Number Theory II: Worksheet

The following problems illustrate some of the main applications of congruences. Some of the problems will be worked out in class, others will be part of the homework assignments.

1. **Divisibility properties of large numbers:**
   (a) Show that 3 divides $4^n - 1$ for all $n \in \mathbb{N}$.
   (b) Find the remainder of 3^{1001} when divided by 5.
   (c) Find the reminder of 347^{1001} when divided by 3.
   (d) Find the remainder of 347^{2016} when divided by 2017. (Hint: 2017 is prime ...)
   (e) (HW) Find the remainder of 347^{101} when divided by 101. (Hint: 101 is prime ...)
   (f) (HW) Show that 7 divides $4^{3n+1} + 2^{3n+1} + 1$ for all $n \in \mathbb{N}$.

2. **Last digits of large numbers:** The last (rightmost) digit in the base b representation of an integer $n \in \mathbb{N}$ is congruent to n modulo b. This fact can be used, along with the properties of congruences (and especially the fact that congruences can be taken to a fixed power), to quickly, and with minimal amounts of computations, find the last digits of very large numbers, as illustrated by the following examples.
   (a) Find the last decimal digit of 3^{347}.
   (b) For which natural numbers n does 3^n end in the digit 1 (when written in decimal)?
   (c) (HW) Find the last digit in the base 8 expansion of 9^{1000}, 10^{1000}, 11^{1000}.

3. **Divisibility of squares, and polynomials:**
   (a) What are the possible remainders when n^4 is divided by 5?
   (b) Using congruences, show that $n^5 - n$ is divisible by 3 for all $n \in \mathbb{N}$.

4. **Divisibility tests.** First recall the precise meaning of a base b representation of an integer $n \in \mathbb{N}$ (where the base b is an integer with $b \geq 2$):
   (1) $n = (a_k a_{k-1} \dots a_0)_b \iff n = \sum_{i=0}^{k} a_i b^i$, with the "digits" a_i satisfying $a_i \in \{0, 1, \dots, b-1\}$ and $a_k \neq 0$.
   (a) **Divisibility by 9:** Given $n \in \mathbb{N}$, let $s(n)$ denote the sum of the digits of n in decimal (i.e., base 10) representation; i.e., $s(n) = a_0 + a_1 + \cdots$, where the a_i are as in (1). Show that $n \equiv s(n) \mod 9$. Deduce from this result the familiar divisibility test for 9: an integer is divisible by 9 if and only if the sum of its decimal digits is divisible by 9.
   (b) **Divisibility by 11:** Given $n \in \mathbb{N}$, let $t(n)$ denote the *alternating* sum of its decimal digits starting from the right; i.e., $t(n) = a_0 - a_1 + a_2 - a_3 + \cdots$, where the a_i are as in (1). (For example, if $n = 347$, then $t(n) = 7 - 4 + 3 = 6$, and if $n = 1001$, then $t(n) = 1 - 0 + 0 - 1 = 0$.) Show that $n \equiv t(n) \mod 11$. Deduce from this result the following divisibility test for 11: an integer is divisible by 11 if and only if the alternating sum of its decimal digits, starting from the right, is divisible by 9.

5. **Proof-writing practice: Congruence properties.** Prove the following properties of congruences, *using only the basic definition of a congruence (i.e., $a \equiv b \mod m$ means that there exist $k \in \mathbb{Z}$ such that $a = b + km$) or basic properties of divisibility.* (In all statements, $a, b, c, d, \dots$ are assumed to be arbitrary integers and m is a natural number.)
   (a) If $a \equiv b \mod m$ and $c \equiv d \mod m$, then $a + c \equiv b + d \mod m$.
   (b) If $a \equiv b \mod m$ and $b \equiv c \mod m$, then $a \equiv c \mod m$.
   (c) (HW) If $a \equiv b \mod m$ and $c \equiv d \mod m$, then $ac \equiv bd \mod m$.
   (d) (HW) If $a \equiv b \mod m$, then for any $k \in \mathbb{N}$, $a^k \equiv b^k \mod m$.