The first class note of 2016 SCNU Turing Class

October 16, 2016

1 Something about Think_c

- What should CSers focus on?

  data ,type of data,variable(fix-size,fix-size computing),operation:arithmetic,logic.

- We think in the way of recursion,so does program.

  program's execution include these ways:execute in sequence,chose a certain branches to execute(realize with if sentence),execute circularly(do while ,for sentence).So,does recursion equal to "if" and "for while"?

- Function should be separated used,the comment should include what it input and output.

- Think from the angle of data:input date and output it.

2 Power and multiple

- Position notation

  $Number == a_n B^n + a_{n-1} B^{n-1} + a_{n-2} B^{n-2} + a_{n-3} B^{n-3} + \cdots + a_1 B^1$

  a is co-efficent and B is base(when Number is a binary ,then B is 2,when Number is decimal the B is 10);

- the power $A^B == A^{b_n*2^{n-1}++b_{n-1}*2^{n-2}+b_{n-2}*2^{n-3}+\cdots+b_1*2^0} == A^{2B'+b_1}$

  $B' == b_n*2^{n-2}+b_{n-1}*2^{n-3}+b_{n-2}*2^{n-4}+\cdots+b_2*2^0$

  so the recursion of power are displayed

  a recursion to realize multiply is following:

```
function multiply(a,b)
if b==0:
        return 0;
if b==1:
        return a;
if isEven(b): # b is even;
        return 2*multiply(a,b/2);
else:  # b is odd;
        return 2*multiply(a,b/2)+a;
```

- task 1:use iteration to get $a*b$ and get a^b.$(a, b \in N^+)$

- task 2:unsigned char $a = 2, b = 129$,what's the result of $a * b$?

- variable of type byte has 8 bits,word has 32 bits or 64 bits or 128 bits which decide by CPU itself;

3 Group,ring,domain

group

- definition:

  - manifold G isn't empty ,and has operand multiple or addition.

  - each operation need to mod n $n == (large\ number\ of\ this\ manifold+1)$.

  - results of operations to elements in the manifold

are included in the manifold,which is called closure.

- $a, e, b \in G, if\ a+e == a, then\ e\ is\ called\ IdentityElement; and\ if\ a+b == e, then\ b\ is\ called\ a's\ inverse\ element, of\ course, a\ is\ b's\ inverse$

- multiply or addition (of course,each operation need to mod n)satisfy associative law.

- Z_Z^+ is a group
- Z_Q^* is a group
- Z_N^+ is not a group

- how to structure a multiplicative group? if n is a primer number,then Z_n^* is a multiplicative group;and if the element of the group is create by generating element (mod n),then this is a Z_n^* too.

- understanding of complement

n bits' complement is a additive group G which bases on mod 2^n,and any element of it has its inverse element $a^{'}$,which make $a + a^{'} == 0\ (mod\ 2^n)$.so,for every $a \in G$,its inverse element $a^{'}$ is $2^n - a$.this is binary complement that we usually defined to express signed integers.all in all,complement is a simple application of group's inverse element.

- however,if we directly multiply some negative number(such as 100000001) by 2,we will get error.so while addition and subtraction is natural,but multiple and division are not natural,because we take out the sign first,next do multiple between two positive integers,later add the sign.

ring

- definition:

- if delete 0 from a additive group,and the rest can't form a multiplicative group because the lack of inverse element.this group and "not group" form a ring.

domain

- definition:
  - if delete 0 from a additive group,and the rest can form a multiplicative group.this two group form a domain.
- for more knowledge of ring,group and domain,please refer to *aata*

4 Matrix and group

- determinant's group,unit element is unit matrix,inverse element is inverse computing(there is stil somethings unclear,we can complete it later)