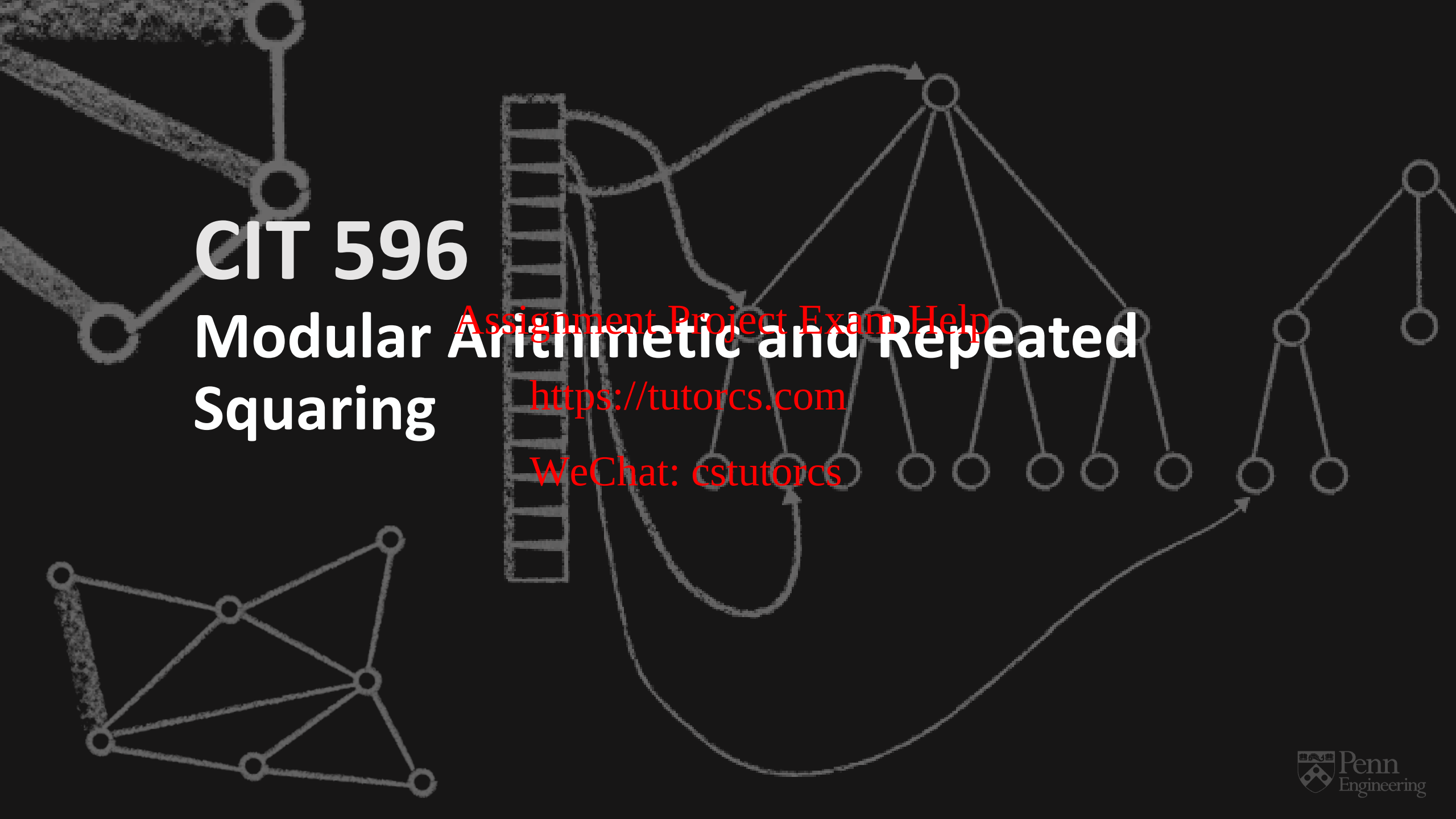

CIT 596

Modular Arithmetic and Repeated Squaring

Assignment Project Exam Help
https://tutorcs.com
WeChat: cstutorcs

Penn Engineering

MODULAR ARITHMETIC

- If it is 8 o'clock now, what time will it be in 7 hours?
- If you said "15 hours," you probably live in Europe! In the US, people would say "3 o'clock."
- We arrived at the answer by doing modular arithmetic using 12 as the modulus
- Modular arithmetic: subtract multiple of modulus from result, leaving only remainder
- Examples: 12+19 mod 23 = 8
  3+6 mod 19 = 9
  5x7 mod 11 = 2

Assignment Project Exam Help
https://tutorcs.com
WeChat: cstutorcs

FURTHER PROPERTIES

- We can keep intermediate results small by taking mod at any point

  Example: 11 x 5 x 9 x 8 mod 13

  11 x 5 = 55 = 3 mod 13

  (11 x 5) x 9 = 3 x 9 = 27 = 1 mod 13

  ((11 x 5) x 9) x 8 = 1 x 8 = 8 mod 13

Assignment Project Exam Help
https://tutorcs.com
WeChat: cstutorcs

- We could have computed the entire product first as 3,960 and taken its remainder when divided by 13
  - Which gives the same answer of 8

- But it is more efficient to keep numbers small and reduce them by the modulus

MODULAR EXPONENTIATION

- Given $a, b,$ and m we want to compute a^b mod m
- Suppose $a, b,$ and m are n bit numbers: how do we do this?
- We could multiply a by itself b times, always reducing by m but this takes b steps
  - As for factoring, if b has 500 bits, it would take at least 2^{499} steps. Not good!
- Instead we use an idea that is similar to divide and conquer.

Assignment Project Exam Help
https://tutorcs.com
WeChat: cstutorcs

REPEATED SQUARING

- We can compute $a, a^2, a^{2^2}, \ldots, a^{2^n}$ by squaring and reducing mod m repeatedly n times
- Now $b = b_{n-1}b_{n-2}\cdots b_0$ is the binary representation of b

Assignment Project Exam Help

$$a^b = a^{b_{n-1}b_{n-2}\cdots b_0} = \prod_{0}^{n-1} a^{b_i 2^i}$$

https://tutorcs.com

- Example: compute 7^5 mod 11: Note that $5 = 101$ in binary.

WeChat: cstutorcs

$7 \bmod 11 = 7,\ 7^2 \bmod 11 = 5,\quad 7^4 \bmod 11 = 5^2 \bmod 11 = 3$

$$7^5 (\bmod 11) = 7^4 \times 7 (\bmod 11) = 3 \times 7 (\bmod 11) = 10 (\bmod 11)$$