Elementary Number Theory and Cryptography,
Michaelmas 2011, Problem Sheet 8. (RSA attack, orders mod p)

1. (Factoring with high probability.) [A calculator is probably needed for (a).]
   (a) Suppose you are given the public RSA key $(n, e) = (93433, 1071)$, and you obtain the information that the decryption key is $d = 10831$. Putting $m = d \cdot e - 1$, for which $m = (1011000100000000010000000)_2$ is the binary expansion, compute $\rho := 3^{m/16} \pmod{n}$.
   (b) Using the ρ from part (a) above, or else assuming that a possible solution is $\rho = 501650$, find a factorization of n.
2. (Summation formula for Euler's φ-function.)
   Let d_1, d_2, …, d_r be the (positive) divisors of $n \geqslant 1$. Then
   $$\varphi(d_1) + \varphi(d_2) + \cdots + \varphi(d_r) = n\,.$$
   [Hint: Show it first for n a prime power, then use multiplicativity.]
3. Let $p = 31$.
   (a) For any (positive) divisor d of $\varphi(p)$, find
   $$S_p(d) = \{1 \leqslant a \leqslant p-1 \mid \operatorname{ord}_p(a) = d\}\,.$$
   (b) Using part (a), determine $\sum_{d|p} \#S_p(d)$.
   (c) Find all primitive roots modulo p.
4. Compute the following orders $\operatorname{ord}_p(a)$ modulo a prime p (try to economise your effort by avoiding to compute all powers):
   (a) for $p = 13$ and $a = 5$, $a = 7$ and $a = 9$;
   (b) for $p = 641$ and $a = 11$.
5. (Computing the order modulo *any integer* m.)
   For any integers a and $m > 0$ with $\gcd(a, m) = 1$ we define the *order* of a modulo m as
   $$\operatorname{ord}_m(a) = \min\{e \in \mathbb{Z}_{>0} \mid a^e \equiv 1 \pmod{m}\}\,.$$
   (a) Compute the following values:
   $$\operatorname{ord}_{21}(2)\,, \qquad \operatorname{ord}_{25}(2)\,, \qquad \operatorname{ord}_{32}(3)\,, \qquad \operatorname{ord}_{14}(3)\,.$$
   (b) Show that $\operatorname{ord}_m(a)$ is always a divisor of $\varphi(m)$.
6. (a) Create a table of indices modulo 17 using the primitive root 3.
   (b) Use this table to solve the congruence $13x \equiv 6 \pmod{17}$.
   (c) With the help of the above table, solve the congruence
   $$5x^7 \equiv 7 \pmod{17}\,.$$
7. Let p be an odd prime number.
   (a) Determine
   $$1 + 2 + 3 + \cdots + (p-1) \pmod{p}\,.$$
   (b) Distinguishing the cases $p = 3$ and $p > 3$, determine
   $$1^2 + 2^2 + 3^2 + \cdots + (p-1)^2 \pmod{p}\,.$$
   (c) By experimenting with a few small primes, or otherwise, make a guess as to what the value of
   $$1^k + 2^k + 3^k + \cdots + (p-1)^k \pmod{p}$$
   is, for any $k \geqslant 1$.
   [You may want to distinguish two essentially different cases.]
   (*) (d) Prove your guess from (c) if $\gcd(k, p-1) = 1$ or $p-1$. [Other cases?]