Elementary Number Theory and Cryptography, Michaelmas 2014

Problem Sheet 3, (Due: Monday Nov 17, at 12:00 in CM116)

Please hand in 2, 4, 5, 8(a), 13(c).
Problems 3, 7(a), 9(b), 10, 11, 12, 14 will be discussed in the tutorials, (depending on time).

1. Solve the linear congruences
   (a) $3x \equiv 7 \pmod{11}$;
   (b) $5x \equiv 3 \pmod{13}$;
2. Are the following linear congruences solvable? If they are then find a solution.
   (a) $663x \equiv 151 \pmod{2011}$;
   (b) $1857x \equiv 209 \pmod{2013}$.
3. (i) Show that 2, 4, 6, ..., $2m$ constitutes a complete set of residues modulo m, provided m is *odd*.
   (ii) Show that 1^2, 2^2, 3^2, ..., m^2 is *not* a complete set of residues modulo m, if $m > 2$.
4. For a positive integer n, let $\tau(n)$ denote the number of positive divisors of n, and $\sigma(n)$ denote the sum of these divisors. Show that the functions $\tau(n)$ and $\sigma(n)$ are multiplicative. Are they also completely multiplicative?
5. Let $f : \mathbb{N} \to \mathbb{N}$ be a multiplicative function. Prove that the function $F(n) := \sum_{0<d|n} f(d)$ is also multiplicative. Then use this to show again that the functions $\tau(n)$ and $\sigma(n)$ from above are multiplicative.
6. Determine $\varphi(n)$ (Euler's totient function) for n equals to: $n = 275$, $n = 2^7$; and $n = 404$.
7. (a) For which values of $n \in \mathbb{N}$ is Euler's totient function $\varphi(n)$ an odd integer?
   (b) Find all values of $n \in \mathbb{N}$ that solve
      i. $\varphi(n) = n/2$,
      ii. $\varphi(n) = n/3$
8. For the following question, Fermat's Little Theorem may be helpful.
   (a) Find a number $0 \leq a < 67$ such that $a \equiv 9^{728} \pmod{67}$.
   (b) Find the last digit of the number 6^{166}.
   (c) Find the last digit of the number $7^{(7^{77})}$.
9. (a) Find an integer x such that $x^{86} \equiv 6 \pmod{29}$.
   (b) Find an integer x such that $x^{39} \equiv 8 \pmod{13}$.

10. 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?

11. Show that, for $n > 4$ *composite*,

$$(n-1)! \equiv 0 \pmod{n}.$$

12. Show that, for a prime p such that $p \equiv 3 \pmod{4}$, one has

$$\left(\frac{p-1}{2}\right)! \equiv \pm 1 \pmod{p}.$$

13. 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 $x \equiv 8 \pmod{13}$.

14. A band of 17 pirates stole a sack of gold coins. When they tried to divide the fortune into equal portions, 3 coins remained. In the ensuing brawl over who should get the extra coins, one pirate was killed. The wealth was redistributed, but this time an equal division left 10 coins. Again an argument developed and another pirate was killed. But now the total fortune was evenly distributed among the survivors. What was the least number of coins that could have been stolen?