Math 4100 Quiz 5

Name:_____

1. Checksums. Verify the follwing check sums are correct or incorrect for the ISBN's.

(a)

Schaum's Outline of Computer Architecture by Nick Carter			
ISBN-10:	007136207X	ISBN-13:	978-0071362078

(b)

Java Web Services: Up and Running by Martin Kalin			
ISBN-10:	059652112X	ISBN-13:	978-0596521127

(c)

The Colossal Book of Short Puzzles and Problems by Martin Gardner			
ISBN-10:	0393061140	ISBN-13:	978-0393061147

(d)

The Code Book by Simon Singh			
ISBN-10:	0385495323	ISBN-13:	978-0385495325

(e)

The Devil Wears Pinstripes by Jim Caple			
ISBN-10:	0452285984	ISBN-13:	978-0452285989

(f)

Harmonic Analysis by Elias M. Stein			
ISBN-10:	0691032165	ISBN-13:	978-0691032160

(g)

Banach Spaces and their Applications in Analysis editors Beata Randrianantoanina and Narcisse Randrianantoanina			
ISBN-10:	311019449X	ISBN-13:	978-3110194494

1 ISBN

The International Standard Book Number, or ISBN , is an unique, numeric commercial book identifier. The 10-digit (ISBN-10) format was developed by the International Organization for Standardization and was published in 1970; and the 13 digit format (ISBN-13) was implemented on January 1, 2007. The new ISBN-13 supplants the old format with 978-ISBN-10 code. And as newer books given identifiers additional 3-digit prefixes will be chosen. We are only concerned with the last digit - the check digit (or checksum). This digit means nothing in identifying the book it only serves to verify that there was no error in transmission (or in transcribbing) the code.

Example: Notice the ISBN-13 is 978 followed by the first 9 digits of the ISBN-10 followed by the checksum.

Twilight (The Twilight Saga, Book 1)
by Stephenie Meyer
ISBN-10: 0316015849
ISBN-13: 978-0316015844

How do we compute the check digit (d_{10}). The book identification part of the number is $d_1d_2d_3d_4d_5d_6d_7d_8d_9 = 031601584$. We will show how to compute $d_{10} = 9$.

1.1 Computing ISBN-10 Check Digits

$$\begin{array}{rrrrrrrrrr} = 10d_1 & +9d_2 & +8d_3 & +7d_4 & +6d_5 & +5d_6 & +4d_7 & +3d_8 & +2d_9 & \\ = 10(0) & +9(3) & +8(1) & +7(6) & +6(0) & +5(1) & +4(5) & +3(8) & +2(4) & \text{Then} \\ = 0 & +27 & +8 & +42 & +0 & +5 & +20 & +24 & +8 & \\ = 134 & & & & & & & & & \end{array}$$

134 / 11 = 12 remainder 2

$d_{10} = 11 - 2 = 9$

Alternately we can compute

$$\begin{aligned} d_{10} &= 11 - (10d_1 + 9d_2 + 8d_3 + 7d_4 + 6d_5 + 5d_6 + 4d_7 + 3d_8 + 2d_9 \mod 11) \\ &= 11 - (134 \mod 11) \\ &= 11 - (2) = 9 \end{aligned}$$

So the ISBN-10 is 031601584 - check digit = 031601584 - 9 = 0316015849. One warning, if you compute $d_{10} = 10$ use the single digit $d_{10} = x$.

1.2 Computing ISBN-13 Check Digits

How do we compute the check digit (d_{13}). The book identification part of the number is $d_1d_2d_3 - d_4d_5d_6d_7d_8d_9d_{11}d_{12}d_{13} = 978 - 031601584$. We will show how to compute $d_{13} = 4$.

$$\begin{array}{rrrrrrrrrrrr} d_1 & +3d_2 & +d_3 & +3d_4 & +d_5 & +3d_6 & +d_7 & +3d_8 & +d_9 & +3d_{10} & +d_{11} & +3d_{12} \\ = 9 & +(3)7 & +8 & +(3)0 & +3 & +(3)1 & +6 & +(3)0 & +1 & +(3)5 & +8 & +(3)4 \\ = 9 & +21 & +8 & +0 & +3 & +3 & +6 & +0 & +1 & +15 & +8 & +12 \\ = 86 & & & & & & & & & & & \end{array}$$

Then 86 / 10 = 8 remainder 6

$d_{13} = 10 - 6 = 4$

Alternately we can compute

$$\begin{aligned} d_{13} &= 10 - (d_1 + 3d_2 + d_3 + 3d_4 + d_5 + 3d_6 + d_7 + 3d_8 + d_9 + 3d_{10} + d_{11} + 3d_{12} \mod 10) \\ &= 10 - (86 \mod 10) \\ &= 10 - (6) = 4 \end{aligned}$$

So the ISBN-13 is 978-031601584 - check digit = 978-031601584 - 4 = 978-0316015844. No danger of getting a 10 since we are working mod 10

2. Elliptical Curves. We will reference $EC_7(2,6)$.

   (a) Find all elements in the group $EC_7(2,6)$. Remember the identity $0 \in EC_7(2,6)$ and all other points have x-coordinates and y-coordinates. For example $(3,2) \in EC_7(2,6)$.

   (b) Find the order of the element $(3,2) \in EC_7(2,6)$.

   (c) Solve the follwing equation in $EC_7(2,6)$ for the point H

$$3 \cdot \mathrm{H} = (3,2).$$

3. Elliptical Curves. We will reference $EC_{23}(1, 1)$.

   (a) You already know the elements in $EC_{23}(1, 1)$ and we have discussed an alphabet. Use these and the public key of $G = (0, 22)$. And private keys $n_A = 3$ and $n_B = 11$. Compute the public key components P_A and P_B.

   (b) Encipher the plaintext word P = "TURTLE". That is you are person A and you are sending your message to person B. Your output should look like pairs of points like: $C_1 = \{(3, 13), (7, 12)\}$, $C_2 = \{(1, 16), (18, 3)\}$. But they are probably different points.

4. The following two problems have nothing to do with cryptography or isbn's.

   (a) Can you find six distinct odd numbers a_1, a_2, a_3, a_4, a_5 and a_6 so that

$$\frac{1}{a_1} + \frac{1}{a_2} + \frac{1}{a_3} + \frac{1}{a_4} + \frac{1}{a_5} + \frac{1}{a_6} = 1$$

   (b) Find and guess the pattern and prove your your guess.

$$\begin{aligned} 1 &= 0 + 1 \\ 2 + 3 + 4 &= 1 + 8 \\ 5 + 6 + 7 + 8 + 9 &= 8 + 27 \\ 10 + 11 + 12 + 13 + 14 + 15 + 16 &= 27 + 64 \end{aligned}$$