Number Theory\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Modular Arithmetic\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Euler’s Totient Function

    For any **integer n**, the number of **coprime** positive integers to **n** that are **less than n**

https://lh4.googleusercontent.com/eS77y_Nq0MMBJslPBpk-im6VCOpSW_WpvJ_CX89C0mPLcsqCFW8SmLjwfb2k812F5Hycw6WZqoRU4b7Za-7m5VJUBDYreiA_hCU7YSNM95cdk7ModhBOqsPSDQBsSNB2DsLqgJBQ

    Where p\_1, p\_2 … are the prime factors of **n**.

    The totient function is usually denoted by phi, https://lh4.googleusercontent.com/3mYg79L-VnhyhNQGcxEvlI2A6NZsvQboAwTP_uZr_sxPfLWqzGCeTiMBYmLvFQHDrqv7BQ8wHFDxVa8ADjHWn25Avabi3KDsS_jANQDwG1acEzLLjLkyy6vk0ZcigzMjGW3yaF5j.

Euler’s Totient Theorem

    Any positive integer **a** **coprime to n** satisfies this theorem.

https://lh6.googleusercontent.com/i19F46YEuhS8ECirejwJav_KB5y5w1cmnfwuk4n-kq4LSz7CYmDaNcAGKxmmhS0wUt9fjDvpbBV_hdLRcnf6CqdedDJfbCxFUYx7yWtXNbLFuKnYF4j81X8ES-BwhivhD3BRcbvM

Chinese Remainder Theorem

    Given an integer **n** which satisfies multiple modulo congruencies

https://lh6.googleusercontent.com/K2F7xkwjWfKe2mwLUd0BToxKaZCFy9AzMrAwF_yntHd32-1PHDAjlZEwncVZMImMeUMTKzMnKfb_NAEyk-uFB8tNbbPTVS52Uf1_vZNXOfSZDShImZRWgZBPE0Lmu606OrRxpW27

**n** can be determined through the following formula

https://lh4.googleusercontent.com/UtCygSGkr7riwtMlVWz-032sdyviDyJTIGAVO0XvhYY5Dx_KAZnmkDm3O6HQbiHe-4rkxT6QIkzMethfNCYlSbOrfpFIQN-jpc-9gHs1wEZD4mgekBhwAEz3UdFDnr387_MA6T58

    Where **b** is defined as

https://lh3.googleusercontent.com/esAZG-g82tUKeUsWQQQC5L48qiYsIPSU8BFEx2jzgB5O7KKjIIuPsNkYvdnT8nttXST3WX-4VIOLF_H0f6GMeuHbXhF3A3pMVcXlj3h_ViWtbbEZW-GH0b_4hQ_jHxx4CcXJqXbX

    And **M** is

https://lh5.googleusercontent.com/IJaGG2QRnzyVk_7fNZvoRRPFSWxhrhMb2iPlNzy92r6Jjo4staQCnP1uwXDio1z3oePTIoEyRwjOFeuH61t8Tguo1ao3EiGoRm1XWnqwQg0Rs6n7NTCeL68wr0pr1OunFJMF7ou-

**An example problem using Chinese Reminder therom and Euler’s totient:**

Find redminder of 2345 when divided by 400.

M = 400 = m1  m2  = 16 x 25

a1 = 2345 Mod(16) = 0

a2 = 2345 Mod(25), to find this we can use euler’s totient.

Φ (25) = 25 ( 1 – 1/5) = 20, so 220 = 1 Mod(25), thus 2345 Mod(25) = 25 Mod(25) = 7

b1: 25b1 = 1 Mod(16), so b1 = 9 (in fact we don’t need to find this because a1 is 0)

b2: 16b2 = 1Mod(25), b2 = 7

result = (a2 x b2 x 16) Mod(400) = (7 x 7 x 16) Mod(400) = -16 mod(400) = 384