CS 1310 : Discrete Structures 1
Exam 3
11 October 2018, Thursday
Marks : 80 **Duration** : 1.5 hour

"You know what seems odd to me? Numbers that aren't divisible by two."
Wish you good luck with the final exam !

Q1) All books are identified by an International Standard Book Number (ISBN-10), a 10-digit code $x_1x_2 . . . x_{10}$, assigned by the publisher. An ISBN-10 consists of blocks identifying the language, the publisher, the number assigned to the book by its publishing company, and finally, a check digit that is either a digit or the letter X (used to represent 10). This check digit is selected so that
x10 ≡ \sum_{i=1}^9 ix_i (mod 11),
or equivalently, so that
\sum_{i=1}^10 ix_i ≡ 0 (mod 11).
Answer these questions about ISBN-10s:

(a) The first nine digits of the ISBN-10 of the sixth edition of this book are 007288008. What is the check digit?

(b) Is 084930149X a valid ISBN-10?

A single error, an error in one digit of an identification number, is perhaps the most common type of error. Another common kind of error is a transposition error, which occurs when two digits are accidentally interchanged.
Show that we can detect the following errors (where we include the possibility that one of the two digits is the check digit X, representing 10) using ISBN-10.

(c) single error
(d) transposition of two digits

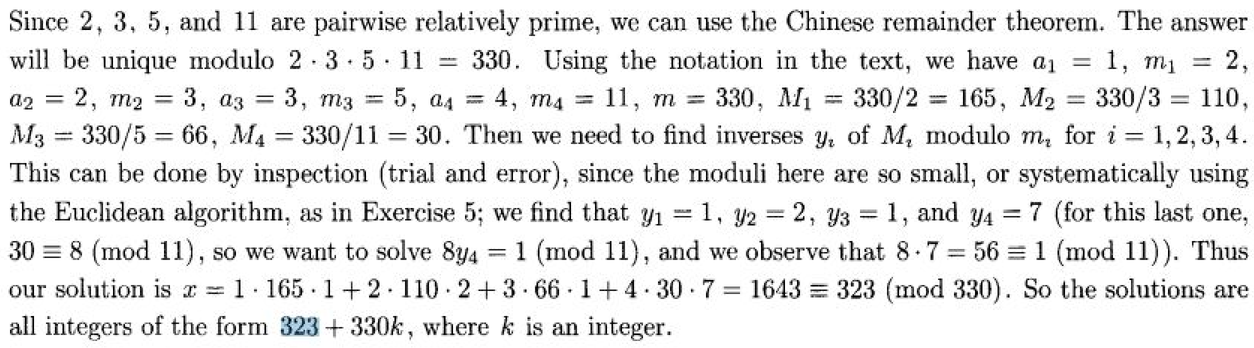
Marks : 2 + 2 + 3 + 3 =10

Solution: (a) The check digit is determined by the congruence □10 ix ≡ 0 (mod 11). Inserting
i=1 i
the digits 007288008 gives x10 ≡1·0+2·0+3·7+4·2+5·8+6·8+7·0+8·0+
9·8 (mod 11).This means that x10 ≡0+0+21+8+40+48+0+0+72 (mod 11), so x10 ≡189≡2(mod 11). Hence, **x10 =2**. □
(b) To see whether 084930149X is a valid ISBN-10, we see if 10 ix ≡ 0 (mod 11). Wei=1 i
see that 1 · 0 + 2 · 8 + 3 · 4 + 4 · 9 + 5 · 3 + 6 · 0 + 7 · 1 + 8 · 4 + 9 · 9 + 10 · 10 = 0 + 16 +12 + 36 + 15 + 0 + 7 + 32 + 81 + 100 = 299 ≡ 2/≡ 0 (mod 11). Hence, 084930149X is **not a valid** ISBN-10.

Q2) An old woman goes to the market with a basket of eggs. She sets the basket down and a horse accidentally steps on it, crushing all the eggs. The horse rider offers to pay her for the damaged eggs and asks how many eggs did she have. She tells the rider that she cannot remember but that when she had taken all of the eggs out 2 at a time, there were 1 left in the basket. When she took them out 3 at a time, there were 2 left. When she took them out 5 at a time, there were 3 left, and when she took them out 11 at a time, there were 4 left. Use Chinese remainder theorem to find the smallest number of eggs she could have had and verify the same using the back substitution method?

Marks : 10 + 10 =20

Solution:



Since 2, 3, 5, and 11 are pairwise relatively prime, we can use the Chinese remainder theorem. The answer will be unique modulo $2 \cdot 3 \cdot 5 \cdot 11 = 330$. Using the notation in the text, we have $a_1 = 1$, $m_1 = 2$, $a_2 = 2$, $m_2 = 3$, $a_3 = 3$, $m_3 = 5$, $a_4 = 4$, $m_4 = 11$, $m = 330$, $M_1 = 330/2 = 165$, $M_2 = 330/3 = 110$, $M_3 = 330/5 = 66$, $M_4 = 330/11 = 30$. Then we need to find inverses y_i of M_i modulo m_i for $i = 1, 2, 3, 4$. This can be done by inspection (trial and error), since the moduli here are so small, or systematically using the Euclidean algorithm, as in Exercise 5; we find that $y_1 = 1$, $y_2 = 2$, $y_3 = 1$, and $y_4 = 7$ (for this last one, $30 \equiv 8 \pmod{11}$, so we want to solve $8y_4 = 1 \pmod{11}$, and we observe that $8 \cdot 7 = 56 \equiv 1 \pmod{11}$). Thus our solution is $x = 1 \cdot 165 \cdot 1 + 2 \cdot 110 \cdot 2 + 3 \cdot 66 \cdot 1 + 4 \cdot 30 \cdot 7 = 1643 \equiv 323 \pmod{330}$. So the solutions are all integers of the form $323 + 330k$, where k is an integer.

Smallest number of eggs=323

Is Back substitution solving a set of equations or just checking if answer modulo given divisors match the given remainders?

Q3) Find each of these values.

a) $(99^2$ mod $32)^3$ mod 15

b) (−133mod23+ 261 mod 23) mod 23

c) (457mod23 * 182mod23) mod 23

Marks : 2 + 2 + 2 = 6

Solution:

a) $(99^2$ mod $32)^3$ mod 15 = 9^3 mod 15 = 729 mod 15 = **9**

b) (−133 mod 23+ 261 mod 23) mod 23 = (-133+261) mod 23 = 128 mod 23 = **13**

c) (457mod23 * 182mod23) mod 23 = (457*182) mod 23 = 83174 mod 23 = **6**

Q4) Find the sum and product of each of these pairs of numbers. Marks: 2 + 2 = 4

Express your answers in appropriate expansion.

a) $(763)_8$, $(147)_8$

b) $(112)_3$, $(210)_3$

Solution:

for convenience. leaving subscripts

a) 763 + 147 = **1132** (decimal: 499 + 103 = 602) and 763 · 147 = **144,305** (decimal: 499 · 103 = 51,397)

b) 112 + 210 = **1022** (decimal: 14 + 21 = 35) and 112.210 = **101220** (decimal: 14.21 = 294)

Q5) Show that if a, b, k, and m are integers such that k ≥ 1, m ≥ 2, and a ≡ b (mod m), then a^k ≡ b^k(mod m)

Marks: 5

Solution:

We know that if m be a positive integer and a ≡ b (mod m) and c ≡ d (mod m), then

a + c ≡ b + d (mod m) and ac ≡ bd (mod m)
Since a= b (mod m) implies that a· a = b · b (mod m), i.e., a^2 = b^2 (mod m). Invoking the Theorem again, since a= b (mod m) and a^2 = b^2 (mod m), we obtain a^3 = b^3 (mod m). After k - 1 applications of this process, we obtain a^k =b^k (mod m).

Alternately, we can argue directly, using the algebraic identity

$$a^{k}-b^{k} = (a-b)(a^{k-l} +a^{k-2}b+\cdot\cdot\cdot+ab^{k-2} +b^{k-l}).$$

Specifically, the hypothesis that a= b (mod m) means that m | (a - b). Therefore by the Theorem if a | b, then a | bc for all integers c ; m divides the right-hand side of this identity, so m | (a^{k} - b^{k}). This means precisely that a^{k}=b^{k} (mod m).

Q6) Decrypt the ciphertext message “PPBO ZACKLUAZ HZL HDLZVTL” that was encrypted with by shifting the alphabets in the original message as (p + 7) mod 26. (Please note that p represents integer representation of english alphabets starting from 0, i.e. A=0, K=10, Z=25

Marks: 5

Solution:

To decrypt the ciphertext “PPBO ZACKLUAZ HZL HDLZVTL” we first translate the letters back to elements of **Z**26. We obtain

15 15 1 14   25 0 2 10 11 20 0 25   7 24 11   7 3 11 25 21 19 11

Next, we shift each of these numbers by −k = −7 modulo 26 to obtain

8 8 19 7   18 19 20 3 4 13 19 18   0 17 4   0 22 4 18 14 12 4

Finally, we translate these numbers back to letters to obtain the plaintext. We obtain
IITH STUDENTS ARE AWESOME

Q7) Compute the following using Fermat’s little theorem and exponentiation method
3^{302} mod 11   Marks: 5 + 5 = 10 marks

Solution:

According to Fermat’s little theorem If p is prime and a is an integer not divisible by p, then

a^{p-1} ≡ 1 (mod p).

Furthermore, for every integer a we have

a^{p} ≡ a (mod p)

So,

3^{302} mod 11 = $(3^{10})^{30}.3^{2}$ mod 11 = $(1)^{30}$.9 mod 11 = 9

exponentiation method :

a_j = 302 = $(100101110)_2$

x = 1 , p = 3.3 (mod 11) = 9
x= 1.9 (mod 11) = 9, p = 9.9 (mod 11) = 4

x = 9.4 (mod 11) = 3, p = 4.4 (mod 11) = 5
x = 3.5 (mod 11) = 4, p = 5.5 (mod 11) = 3
x = 4 , p = 3.3 (mod 11) = 9
x = 4.9 (mod 11) = 3, p = 9.9 (mod 11) = 4
x= 3, p = 4.4 (mod 11) = 5
x= 3, p = 5.5 (mod 11) = 3
x= 3.3 (mod 11) = 9 , p = 3.3(mod 11) = 9
So, $3^{\mathbf{302}}$ **mod 11 = x = 9**

Q8) State the fundamental theorem of arithmetic and use it show that $\log_2 3$ is an irrational number. Marks: 2+3 = 5

Solution:

fundamental theorem of arithmetic: Every integer greater than 1 can be written uniquely as a prime or as the product of two or more primes where the prime factors are written in order of nondecreasing size.

Ex:

$100 = 2 \cdot 2 \cdot 5 \cdot 5 = 2^2 . 5^2$,
641 = 641,
$999 = 3 \cdot 3 \cdot 3 \cdot 37 = 3^3 \cdot 37$

Showing that $\log_2 3$ is an irrational number :

Proof by contradiction: Suppose that $\log_2 3$ is the rational number p/q, where p and q are integers. Since $\log_2 3 > 0$, we can assume that p and q are positive. Translating the equation $\log_2 3 = p / q$ into its exponential equivalent,
we obtain $3 = 2^{p/q}$.
Raising both sides to the qth power yields $3^q = 2^P$.
Now this is a violation of the Fundamental Theorem of Arithmetic, since it gives two different prime factorizations of the same number. Hence our assumption (that $\log_2 3$ is rational) must be wrong, and we conclude that $\log_2 3$ is irrational.

Q9) Use the Euclidean algorithm to find gcd(144, 89) and express its as linear combination of 144 and 89 by finding the bezout coefficients. Marks: 5+3 = 8

Solution:

Applying the Euclidean algorithm,

$144 = 1 \cdot 89 + 55$
$89 = 1 \cdot 55 + 34$
$55 = 1 \cdot 34 + 21$
$34 = 1 \cdot 21 + 13$
$21 = 1 \cdot 13 + 8$
$13 = 1 \cdot 8 + 5$
$8 = 1 \cdot 5 + 3$
$5 = 1 \cdot 3 + 2$

$3 = 1 \cdot 2 + 1$
$2 = 2 \cdot 1$

It follows that gcd(144, 89) = 1.

Furthermore, back substitution yields

$$\begin{aligned}
1 &= 3 - 1 \cdot 2 = 3 - 1[5 - 1 \cdot 3] \\
&= 2 \cdot 3 - 1 \cdot 5 = 2[8 - 1 \cdot 5] - 1 \cdot 5 \\
&= 2 \cdot 8 - 3 \cdot 5 = 2 \cdot 8 - 3[13 - 1 \cdot 8] \\
&= 5 \cdot 8 - 3 \cdot 13 = 5[21 - 1 \cdot 13] - 3 \cdot 13 \\
&= 5 \cdot 21 - 8 \cdot 13 = 5 \cdot 21 - 8[34 - 1 \cdot 21] \\
&= 13 \cdot 21 - 8 \cdot 34 = 13[55 - 1 \cdot 34] - 8 \cdot 34 \\
&= 13 \cdot 55 - 21 \cdot 34 = 13 \cdot 55 - 21[89 - 1 \cdot 55] \\
&= 34 \cdot 55 - 21 \cdot 89 = 34[144 - 1 \cdot 89] - 21 \cdot 89 \\
&= 34 \cdot 144 - 55 \cdot 89.
\end{aligned}$$

The Bezout coefficients are 34, - 55.

Q10) Aladdin finds three boxes in a cave. Each box has imprinted on it a clue as to its contents; the clues are:
Box 1 “The gold is not here”
Box 2 “The gold is not here”
Box 3 “The gold is in Box 2”
Let Bi with i ∈ {1, 2, 3} be the propositions that represent “gold is in the i-th box”. Also its given that, One contains gold, the other two are empty; Only one message is true and the other two are false. Formalise these statements in Propositional Logic and help Aladdin to find which box contains gold using rules of inference. Mark : 4 + 3 = 7

Solution:
Let B_i with i ∈ {1,2,3} stand for “gold is in the i-th box”. We can formalize the statements of the problem as follows

Propositional Logic

1. *One box contains gold, the other two are empty.*

$$(B_1 \land \neg B_2 \land \neg B_3) \lor (\neg B_1 \land B_2 \land \neg B_3) \lor (\neg B_1 \land \neg B_2 \land B_3) \tag{2.1}$$

2. *Only one message is true; the other two are false.*

$$(\neg B_1 \land \neg\neg B_2 \land \neg B_2) \lor (\neg\neg B_1 \land \neg B_2 \land \neg B_2) \lor (\neg\neg B_1 \land \neg\neg B_2 \land B_2) \tag{2.2}$$

(2.2) is equivalent to:

$$(B_1 \land \neg B_2) \lor (B_1 \land B_2) \tag{2.3}$$

Let us compute the truth table for (2.1) and (2.3)

B_1	B_2	B_3	(2.1)	(2.3)
T	T	T	F	T
T	T	F	F	T
T	F	T	F	T
T	**F**	**F**	**T**	**T**
F	T	T	F	F
F	T	F	T	F
F	F	T	T	F
F	F	F	F	F

The only assignment I that verifies both (2.1) and (2.3) is the one with $I(B_1) = T$ and $I(B_2) = I(B_3) = F$, which implies that the gold is in the first box.