Elementary Number Theory and Cryptography,
M'mas 2011, Problem Sheet 5. (Fermat, Euler φ, Chinese Remainder)

1. For the following question, Fermat's Little Theorem may be helpful.
   (a) Find a number $0 \leqslant a < 67$ such that $a \equiv 9^{728} \pmod{67}$.
   [Justify your answer.]
   (b) Solve the congruence $x^{86} \equiv 6 \pmod{29}$.
   (c) Solve the congruence $x^{39} \equiv 8 \pmod{13}$.

2. Carefully state Fermat's Little Theorem and check for each of the following statements whether it is applicable or not.
   (a) The congruence $7^{1734250} \equiv 1660565 \pmod{1734251}$ is true. Can you conclude that 1734251 is a composite number?
   (b) The congruence $301^{64026} \equiv 29670 \pmod{64027}$ is true. Can you conclude that 64027 is a composite number?
   (c) The congruence $2^{52632} \equiv 1 \pmod{52633}$ is true. Can you conclude that 52633 is a prime number?

3. For each part, find an x that solves the simultaneous congruences
   (a) $x \equiv 3 \pmod 5$ and $x \equiv 7 \pmod{11}$.
   (b) $x \equiv 3 \pmod{37}$ and $x \equiv 1 \pmod{87}$.
   (c) $x \equiv 5 \pmod 7$, $x \equiv 3 \pmod{12}$ and $x \equiv 8 \pmod{13}$.

4. (a) Show that $2^{341} \equiv 2 \pmod{341}$. [Hint: Consider, e.g., 2^5 modulo the different prime powers in the factorization of 341.]
   (b*) Factor 561 and prove that $a^{561} \equiv a \pmod{561}$ for any $a \in \mathbb{Z}$ **(not easy!)**.

5. (a) For which values of $n \in \mathbb{N}$ is Euler's totient function $\varphi(n)$ odd?
   (b) Find all values of $n \in \mathbb{N}$ that solve

$$\text{(i)} \quad \varphi(n) = n/2 \qquad \text{or} \qquad \text{(ii)} \quad \varphi(n) = n/3\,.$$

6. (a) Find the last two decimal digits of 3^{400} "by hand".
   [Hint: Look at smaller powers and try to "compose" the results to deduce the last two digits for 3^d with d some divisor of 400. Or else use a result from the lectures.]
   (b) Use the method of successive squaring to compute each of the following powers:
   (i) $5^{13} \pmod{23}$,
   (ii) $28^{749} \pmod{1147}$.

7. **Partially experimental/computer question:**
   (a) For $2 \leqslant a \leqslant 10$, find the last four digits of a^{1000}. (Without computer, you should actually be able to answer this for $\gcd(a, 10) = 1$.)
   (b) Based on your experience in (a), give a simple criterion that allows you to predict the last four digits for any a^{1000}, $a \in \mathbb{N}$.
   (c*) Prove that your criterion in (b) is correct. [Possibly helpful: Euler–Fermat, binomial expansion, Chinese Remainder Theorem]