Problem Set

1. Determine whether each of the following statements is true or false.
   (a) $17 \equiv 2 \mod 5$
   (b) $14 \equiv -6 \mod 10$
   (c) $97 \equiv 5 \mod 13$
2. Compute each of the following:
   (a) 30 modulo 4
   (b) 21 modulo 6
   (c) 100 modulo 9
   (d) 32 modulo 8
   (e) 29 modulo 5
   (f) 75 modulo 11
3. (a) Verify each of the following statements.
      i. $3 \cdot 5 \equiv 3 \cdot 13 \mod 4$
      ii. $7 \cdot 18 \equiv 7 \cdot (-2) \mod 10$
      iii. $3 \cdot 4 \equiv 3 \cdot 14 \mod 6$
   (b) Determine whether each of the following statements is true or false.
      i. $5 \equiv 13 \mod 4$
      ii. $18 \equiv -2 \mod 10$
      iii. $4 \equiv 14 \mod 6$
4. Can we add congruences? If $a \equiv b \mod m$ and $c \equiv d \mod m$, is it necessarily true that $a + c \equiv b + d \mod m$? If so, why? If not, provide an example that illustrates why not. To get started on this question, do some numerical examples.
5. Can we subtract congruences? If $a \equiv b \mod m$ and $c \equiv d \mod m$, is it necessarily true that $a - c \equiv b - d \mod m$? If so, why? If not, provide an example that illustrates why not. To get started on this question, do some numerical examples.
6. Can we multiply congruences? If $a \equiv b \mod m$ and $c \equiv d \mod m$, is it necessarily true that $ac \equiv bd \mod m$? If so, why? If not, provide an example that illustrates why not. To get started on this question, do some numerical examples.
7. Can we take powers of congruences? If $a \equiv b \mod m$ and $n \geq 1$ is a positive integer, is it necessarily true that $a^n \equiv b^n \mod m$? If so, why? If not, provide an example that illustrates why not. To get started on this question, do some numerical examples.

8. Can we cancel congruences? If $ab \equiv ac \mod m$, is it necessarily true that $b \equiv c \mod m$? If so, why? If not, provide an example that illustrates why not. To get started on this question, do some numerical examples.

9. Suppose that
$$ac \equiv bc \mod m$$
and that
$$\gcd(c, m) = 1.$$
Prove that
$$a \equiv b \mod m$$
in this case.

10. Find a if $a \equiv 97 \mod 7$ and $1 \leq a \leq 7$.

11. Find a if $a \equiv 32 \mod 19$ and $52 \leq a \leq 70$.

12. Construct the tables for addition and multiplication modulo 7.

Problem Set 1

1. Compute each of the following:
   (a) $51 \mod 13$
   (b) $342 \mod 85$
   (c) $62 \mod 15$
   (d) $10 \mod 15$
   (e) $(82 \cdot 73) \mod 7$
   (f) $(51 + 68) \mod 7$
   (g) $(35 \cdot 24) \mod 11$
   (h) $(47 + 68) \mod 11$
2. List all integers x in the range $1 \leq x \leq 100$ that satisfy $x \equiv 7 \mod 17$.
3. If an integer x is even, observe that it must satisfy the congruence $x \equiv 0 \mod 2$. If an integer y is odd, what congruence does it satisfy? What congruence does an integer z of the form $6k + 1$ satisfy?
4. Write a single congruence that is equivalent to the pair of congruences $x \equiv 1 \mod 4$, $x \equiv 2 \mod 3$.
5. Suppose that p is a prime number and that
$$a^2 \equiv b^2 \mod p.$$
Show that
$$p \mid (a + b) \text{ or } p \mid (a - b).$$
6. Show that if $a \equiv b \mod n$ and $d \mid n$, then $a \equiv b \mod d$.
7. Show that a perfect square is congruent to either 0 or 1 modulo 4.
8. (a) Compute $5^2 \mod 3$.
   (b) Use (a) to compute $5^3 \mod 3$.
   (c) Use (a) and (b) to compute $5^{101} \mod 3$.
   (d) What is the remainder when 5^{101} is divided by 3?
9. (a) Compute $2^2 \mod 3$.
   (b) Compute $4^2 \mod 5$.
   (c) Compute $6^2 \mod 7$.
   (d) Compute $10^2 \mod 11$.

(e) Make a conjecture about the value of

$$(p-1)^2 \mod p,$$

where p is a prime number. Prove that your conjecture is true for all primes p.

10. (a) Compute $1 \cdot 2 \mod 3$.
    (b) Compute $1 \cdot 2 \cdot 3 \cdot 4 \mod 5$.
    (c) Compute $1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \mod 7$.
    (d) Compute $1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7 \cdot 8 \cdot 9 \cdot 10 \mod 11$.
    (e) Make a conjecture about the value of

$$(p-1)! \mod p,$$

where p is a prime number. This result is known as Wilson's Theorem.
    (f) Try to prove that your conjecture is correct for all primes p.

11. (a) Find (by trial and error or otherwise) all numbers x, $0 \leq x \leq 2$, such that $x^2 \equiv 1 \mod 3$.
    (b) Find (by trial and error or otherwise) all numbers x, $0 \leq x \leq 4$, such that $x^2 \equiv 1 \mod 5$.
    (c) Find (by trial and error or otherwise) all numbers x, $0 \leq x \leq 6$, such that $x^2 \equiv 1 \mod 7$.
    (d) Find (by trial and error or otherwise) all numbers x, $0 \leq x \leq 10$, such that $x^2 \equiv 1 \mod 11$.
    (e) Suppose that p is a prime. Make a conjecture about the numbers x, $0 \leq x \leq p-1$ such that $x^2 \equiv 1 \mod p$.

12. The **inverse** of a number x modulo m is the number y such that

$$xy \equiv 1 \mod m.$$

For example, since $3 \cdot 5 \equiv 1 \mod 7$, 5 is the inverse of 3 modulo 7 and 3 is the inverse of 5 modulo 7.

    (a) Find the inverse of 1 modulo 7.
    (b) Find the inverse of 2 modulo 7.
    (c) Find the inverse of 4 modulo 7.
    (d) Find the inverse of 6 modulo 7.

13. Let n be a positive integer greater than 3. Show that n, $n+2$, and $n+4$ cannot all be prime.

14. Let a, b, s, t be integers. If $a \equiv b \mod st$, show that $a \equiv b \mod s$ and $a \equiv b \mod t$.

15. A United States Postal Service money order has an identification number consisting of 10 digits together with an extra digit called a *check*. The check digit is the 10-digit number modulo 9. Thus, the number 3953988164 has the check digit 2 since

$$3953988164 \equiv 2 \mod 9.$$

If the number 39539881642 were incorrectly entered into a computer (programmed to calculate the check digit) as, say, 39559881642 (an error in the fourth position), the machine would calculate the check as 4, whereas the entered check digit would be 2. Thus, the error would be detected.

(a) Determine the check digit for a money order with identification number 7234541780.

(b) Suppose that in one of the noncheck positions of a money order number, the digit 0 is substituted for the digit 9, or vice versa. Prove that this error will not be detected by the check digit. Prove that all other errors involving a single position are detected.

(c) Suppose that a money order with identification number and check digit 21720421168 is erroneously copied as 27750421168. Will the check digit detect the error?

(d) A transposition error involving distinct adjacent digits is one of the form

$$...ab... \to ...ba...$$

with $a \neq b$. Prove that the money order check digit scheme will not detect such errors until the check digit itself is transposed.

16. As you have shown in the previous problem, the method used by the Postal Service does not detect all single-digit errors. One method that does detect all single-digit errors, as well as nearly all errors involving the transposition of two adjacent digits, is the Universal Product Code (UPC). A UPC identification number has 12 digits. The first 6 digits identify the manufacturer, the next 5 identify the product, and the last is a check. To explain how the check digit is calculated, we introduce the dot product notation for two k-tuples:

$$(a_1, a_2, \ldots, a_k) \cdot (b_1, b_2, \ldots, b_k) = a_1b_1 + a_2b_2 + \cdots + a_kb_k.$$

An item with UPC identification number $a_1a_2 \cdots a_{12}$ satisfies the condition

$$(a_1, a_2, \ldots, a_{12}) \cdot (3, 1, 3, 1, \ldots, 3, 1) \equiv 0 \mod 10.$$

Thus, the the UPC identification number 021000658978 has check digit 8 because

$$0{\cdot}3+2{\cdot}1+1{\cdot}3+0{\cdot}1+0{\cdot}3+0{\cdot}1+6{\cdot}3+5{\cdot}1+8{\cdot}3+9{\cdot}1+7{\cdot}3+8{\cdot}1 = 90 \equiv 0 \mod 10.$$

(a) Determine the UPC check digit for the number 07312400508.

(b) Explain why the UPC check digit scheme will identify all single-digit errors.

(c) Show that the only undetected transposition errors of adjacent digits a and b in the UPC scheme are those in which $|a - b| = 5$.

17. Identification numbers printed on bank checks (on the bottom left between the two colons) consist of an eight-digit number $a_1a_2 \cdots a_8$ and a check digit a_9 so that

$$(a_1, a_2, \ldots, a_9) \cdot (7, 3, 9, 7, 3, 9, 7, 3, 9) \equiv 0 \mod 10.$$

As in the case for the UPC scheme, this method detects all single-digit errors and all errors involving the transposition of adjacent digits a and b except when $|a - b| = 5$. It also detects most errors of the form $\cdots abc \cdots \to \cdots cba \cdots$, whereas the UPC method detects no errors of this form. Use this method to determine the check digit for the number 09190204.

18. The International Standard Book Number (ISBN) $a_1a_2 \cdots a_{10}$ has the property that

$$(a_1, a_2, \ldots, a_{10}) \cdot (10, 9, 8, 7, 6, 5, 4, 3, 2, 1) \equiv 0 \mod 11.$$

The digit a_{10} is the check digit. When a_{10} is required to be 10 to satisfy the congruence, the character X is used as the check digit.

(a) The ISBN assigned to one of my favorite number theory books (that you will receive a copy of at the end of the session!) is 0-13-186137-9. Verify that this ISBN satisfies the necessary congruence.

(b) Verify the check digit for the ISBN assigned to your favorite book (or any book that you have with you).

(c) The ISBN 0-669-03925-4 is the result of a transposition of two adjacent digits not involving the first or last digit. Determine the correct ISBN.

Problem Set 2

Applications of Congruences

1. Compute 5^{15} modulo 7 and 7^{13} modulo 11.
2. Find the number of integers n, $1 \leq n \leq 25$, such that $n^2 + 15n + 122$ is divisible by 6. Hint: $n^2 + 15n + 122 \equiv n^2 + 3n + 2 \equiv (n+1)(n+2) \mod 6$.
3. Find the remainder when $6^{83} + 8^{83}$ is divided by 49.
4. Prove that if $9 \mid (a^3 + b^3 + c^3)$, then $3 \mid abc$, for integers a, b, c.
5. Prove that there are no integers x, y that satisfy the equation $x^2 - 7y = 3$.
6. Prove that if $7 \mid (a^2 + b^2)$ then $7 \mid a$ and $7 \mid b$.
7. Show that if $x^3 + y^3 = z^3$, then one of x, y, z must be a multiple of 7.
8. Prove that there are no integers x, y, z that satisfy the equation
$$800000007 = x^2 + y^2 + z^2.$$
9. Prove that the sum of the decimal digits of a perfect square cannot be equal to 1991.
10. Prove that
$$7 \mid 4^{2^n} + 2^{2^n} + 1$$
for all natural numbers n.
11. Find the last two digits of 3^{100}.
12. Show that a perfect square is congruent to either 0, 1, or 4 modulo 8.
13. Show that for all positive integers n, $n^3 \equiv n \mod 3$.
14. Show that if $5 \nmid n$, then $n^4 \equiv 1 \mod 5$.
15. Show that any odd prime number p is either congruent to 1 modulo 4 or congruent to 3 modulo 4.
16. Find all possible values of the sum of two squares modulo 4. Use your result to show that the number 2003 cannot be written as the sum of two squares.
17. Suppose that m is an integer greater than or equal to 0. Show that
$$49 \mid 5 \cdot 3^{4m+2} + 53 \cdot 2^{5m}.$$
18. Show that there are infinitely many integers n such that
$$43 \mid (n^2 + n + 41).$$