Number Theory and Cryptography

Chapter 4

Because learning changes everything.™

Division

Definition: If a and b are integers with $a \neq 0$, then a *divides* b if there exists an integer c such that $b = ac$.

- When a divides b we say that a is a *factor* or *divisor* of b and that b is a multiple of a.
- The notation $a \mid b$ denotes that a divides b.
- If $a \mid b$, then $\frac{b}{a}$ is an integer.
- If a does not divide b, we write $a \nmid b$.

Example: Determine whether $3 \mid 7$ and whether $3 \mid 12$.

Divisibility and Modular Arithmetic

Section 4.1

Properties of Divisibility

Theorem 1: Let a, b, and c be integers, where $a \neq 0$.

i. If $a \mid b$ and $a \mid c$, then $a \mid (b + c)$;
ii. If $a \mid b$, then $a \mid bc$ for all integers c;
iii. If $a \mid b$ and $b \mid c$, then $a \mid c$.

Proof: (i) Suppose $a \mid b$ and $a \mid c$, then it follows that there are integers s and t with $b = as$ and $c = at$. Hence,

$b + c = as + at = a(s + t)$. Hence, $a \mid (b + c)$

(Exercises 3 and 4 ask for proofs of parts (ii) and (iii).)

Corollary: If a, b, and c be integers, where $a \neq 0$, such that $a \mid b$ and $a \mid c$, then $a \mid mb + nc$ whenever m and n are integers.

Division Algorithm

When an integer is divided by a positive integer, there is a quotient and a remainder. This is traditionally called the "Division Algorithm," but is really a theorem.

Division Algorithm: If a is an integer and d a positive integer, then there are unique integers q and r, with $0 \le r < d$, such that $a = dq + r$ (*proved in Section* 5.2).

- d is called the *divisor*.
- a is called the *dividend*.
- q is called the *quotient*.
- r is called the *remainder*.

Definitions of Functions **div** and **mod**

$q = a \textbf{ div } d$

$r = a \textbf{ mod } d$

Examples:

- What are the quotient and remainder when 101 is divided by 11?
- **Solution**: The quotient when 101 is divided by 11 is $9 = 101 \textbf{ div } 11$, and the remainder is $2 = 101 \textbf{ mod } 11$.
- What are the quotient and remainder when −11 is divided by 3?
- **Solution**: The quotient when −11 is divided by 3 is $-4 = -11 \textbf{ div } 3$, and the remainder is $1 = -11 \textbf{ mod } 3$.

More on Congruences

Theorem 4: Let m be a positive integer. The integers a and b are congruent modulo m if and only if there is an integer k such that $a = b + km$.

Proof:

- If $a \equiv b \pmod{m}$, then (by the definition of congruence) $m \mid a - b$. Hence, there is an integer k such that $a - b = km$ and equivalently $a = b + km$.
- Conversely, if there is an integer k such that $a = b + km$, then $km = a - b$. Hence, $m \mid a - b$ and $a \equiv b \pmod{m}$.

Congruence Relation

Definition: If a and b are integers and m is a positive integer, then ***a* is *congruent* to *b modulo m* if *m* divides *a* − *b***.

- The notation $a \equiv b \pmod{m}$ says that a is congruent to b modulo m.
- We say that $a \equiv b \pmod{m}$ is a *congruence* and that m is its *modulus.*
- Two integers are congruent mod m if and only if they have the same remainder when divided by m.
- If a is not congruent to b modulo m, we write $a \not\equiv b \pmod{m}$

Example: Determine whether 17 is congruent to 5 modulo 6 and whether 24 and 14 are congruent modulo 6.

Solution:

- $17 \equiv 5 \pmod{6}$ because 6 divides $17 - 5 = 12$.
- $24 \not\equiv 14 \pmod{6}$ since $24 - 14 = 10$ is not divisible by 6.

The Relationship between (mod *m*) and **mod** *m* Notations

The use of "mod" in $a \equiv b \pmod{m}$ and $a \textbf{ mod } m = b$ are different.

- $a \equiv b \pmod{m}$ is a relation on the set of integers.
- In $a \textbf{ mod } m = b$, the notation **mod** denotes a function.

The relationship between these notations is made clear in this theorem.

Theorem 3: Let a and b be integers, and let m be a positive integer. Then $a \equiv b \pmod{m}$ if and only if $a \textbf{ mod } m = b \textbf{ mod } m$.

Congruences of Sums and Products

Theorem 5: Let m be a positive integer. If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $a + c \equiv b + d \pmod{m}$ and $ac \equiv bd \pmod{m}$

Proof:

- Because $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, by Theorem 4 there are integers s and t with $b = a + sm$ and $d = c + tm$.
- Therefore,
  - $b + d = (a + sm) + (c + tm) = (a + c) + m(s + t)$ and
  - $b\,d = (a + sm)\,(c + tm) = ac + m(at + cs + stm)$.
- Hence, $a + c \equiv b + d \pmod{m}$ and $ac \equiv bd \pmod{m}$.

Example: Because $7 \equiv 2 \pmod{5}$ and $11 \equiv 1 \pmod{5}$, it follows from Theorem 5 that

$18 = 7 + 11 \equiv 2 + 1 = 3 \pmod{5}$

$77 = 7 \cdot 11 \equiv 2 \cdot 1 = 2 \pmod{5}$

Computing the **mod** *m* Function of Products and Sums

We use the following corollary to Theorem 5 to compute the remainder of the product or sum of two integers when divided by *m* from the remainders when each is divided by *m*.

Corollary: Let m be a positive integer and let a and b be integers. Then

$(a + b)\ (\textbf{mod}\ m) = ((a\ \textbf{mod}\ m) + (b\ \textbf{mod}\ m))\ \textbf{mod}\ m$

and

$ab\ \textbf{mod}\ m = ((a\ \textbf{mod}\ m)\ (b\ \textbf{mod}\ m))\ \textbf{mod}\ m$.

Algebraic Manipulation of Congruences

Multiplying both sides of a valid congruence by an integer preserves validity.

If $a \equiv b \pmod{m}$ holds then $c{\cdot}a \equiv c{\cdot}b \pmod{m}$, where c is any integer, holds by Theorem 5 with $d = c$.

Adding an integer to both sides of a valid congruence preserves validity.

If $a \equiv b \pmod{m}$ holds then $c + a \equiv c + b \pmod{m}$, where c is any integer, holds by Theorem 5 with $d = c$.

Dividing a congruence by an integer <u>does not always</u> produce a valid congruence.

Example: The congruence $14 \equiv 8 \pmod{6}$ holds. But dividing both sides by 2 does not produce a valid congruence since $14/2 = 7$ and $8/2 = 4$, but $7 \not\equiv 4 \pmod{6}$.

Arithmetic Modulo *m* 1

Definitions: Let $\mathbf{Z}_m$ be the set of nonnegative integers less than m: $\{0,1, \ldots., m-1\}$

- The operation $+_m$ is defined as $a +_m b = (a + b)\ \textbf{mod}\ m$. This is *addition modulo m*.
- The operation $\cdot_m$ is defined as $a \cdot_m b = (a \cdot b)\ \textbf{mod}\ m$. This is *multiplication modulo m*.
- Using these operations is said to be doing *arithmetic modulo m*.

Example: Find $7 +_{11} 9$ and $7 \cdot_{11} 9$.

Solution: Using the definitions above:

- $7 +_{11} 9 = (7 + 9)\ \textbf{mod}\ 11 = 16\ \textbf{mod}\ 11 = 5$
- $7 \cdot_{11} 9 = (7 \cdot 9)\ \textbf{mod}\ 11 = 63\ \textbf{mod}\ 11 = 8$

Arithmetic Modulo m_2

The operations $+_m$ and $\cdot_m$ satisfy many of the same properties as ordinary addition and multiplication.

- ***Closure***: If a and b belong to $\mathbf{Z}_m$, then $a +_m b$ and $a \cdot_m b$ belong to $\mathbf{Z}_m$.
- ***Associativity***: If a, b, and c belong to $\mathbf{Z}_m$, then $(a +_m b) +_m c = a +_m (b +_m c)$ and $(a \cdot_m b) \cdot_m c = a \cdot_m (b \cdot_m c)$.
- ***Commutativity***: If a and b belong to $\mathbf{Z}_m$, then $a +_m b = b +_m a$ and $a \cdot_m b = b \cdot_m a$.
- ***Identity elements***: The elements 0 and 1 are identity elements for addition and multiplication modulo m, respectively.
  - If a belongs to $\mathbf{Z}_m$, then $a +_m 0 = a$ and $a \cdot_m 1 = a$.

Solving Congruences

Section 4.4

Arithmetic Modulo m_3

- ***Additive inverses***: If $a \neq 0$ belongs to $\mathbf{Z}_m$, then $m - a$ is the additive inverse of a modulo m and 0 is its own additive inverse.
  - $a +_m (m - a) = 0$ and $0 +_m 0 = 0$
- ***Distributivity***: If a, b, and c belong to $\mathbf{Z}_m$, then
  - $a \cdot_m (b +_m c) = (a \cdot_m b) +_m (a \cdot_m c)$ and $(a +_m b) \cdot_m c = (a \cdot_m c) +_m (b \cdot_m c)$.

Multiplicatative inverses have not been included since they do not always exist. For example, there is no multiplicative inverse of 2 modulo 6.

(*optional*) Using the terminology of abstract algebra, $\mathbf{Z}_m$ with $+_m$ is a commutative group and $\mathbf{Z}_m$ with $+_m$ and $\cdot_m$ is a commutative ring.

Linear Congruences

Definition: A congruence of the form

$$ax \equiv b \pmod{m},$$

where m is a positive integer, a and b are integers, and x is a variable, is called a *linear congruence*.

The solutions to a linear congruence $ax \equiv b(\bmod m)$ are all integers x that satisfy the congruence.

Definition: An integer $\bar{a}$ such that $\bar{a}a \equiv 1(\bmod m)$ is said to be an *inverse* of a modulo m.

Example: 5 is an inverse of 3 modulo 7 since $5 \cdot 3 = 15 \equiv 1(\bmod 7)$

- One method of solving linear congruences makes use of an inverse $\bar{a}$, if it exists. Although we can not divide both sides of the congruence by a, we can multiply by $\bar{a}$ to solve for x.

Inverse of a modulo m

The following theorem guarantees that an inverse of a modulo m exists whenever a and m are relatively prime.

Theorem 1: If a and m are relatively prime integers and $m > 1$, then an inverse of a modulo m exists. Furthermore, this inverse is unique modulo m. (This means that there is a unique positive integer $\bar{a}$ less than m that is an inverse of a modulo m and every other inverse of a modulo m is congruent to $\bar{a}$ modulo m.)

Proof: Since gcd(a,m) = 1, by Bezout's Theorem, there are integers s and t such that $sa + tm = 1$.

- Hence, $sa + tm \equiv 1 \pmod{m}$.
- Since $tm \equiv 0 \pmod{m}$, it follows that $sa \equiv 1 \pmod{m}$
- Consequently, s is an inverse of a modulo m.
- Suppose there are two different inverses s and s' modulo m, then $sa\text{-}s'a=(s\text{-}s')a \equiv 0 \pmod{m}$. But that means $m \mid (s\text{-}s')$, which is impossible.

Finding Inverses 1

The Euclidean algorithm and Bézout coefficients gives us a systematic approaches to finding inverses.

Example: Find an inverse of 3 modulo 7.

Solution: Because gcd(3,7) = 1, by Theorem 1, an inverse of 3 modulo 7 exists.

- Using the Euclidian algorithm: $7 = 2\cdot 3 + 1$.
- From this equation, we get $-2\cdot 3 + 1\cdot 7 = 1$, and see that -2 and 1 are Bézout coefficients of 3 and 7.
- Hence, -2 is an inverse of 3 modulo 7.
- Also every integer congruent to -2 modulo 7 is an inverse of 3 modulo 7, i.e., 5, -9, 12, etc.

Finding Inverses 2

Example: Find an inverse of 101 modulo 4620.

Solution: First use the Euclidian algorithm to show that gcd(101,4620) = 1.

$4620 = 45\cdot 101 + 75$

$101 = 1\cdot 75 + 26$

$75 = 2\cdot 26 + 23$

$26 = 1\cdot 23 + 3$

$23 = 7\cdot 3 + 2$

$3 = 1\cdot 2 + 1$

$2 = 2\cdot 1$

Since the last nonzero remainder is 1, gcd(101,4620) = 1

Bézout coefficients : -35 and 1601

Working Backwards:

$1 = 3 - 1\cdot 2$

$1 = 3 - 1\cdot(23 - 7\cdot 3) = -1\cdot 23 + 8\cdot 3$

$1 = -1\cdot 23 + 8\cdot(26 - 1\cdot 23) = 8\cdot 26 - 9\cdot 23$

$1 = 8\cdot 26 - 9\cdot(75 - 2\cdot 26) = 26\cdot 26 - 9\cdot 75$

$1 = 26\cdot(101 - 1\cdot 75) - 9\cdot 75$

$= 26\cdot 101 - 35\cdot 75$

$1 = 26\cdot 101 - 35\cdot(4620 - 45\cdot 101)$

$= -35\cdot 4620 + 1601\cdot 101$

1601 is an inverse of 101 modulo 4620

Using Inverses to Solve Congruences

We can solve the congruence $ax \equiv b \pmod{m}$ by multiplying both sides by $\bar{a}$.

Example: What are the solutions of the congruence $3x \equiv 4 \pmod{7}$.

Solution: We found that 5 is an inverse of 3 modulo 7. We multiply both sides of the congruence by giving

$$5 \cdot 3x \equiv 5 \cdot 4 \pmod{7}.$$

It follows that if x is a solution, then $x \equiv 6 \pmod{7}$

The solutions are the integers x such that $x \equiv 6 \pmod{7}$, namely, 6,13,20 … and -1, -8, -15,…

The Chinese Remainder Theorem$_1$

In the first century, the Chinese mathematician Sun-Tsu asked:

There are certain things whose number is unknown. When divided by 3, the remainder is 2; when divided by 5, the remainder is 3; when divided by 7, the remainder is 2. What will be the number of things? 有物不知其數，三三數之剩二，五五數之剩三，七七數之剩二。問物幾何？

This puzzle can be translated into the solution of the system of congruences:

$x \equiv 2 \pmod 3$,

$x \equiv 3 \pmod 5$,

$x \equiv 2 \pmod 7$?

We'll see how the theorem that is known as the *Chinese Remainder Theorem* can be used to solve Sun-Tsu's problem.

The Chinese Remainder Theorem$_2$

Theorem 2: (*The Chinese Remainder Theorem*) Let $m_1, m_2, \ldots, m_n$ be pairwise relatively prime positive integers greater than one and $a_1, a_2, \ldots, a_n$ arbitrary integers. Then the system

$$x \equiv a_1 \pmod{m_1}$$
$$x \equiv a_2 \pmod{m_2}$$
$$\vdots$$
$$x \equiv a_n \pmod{m_n}$$

has a unique solution modulo $m = m_1 m_2 \cdots m_n$.

(That is, there is a solution x with $0 \le x < m$ and all other solutions are congruent modulo m to this solution.)

Proof: We'll show that a solution exists by describing a way to construct the solution. Showing that the solution is unique modulo m is Exercise 30.

Back Substitution

We can solve systems of linear congruences with pairwise relatively prime moduli by rewriting a congruences as an equality using Theorem 4 in Section 4.1, substituting the value for the variable into another congruence, and continuing the process until we have worked through all the congruences. This method is known as *back substitution*.

Example: Use the method of back substitution to find all integers x such that $x \equiv 1 \pmod 5$, $x \equiv 2 \pmod 6$, and $x \equiv 3 \pmod 7$.

Solution: By Theorem 4 in Section 4.1, the first congruence can be rewritten as $x = 5t + 1$, where t is an integer.

- Substituting into the second congruence yields $5t + 1 \equiv 2 \pmod 6$.
- Solving this tells us that $t \equiv 5 \pmod 6$.
- Using Theorem 4 again gives $t = 6u + 5$ where u is an integer.
- Substituting this back into $x = 5t + 1$, gives $x = 5(6u + 5) + 1 = 30u + 26$.
- Inserting this into the third equation gives $30u + 26 \equiv 3 \pmod 7$.
- Solving this congruence tells us that $u \equiv 6 \pmod 7$.
- By Theorem 4, $u = 7v + 6$, where v is an integer.
- Substituting this expression for u into $x = 30u + 26$, tells us that $x = 30(7v + 6) + 26 = 210u + 206$.

Translating this back into a congruence we find the solution $x \equiv 206 \pmod{210}$.

The Chinese Remainder Theorem$_3$

To construct a solution first let $M_k = m/m_k$ for $k = 1,2,\ldots,n$ and $m = m_1 m_2 \cdots m_n$. Since $\gcd(m_k, M_k) = 1$, by Theorem 1, there is an integer y_k, an inverse of M_k modulo m_k, such that

$$M_k y_k \equiv 1 \pmod{m_k}.$$

Form the sum

$$x = a_1 M_1 y_1 + a_2 M_2 y_2 + \cdots + a_n M_n y_n.$$

Note that because $M_j \equiv 0 \pmod{m_k}$ whenever $j \neq k$, all terms except the kth term in this sum are congruent to 0 modulo m_k.

Because $M_k y_k \equiv 1 \pmod{m_k}$, we see that $x \equiv a_k M_k y_k \equiv a_k \pmod{m_k}$, for $k = 1,2,\ldots,n$.

Hence, x is a simultaneous solution to the n congruences.

$$x \equiv a_1 \pmod{m_1}$$
$$x \equiv a_2 \pmod{m_2}$$
$$\vdots$$
$$x \equiv a_n \pmod{m_n}$$

The Chinese Remainder Theorem[4]

Example: Consider the 3 congruences from Sun-Tsu's problem:

$x \equiv 2 \ (\text{mod } 3)$, $x \equiv 3 \ (\text{mod } 5)$, $x \equiv 2 \ (\text{mod } 7)$.

- Let $m = 3 \cdot 5 \cdot 7 = 105$, $M_1 = m/3 = 35$, $M_2 = m/5 = 21$, $M_3 = m/7 = 15$.
- We see that
  - 2 is an inverse of $M_1 = 35$ modulo 3 since $35 \cdot 2 \equiv 2 \cdot 2 \equiv 1 \pmod 3$
  - 1 is an inverse of $M_2 = 21$ modulo 5 since $21 \equiv 1 \pmod 5$
  - 1 is an inverse of $M_3 = 15$ modulo 7 since $15 \equiv 1 \pmod 7$
- Hence,
  $x = a_1M_1y_1 + a_2M_2y_2 + a_3M_3y_3$
  $= 2 \cdot 35 \cdot 2 + 3 \cdot 21 \cdot 1 + 2 \cdot 15 \cdot 1 = 233 \equiv 23 \pmod{105}$
- We have shown that 23 is the smallest positive integer that is a simultaneous solution. Check it!

Hashing Functions

Definition: A *hashing function h* assigns memory location $h(k)$ to the record that has k as its key.

- A common hashing function is $h(k) = k$ **mod** m, where m is the number of memory locations.
- Because this hashing function is onto, all memory locations are possible.

Example: Let $h(k) = k$ **mod** 111. This hashing function assigns the records of customers with social security numbers as keys to memory locations in the following manner:

h(064212848) = 064212848 **mod** 111 = 14
h(037149212) = 037149212 **mod** 111 = 65
h(107405723) = 107405723 **mod** 111 = 14, but since location 14 is already occupied, the record is assigned to the next available position, which is 15.

The hashing function is not one-to-one as there are many more possible keys than memory locations. When more than one record is assigned to the same location, we say a *collision* occurs. Here a collision has been resolved by assigning the record to the first free location.

For collision resolution, we can use a *linear probing function*:
$h(k,i) = (h(k) + i)$ **mod** m, where i runs from 0 to $m - 1$.

There are many other methods of handling with collisions. You may cover these in a later CS course.

Applications of Congruences

Section 4.5

Pseudorandom Numbers[1]

Randomly chosen numbers are needed for many purposes, including computer simulations.

Pseudorandom numbers are not truly random since they are generated by systematic methods.

The *linear congruential method* is one commonly used procedure for generating pseudorandom numbers.

Four integers are needed: the *modulus m*, the *multiplier a*, the *increment c*, and *seed* x_0, with $2 \le a < m$, $0 \le c < m$, $0 \le x_0 < m$.

We generate a sequence of pseudorandom numbers $\{x_n\}$, with $0 \le x_n < m$ for all n, by successively using the recursively defined function $x_{n+1} = (ax_n + c) \ \mathbf{mod} \ m.$

If psuedorandom numbers between 0 and 1 are needed, then the generated numbers are divided by the modulus, x_n/m.

Pseudorandom Numbers 2

Example: Find the sequence of pseudorandom numbers generated by the linear congruential method with modulus $m = 9$, multiplier $a = 7$, increment $c = 4$, and seed $x_0 = 3$.

Solution: Compute the terms of the sequence by successively using the congruence

$$x_{n+1} ?\overset{?}{=} (7x_n + 4)\ \mathbf{mod}\ 9,\ \text{with}\ x_{0?} = 3.$$

$$\begin{aligned}
x_1 &\overset{?}{=} x_0 + 4\ \mathbf{mod}\ 9 \overset{?}{=} \cdot 3 + 4\ \mathbf{mod}\ 9 = 25\ \mathbf{mod}\ 9 = 7,\\
x_2 &\overset{?}{=} x_1 + 4\ \mathbf{mod}\ 9 \overset{?}{=} \cdot 7 + 4\ \mathbf{mod}\ 9 = 53\ \mathbf{mod}\ 9 = 8,\\
x_3 &\overset{?}{=} x_2 + 4\ \mathbf{mod}\ 9 \overset{?}{=} \cdot 8 + 4\ \mathbf{mod}\ 9 = 60\ \mathbf{mod}\ 9 = 6,\\
x_4 &\overset{?}{=} x_3 + 4\ \mathbf{mod}\ 9 \overset{?}{=} \cdot 6 + 4\ \mathbf{mod}\ 9 = 46\ \mathbf{mod}\ 9 = 1,\\
x_5 &\overset{?}{=} x_4 + 4\ \mathbf{mod}\ 9 \overset{?}{=} \cdot 1 + 4\ \mathbf{mod}\ 9 = 11\ \mathbf{mod}\ 9 = 2,\\
x_6 &\overset{?}{=} x_5 + 4\ \mathbf{mod}\ 9 \overset{?}{=} \cdot 2 + 4\ \mathbf{mod}\ 9 = 18\ \mathbf{mod}\ 9 = 0,\\
x_7 &\overset{?}{=} x_6 + 4\ \mathbf{mod}\ 9 \overset{?}{=} \cdot 0 + 4\ \mathbf{mod}\ 9 = 4\ \mathbf{mod}\ 9 = 4,\\
x_8 &\overset{?}{=} x_7 + 4\ \mathbf{mod}\ 9 \overset{?}{=} \cdot 4 + 4\ \mathbf{mod}\ 9 = 32\ \mathbf{mod}\ 9 = 5,\\
x_9 &\overset{?}{=} x_8 + 4\ \mathbf{mod}\ 9 \overset{?}{=} \cdot 5 + 4\ \mathbf{mod}\ 9 = 39\ \mathbf{mod}\ 9 = 3.
\end{aligned}$$

The sequence generated is 3,7,8,6,1,2,0,4,5,3,7,8,6,1,2,0,4,5,3,…

It repeats after generating 9 terms.

Commonly, computers use a linear congruential generator with increment $c = 0$. This is called a *pure multiplicative generator*. Such a generator with modulus $2^{31} - 1$ and multiplier $7^5 = 16{,}807$ generates $2^{31} - 2$ numbers before repeating.

Check Digits:ISBNs

Books are identified by an *International Standard Book Number* (ISBN-10), a 10 digit code. The first 9 digits identify the language, the publisher, and the book. The tenth digit is a check digit, which is determined by the following congruence

$$x_{10} \equiv \sum_{i=1}^{9} i x_i \pmod{11}.$$

The validity of an ISBN-10 number can be evaluated with the equivalent $\sum_{i=1}^{10} i x_i \equiv 0 \pmod{11}$.

a. Suppose that the first 9 digits of the ISBN-10 are 007288008. What is the check digit?

b. Is 084930149X a valid ISBN10?

X is used for the digit 10.

Solution:

a. $X_{10} \equiv 1\cdot0 + 2\cdot0 + 3\cdot7 + 4\cdot2 + 5\cdot8 + 6\cdot8 + 7\cdot0 + 8\cdot0 + 9\cdot8 \pmod{11}$.
$X_{10} \equiv 0 + 0 + 21 + 8 + 40 + 48 + 0 + 0 + 72 \pmod{11}$.
$X_{10} \equiv 189 \equiv 2 \pmod{11}$. Hence, $X_{10} = 2$.

b. $1\cdot0 + 2\cdot8 + 3\cdot4 + 4\cdot9 + 5\cdot3 + 6\cdot0 + 7\cdot1 + 8\cdot4 + 9\cdot9 + 10\cdot10 =$
$0 + 16 + 12 + 36 + 15 + 0 + 7 + 32 + 81 + 100 = 299 \equiv 2 \not\equiv 0 \pmod{11}$

Hence, 084930149X is not a valid ISBN-10.

A *single error* is an error in one digit of an identification number and a *transposition error* is the accidental interchanging of two digits. Both of these kinds of errors can be detected by the check digit for ISBN-10.

Check Digits: UPCs

A common method of detecting errors in strings of digits is to add an extra digit at the end, which is evaluated using a function. If the final digit is not correct, then the string is assumed not to be correct.

Example: Retail products are identified by their *Universal Product Codes* (*UPCs*). Usually these have 12 decimal digits, the last one being the check digit. The check digit is determined by the congruence:

$$3x_1 + x_2 + 3x_3 + x_4 + 3x_5 + x_6 + 3x_7 + x_8 + 3x_9 + x_{10} + 3x_{11} + x_{12} \equiv 0 \pmod{10}.$$

a. Suppose that the first 11 digits of the UPC are 79357343104. What is the check digit?

b. Is 041331021641 a valid UPC?

Solution:

a. $3\cdot7 + 9 + 3\cdot3 + 5 + 3\cdot7 + 3 + 3\cdot4 + 3 + 3\cdot1 + 0 + 3\cdot4 + x_{12} \equiv 0 \pmod{10}$
$21 + 9 + 9 + 5 + 21 + 3 + 12 + 3 + 3 + 0 + 12 + x_{12} \equiv 0 \pmod{10}$
$98 + x_{12} \equiv 0 \pmod{10}$
$x_{12} \equiv 2 \pmod{10}$ So, the check digit is 2.

b. $3\cdot0 + 4 + 3\cdot1 + 3 + 3\cdot3 + 1 + 3\cdot0 + 2 + 3\cdot1 + 6 + 3\cdot4 + 1 \equiv 0 \pmod{10}$
$0 + 4 + 3 + 3 + 9 + 1 + 0 + 2 + 3 + 6 + 12 + 1 = 44 \equiv 4 \not\equiv 0 \pmod{10}$
Hence, 041331021641 is not a valid UPC.

Check Digits:ISBNs

<u>Single error</u>: $y_j = x_j + a$

Then

$$\sum_{i=1}^{10} i y_i = \sum_{i=1}^{10} i x_i + ja \equiv ja \not\equiv 0 \pmod{11}$$

<u>Transposition error</u>: $y_j = x_k$ and $y_k = x_j$

Then

$$\sum_{i=1}^{10} i y_i = \sum_{i=1}^{10} i x_i + j x_k - j x_j + k x_j - k x_k$$
$$\equiv (x_k - x_j)(j - k) \not\equiv 0 \pmod{11}$$