Graduate Assignment B

Han ZHANG

u7235649

I have read the ANU Academic Skills statement regarding collusion. I have not engaged in collusion in relation to this assignment.

Han Zhang

06/05/2021 8pm

Question 1 (You may wish to write code to answer these questions)
If p is a prime, and g is an integer from the set $\{1, 2, \ldots, p-1\}$, we say that g is a **companion of** p when

$$\{g^a \bmod p \mid a \in \mathbb{Z} \text{ and } 1 \le a < p\} = \{1, 2, \ldots, p-1\}.$$

(A) Find all of the companions of 11. Justify your answer.

Companions: $\{2, 6, 7, 8\}$

Set for g: $G = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$ $1 \le a < 11$

Let set $S = \{g^a \bmod p \mid a \in \mathbb{Z}, 1 \le a < P\}$

$g=1$: $g^a = 1^a = 1$ $S = \{1\} \ne G$

$g=2$: $2^1 \bmod 11 = 2$. $2^2 \bmod 11 = 4$. $2^3 \bmod 11 = 8$. $2^4 \equiv 8\times2 \pmod{11} = 5$
$2^5 \equiv 5\times2 \pmod{11} = 10$ $2^6 \equiv 10\times2 \pmod{11} = 9$. $2^7 \equiv 9\times2 \pmod{11} = 7$
$2^8 \equiv 7\times2 \pmod{11} = 3$. $2^9 \equiv 3\times2 \pmod{11} = 6$. $2^{10} \equiv 6\times2 \pmod{11} = 1$
$S = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\} = G$.

$g=3$: $3^1 \equiv 3^6 \pmod{11} = 3$ $\therefore$ size of $S <$ size of G. $S \ne G$.

$g=4$: $4^1 \equiv 4^6 \pmod{11} = 4$. $\therefore$ size of $S <$ size of G. $S \ne G$

$g=5$: $5^1 \equiv 5^6 \pmod{11} = 5$ $\therefore$ size of $S <$ size of G. $S \ne G$

$g=6$: $6^1 \bmod 11 = 6$. $6^2 \bmod 11 = 3$. $6^3 \equiv 3\times6 \pmod{11} = 7$.
$6^4 \equiv 6\times7 \pmod{11} = 9$. $6^5 \equiv 9\times6 \pmod{11} = 10$. $6^6 \equiv 7\times7 \pmod{11} = 5$
$6^7 \equiv 5\times6 \pmod{11} = 8$ $6^8 \equiv 8\times6 \pmod{11} = 4$. $6^9 \equiv 4\times6 \pmod{11} = 2$.
$6^{10} \equiv 6\times2 \pmod{11} = 1$. $S = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\} = G$.

$g=7$: $7^1 \bmod 11 = 7$. $7^2 \bmod 11 = 5$, $7^3 \equiv 5\times7 \pmod{11} = 2$.
$7^4 \equiv 2\times7 \pmod{11} = 3$, $7^5 \equiv 3\times7 \pmod{11} = 10$, $7^6 \equiv 2\times2 \pmod{11} = 4$,
$7^7 \equiv 4\times7 \pmod{11} = 6$. $7^8 \equiv 6\times7 \pmod{11} = 9$. $7^9 \equiv 9\times7 \pmod{11} = 8$,
$7^{10} \equiv 8\times7 \pmod{11} = 1$. $S = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\} = G$

$g=8$: $8^1 \bmod 11 = 8$. $8^2 \bmod 11 = 9$, $8^3 \equiv 8\times9 \pmod{11} = 6$.
$8^4 \equiv 8\times6 \pmod{11} = 4$, $8^5 \equiv 4\times8 \pmod{11} = 10$, $8^6 \equiv 6\times6 \pmod{11} = 3$.
$8^7 \equiv 3\times8 \pmod{11} = 2$, $8^8 \equiv 2\times8 \pmod{11} = 5$, $8^9 \equiv 5\times8 \pmod{11} = 7$
$8^{10} \equiv 7\times8 \pmod{11} = 1$ $S = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\} = G$

$g=9$: $9^1 \equiv 9^6 \pmod{11} = 9$. size of $S <$ size of G. $S \ne G$.

$g=10$: $10^1 \equiv 10^3 \pmod{11} = 10$ $\therefore$ size of $S <$ size of G. $S \ne G$.

(B) Describe how you would go about proving or disproving the following statement: 104651 is prime and 24578 is a companion of 104651.

Step 1: prove 104651 is prime.

Start from 2, for a prime p. Calculate $r = 104651 \bmod p$.

If there is a p that $r=0$, then 104651 is not a prime.

Stop when $r \neq 0$ and $r < p$, then 104651 is a prime.

Step 2: prove 24578 is a companion of 104651.

For a in set $\{1, 2, \cdots, 104650\}$, calculate $24578^a \bmod 104651$

When $24578^a > 104651$, $24578^a \equiv 24578^{a-1} \times 24578 \pmod{104651}$

If $\exists a_1, a_2 \in \{1, 2, \cdots, 104650\}$ $a_1 \neq a_2$,

$24578^{a_1} \equiv 24578^{a_2} \pmod{104651}$, then 24578 is not a companion of 104651. Otherwise yes.

(C) Here is a four-step method to quickly compute g^s modulo p without ever computing or storing a number that exceeds p^2:

Let p = 104651, g = 24578 and s = 100418. Compute g^s mod p, showing all your working. In your working you should never compute or write down a number that exceeds p^2.

step 1:

t	24578^t mod 104651
1	24578
2	32512
4	50044
8	90835
16	103083
32	51651
64	62509
128	20694
256	9744
512	27079
1024	87335
2048	18741
4096	16325
8192	64179
16384	89983
32768	92419
65536	75545

Step 2: $S = 100418 = 2^{16} + 2^{15} + 2^{11} + 2^{6} + 2^{1} = 65536 + 32768 + 2048 + 64 + 2$

Step 3: $24578^{100418} \bmod 104651$

$= 75545 \times 92419 \times 18741 \times 62509 \times 32512$

Step 4: $75545 \bmod 104651 = 75545$

$75545 \times 92419 \bmod 104651 = 1890$

$1890 \times 18741 \bmod 104651 = 48452$

$48452 \times 62509 \bmod 104651 = 86128$

$86128 \times 32512 \bmod 104651 = 46729$.

$\therefore$ The result is 46729.

(D) Let s be an integer such that $1 \leq s < 104651$ and

$$24578^s \bmod 104651 = 3190$$

Find s and explain how you found it.

$S = 36068$.

Let $g = 24578$, $p = 104651$, $t = 3190$.

Let S start from 1, calculate $r = g^S \bmod p$. If $r = p$, then S is the result. Otherwise, let pre $= r$, $S = S + 1$. calculate $r = \text{pre} \times g \bmod p$.

Repeat until $r = p$, then S is the result.

Question 2 A new 16-bit standard for storing floating point numbers, called **bfloat16**, has become popular in the last couple of years for use in machine learning programs. It is a truncated form of single precision floating point (which uses 32 bits) but is different to half precision floating point (which also uses 16 bits). Please read the Wikipedia article `https://en.wikipedia.org/wiki/Bfloat16_floating-point_format` before attempting the questions below. The article is self contained, so it is not necessary to first know the details of single precision floating point.

For the questions below, show how you obtain your answer - do not use an on-line converter!

(A) What is the value (expressed in decimal notation) of the number stored in bfloat16 format as $\texttt{BADE}_{16}$?

$BADE_{16} = 1011\ 1010\ 1101\ 1110_2$

$S=1.$ exponent $= 011\ 10101_2 = 117_{10}$ $\quad 117-127=-10$

fraction $= 1011110_2$

$-1.1011110_2 \times 2^{-10} = -1.734375_{10} \times 2^{-10} \approx -0.001694$

(B) What is the (very small) value of the number stored in bfloat16 format as $\texttt{8008}_{16}$? Express your answer in decimal scientific form with two decimal places. Careful!

$8008_{16} = 1000\ 0000\ 0000\ 1000_2$

$S=1.$ exponent $=0$ $\quad 0-127=-127$

fraction $= 0001000_2$

Value: $-1.0001_2 \times 2^{-127} = 1.0625_{10} \times 2^{-127} \approx 6.24 \times 10^{-39}$

(C) In bfloat16 format, the word $\texttt{7FC0}_{16}$ does not store a number. Why not?

$7FC0_{16} = 0111\ 1111\ 1100\ 0000_2$

exponent $= 11111111_2$. By defination, it represents NaN, not a number.

(D) When one million is stored (approximately) in bfloat16 format, what is the exact (decimal) value of the number stored?

One million $= 1000000_{10} \approx 1.1110100_2 \times 2^{-15}$

$S=0$. exponent $= -15+127 = 112_{10} = 01110000_2$

fraction $= 1110100_2$

Value : $0011100001110100_2 = 14452_{10}$

(E) The bfloat16 format is not recommended for storing integer values. What is the least $n \in \mathbb{N}$ which cannot be stored exactly in bfloat16 format?

$S=0$. exponent $= 11111110_2 = 254_{10}$ $254-127=127$.

fraction $= 1111111_2$

$\therefore$ Value $= 1.1111111_2 \times 2^{127} = 1.9921875 \times 2^{127}$

$= 3.38953138925153 55 \times 10^{38}$

Question 3 A popular method of sorting a sequence is called *Insertion Sort* (or *InsertionSort*). You can read about it in our recommended textbook[1] by Epp in §11.3 (4&5ed), §9.3 (3ed) and on many websites including Wikipedia `https://en.wikipedia.org/wiki/Insertion_sort` and Khan Academy `https://www.khanacademy.org/computing/computer-science/algorithms/insertion-sort/a/insertion-sort`. (That one has a nice slow animation.)

(A) Apply the algorithm to sort the sequence F,D,C,E,B,C into alphabetical order. Show the state of the sequence each time the '$i \le n$' test in line 2 of the method is performed.

n=6. a = FDCEBC
i=2: DFCEBC
i=3: CDFEBC
i=4: CDEFBC
i=5: BCDEFC
i=6: BCCDEF

(B) How many item comparisons '$x < a_j$' are performed for the application (A)?

1+2+2+4+5=14

(C) In no more that 50 words compare the efficiencies of *Selection Sort* and *Insertion Sort*, mentioning any situations where one is superior to the other. Be sure to reference any sources you use for your answer. (References are not included in the word count.)

Selection Sort is superior when most of the elements in the sequence are reversive. The more ordered the sequence, the more superior the insertion sort is.

(D) Rewrite the algorithm using indirect addressing, so that no sequence items are actually moved. The INPUT should be unchanged, but the OUTPUT should now read: OUTPUT: A permutation $\pi : \{1, .., n\} \to \{1, .., n\}$ for which the sequence $(a_{\pi(i)})_{1..n}$ is

in non-decreasing order with respect to $<$.

METHOD:

```
res ← {1, ..., n}
ind ← {1, ..., n}  (the position of the nth element in the new sequence)
i ← 2
while i ≤ n
    x ← a[i]
    j ← i-1
    y ← j  (y holds the origional value of j)
    while j > 0:
        if x < a[res[j]] (get the element in the new sequence by res[j])
        then
            res[j+1] = res[j]  (yes, set a_{j+1} to a_j)
            ind[res[j]] ← ind[res[j]]+1 (update the position of a_j)
            j ← j-1
        else
            res[j+1] = i   (no, insert x here)
            ind[res[j+1]] = y
            j ← -1
        end if
    end while
    if j=0
    then
        ind[i] = 1
        res[1] = i
    end if.
    i ← i+1
end while
return res
```