1) Un mazo de 50 cartas españolas, posee 10 cartas especiales que son los 8 y 9 de cada palo, más los dos comodines. Además de estas 10 cartas especiales, vienen las 40 cartas clásicas. Un fábrica de cartas decide empaquetar sus cartas poniendo las 40 cartas comunes ordenadas por número y palo (viniendo primero los oros, luego las copas, luego las espadas y por último los bastos) y colocando las otras 10 cartas especiales en cualquier orden, intercaladas entre las 40 cartas comunes. ¿De cuántas maneras puede venir el mazo?

$$\binom{n+k-1}{n} = \binom{50}{10} \cdot 10! = \frac{50!}{40!}$$

2) El objetivo de este ejercicio es demostrar el resultado conocido de la conmutatividad del producto de números naturales (con lo cual no se puede usar esta propiedad). Para ello definimos una función $p : N \times N \to N$ dada por:

$$\begin{aligned} p(m,n) &= m && n = 1 \\ p(m,n) &= p(m,n-1) + m && n \neq 1 \end{aligned}$$

Probar que para todo par de naturales (m,n) vale que:
$p(m,n) = p(n,m)$

Caso $n = 1$:
Quiero ver que $\forall m \in N,\ p(1,m) = p(m,1)$
Hago inducción en *m*
Si $m = 1$ nos queda $p(1,1) = p(1,1)$ (trivial)
Inducción en *m*: si $p(1,m) = p(m,1)$, quiero ver que $p(1,m+1) = p(m+1,1)$
Por definición de la función tenemos que:
$p(1,m+1) = p(1,m) + 1$
$p(m+1,1) = m + 1$
$p(1,m) = p(m,1) = m (HI)$
$p(1,m+1) = p(m,1) + 1 = m + 1 = p(m+1,1)$

Inducción en *n*:
HIn: $p(m,n) = p(n,m)$,
quiero ver que $p(m,n+1) = p(n+1,m)$
Inducción en *m*.
Si $m = 1$ tenemos que probar que $p(1,n+1) = p(n+1,1)$, sabiendo que $p(1,n) = p(n,1)$

$p(1,n+1)=p(1,n)+1$

$p(n+1,1)=n+1$

$p(1,n)\underset{HI}{=}p(n,1)=n$

$p(1,n+1)=p(n,1)+1=n+1=p(n+1,1)$

Paso inductivo:

HIm: $p(m,n+1)=p(n+1,m)$

quiero ver que $p(n+1,m+1)=p(m+1,n+1)$

$p(n+1,m+1)=p(n+1,m)+n\underset{HI.m}{=}p(m,n+1)+n=p(m,n)+m+n$

$p(m+1,n+1)=p(m+1,n)\underset{HI.m}{=}p(n,m+1)+m=p(n,m)+n+m=p(n+1,m+1)$, como queríamos probar.

Entonces vale que $p(n+1,m)=p(m,n+1)\forall m\in N$, entonces vale la inducción en *n*, entonces vale el resultado que queríamos probar.

3)

a) Encontrar un número primo *p* y un número primo *q*, tales que la ecuación $x^2+1\equiv 0(p)$ sea resoluble pero la ecuación $x^2+1\equiv 0(q)$ no tenga solución.

$x^2\equiv p-1(p)$

$x^2=kp+p-1$

Supongamos la solución con *k*=0

$x=\sqrt{p-1}$

Tabla de restos:

$p=2$

$r_p(x)$	0	1
$r_p(x^2)$	0	1
$r_p(x^2+1)$	1	0

Tiene solución $x=2k+1$

$p=3$

$r_p(x)$	0	1	2
$r_p(x^2)$	0	1	1
$r_p(x^2+1)$	1	2	2

No tiene solución

b) Encontrar un número natural *m* que sea producto de 3 primos, y además la ecuación $x^2+1\equiv 0(m)$ tenga exactamente 4 soluciones modulo *m*.

$m = pqk$

$x^2 \equiv p-1(p)$

$x^2 \equiv q-1(q)$

$x^2 \equiv k-1(k)$

Tomando p=2, q=5 (con 3 no hay solución)

$x^2 \equiv 1(2)$

$x \equiv 1(2)$

$x^2 \equiv 4(5)$

$x \equiv 2(5) \vee x \equiv 3(5)$

$x^2 \equiv k-1(k)$

Para cada combinación de ecuaciones hay una solución única módulo m por TCR. Luego,

$x^2 \equiv k-1(k)$ debe tener dos soluciones.

$x^2 \equiv 6(7)$ No tiene solución

$x^2 \equiv 10(11)$ No tiene solución

$x^2 \equiv 12(13) \leftrightarrow x \equiv 6(13) \vee x \equiv 7(13)$

$m = 130$

c) Encontrar un número natural m que sea producto de 3 primos, y además la ecuación $x^2+1 \equiv 0(m)$ tenga exactamente 8 soluciones modulo m.

Reemplacemos k por un número que tenga 2 soluciones.

$x^2 \equiv 16(17) \leftrightarrow x \equiv 4(17) \vee \equiv 13(17)$ $\begin{matrix} x^2 \equiv -1(k) \\ x \equiv -x^{-1}(k) \\ x + x^{-1} \equiv 0(k) \end{matrix}$ El inverso multiplicativo debe ser = al inverso aditivo.

m=1105

4) Consideremos un polinomio cúbico $q(x) = x^3 + ax^2 + bx + c$, donde $a, b, c \in C$ y supongamos que $q(x)$ tenga al menos dos raíces racionales.

a) Probar que si $a \in Q$ entonces $q \in Q(x)$ y todas sus raíces son racionales.

$$a = -\left(r_3 + \frac{p_2}{q_2} + \frac{p_1}{q_1} \right) \quad p_n, q_n \in Z \quad r \in C$$

$r_3 \in Q$

Porque la suma entre racionales es cerrada

$\left.\begin{matrix} b \in Q \\ c \in Q \end{matrix}\right\} \Rightarrow q \in Q(x)$

Porque la multiplicación también

b) ¿Es cierto que si $c \in Q$ entonces $q \in Q(x)$ y todas sus raíces son racionales? (dar una demostración o un contraejemplo)

$$c = -\left(r_3 \frac{p_2}{q_2} \frac{p_1}{q_1} \right) p_n, q_n \in Z \quad r \in C$$

Si c=0, y una de las otras raíces es 0, r_3 puede ser irracional.

Ejemplo:
$$r_3 = \sqrt{2}$$
$$r_2 = 0$$
$$r_1 = 1$$
$$q = x^3 - \left(1 + \sqrt{2}\right)x^2 - \sqrt{2}x$$

c) ¿Es cierto que si $b \in Q$ entonces $q \in Q(x)$ y todas sus raíces son racionales? (dar una demostración o un contraejemplo).

$$b = r_3 \frac{p_1}{q_1} + \frac{p_2}{q_2} \frac{p_1}{q_1} + r_3 \frac{p_2}{q_2} \; p_n, q_n \in Z \quad r \in C$$

Puede no darse, si r es irracional pero $r_3 \frac{p_2}{q_2} + r_3 \frac{p_1}{q_1}$ es racional:

Ejemplo:
$$r_3 = \sqrt{2}$$
$$r_2 = -1$$
$$r_1 = 1$$
$$q = x^3 - \sqrt{2}x^2 - x + \sqrt{2}$$

5)

Recordar que si n es un número natural, el *n*-ésimo número de Fermat se define como

$$F_n = 2^{2^n} + 1$$

Probar las siguientes afirmaciones:

a) El número F_n es divisible por 5 si y solo si n = 1.

$$2^{2^n} \equiv 4(5)$$
$$2^{4n+a} \equiv 4(5) \leftrightarrow a = 2$$
$$2^n \equiv 2(4)$$

Si $n > 1$

$$2^n = 2^2 2^{n+2} \equiv 0(4)$$

Si $n = 1$

$$2^1 \equiv 2(4)$$

b) El número F_n nunca es divisible por 7.

$2^{2^n} \equiv 6(7)$

$2^{3k} \equiv 1(7)$

$2^{3k+1} \equiv 2(7)$

$2^{3k+2} \equiv 4(7)$

$2^k \not\equiv 6(7)$

c) El número F_n nunca es divisible por 11.

$2^{2^n} \equiv 10(11)$

$2^{10k} \equiv 1(11)$

$2^{10k+a} \equiv 10(11) \leftrightarrow a = 5$

$2^n \equiv 5(10)$

$2^n \not\equiv 0(a) \leftarrow 2 \nmid a$