1. (i) Find the remainder of $5^{143}$ when divided by 29.

(ii) Show that, for every integer $a$ such that $\gcd(a, 100) = 1$, $a^{20} \equiv 1 \pmod{100}$, and use this to compute the last two digits of $(17)^{122}$.
(Note that $\phi(100) = 40$, so this improves on Euler’s generalization.)

2. Let $G$ be a group (not necessarily finite), let $H_1$ and $H_2$ be two finite subgroups of $G$, and suppose that $\#(H_1) = n_1$ and $\#(H_2) = n_2$ with $\gcd(n_1, n_2) = 1$. Show that $H_1 \cap H_2 = \{1\}$.

3. Let $G$ be a group of order $p^n$, where $p$ is a prime. Show that $G$ contains an element of order $p$. (Show first that every element of $G$ has order $p^k$ for some $k \leq n$.)

4. Let $G$ be a group and let $H$ be a subgroup of $G$, not necessarily normal. Show that $g_1 \equiv_{H} g_2 \mod H \iff g_1^{-1} \equiv_{H} g_2^{-1} \mod H$. Conclude that the function $f : G/H \rightarrow H \backslash G$ given by $f(gH) = Hg^{-1}$ is well-defined, i.e. does not depend on the choice of a representative for $G/H$, and defines a bijection from $G/H$ to $H \backslash G$. (Note: However, the “function” $F : G/H \rightarrow H \backslash G$ given by $F(gH) = Hg$ is well-defined if and only if $H$ is normal.)

5. By Problem 3 of HW 10, if $f : \mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z} \times \mathbb{Z}$ is a homomorphism, then there exist $a, b, c, d \in \mathbb{Z}$ such that $f$ is of the form $f(n, m) = n(a, c) + m(b, d) = (an + bm, cn + dm)$, where $f(1, 0) = (a, c)$ and $f(0, 1) = (b, d)$. Thus $f$ corresponds to a $2 \times 2$ matrix $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ with integer coefficients, and conversely, every such $2 \times 2$ matrix with integer coefficients defines a homomorphism $f : \mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z} \times \mathbb{Z}$.

(a) Using a little linear algebra, or directly, show that $\ker f = \{(0, 0)\}$ (i.e. $f$ is injective) $\iff (a, c)$ and $(b, d)$ are linearly independent as vectors in $\mathbb{R}^2$ $\iff \det A \neq 0$, and in this case

$$H = \text{Im } f = \langle (a, c), (b, d) \rangle = \{n(a, c) + m(b, d) : n, m \in \mathbb{Z}\}$$

$$= \{(an + bm, cn + dm) : n, m \in \mathbb{Z}\}$$

is a subgroup of $\mathbb{Z} \times \mathbb{Z}$ isomorphic to $\mathbb{Z} \times \mathbb{Z}$. 
(b) Show that $H = \text{Im } f$ is equal to $\mathbb{Z} \times \mathbb{Z}$, i.e. $(a, c)$ and $(b, d)$ generate the group $\mathbb{Z} \times \mathbb{Z}$, $\iff$ det $A = \pm 1$. (Hint: $H = \mathbb{Z} \times \mathbb{Z}$ $\iff$ $f$ is surjective $\iff$ $f$ is an isomorphism $\iff$ there exists an inverse isomorphism $g$: $\mathbb{Z} \times \mathbb{Z} \to \mathbb{Z} \times \mathbb{Z}$, necessarily corresponding to a $2 \times 2$ matrix $B$ with integer coefficients. Show that, in this case, $AB = I$, and hence, since det $A$ and det $B$ are integers, that det $A = \pm 1$. Conversely, if det $A = \pm 1$, show that $A$ is invertible and that $A^{-1}$ has integer coefficients, and thus defines a homomorphism $g$: $\mathbb{Z} \times \mathbb{Z} \to \mathbb{Z} \times \mathbb{Z}$ which is an inverse for $f$.)

6. Compute the matrix product

$$\left( \begin{array}{cc} 1 & 1 \\ 0 & 1 \end{array} \right) \left( \begin{array}{cc} 0 & -1 \\ 1 & 0 \end{array} \right) \left( \begin{array}{cc} 1 & 1 \\ 0 & 1 \end{array} \right)^{-1}.$$

Using this, show that $O_2$ and $SO_2$ are not normal subgroups of $GL_2(\mathbb{R})$.

7. Consider the following subgroup of $A_4$ (considered in HW 9):

$$H = \{1, (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\}.$$

(i) Show that $H = \{\sigma \in S_4 : \sigma \text{ is even and } \sigma \text{ has order 1 or 2}\}$.

(ii) Show that $H$ is a normal subgroup of $A_4$ and of $S_4$. (If $\sigma \in H$ and $\tau \in S_4$, what can you say about the shape of $\tau \sigma \tau^{-1}$?)

(iii) Show that $A_4/H$ has order 3 and that $S_4/H$ has order 6. (In fact, one can show that $S_4/H \cong S_3$.)

(iv) Show that $K = \{1, (1,2)(3,4)\}$ is a normal subgroup of $H$ but not of $A_4$. Thus $K \triangleleft H$ and $H \triangleleft A_4$ but $K \ntriangleleft A_4$. (There are similar examples for $D_4$.)

8. (i) Let $G$ be a group and let $H, K$ be two subgroups of $G$. Show that, if $H \triangleleft G$ and $K \triangleleft G$, then $H \cap K \triangleleft G$.

(ii) With $G, H, K$ as in (i), show that, if $H \triangleleft G$, then $H \cap K \triangleleft K$.

(iii) With $G, H, K$ as in (i), show that, if $H \triangleleft G$ and $K \leq G$, then $HK = \{hk : h \in H, k \in K\}$ is a subgroup of $G$ containing $H$ and $K$. 