Elementary Number Theory and Cryptography, Michaelmas 2014

Problem Sheet 4, (Due: Monday Dec 1, at 12:00 in CM116)

Please hand in Problems 1(a,c), 2(b), 6(c), 7(b).
Problems 2(a), 7(a) 8, 9, 11 will be discussed in the tutorials, (depending on time).

1. By the method of successive squaring, or otherwise, compute the following powers:

   (a) Find the last two decimal digits of 3^{400}.

   (b) $5^{13} \pmod{23}$,

   (c) $2011^{2012} \pmod{2013}$.

2. Find one solution for each of the following congruences

   (a) $x^{11} \equiv 2 \pmod{17}$;

   (b) $x^{17} \equiv 5 \pmod{23}$;

   (c) $x^{9} \equiv 12 \pmod{29}$.

   Check your results using the method of successive squaring.

3. How many solutions (modulo 24) of the following congruence can you find

$$x^2 \equiv 9 \pmod{24}?$$

4. Note that $2^3 \equiv 8 \pmod{23}$. By finding an inverse of 3 in $\mathbb{Z}/22\mathbb{Z}$, or otherwise, find an integer x such that

$$8^x \equiv 2 \pmod{23}.$$

5. Compute the following orders $\mathrm{ord}_p(a)$ modulo a prime p (try to economize 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 $a = 11$.

6. Compute the following values:

   (a) $\mathrm{ord}_{21}(2)$,

   (b) $\mathrm{ord}_{25}(2)$,

   (c) $\mathrm{ord}_{32}(3)$,

   (d) $\mathrm{ord}_{14}(3)$,

7. Find a primitive root modulo p for p equals to:

   (a) 17;

(b) 23.

8. (a) Let $a \in \mathbb{Z}$, $n \in \mathbb{N}$ with $gcd(a,n) = 1$. So that for any integer k we have $a^k \equiv 1 \pmod{n}$ if and only if $k \equiv 0 \pmod{ord_n(a)}$.

   (b) With a and n as above and $b \in \mathbb{N}$, show that $ord_n(a^b) = \frac{ord_n(a)}{gcd(b, ord_n(a))}$. In particular $ord_n(a^b) = ord_n(a)$ if and only if $gcd(b, ord_n(a)) = 1$.

9. Show that if $F_n = 2^{2^n} + 1$, $n > 1$ is a prime, then 2 is not a primitive root modulo F_n. (Hint: Note that $2^{2^{n+1}} - 1 = (2^{2^n} - 1)(2^{2^n} + 1)$).

10. Let m, n be positive integers with $gcd(m,n) = 1$ and $m, n > 2$.

   (a) Write b for $lcm(\phi(m), \phi(n))$. Show that $b \leq \frac{\phi(m)\phi(n)}{2}$. (Hint: Question 7(a) in Problem Sheet 3 and Question 10 in Problem Sheet 2 may be helpful).

   (b) Show that for any $a \in \mathbb{Z}$ with $gcd(a,m) = 1$ we have $a^b \equiv 1 \pmod{m}$. Similarly show that for any $a \in \mathbb{Z}$ with $gcd(a,n) = 1$ we have $a^b \equiv 1 \pmod{n}$.

   (c) Using the above conclude that there is no primitive root modulo mn.

11. (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

$$5x^7 \equiv 7 \pmod{17}.$$