Math 223
Assignment 4: Applications of Modular Arithmetic to Codes and Cryptography

Quinn Neumiiller

October 15, 2013

Question 1. Check-digit codes. Check whether or not the following codewords are valid for the code given.

Question 1a. the UPC number 7-80133-19831-7

i	7	8	0	1	3	3	1	9	8	3	1	7
a	3	1	3	1	3	1	3	1	3	1	3	1
(i*a)	21	8	0	1	9	3	3	9	24	3	3	7

$$=21+8+0+1+9+3+3+9+24+3+3+7 \bmod 10$$
$$=91 \bmod 10$$
$$=1 \bmod 10$$

Not Valid.

Question 1b. the ISBN-10 number 0-87150-334-X.

i	0	8	7	1	5	0	3	3	4	10
a	10	9	8	7	6	5	4	3	2	1
(i*a)	0	72	56	7	30	0	12	9	8	10

$$=0+72+56+7+30+0+12+9+8+10 \bmod 11$$
$$=204 \bmod 11$$
$$=6 \bmod 11$$

Not Valid.

Question 1c. the ISBN-10 number 0-13-319831-0.

i	0	1	3	3	1	9	8	3	1	0
a	10	9	8	7	6	5	4	3	2	1
(i*a)	0	9	24	21	6	45	32	9	2	0

$$=0+9+24+21+6+45+32+9+2+0 \bmod 11$$
$$=148 \bmod 11$$
$$=5 \bmod 11$$

Not Valid.

Question 1d. the ISBN-13 number 978-1-4292-6009-1

i	9	7	8	1	4	2	9	2	6	0	0	9	1
a	1	3	1	3	1	3	1	3	1	3	1	3	1
(i*a)	9	21	8	3	4	6	9	6	6	0	0	27	1

$$=9+21+8+3+4+6+9+6+6+0+0+27+1 \bmod 10$$
$$=100 \bmod 10$$
$$=0 \bmod 10$$

Valid.

Question 1e. the Bank ID number 145-79429-1.

i	1	4	5	7	9	4	2	9	1
a	7	3	9	7	3	9	7	3	9
(i*a)	7	12	45	49	27	36	14	27	9

$$=7+12+45+49+27+36+14+27+9 \bmod 10$$
$$=226 \bmod 10$$
$$=6 \bmod 10$$

Not valid, $5 \neq 6$

Question 2. Error correction? You, the bookseller, have entered the following ISBN-13 number for the book you are trying to ring through the till: 978-0-321-75277-2 Although the codeword appears to be valid in the ISBN-13 system, it does not correspond to a book in your store's inventory. Assuming the ISBN is incorrect only because of a switch of 2 adjacent digits, what is its correct ISBN-13? (For fun: look up the actual title, author, and publisher of this book online.)

$$7-9=-2$$
$$8-7=1$$
$$0-8=-8$$
$$3-0=3$$
$$2-3=-1$$
$$1-2=-1$$
$$7-1=6$$
$$5-7=-2$$
$$2-5=-3$$
$$2-7=-5$$

Try switching 2 and 7.

i	9	7	8	0	3	2	1	7	5	7	2	7	2
a	1	3	1	3	1	3	1	3	1	3	1	3	1
(i*a)	9	21	8	0	3	6	1	21	5	21	2	21	2

$$=9+21+8+0+3+6+1+21+5+21+2+21+2 \bmod 10$$
$$=120 \bmod 10$$
$$=0 \bmod 10$$

ISBN-13: 978-0-321-75727-2
Title: Statistics : Informed Decisions Using Data with CD 4th
Author: Michael Sullivan III
Publisher: Addison Wesley

Question 3. Passport numbers. The identication code used for international passports is: [(6 or 9-digit passport number)-(check digit)]- (3 letter country code)-[(6-digit birth date)-(check digit)]- (an M or F)-[(6-digit expiry date)-(check digit)]>>>>>(overall check digit) Each check digit is calculated using the check vector pattern (7; 3; 1; 7; 3; 1; :::) mod 10. The overall check digit is calculated with all of the preceding digits in the passport ID, including check digits, excluding letters.

Question 3a. Verify the validity of the passport number 044455533-1-USA-460920-5-M-040913-1>>>>>>>>>>>>>8

For my purposeses, I'm going to drop all the letters, and seperate the sections. [[044455533-1]-[460920-5]-[040913-1]>>>>>>>>>>>>>8]

Checking passport number.

i	0	4	4	4	5	5	5	3	3	1
a	7	3	1	7	3	1	7	3	1	7
(i*a)	0	12	4	28	15	5	35	9	3	7

$$=0+12+4+28+15+5+35+9+3+7 \bmod 10$$
$$=118 \bmod 10$$
$$=8 \bmod 10$$

Passport number is invalid, hence the passport is invalid.

Question 3b. Determine check digits to complete the following (fake) Canadian passport number: 203241-?-CAN-840712-?-F-090215-?>>>>>>>>>>>?

Finding passport number.

i	2	0	3	2	4	1
a	7	3	1	7	3	1
(i*a)	14	0	3	14	12	1

$$=14+0+3+14+12+1 \bmod 10$$
$$=44 \bmod 10$$
$$=4 \bmod 10$$

$$=4+7(x) \bmod 10$$
$$11 =4+7(1) \bmod 10$$
$$18 =4+7(2) \bmod 10$$
$$25 =4+7(3) \bmod 10$$
$$32 =4+7(4) \bmod 10$$
$$39 =4+7(5) \bmod 10$$
$$46 =4+7(6) \bmod 10$$
$$53 =4+7(7) \bmod 10$$
$$60 =4+7(8) \bmod 10$$

Check digit for the passport number is 8.

Checking birth date

i	8	4	0	7	1	2
a	7	3	1	7	3	1
(i*a)	56	12	0	49	3	2

$$=56+12+0+49+3+2 \bmod 10$$
$$=122 \bmod 10$$
$$=2 \bmod 10$$

$$
\begin{aligned}
&=2+7(x) \bmod 10\\
9 &=2+7(1) \bmod 10\\
16 &=2+7(2) \bmod 10\\
23 &=2+7(3) \bmod 10\\
30 &=2+7(4) \bmod 10
\end{aligned}
$$

$$
\begin{aligned}
&=56+12+0+49+3+2+7(4) \bmod 10\\
&=56+12+0+49+3+2+28 \bmod 10\\
&=150 \bmod 10\\
&=0 \bmod 10
\end{aligned}
$$

Check digit for the birth date is 4.
Checking Expiry date 090215

i	0	9	0	2	1	5
a	7	3	1	7	3	1
(i*a)	0	27	0	14	3	5

$$
\begin{aligned}
&=0+27+0+14+3+5 \bmod 10\\
&=49 \bmod 10\\
&=9 \bmod 10
\end{aligned}
$$

$$
\begin{aligned}
&=9+7(x) \bmod 10\\
16 &=9+7(1) \bmod 10\\
23 &=9+7(2) \bmod 10\\
30 &=9+7(3) \bmod 10
\end{aligned}
$$

$$
\begin{aligned}
&=0+27+0+14+3+5+7(3) \bmod 10\\
&=0+27+0+14+3+5+21 \bmod 10\\
&=70 \bmod 10\\
&=0 \bmod 10
\end{aligned}
$$

Check digit for expiry date is 3.
Checking the full passport, aka: 203241884071240902153?

i	2	0	3	2	4	1	8	8	4	0	7	1	2	4	0	9	0	2	1	5	3
a	7	3	1	7	3	1	7	3	1	7	3	1	7	3	1	7	3	1	7	3	1
(i*a)	14	0	3	14	12	1	56	24	4	0	21	1	14	12	0	63	0	2	7	15	3

$=14+3+14+12+1+56+24+4+21+1+14+12+63+2+7+15+3 \bmod 10$

$=266 \bmod 10$

$=6 \bmod 10$

$$\begin{aligned} &=6+7(x) \bmod 10 \\ 3 &=6+7(1) \bmod 10 \\ 0 &=6+7(2) \bmod 10 \end{aligned}$$

Final checkdigit on the passport is 2.
Total valid passport is: 203241-8-CAN-840712-4-F-090215-3>>>>>>>>>>>2

Question 4. Hacking RSA cryptosystems.

Question 4a. Suppose an RSA cryptosystem has public key $(n, e) = (6282, 197)$. Find the associated private key $(\phi(n), d)$

$$\begin{aligned} \phi(n) &= \phi(3141) * \phi(2) \\ &= \phi(3141) * \phi(2) \\ &= \phi(349) * \phi(3^2) * \phi(2) \\ &= \phi(349) * \phi(3^2) * \phi(2) \\ &= 349^{1-1}(349-1) * 3^{2-1}(3-1) \\ &= 1(349-1) * 3(3-1) \\ &= 348 * 3(2) \\ &= 348 * 6 \\ &= 2088 \end{aligned}$$

private key = $(2088, d)$

$$(d)(e) = 1 \bmod 2088 = 197d = 1 \bmod 2088$$

$$\begin{aligned} 2088 &= 197(10) + 118 \\ 197 &= 118(1) + 79 \\ 118 &= 79(1) + 39 \\ 79 &= 39(2) + 1 \end{aligned}$$

$$
\begin{aligned}
1 &= 79 - 39(2) \\
1 &= 79 - (118 - 79)(2) \\
1 &= -118(2) + 79(3) \\
1 &= -118(2) + (197 - 118)(3) \\
1 &= 197(3) - 118(5) \\
1 &= 197(3) - (2088 - 197(10))(5) \\
1 &= 197(3) - 2088(5) + 197(50) \\
1 &= -2088(5) + 197(53) \\
1 + 2088(5) &= 197(53)
\end{aligned}
$$

private key = (2088, 53)

Question 4b. Let $(n,\ e) = (9991,\ 11)$ be the public key for an RSA cryptosystem that encrypts letters using the standard ASCII system. Decipher the transmitted message: 5752 7155

$$
\begin{aligned}
\phi(n) &= \phi(9991) \\
&= \phi(97)\phi(103) \\
&= 96 * 102 \\
&= 9792
\end{aligned}
$$

$$(d)(e) = 1 \bmod 9792 = 11d = 1 \bmod 9792$$

$$
\begin{aligned}
9792 &= 11(890) + 2 \\
11 &= 2(5) + 1
\end{aligned}
$$

$$
\begin{aligned}
1 &= 11 - 2(5) \\
1 &= 11 - (9792 - 11(890))(5) \\
1 &= 11 - 9792(5) + 11(5)(890) \\
1 &= -9792(5) + 11(4451) \\
1 + 9792(5) &= 11(4451)
\end{aligned}
$$

private key = (9792, 4451)

$$5752^{4451} \bmod 9991 = 2440$$
$$7155^{4451} \bmod 9991 = 4228$$

24 40 42 28
↑ (∗⌊

Question 5. Digital signatures. Bob's RSA cryptosystem uses public key (9379, 1837). Alice's uses public key (8453, 7).
$(n_A, e_A) = (8453, 7)$
$(n_B, e_B) = (9379, 1837)$

Question 5a. Verify that Bob's private key is (9184, 5) and Alice's private key is (8268, 7087).
Bob's private key

$$\begin{aligned}\phi(n) &= \phi(9379)\\ &= \phi(83)\phi(113)\\ &= 82 * 112\\ &= 9184\end{aligned}$$

$$(d)(e) = 1 \bmod 9184 = 1837d = 1 \bmod 9184$$

$$\begin{aligned}9184 &= 1837(4) + 1836\\ 1837 &= 1836 + 1\end{aligned}$$

$$\begin{aligned}1 &= 1837 - 1836\\ 1 &= 1837 - (9184 - 1837(4))\\ 1 &= 1837 - 9184 + 1837(4)\\ 1 &= 1837(5) - 9184\\ 1 \bmod 9184 &= 1837(5)\end{aligned}$$

private key (9184,5)
Alice's private key

$$\begin{aligned}\phi(n) &= \phi(8453)\\ &= \phi(107)\phi(79)\\ &= 106 * 78\\ &= 106 * 78\\ &= 8268\end{aligned}$$

$$\begin{aligned}(d)(e) = 1 \bmod 8268 & \\ &= 7d \bmod 8268\\ &= 7(7087) \bmod 8268\\ &= 49609 \bmod 8268\\ &= 49609 \bmod 8268\\ &= 1 \bmod 8268\end{aligned}$$

Question 5b. Alice wants to send the signed message *ALGEBRA* to Bob. She will encrypt in 2-letter (4-digit) blocks using standard ASCII. What message should she transmit? Provide the calculations Bob will use to verify the signed message he receives without knowledge of Alice's private key.

A	L	G	E	B	R	A
65	76	71	69	66	82	65

ALGEBRA split up into 4-digit blocks : 6576 7169 6682 0065
Encoding ALGEBRA

$$\begin{aligned}m^d \bmod n &= c_a\\ 6576^{7087} \bmod 8453 &= 6188\\ 7169^{7087} \bmod 8453 &= 1070\\ 6682^{7087} \bmod 8453 &= 4486\\ 0065^{7087} \bmod 8453 &= 1144\end{aligned}$$

$$\begin{aligned}c_a^{e_b} \bmod n_b &= c_{ab}\\ 6188^{1837} \bmod 9379 &= 9114\\ 1070^{1837} \bmod 9379 &= 57\\ 4486^{1837} \bmod 9379 &= 476\\ 1144^{1837} \bmod 9379 &= 1889\end{aligned}$$

Alice would send 9114 57 476 1889
Bob decrypting

$$c^{d_b} \bmod n_b = c_b$$
$$9114^5 \bmod 9379 = 6188$$
$$57^5 \bmod 9379 = 1070$$
$$476^5 \bmod 9379 = 4486$$
$$1889^5 \bmod 9379 = 1144$$

$$c^{e_a} \bmod n_a = m$$
$$6188^7 \bmod 8453 = 6576$$
$$1070^7 \bmod 8453 = 7169$$
$$4486^7 \bmod 8453 = 6682$$
$$1144^7 \bmod 8453 = 0065$$

6576 7169 6682 0065 = ALGEBRAy