prove that d divides n if and only if d divides $a_k + a_{k-1} + \cdots + a_0$

Solution: We have $n = (a_k a_{k-1} \cdots a_1 a_0)_b$

$= b^k a_k + b^{k-1} a_{k-1} + \cdots + b \cdot a_1 + a_0$

Since d divides $b-1$, we find that $b \equiv 1 \pmod{d}$

Hence $b^i \equiv 1 \pmod{d}$ for all integers $i \geq 1$. From the above representation of n, it follows that

$$n \equiv (1 \cdot a_k + 1 \cdot a_{k-1} + \cdots + a_1 + a_0) \pmod{d}$$

i.e $$n \equiv (a_k + a_{k-1} + \cdots + a_1 + a_0) \pmod{d}$$

Hence n is divisible by d if and only if $a_k + a_{k-1} + \cdots + a_0$ is divisible by d.

Check digits : In our everyday life we see many consumer goods in packets bearing some identification numbers; even in some books such marks are given. On each of them there is an identification code which is a string of digits. We first describe how congruences are used to detect errors in strings of digits which are used to identify books.

Since 1972, each book published throughout the world began to receive ten-digit numerical label called International Standard Book Number (ISBN). For example, the ISBN of Abstract Algebra by I. N. Herstein is 0-02-353820-1, the ISBN of Discrete Mathematics by Richard Johnsonbaugh (Third Edition) is 0-02-360721-1. One may see the ISBN of a book on the back of the last cover page or in the beginning of the book. Now in the ISBN 0-02-353820-1 of Herstein's Abstract Algebra, the leading digit 0 means that the book is published in the English speaking world like United Kingdom, United States, Australia, Canada, New Zealand, South Africa. The next group of digits, 02 identifies the publisher (in this case, Macmillan Publishing company)

This block 353820 is the number assigned to the book by the publisher, that is 353820 designates this particular book among all those published by Macmillan. The final block of the above ISBN is 1. This number is called the check digit. This check digit makes the ISBN into an example of error correcting code. With the help of this check digit, publishers, booksellers are often able to detect an incorrect ISBN that may occur when the ISBN is incorrectly typed or transmitted by telephone line, or by e-mail etc. and can avoid costly shipping charges that would result from filling an incorrect order.

Formally we describe an ISBN in the following way:

An ISBN is an expression $x_1 x_2 x_3 \cdots x_9 x_{10}$ of ten digits, divided into four blocks, the first block represents the country from which it is published, the second block represents the publishing company, the third block is the number assigned to the book by the publisher, the final block consists of only one digit called the check digit. For $i = 1, 2, \ldots, 9$ each x_i is one of the digits $0, 1, 2, 3, \ldots, 9$. The check digit x_{10} has eleven possible values: $0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10$. Notice that if x_{10} is 10 then this check digit consists of two digits. Since we use only one digit for check digit, we replace 10 by X. Then the possible check digits are $0, 1, 2, 3, 4, 5, 6, 7, 8, 9, X$

We now explain how a check digit is assigned to a particular book. For this we take the help of congruence. Suppose the first nine digits $x_1, x_2, x_3, \ldots, x_9$ of an ISBN are chosen. Then the check digit x_{10} which is one of $0, 1, 2, 3, 4, 5, 6, 7, 8, 9, X$, is determined by the congruence

$$1x_1 + 2x_2 + 3x_3 + 4x_4 + 5x_5 + 6x_6 + 7x_7 + 8x_8 + 9x_9 + 10x_{10} \equiv 0 \pmod{11}$$

That is $$\sum_{i=1}^{9} i x_i + 11 x_{10} - x_{10} \equiv 0 \pmod{11}$$

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

Example: Let the first 9 digits of the ISBN of a particular book be 0-673-38582. Then the check digit x_{10} is

given by

$$1\cdot0 + 2\cdot6 + 3\cdot7 + 4\cdot3 + 5\cdot3 + 6\cdot8 + 7\cdot5 + 8\cdot8 + 9\cdot2 \equiv x_{10} \pmod{11}$$

That is $0 + 12 + 21 + 12 + 15 + 48 + 35 + 64 + 18 \equiv x_{10} \pmod{11}$

i.e., $(11+1) + (22-1) + (11+1) + (11+4) + (44+4) + (33+2) + (66-2) + 22-4 \equiv x_{10} \pmod{11}$

i.e., $5 \equiv x_{10} \pmod{11}$. Since $0 \le x_{10} \le 10$, it follows that $x_{10} = 5$.

Example 2. In this example we consider the ISBN $3-540-05329-x_{10}$ of a book. The check digit is one of the digits $0, 1, 2, 3, 4, 5, 6, 7, 8, 9, X$ and it satisfies

$$1\cdot3 + 2\cdot5 + 3\cdot4 + 4\cdot0 + 5\cdot0 + 6\cdot5 + 7\cdot3 + 8\cdot2 + 9\cdot9 \equiv x_{10} \pmod{11}$$

or, $3 + 10 + 12 + 0 + 0 + 30 + 21 + 16 + 81 \equiv x_{10} \pmod{11}$

or, $3 + (11-1) + (11+1) + (33-3) + (22-1) + (11+5) + (77+4) \equiv x_{10} \pmod{11}$

or, $8 \equiv x_{10} \pmod{11}$. Since $0 \le x_{10} \le 10$,

So, $x_8 = 8$.

Exercise 1. Let $0-85312-612-x_{10}$ be the ISBN of a book. Find the check digit.

2. Let $0-201-06561-x_{10}$ be the ISBN of a book. Find the check digit.

3. Determine whether the following ISBNs are valid

(a) $3-540-19102-X$ (b) $81-2713-0871-9$

Universal product code: Many products sold in the market have an identification number called a universal product number. A universal product code is a to represent a universal product number as a pattern of black and white stripes of varion thickness. For this reason it is also called a bar code. It is denoted by

UPC. It has 13 digits. It has four blocks of numbers They are 1. The number system 2. The manufacturer code 3. The product code 4. Check digit.

The number system digit, usually, is printed just to the left of the bar code, the check digit to the right of the bar code, and the manufacturer and product codes are printed just below the barcode.

The following strings demonstrate a UPC for the Britannia Bisenit Cream Cracker: 8 901063 211070

Here the 13th digit 0 is the check digit. We now explain how the check digit is obtained. Consider a particular product manufactured by a particular manufacturer. Then the first 12 digits $x_1, x_2, \ldots, x_{12}$ are fixed. The check digit x_{13} is an integer such that $0 \le x_{13} < 10$ and it satisfies the congruence

$$x_{13} \equiv -(1x_1 + 3x_2 + 1\cdot x_3 + 3x_4 + \ldots + 1\cdot x_{11} + 3\cdot x_{12}) \pmod{10}$$

i.e., $x_1 + 3x_2 + x_3 + 3x_4 + x_5 + 3x_6 + \ldots + x_{11} + 3x_{12} + x_{13} \equiv 0 \pmod{10}$

Example: Check whether 8 901063 211070 is a valid UPC or not.

Solution: If x_{13} be the check digit, then

$$8 + 3\cdot 9 + 0 + 3\times 1 + 0 + 3\times 6 + 3 + 3\times 2 + 1 + 3\times 1 + 0 + 3\times 7 + x_{13} \equiv 0 \pmod{10}$$

or, $8 + 7 + 3 + 8 + 6 + 1 + 3 + 1 + x_{13} \equiv 0 \pmod{10}$

or, $8 + (20+7) + 3 + (10+8) + 3 + 6 + 1 + 3 + (20+1) + x_{13} \equiv 0 \pmod{10}$

or, $40 + x_{13} \equiv 0 \pmod{10}$

or, $x_{13} \equiv 0 \pmod{10}$

As $0 \le x_{13} < 10$ So, $x_{13} = 0$

So, 8 901063 211070 is a valid UPC.

Exercise 1. Is 8 901030 114519 a correct UPC for some product?

Boolean Algebra: Definition : By a Boolean Algebra we mean a system $(B, +, \cdot, ')$ where B is a non-empty set, $+$ and $\cdot$ are two binary operations on B called addition and multiplication and $'$ is a unary operation (i.e., $'$ is a mapping from B to B) on B satisfying the following axioms:

A1. $a+b = b+a$ and $a \cdot b = b \cdot a$ for all $a, b \in B$ ($+$ and $\cdot$ are commutative)

A2. $a + (b \cdot c) = (a+b) \cdot (a+c)$

and $a \cdot (b+c) = a \cdot b + a \cdot c$ for all $a, b \in B$

(Each binary operation distributes over the other)

A3. B contains distinct identity elements 0 and 1 (known as zero and unit element) with respect to the operations $+$ and $\cdot$ respectively. i.e., $a+0 = a$, $a \cdot 1 = a$ for all $a \in B$

A4. For each $a \in B$, there exists an element $a' \in B$ such that $a + a' = 1$ and $a \cdot a' = 0$

Note: 1. a' is called the complementation of a. Very often we shall denote $a \cdot b$ by ab

2. A Boolean Algebra is generally denoted by a 6-tuple $(B, +, \cdot, ', 0, 1)$ or by $(B, +, \cdot, ')$ or simply by the set B itself.

Example 1. Let A be a non-empty set and let $B = P(A) =$ the power set of A. Then B is a Boolean Algebra under the usual operations of union, intersection and complementation in B. The sets ϕ and A are zero element and unit element of B. Observe if A is an infinite set then Boolean Algebra $B = P(A)$ is also infinite

2. Let B be the set of all positive integers which are divisors of 70, i.e., $B = \{1, 2, 5, 7, 10, 14, 35, 70\}$

For $a, b \in B$, let $a+b$ = l.c.m of a, b and $a \cdot b$ = h.c.f of a, b and $a' = 70/a$. Then $(B, +, \cdot, ')$ is a Boolean Algebra Here 1 is the zero element 70 is the unit element.

Definition: By a proposition in a Boolean Algebra we mean either a statement or an algebraic identity in a Boolean Algebra.

Definition: By the dual of a proposition A in a Boolean Algebra we mean the proposition obtained from A by interchanging + and . and exchanging 0 and 1.

For example, the dual of the proposition $x.(y+z) = x.y + x.z$ is the proposition $x+(y.z) = (x+y).(x+z)$ and vice-versa.

If A is the dual of B, then B is the dual of A.

Theorem 32 (Duality Principle): If a proposition A is derivable from the axioms of a Boolean Algebra, then the dual of A is also derivable from those axioms

Proof: In the definition of a Boolean Algebra each axiom is a dual pair of propositions. Hence, if in a proof of the proposition A, we replace every proposition by its dual, the result is again a proof, since axioms are replaced by axioms. But this new proof is a proof of the dual of A.

Theorem 33 In a Boolean Algebra $(B, +, \cdot, ')$ the following hold:

(i) The elements 0 and 1 are unique
(ii) Each $a \in B$ has a unique complementation $a' \in B$
(iii) For each $a \in B$, $(a')' = a$
(iv) $0' = 1$ and $1' = 0$
(v) (Idempotent Law) $a+a = a$ and $a.a = a$ for all $a \in B$
(vi) $a+1 = 1$, $a.0 = 0$ for every $a \in B$.
(vii) (Absorption Law) $a.(a+b) = a$ and $a+(a.b) = a$ for all $a, b \in B$

Proof: If possible, Let 0_1 and 0_2 be two zero elements of B. Then, by definition $a+0_1 = a$ and $a+0_2 = a$ for each $a \in B$

Hence $0_2 + 0_1 = 0_2$ and $0_1 + 0_2 = 0_1$. But $0_1+0_2 = 0_2+0_1$

So, $0_1 = 0_2$. So zero element is unique. By duality,

unit element 1 is unique.

(ii) Let a_1', a_2' be two complementation of a. Then,

$$a+a_1' = 1,\ a\cdot a_1' = 0 \text{ and } a+a_2' = 1,\ a\cdot a_2' = 0$$

Now, $a_1' = a_1'\cdot 1 = a_1'\cdot(a+a_2') = a_1'\cdot a + a_1'\cdot a_2' = 0 + a_1'\cdot a_2' = a_1'\cdot a_2'$

Similarly we can show that $a_2' = a_2'\cdot a_1'$. Hence $a_1' = a_2'$ as

$$a_1'\cdot a_2' = a_2'\cdot a_1'$$

(iii) For each $a \in B$, there exists a unique $a' \in B$ such that

$a\cdot a' = 0$ and $a+a' = 1$ Hence

$$a'+a = 1 \text{ and } a'\cdot a = 0 \quad \text{(commutative laws)}$$

So, $(a')' = a$

(iv) By axiom 3 (A3), $a\cdot 1 = a$ and $0+a = a$ for every $a \in B$.

Replacing a by 0 and 1 respectively $0\cdot 1 = 0$ and $0+1 = 1$. So, by axiom 4 (A4) $0' = 1$. The second part is the dual of the first.

(v) $a+a = (a+a)\cdot 1$ (A3)
$= (a+a)\cdot(a+a')$ (A4)
$= a+(a\cdot a')$ (A2)
$= a+0$ (A4)
$= a$ (A3)

The second part is the dual of the first part.

(vi) $a+1 = (a+1)\cdot 1$ (A3)
$= 1\cdot(a+1)$ (A1)
$= (a+a')(a+1)$ (A4)
$= a+(a'\cdot 1)$ (A2)
$= a+a'$ (A3)
$= 1$ (A4)

The second part is the dual of the first part

(vii) $a\cdot(a+b) = (a+0)\cdot(a+b)$ (A3)
$= a+(0\cdot b)$ (A2)
$= a+0$ (Result (vi))
$= a$ (A3)

The second part is the dual of the first part.

Theorem 34: In a Boolean Algebra $(B, +, \cdot, ')$ the following hold:

For all $a, b, c \in B$,

(i) If $b+a = c+a$ and $b+a' = c+a'$, then $b = c$. Also if $b \cdot a = c \cdot a$ and $b \cdot a' = c \cdot a'$ then $b = c$

(ii) $\left.\begin{aligned} a+(b+c) &= (a+b)+c \\ a \cdot (b \cdot c) &= (a \cdot b) \cdot c \end{aligned}\right\}$ Associative Laws

(iii) $\left.\begin{aligned} (a+b)' &= a' \cdot b' \\ (a \cdot b)' &= a' + b' \end{aligned}\right\}$ De Morgan's Laws

(iv) $a+b = (a' \cdot b')'$ and $a \cdot b = (a' + b')'$

(v) $a + b' = 1$ if and only if $a + b = a$

Also $a \cdot b' = 0$ if and only if $a \cdot b = a$

(vi) $a + (a' \cdot b) = a + b$ and $a \cdot (a' + b) = a \cdot b$

Proof: (i) We assume $b+a = c+a$ and $b+a' = c+a'$. Then,

$$\begin{aligned} b &= b + 0 && (A3) \\ &= b + (a \cdot a') && (A4) \\ &= (b+a) \cdot (b+a') && (A2) \\ &= (c+a) \cdot (c+a') && (\text{Given assumptions}) \\ &= c + (a \cdot a') && (A2) \\ &= c + 0 && (A4) \\ &= c && (A3) \end{aligned}$$

The second part is the dual of the first part.

(ii) We show that (a) $(a+(b+c)) \cdot a = ((a+b)+c) \cdot a$ and

and (b) $(a+(b+c)) \cdot a' = ((a+b)+c) \cdot a'$

Proof of (a) $(a+(b+c)) \cdot a = a \cdot (a+(b+c)) = a$ (Absorption Law)

Also, $((a+b)+c) \cdot a = a \cdot ((a+b)+c) = a \cdot (a+b) + a \cdot c$

$= a + a \cdot c$ (Absorption Law)

$= a$ (Absorption Law)

Thus (a) is proved.

Proof of (b): $(a+(b+c)) \cdot a' = a' \cdot (a+(b+c))$

$= (a' \cdot a) + a' \cdot (b+c) = 0 + a' \cdot (b+c) = a' \cdot (b+c)$

Again, $((a+b)+c).a' = a'.((a+b)+c) = a'.(a+b)+a'.c$

$= (a'.a + a'.b)+a'.c = (0+a'.b)+a'.c$

$= a'.b + a'.c = a'.(b+c)$

Then $(a+(b+c)).a' = ((a+b)+c).a'$

Here using second part of (i) of this theorem we have $a+(b+c) = (a+b)+c$

The second part is the dual of the first part.

Note: From now on we shall write $a.(b.c)$ and $(a.b).c$ as abc similarly $a+(b+c)$ and $(a+b)+c$ as $a+b+c$

(iii) we have $(a+b)+(a'.b') = ((a+b)+a').((a+b)+b')$

$= (a'+(a+b)).(a+(b+b'))$

$= ((a'+a)+b).(a+1)$

$= (1+b).(a+1) = 1.1 = 1$ ... (1)

Again $(a+b).(a'.b') = ((a+b).a').b' = (a'.(a+b)).b'$

$= ((a'.a)+(a'.b)).b'$

$= (0+(a'.b)).b' = (a'.b).b'$

$= a'.(b.b') = a'.0 = 0$ ... (2)

From (1) and (2), it follows that $(a+b)' = a'.b'$

The second part is the dual of the first part.

(iv) $(a+b)' = a'.b'$ Here $((a+b)')' = (a'.b')'$

or, $a+b = (a'.b')'$

The second part is the dual of the first part.

(v) Let $a+b' = 1$. Now

$a+b = (a+b).1 = (a+b).(a+b')$ (Assumption)

$= a+(b.b') = a+0 = a$

Similarly, let $a+b = a$ Now,

$a+b' = 1.(a+b') = (a+a').(a+b')$

$= a + (a'.b') = a + (a+b)'$ (De Morgan's Law)

$= a + a'$ (Complement)

$= 1$

The second part is the dual of the first part.

(vi) $a + (a'.b) = (a+a').(a+b)$ (Distributive law)

$= 1.(a+b) = a+b$

The second part is the dual of the other.

Example 1. Prove that $a.(a.b)' = a.b'$ in a Boolean Algebra where $a, b \in B$

Proof: $a.(a.b)' = a.(a'+b')$ (De Morgan's law)

$= a.a' + a.b' = 0 + a.b' = a.b'$

Example 2: For any Boolean algebra B, prove that

$(a+b)(b+c)(c+a) = ab + bc + ca$ for all $a, b, c \in B$.

Solution: $(a+b)(b+c)(c+a) = (a+b)(bc+ba+c+ca)$

$= abc + aba + ac + aca + bbc + bba + bc + bca$

$= (abc + abc) + (ac + ac) + (bc + bc) + (ba + ba)$

$= abc + ac + bc + ab$

$= ac(b+1) + bc + ab$

$= ac.1 + bc + ab$

$= ab + bc + ca$

Exercises: In a Boolean algebra B, prove that

(i) $(a+b)(a'+c)(b+c) = ac + a'b + bc$ for all $a, b, c \in B$

(ii) $ac + a'b + bc = (a+b)(a'+c)$ for all $a, b, c \in B$

END