Esbozo de las soluciones del segundo parcial 2020

1. **Ejercicio 1**

   Ver material teórico Teorema de Lagrange (3.8.1 pag. 55 y 56).

2. **Ejercicio 2**

   La clave en común k es 11^{31} $(m\acute{o}d 103)$. Para calcularla se usa el método de exponenciación rápida y se llega a $k = 96$.

3. **Ejercicio 3**

   Sea $p \in N$, $p \geq 2$. Probar que p es primo si y solo si $\forall a \in \{1, 2, ..., p-1\}$ existe $x \in N$ tal que $ax \equiv 1$ $(m\acute{o}d\ p)$.

   - (Directo) Sea p primo. Si $a \in \{1, 2, ..., p-1\}$ se cumple que a y p son coprimos, entonces por Bezout se sabe que existen x, y enteros tales que $ax + py = 1$. Por lo tanto $ax \equiv 1$ $(m\acute{o}d p)$. Sea $\hat{x}$ el resto de dividir x entre p. Entonces $\hat{x} \in \{0, 1, 2, ..., p-1\}$, $\hat{x} \neq 0$ (pues p no divide a x) y $a\hat{x} \equiv 1$ $(m\acute{o}d p)$.
   - (Recíproco) Supongamos que p no es primo, entonces existen $a, b \in \{1, 2, ..., p-1\}$ tal que $p = ab$. Por hipótesis existe $x \in N$ tal que $ax \equiv 1$ $(m\acute{o}d\ p)$. Luego, $bax \equiv b$ $(m\acute{o}d\ p)$ pero $ba = p \sim 0$ $(m\acute{o}d\ p)$. Llegamos a un absurdo ya que $0x \equiv b$ $(m\acute{o}d\ p)$.

4. **Ejercicio 4**

   Para hallar un número natural $x < 81$ tal que $50x \equiv 1$ $(m\acute{o}d 81)$, debemos resolver la ecuación diofántica $50x - 81y = 1$. Como 50 y 81 son coprimos se sabe que existe solución y es única $m\acute{o}d 81$. Se aplica el algoritmo de Euclides extendido y se llega a que $x = -34, y = -21$ verifican la ecuación. La solución del ejercicio es $x = -34 + 81 = 47$.