Number Theory II: Worksheet —Solutions

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 $n \in \mathbb{N}$.

   Solution: *The claim is equivalent to* $4^n - 1 \equiv 0 \bmod 3$ *for all* $n \in \mathbb{N}$. *Using the properties of congruences, this can be proved as follows:*

   $$\begin{aligned} 4 &\equiv 1 \bmod 3, \\ 4^n &\equiv 1^n = 1 \bmod 3, \\ 4^n - 1 &\equiv 0 \bmod 3. \end{aligned}$$

   (b) Find the remainder of 3^{1001} when divided by 5.

   Solution: $3^4 = 81 \equiv 1 \mod 5$, $3^{1001} \equiv (3^4)^{250} \cdot 3 \equiv 1^{250} \cdot 3 = \boxed{3} \mod 5$.

   (c) Find the reminder of 347^{1001} when divided by 3.

   Solution: $347 \equiv 2 \mod 3$, $2^2 = 4 \equiv 1 \mod 3$, $347^{1001} \equiv 2^{1001} \equiv (2^2)^{500} \cdot 2 \equiv 1^{500} \cdot 2 = \boxed{2} \mod 3$.

   (d) Find the remainder of 347^{2016} when divided by 2017. (Hint: 2017 is prime ...)

   Solution: *Note that* 2017 *is a prime, so by Fermat's Little Theorem,* $347^{2016} \equiv \boxed{1} \mod 2017$.

   (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}.

   Solution: *We need to find the unique number among* $\{0, 1, \ldots, 9\}$ *to which* 3^{347} *is congruent modulo* 10. *We proceed as follows: First, we find a small power of* 3 *that is congruent to* 1 *modulo* 10*: This is easily done by trial and error:*

   $$3^2 = 9 \equiv -1 \mod 10, \quad 3^4 \equiv (3^2)^2 \equiv (-1)^2 = 1 \mod 10.$$

   Next, we use the division algorithm to represent the given exponent 347 *as a multiple of this (small) exponent we have found plus a remainder:*

   $$347 = 4 \cdot 86 + 3.$$

   Finally, we use the properties of congruences and the fact that $3^4 \equiv 1 \mod 10$ *to find the congruence sought:*

   $$3^{347} = 3^{4 \cdot 86 + 3} = (3^4)^{86} \cdot 3^3 \equiv 1^{86} \cdot 27 \equiv 7 \mod 10.$$

   Hence the last digit of 3^{347} *in base* 10 *is* 7.

   (b) For which natural numbers n does 3^n end in the digit 1 (when written in decimal)?

   Solution: *This is equivalent to determining those* n *for which* $3^n \equiv 1 \bmod 10$. *Now* $3^4 = 81 \equiv 1 \bmod 3$, *so* $3^{4k} \equiv 1^k = 1 \bmod 10$ *for any* $k \in \mathbb{N}$. *Thus, if* n *is a multiple of* 4, *then* 3^n *ends in a* 1. *On the other hand, if* n *is not a multiple of* 4, *then* n *is of the form* $4k + 1, 4k + 2, 4k + 3$. *In this case* 3^n *is congruent modulo* 10 *to* $3^1 = 3, 3^2 = 9, 3^3 = 27$, *respectively, and thus has last digit* $3, 9, 7$, *respectively. Hence the natural numbers* n *for which* 3^n *ends in a* 1 *are exactly the multiples of* 4.

   (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?

Solution: *Note that any n must be congruent to one of* $(*)$ $0, 1, 2, 3, 4$ *modulo* 5*, so the possible remainders of* n^4 *modulo* 5 *are the same as those of the numbers* $0^4, 1^4, 2^4, 3^4, 4^4$*. Now* $0^4 \equiv 0 \bmod 5, 1^4 \equiv 1 \bmod 5, 2^4 = 16 \equiv 1 \mod 5, 3^4 = 81 \equiv 1 \mod 5, 4^4 = 256 \equiv 1 \mod 5$*, so* 0 *and* 1 *are the only possible remainders of* $n^4 \mod 5$*.*

(b) Using congruences, show that $n^5 - n$ is divisible by 3 for all $n \in \mathbb{N}$.

Solution: *We need to show that* $n^5 - n \equiv 0 \bmod 3$ *for all* $n \in \mathbb{N}$*. We establish this congruence by verifying it directly for each of the possible remainders modulo* 3 *of* n*:*

- *If* $n \equiv 0 \mod 3$*, then* $n^5 \equiv 0^5 = 0 \bmod 3$*, so* $n^5 - n \equiv 0 - 0 = 0 \equiv 0 \bmod 3$*.*
- *If* $n \equiv 1 \mod 3$*, then* $n^5 \equiv 1^5 = 1 \bmod 3$*, so* $n^5 - n \equiv 1 - 1 = 0 \equiv 0 \bmod 3$*.*
- *If* $n \equiv 2 \mod 3$*, then* $n^5 \equiv 2^5 = 32 \equiv 2 \bmod 3$*, so* $n^5 - n \equiv 2 - 2 = 0 \equiv 0 \bmod 3$*.*

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.

Solution: *The key observation is that* $10 \equiv 1 \bmod 9$ *and therefore* $10^i \equiv 1^i \bmod 9$ *for each positive integer* i*. Hence, with* n *given as in (1) with base* $b = 10$ *we have*

$$\begin{aligned} n &= 10^k a_k + 10^{k-1} a_{k-1} + \cdots + 10 a_1 + a_0 \\ &\equiv 1^k a_k + 1^{k-1} a_{k-1} + \cdots + 1 a_1 + a_0 \bmod 9 \\ &= a_k + a_{k-1} + \cdots + a_1 + a_0 = s(n) \bmod 9 \end{aligned}$$

as claimed. In particular, this implies that $n \equiv 0 \bmod 9$ *(i.e.,* n *is divisible by* 9*) holds if and only if* $s(n) \equiv 0 \bmod 9$ *(i.e.,* $s(n)$ *is divisible by* 9*). This is the divisibility test for* 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 $a + c \equiv b + d \mod m$.

Solution: ***Proof:*** *Suppose* $a \equiv b \mod m$ *and* $c \equiv d \mod m$*. Then, by the definition of a congruence, there exist* $h, k \in \mathbb{Z}$ *such that* $a = b + hm$ *and* $c = d + km$*. Adding these two equations, we get* $a + c = b + d + (h + k)m$*. Since* h *and* k *are integers, so is* $h + k$*. Hence* $a + b \equiv b + d \mod m$*, by the definition of a congruence.*

(b) If $a \equiv b \mod m$ and $b \equiv c \mod m$, then $a \equiv c \mod m$.

Solution: ***Proof:*** *Suppose* $a \equiv b \mod m$ *and* $b \equiv c \mod m$*. Then, by the definition of a congruence, there exist* $h, k \in \mathbb{Z}$ *such that* $a = b + hm$ *and* $b = c + km$*. Combining the two equations, we get* $a = (c + km) + hm = c + (h + k)m$*. Since* h *and* k *are both integers, so is* $h + k$*. Hence* $a \equiv c \mod m$*, by the definition of a congruence.*

(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 $k \in \mathbb{N}$, $a^k \equiv b^k \mod m$.