute the gcd $(n^3+n^2-6n+2)\wedge(2n^2+5n-3)$.

Exercice 4. Solve the following congruences, for $x \in \mathbb{Z}$:

(1) $3x \equiv 4 \pmod 7$,
(2) $9x \equiv 12 \pmod{21}$,
(3) $103x \equiv 612 \pmod{676}$.

Exercice 5. Compute the following congruences :

(1) 135463^{2315} modulo 19,
(2) 763^{234} modulo 20,
(3) 2222^{321} modulo 20.

Exercice 6 (Egyptian fractions). Egyptian fractions are those of the form $\frac{1}{n}$ for $n \in \mathbb{N}^*$. We are interested in the problem of writing a positive rational number $\frac{a}{b}$ as a sum of distinct Egyptian fractions.

(1) Using the identity $\frac{1}{b} = \frac{1}{b+1} + \frac{1}{b(b+1)}$, show that every fraction $\frac{a}{b}$ with $a, b \in \mathbb{N}^*$ can be written as a sum of a finite number of distinct Egyptian fractions by providing an algorithm that outputs such a decomposition. Give the number of terms in the sum as a function of a. Give an bound on the largest denominator appearing in the decomposition.
(2) Assume $\frac{a}{b} < 1$ and $a \wedge b = 1$. Using Bézout's theorem, give another algorithm of decomposition into a sum of Egyptian fractions, that uses at most a terms and for which all denominators are at most $b(b-1)$.

Exercice 7. (1) Show that 7 divide $3^{105} + 4^{105}$.

(2) Given integers a, b, c, show that $6|a+b+c$ if and only if $6|a^3+b^3+c^3$.
(3) Show that for every integer n, one has $n^7 \equiv n \pmod{42}$.

Exercice 8. Give all group homomorphisms $\mathbb{Z}/3\mathbb{Z} \to \mathbb{Z}/4\mathbb{Z}$, then all of the form $\mathbb{Z}/12\mathbb{Z} \to \mathbb{Z}/15\mathbb{Z}$. Give a necessary and sufficient condition m and n for every morphism $\mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ to be zero.

Exercice 9 (Game of the merchant). Assume we are given only coins with two values a and b, with a and b coprime positive integers.

(1) If the merchant gives back change, what amounts can be paid (using only the coins a and b) ?

(2) Supposons maintenant qu'on ne puisse pas nous rendre la monnaie. On pose $N = ab - a - b$. From now on, assume that the merchant does not give back change. Let $N = ab - a - b$ and let n and m be two integers such that $n + m = N$. Show that if N is payable, then exactly one amount among n and m is payable. Deduce that if $n > N$, then the amount n is payable.

(3) We generalize the problem to several coins of values $a_1, \ldots, a_n$. Show that for every integer $n \geqslant 2$, if $a_1, \ldots, a_n \in \mathbb{Z}*$ are pairwise coprime, then

$$M_n = a_1 \cdot \cdots \cdot a_n \left(n - 1 - \sum_{i=1}^{n} \frac{1}{a_i} \right)$$

is the largest integer that cannot be written in the form $\sum_{i=1}^{n} x_i \prod_{j \neq i} a_j$ with $x_i \in \mathbb{N}$.

Exercice 10. Let $n \in \mathbb{N}^*$. For $k \in \mathbb{Z}/n\mathbb{Z}$, show that $\langle k \rangle$ is the subgroup generated by $k \wedge n$. Deduce that $n = \sum_{d|n} \varphi(d)$.