Answers and hints for homework assignment set 1, (for Monday 23 November)

1. (0.2p) X, Y, Z are finite sets with $Z \subseteq Y$, $|Z| = k \leq |X| = m \leq |Y| = n$.
We want the number of injections $f : X \to Y$ with $Z \subseteq f[X]$.
($f[X] = \{y \in Y \mid y = f(x) \text{ for some } x \in X\}$.)
Answer: There are $(m)_k \cdot (n-k)_{m-k} = \frac{m! \cdot (n-k)!}{(m-k)! \cdot (n-m)!}$ such injections.
One can choose the $x \in X$ with $f(x) = z$ for all $z \in Z$ in $(m)_k = \frac{m!}{(m-k)!}$ ways (injections $Z \hookrightarrow X$) and then the values for the remaining $m-k$ elements in X among the remaining $n-k$ elements in Y (injections $(X \setminus f^{-1}[Z]) \hookrightarrow (Y \setminus Z)$).

2. (0.3p) Find all $x \in \mathbb{Z}$ such that $1632x \equiv 3377^{2595} \pmod{481}$ [$481 = 13 \cdot 37$].
Answer: All solutions are $x = 102 + 481k,\ k \in \mathbb{Z}$.
Since $481 = 13 \cdot 37$ (both primes), $\phi(481) = (13-1)(37-1) = 432$.
$3377 \equiv_{481} 10$, $2595 \equiv_{432} 3$ and $\gcd(10, 481) = 1$ give (Euler's theorem)
$3377^{2595} \equiv_{481} 10^3 = 1000 \equiv_{481} 38$.
$1632 \equiv_{481} 189$, so we want to solve $189x \equiv_{481} 38$. The Euclidean algorithm:
$481 = 189 \cdot 2 + 103,\ 189 = 103 \cdot 1 + 86,\ 103 = 86 \cdot 1 + 17,\ 86 = 17 \cdot 5 + 1$, gives
$1 = 86 - 5(103 - 86) = -5 \cdot 103 + 6(189 - 103) = 6 \cdot 189 - 11(481 - 2 \cdot 189) =$
$= -11 \cdot 481 + 28 \cdot 189$, so $189^{-1} = 28$ in $\mathbb{Z}_{481}$ and one solution is
$x = 28 \cdot 38 = 1064 = 102$ in $\mathbb{Z}_{481}$ and the answer as above.

3. On $\mathbb{N}^{\mathbb{N}} = \{f \mid f : \mathbb{N} \to \mathbb{N}\}$ we define the relation $\mathcal{R}$ by, for all $f, g \in \mathbb{N}^{\mathbb{N}}$:
$$f \mathcal{R} g \text{ iff } |\{x \in \mathbb{N} \mid f(x) \neq g(x)\}| < \infty.$$
We shall find (a., 0.2p) if $\mathcal{R}$ is an equivalence relation and
(b., 0.2p) if $f_1, f_2, g_1, g_2 \in \mathbb{N}^{\mathbb{N}}$ and $f_1 \mathcal{R} f_2$, $g_1 \mathcal{R} g_2$, which (if any) of
$(f_1 + g_1)\mathcal{R}(f_2 + g_2)$, $(f_1 \cdot g_1)\mathcal{R}(f_2 \cdot g_2)$, $(f_1 \circ g_1)\mathcal{R}(f_2 \circ g_2)$ are necessarily true.
Answer a: $\mathcal{R}$ is an equivalence relation,
b: The first two must be true, the third not necessarily.
$|\{x \in \mathbb{N} \mid f(x) \neq f(x)\}| = 0 < \infty$, so $f \mathcal{R} f$ for all $f \in \mathbb{N}^{\mathbb{N}}$ and $\mathcal{R}$ is reflexive,
$\{x \in \mathbb{N} \mid f(x) \neq g(x)\} = \{x \in \mathbb{N} \mid g(x) \neq f(x)\}$,
so $f\mathcal{R}g \Rightarrow g\mathcal{R}f$ for all $f, g \in \mathbb{N}^{\mathbb{N}}$ and $\mathcal{R}$ is symmetric,
$\{x \in \mathbb{N} \mid f(x) \neq h(x)\} \subseteq \{x \in \mathbb{N} \mid f(x) \neq g(x)\} \cup \{x \in \mathbb{N} \mid g(x) \neq h(x)\}$,
so $f\mathcal{R}g$ and $g\mathcal{R}h \Rightarrow f\mathcal{R}h$ for all $f, g, h \in \mathbb{N}^{\mathbb{N}}$ and $\mathcal{R}$ is transitive
(since unions and subsets of finite sets are finite).
$\{x \in \mathbb{N} \mid (f_1 + g_1)(x) \neq (f_2 + g_2)(x)\}$, $\{x \in \mathbb{N} \mid (f_1 \cdot g_1)(x) \neq (f_2 \cdot g_2)(x)\} \subseteq$
$\{x \in \mathbb{N} \mid f_1(x) \neq f_2(x)\} \cup \{x \in \mathbb{N} \mid g_1(x) \neq g_2(x)\}$, but
$f_1(x) = x$, all $x \in \mathbb{N}$, $f_2(x) = x$, all $x \in \mathbb{N} \setminus \{0\}$, $f_2(0) = 1$ and
$g_1(x) = g_2(x) = 0$, all $x \in \mathbb{N}$, give $f_1 \mathcal{R} f_2$, $g_1 \mathcal{R} g_2$ and $(f_1 \circ g_1)\not\mathcal{R}(f_2 \circ g_2)$
($\{x \in \mathbb{N} \mid f_1(x) \neq f_2(x)\} = \{0\}$, $\{x \in \mathbb{N} \mid g_1(x) \neq g_2(x)\} = \varnothing$ and
$\{x \in \mathbb{N} \mid (f_1 \circ g_1)(x) \neq (f_2 \circ g_2)(x)\} = \mathbb{N}$).

4. (0.5p) Given are the permutations $\sigma = (1\ 3\ 7\ 11\ 6)(2\ 9\ 5)(4\ 8\ 10)$ and $\tau = (1\ 10\ 6\ 5\ 11\ 3\ 7)(2\ 9\ 8)$, both in S_{11}.
We shall find all $\pi \in S_{11}$ such that $\pi\sigma\pi = \tau$.
Answer: All such π are $(1\ 2\ 11)(4\ 8\ 6\ 9\ 10)$, $(1\ 2\ 7\ 11\ 9\ 10\ 4\ 8\ 6)(3\ 5)$, $(1\ 2)(3\ 9\ 10\ 4\ 8\ 6)(5\ 7)$ and $(1\ 2\ 3\ 11\ 5)(4\ 8\ 6\ 7\ 9\ 10)$.
$\pi\sigma\pi = \tau \Leftrightarrow (\pi\sigma)^2 = \tau\sigma = (1\ 7\ 3)(2\ 8\ 6\ 10\ 4)(5\ 9\ 11)$.
The square of a $(2k+1)$-cycle is a $(2k+1)$-cycle and the square of a $(2k)$-cycle is two k-cycles, so $\pi\sigma$ can be of type $[3^2 5]$, namely $(1\ 3\ 7)(2\ 10\ 8\ 4\ 6)(5\ 11\ 9)$, or of type $[56]$, namely $(1\ 5\ 7\ 9\ 3\ 11)(2\ 10\ 8\ 4\ 6)$, $(1\ 9\ 7\ 11\ 3\ 5)(2\ 10\ 8\ 4\ 6)$ or $(1\ 11\ 7\ 5\ 3\ 9)(2\ 10\ 8\ 4\ 6)$.
$\pi = (\pi\sigma)\sigma^{-1}$ gives the answer.

5 We shall (a., 0.2p) show that if $a_0, a_1, \ldots, a_n, m, r \in \mathbb{Z}$, $n, s \in \mathbb{Z}_+$, p is a prime, and $f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_0$, then

$$f(m + rp^s) \equiv_{p^{s+1}} f(m) + rp^s f'(m),$$

where $f'(x) = na_n x^{n-1} + (n-1)a_{n-1}x^{n-2} + \ldots + a_1$ and
(b., 0.4p) find all $x \in \mathbb{Z}$ such that $x^3 - x^2 + 4x + 1 \equiv_{125} 0$.
Answer b: All such x are given by $x = 94 + 125k$, $k \in \mathbb{Z}$.
For a., note that when $s \in \mathbb{Z}_+$, $i \geq 2 \Rightarrow i \cdot s \geq s + 1$,

$$\text{so } (m + rp^s)^i \equiv_{p^{s+1}} m^i + \binom{i}{1} m^{i-1} rp^s = m^i + im^{i-1}rp^s.$$

For b., let $f(x) = x^3 - x^2 + 4x + 1$. Then $f(x) \equiv_5 0 \Leftrightarrow x \equiv_5 1$ or $x \equiv_5 4$.
$f(x) \equiv_{125} 0 \Rightarrow f(x) \equiv_5 0$, so any solution must satisfy $x \equiv_5 1$ or -1.
$f'(x) = 3x^2 - 2x + 4$ and we find from a. that
$f(1 + 5r) \equiv_{25} f(1) + 5rf'(1) = 5 + 25r \not\equiv_{25} 0$, so no solution with $x \equiv_5 1$.
$f(-1 + 5r) \equiv_{25} f(-1) + 5rf'(-1) = -5 + 5r \cdot 9 \equiv_{25} 0 \Leftrightarrow -1 + 9r \equiv_5 0 \Leftrightarrow$
$\Leftrightarrow r \equiv_5 -1$, so any solution $x \equiv_{25} -1 + 5(-1) = -6$.
$f(-6 + 25r) \equiv_{125} f(-6) + 25r \cdot f'(-6) = -275 + 25r \cdot 124 =$
$= 25(-11 + 124r) \equiv_{125} 0 \Leftrightarrow -11 + 124r \equiv_5 0 \Leftrightarrow r \equiv_5 -1$ and
$f(x) \equiv_{125} 0 \Leftrightarrow x \equiv_{125} -6 + 25(-1) = -31 \equiv_{125} 94$, the answer.