Study guide

- (§11) Understand the proof of the Chinese Remainder Theorem.
- (§11) Understand the proof of the "computation of $\phi(m)$ theorem."
- (§12) Understand Euclid's proof that there are infinitely many primes, and the variation showing that there are infinitely many primes p such that $p \equiv 3 \pmod 4$.
- (§13) Know the informal version of the prime number theorem (but you don't need to know a proof!).

Note A function f with domain $\mathbb{N}$ is called a *multplicative function* if it has the following feature: for any two *coprime* integers m, n, $f(mn) = f(m)f(n)$. We've seen one very important example: the Euler ϕ function. The first couple problems below explore some other examples.

1. Let $d(n)$ denote the number of positive divisors of n. We will prove that d is a multiplicative function (see the note above), mimicking the argument that ϕ is a multiplicative function.

   (a) Prove that if $m, n \in \mathbb{N}$ are coprime, then there is a bijection between the following two sets.

   $$S = \{d \in \mathbb{N} : \ d \mid mn\}$$
   $$T = \{(d_1, d_2) \in \mathbb{N}^2 : \ d_1 \mid m, \ d_2 \mid n\}.$$

   (There are a few ways to approach this; the most intuitive may be using prime factorization.)

   (b) Deduce that d is a multiplicative function (this can just be a one-sentence proof).

   (c) Let p be prime and $e \in \mathbb{N}$. Find a formula for $d(p^e)$.

   (d) Find (and prove) a formula for $d(n)$ in terms of the prime factorization $n = p_1^{e_1} \cdots p_k^{e_k}$ of n.

2. Let $\sigma(n)$ denote the sum of the positive divisors of n (including 1 and itself). For example, $\sigma(6) = 1 + 2 + 3 + 6 = 12$ and $\sigma(21) = 1 + 3 + 7 + 21 = 32$.

   (a) Prove that σ is a multiplicative function. (It may be useful to refer to your argument in part (a) of the previous problem.)

   (b) Find a formula for $\sigma(p^e)$ when p is prime and $e \in \mathbb{N}$.

   (c) Using your formula (and multiplicativity), evaluate $\sigma(10)$, $\sigma(20)$, $\sigma(1728)$, and $\sigma(4100)$.

3. (Textbook 12.2)
   (Modifying Euclid's proof to consider primes $\pmod 6$)

   (a) Show that there are infinitely many primes that are congruent to 5 modulo 6 . [Hint. Use $A = 6p_1p_2 \cdots p_r + 5$.]

   (b) Try to use the same idea (with $A = 5p_1p_2 \cdots p_r + 4$) to show that there are infinitely many primes congruent to 4 modulo 5 . What goes wrong? In particular, what happens if you start with $\{19\}$ and try to make a longer list?

4. This problem considers a possible modification of Euclid's proof to consider primes of given residue modulo 5. If you trying to problem before Friday 3/14, you should read the book's argument about primes $\equiv 3 \pmod 4$ first.

   (a) Prove that if $a, b \in \mathbb{Z}$ are both congruent to either 1 or -1 mod 5, then also ab is congruent to either 1 or -1 mod 5.

   (b) Deduce if $n \in \mathbb{N}$ satisfies $n \equiv 2 \pmod 5$, then at least one of the prime factors p of n satisfies either $p \equiv 2 \pmod 5$ or $p \equiv 3 \pmod 5$.

   (c) Prove that there are infinitely many primes p such that *either* $p \equiv 2 \pmod 5$ or $p \equiv 3 \pmod 5$.

   (d) Briefly explain why this argument does not easily adapt to show that there are infinitely primes p such that $p \equiv 2 \pmod 5$.

5. Bob is receiving messages using RSA. Following the notation from class, suppose that he publishes the modulus $N = 9797$ and the enciphering exponent $e = 211$. This means that, if Alice wishes to send a message m so Bob, she will compute and send a ciphertext $c \equiv m^{211} \pmod{9797}$. Determine a deciphering exponent d that Bob can use to decipher messages, i.e. that will satisfy $m \equiv c^d \pmod{9797}$.