Computacional Exercício da Teoria Dos Grupos: Ordem de um Elemento do Grupo

2/7/17 Robleh Wais

Resumo

Estudantes universitário em matemática que estuda teoria grupo, vai encontrar objetos chamada grupos. Grupos tem quatro definindo axiomas. Eles são o seguinte:

- *Um grupo é um conjunto que é fechado com uma operação binária (como + ou *)*
- *O conjunto G tem o elemento de identidade e, que elemento e*a=e.*
- *Os membros de conjunto G são associativos, de tal modo que nenhum três membros, a, b, e c, esta igualdade é verdade (a*b)*c = a*(b*c).*
- *Por cada (a) em G há existe um elemento a^{-1} de tal modo que a* a^{-1}= e. Este elemento é chamado um inverso*

Na teoria de número, uma subdivisão de matemática dentro Teoria do Grupo. Há Grupos inteiros com mais a intrigante das propriedades chamada ordem do elemento. Esta propriedade é um inteiro que representa a adição de sucessiva exponenciações do número inteiro membro do grupo, até o processo terminar na identidade do elemento do grupo. É feito no módulo de um grupo. Abaixo, eu dou vários exemplos desta computação e mostro alguns detalhes de como calcular ordem de um elemento do grupo, corretamente.

O primeiro passo é enumerar os elementos dum grupo dependendo no módulo que escolheu. A enumeração é feita com uma lista dos elementos do grupo em ordem ascendente, que são números relativamente primos e **menores do que** o número-alvo. Números relativamente primo significa que o elemento não tem mais do que um ou a si mesmo como divisor.

Exemplo U(10) = (1,3,7.9)

Nota: se você não certeza dos elementos de um módulo de um grupo, você pode procurá-los usando uma operação de método por cada elemento menos do que N, o grupo cardinalidade (tamanho do grupo).

Se o número não eventualmente chega à 1, o elemento identidade, o número não é parte do grupo Por exemplo, os números 2, 4,6,8 não são parte do grupo U(10). Os números 2 e 5 são não parte do grupo por que eles não satisfazem a condição que um número deve menor do que o grupo cardinalidade e relatividade primo para tamanho do grupo. Como 2 pode ser dividido 10 sem nenhum restante, não é não relativamente primo a 10.

Para procurar a ordem destes elementos calcule sucessiva exponenciações do elemento até que a identidade do elemento é alcançada, por ex: 1. O cálculo usa o módulo de um grupo. No caso acima, o Mod é 10. Adicione as exponenciações e a soma é a ordem do elemento no módulo do grupo.

O que é a ordem dos elementos no U(10) acima? Vamos calcular cada elemento, exceto 1, qual é um caso trivial. A ordem de 3 em mod 10 é $3^1= 3$, $3^2 = 1$. Então, a ordem de 3 é 2. A soma de cada exponenciação.

Próximo, a ordem de 7 em mod 10 é $7^1=7$, $7^2=9$, $7^3=3$, $7^4=1$. A ordem de 7 é 4.

Próximo, a ordem de 9 em mod 10 é $9^1=9$, $9^2=1$. A ordem de 9 é 2

Nós podemos praticar este cálculo em grupos outros. Vamos escolher outro grupo aleatoriamente. Ache os elementos dele e então calcule a ordem de cada elemento neste grupo.

Bem, vamos começar com um grupo fácil.

U(6)= (1, 5). 2, e 3 estão fora por que eles podem dividir 6, e 4 está fora por que não é relatividade primo com 6 já que 2 dividido por 6 e 4. Outra vez, 1 e trivial. A ordem de 5 in mod 6 é $5^1=1$, ordem é 1 desde 6-5 = 1

Agora, por um grupo mais expansivo, nós tentar U(21). Nós podemos procura qual elementos são no grupo pelo simplesmente analisando esses nós não são certeza no grupo, depois disso eliminando os obvio números.

Qualquer coisa pode ser divido por 21 sem nenhum restante, não são no grupo. então, 3 e 7 são fora. Claramente, 1 é trivial. Nós podemos começar com o seguinte e elimina qualquer coisa que sucessiva exponenciações não resulta com elemento identidade. O módulo é 21. U(21)=(2,4,5,8,10… não todos mostrado aqui). O cálculo da ordem de 2 mod 21 é $2^1=2$, $2^2=4$, $2^3=8$, $2^4=16$, $2^5=11$, $2^6=1$ A ordem de 2 mod 21 é 6.

É 4 no grupo? Vamos descobrir. $4^1=4$, $4^2=16$, $4^3=1$. é isso, e a ordem mod 21 é 3.

Nota: uma computacional ferramenta é computar a poder além módulo, dividir pelo o módulo, derruba o restante e múltipla o resultado pelo módulo. Depois, subtrair esse resultado de o original módulo, se você chegar 1, então você pare. Aqui é um exemplo:

*4^3= 64/21=3.0476. derruba o restante você tem 3. 3*21= 63. 64-63= 1*

Vamos tentar 5:

$5^1=5$, $5^2=3$, $5^3=20$, $5^4=16$, $5^5=17$, $5^6=1$ (usando o método mostrado acima $5^6=15625/21=744.0476 \approx 744*21=15624$; 15625-15624=1).

A ordem de 5 mod 21 é 6.

Vamos tentar 6:

Esta computação nunca resultado em o elemento identidade e 6 não é no grupo. É verdade por que 6 e 21 tem mais do que 1 como divisores primos, eles ambos têm 3 e ele é verdade por 9,12,14,15 e 18. Desses números tem outras divisores com 21. Por exemplo 14 tem 7 como um divisor. Mesma é verdade dos números 9,12,14,15 e18. Desses números nunca redução á

elemento identidade. Mas, pois, você não me acredite e eu me não acredito, vamos calcular todos.

$8^1=8$, $8^2=1$. A ordem de 8 mod 21é 2.

$10^1=10$, $10^2=16$, $10^3=13$, $10^4=4$, $10^5=19$, $10^6= 1$. A ordem de 10 mod 21 é 6.

Ótimo, bem por agora.....

$11^1=11$, $11^2=16$, $11^3=8$, $11^4=4$, $11^5=2$, $11^6=1$. A ordem de 11mod 21 é 6.

$13^1=13$ $13^2=1$. A ordem de 13 mod 21 é 3.

$16^1=16$, $16^2=4$, $16^3=1$. A ordem de 16 mod 21 é 3.

$17^1=17$, $17^2=16$, $17^3=20$, $17^4=4$, $17^5=5$, $17^6=1$. A ordem de 17 mod 21 é 6.

$19^1=19$, $19^2=4$, $19^3=3$, $19^4=16$, $19^5=10$, $19^6=1$. A ordem de 19 mod 21 é 6.

$20^1=20$, $20^2=1$. A ordem de 20 mod 21 é 2.

Bem, esse é suficiente, é uma grande coleção de ordinais elementos. Há não mais elementos de ordem desse grupo, e obviamente este é um grupo finito. Nós podemos construír um subconjunto coleção de ordinais elementos de U(21). Aqui eles são:

$U(21)_{ordinais}$ = (2,3,6). Este subconjunto é composto de 3 membros. Pois desses números ocorreu repetidamente em cálculo do ordinal, só primeiras ocorrências tem sido mantiveram.

Finalmente, há muito mais eu posso diz sobre este resultado. O que é implica? E se nós não removemos os ordinais que ocorreu repetidamente? São nenhumas implicações cíclicos nesses cálculos? Mas, eu vou deixar dessas questões por outra uma redação.