TOPIC 2: FAST LARGE INTEGER MULTIPLICATION

1. how do we multiply two numbers?

O(n^2) intermediate operations:

O(n^2) elementary multiplications + O(n^2) elementary additions

1. The Karatsuba trick – break into two pieces

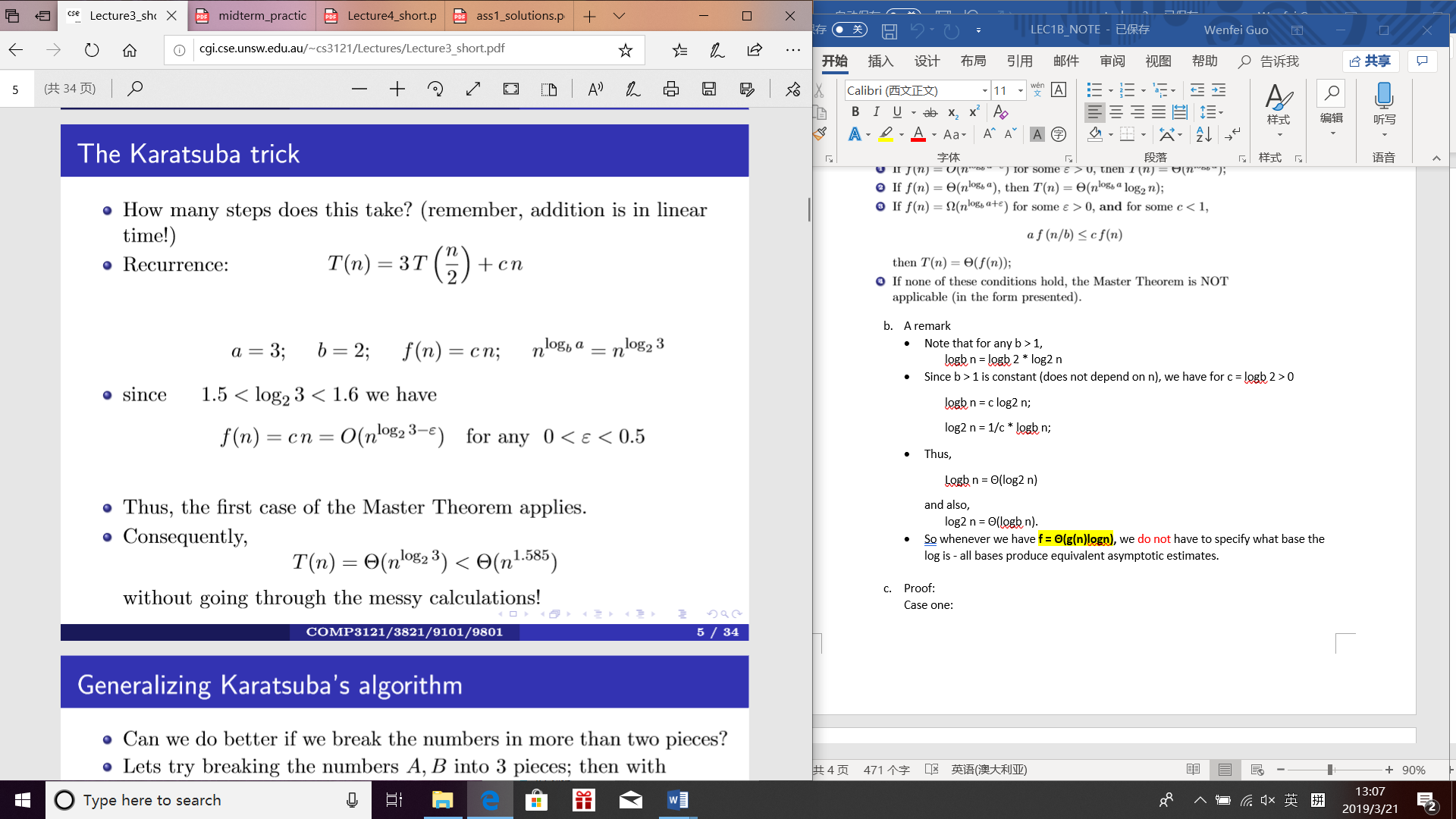
A = A1\*2^(n/2) + A0

B = B1\*2^(n/2) + B0

AB = A1B12^n + (A1B0 + A0B1)2^(n/2) + A0B0

= A1B12^n + ((A1 + A0)(B1 + B0)−A1B1 −A0B0)2^(n/2) + A0B0

= W 2^n + (Y −W −X)2n/2 + X



1. The Karatsuba trick – break into three pieces

A = A2\*2^(2k) + A1\*2^k + A0

B = B2\*2^(2k) + B1\*2^k + B0

PA(x) = A2\*x^2 + A1\*x + A0

PB(x) = B2\*x^2 + B1\*x + B0

A =A2\*(2^k)^2 + A1\*2^k + A0 = PA(2^k)

B =B2\*(2^k)^2 + B1\*2^k + B0 = PB(2^k)

C4 =A2B2

C3 =A2B1 + A1B2

C2 =A2B0 + A1B1 + A0B2

C1 =A1B0 + A0B1

C0 =A0B0

AB = A2\*B2\*2^(4k) + (A2B1 + A1B2)2^(3k) + (A2B0 + A1B1 + A0B2)2^(2k) + (A1B0 + A0B1)2^k + A0B0

PC(x) = PA(x)PB(x) = C4\*x^4 + C3\*x^3 + C2\*x^2 + C1\*x + C0

PA(x) =

PB(x) =

PC(x) = PA(x) \* PB(x)

= ( \* (

= + \* +

+ + + \*

+ \*

+

= + +

+ + +

+

+

= + (+) + (+ + )

+ ( + ( +

= + (+ + ( +

+ ( + ( +

PA(x) =

PB(x) =

PC(x) = PA(x) \* PB(x)

= ( \* (

If we manage to compute somehow the product polynomial

PC(x) = PA(x) \* PB(x)

with only 6 multiplications, we can then obtain the product of numbers A and B simply as

PC(x) = PA(x) \* PB(x)

= + + + + +

Since the product polynomial PC(x) = PA(x)PB(x) is of 5 different degree, we need 6 values to uniquely determine PC(x).

We choose the smallest possible 5 integer values (smallest by their absolute value), i.e., -4, −2, −1, 0, 1, 2, 4

Thus, we compute

PA(−4),PA(−2),PA(−1),PA(0),PA(1),PA(2),PA(4),

PB(−4),PB(−2),PB(−1),PB(0),PB(1),PB(2) ,PB(4)

For PA(x) = we have

PA(−4) = = 4096 - 64+

PA(−2) = = 64 - 8+

PA(−1) = = - +

PA(0) = =

PA(1) = = - +

PA(2) = = 64 + 8+

PA(4) = = 4096 + 64+

Similarly, for PB(x) = we have

PB(−4) = = 262144

PB(−2) = = -512

PB(−1) = = -

PB(0) = =

PB(1) = =

PB(2) = = 512

PB(4) = =

Having obtained PA(−4),PA(−2),PA(−1),PA(0),PA(1),PA(2),PA(4) and

PB(−4),PB(−2),PB(−1),PB(0),PB(1),PB(2) ,PB(4)

we can now obtain PC(−4),PC(−2),PC(−1),PC(0),PC(1),PC(2), PC(4)

with only 6 multiplications of large numbers:

PC(−4) = PA(−4)PB(−4) = (4096 - 64+ ) \* (

PC(−2) = PA(−2)PB(−2) = (64 - 8+ ) \* (-512)

PC(−1) = PA(−1)PB(−1) = ( - + ) \* (-)

PC(0) = PA(0)PB(0) =

PC(1) = PA(1)PB(1) = ( ++ ) \* ()

PC(2) = PA(2)PB(2) = (64 + 8+ ) \* (512)

PC(4) = PA(4)PB(4) = (4096 + 64+ ) \* (

Thus, if we represent the product C(x) = PA(x)PB(x) in the coeﬃcient form as

C(x) = + + + + + we get

PC(−4) = PA(−4)PB(−4) = + - + - +

PC(−2) = PA(−2)PB(−2) = + - + - +

PC(−1) = PA(−1)PB(−1) = + - + - +

PC(0) = PA(0)PB(0) =

PC(1) = PA(1)PB(1) = + + + + +

PC(2) = PA(2)PB(2) = + ++ + +

PC(3) = PA(3)P(3) = + + + + +

= PC(0)

Note that these expressions do not involve any multiplications of TWO large numbers and thus can be done in linear time.

With the coeﬃcients C0,C1,C2,C3,C4 obtained, we can now form the polynomial C(x) = + + + + +

We can now compute PC(x) = + + + + + in linear time, because computing PC(x) involves only binary shifts of the coeﬃcients plus O(k) additions.

Thus we have obtained A·B = PA(x)PB(x) = PC(x) with only 6 multiplications!