Math 342 Problem set 5 (due 9/2/09)

Congruences

1. We will calculate 15^{321} modulu 121 by a method called “repeated squaring”.
   (a) Find a small representative for 15^2 modulu 121.
   (b) Find a small representative for 15^4 modulu 121 (hint: $15^4 = (15^2)^2$)
   (c) Find a small representative for 15^8 modulu 121 (hint: $15^8 = (15^4)^2$)
   (d) Find small representatives for 15^{16}, 15^{32}, 15^{64}, 15^{128} and 15^{256} modulu 121.
   (e) Write 321 as a sum of powers of two.
   (f) Using the formula $15^{a+b} \equiv 15^a \cdot 15^b\,(121)$, find a small representative for 15^{321} modulu 121 by multiplying some of the numbers you got in parts (a)-(d) (as well as $15^1 = 15$) . You should only need to use each intermediate result at most once.

2. Solve the following congruences:
   (a) $x+7 \equiv 3\,(18)$.
   (b) $5x \equiv 12\,(100)$
   (c) $5x \equiv 15\,(100)$
   (d) $x^2+3 \equiv 2\,(5)$

3. For each pair of a,m below use Euclid’s algorithm to find $\bar{a}$ so that $a\cdot\bar{a} \equiv 1\,(m)$.
   (a) $m = 5$, $a = 2$.
   (b) $m = 12$, $a = 5$.
   (c) $m = 30$, $b = 7$.

4. Multiplying by the inverses from the previous problem, solve the following congruences:
   (a) $2x \equiv 9\,(5)$.
   (b) $5x+3 \equiv 11\,(12)$.
   (c) $14x \equiv 28\,(60)$.

Luhn’s Algorithm

5. Replace x with an appropriate final digit so that the following digit sequences satisfy Luhn’s Algorithm:
   (a) $45801453x$.
   (b) $6778312x$.

6. Show that adding zero digits *on the left* to a digit sequence does not affect whether it passes the check.

7. Let $n = \sum_{i=0}^{d} a_i 10^i$ be a number written in base 10.
   (a) Show that changing any single digit, or transposing any two neighbouring digits, will change the residue class of n modulu 11.
   (b) Starting with the number 15, one of the numbers $150, 151, 152, \cdots, 159$ is divisible by 11 (which?). Find an example of a number n such that adding a digit to n on the right will never give a number divisible by 11.
   (c) Explain why the previous example rules out using the ‘mod 11’ algorithm in place of Luhn’s algorithm.

Foundations of Modular arithmetic

8. Show that arithmetic in $\mathbb{Z}/m\mathbb{Z}$ satisfies the distributive law for multiplication over addition.

Optional

A. Explain how to use the idea of problem 1 to calculate the residue class $[a^b]_m$ using only $2(1+\log_2 b)$ multiplications instead of b multiplications. This algorithm is known as "exponentiation by repeated squaring".