- P926 In this chapter, a “large input” typically means an input containing “large integers” rather than an input containing “many integers” (as for sorting).
- P927 circled paragraph
- We assume the multiplication/division/remainder between two β-bit integers takes $\theta(\beta^2)$.

31.1 Elementary number-theoretic notions

- Natural numbers are 0, 1, 2, …
- Z denotes all integers, N denotes all natural numbers
- d | a means “d divides a”
- Every integer divides 0
- P928 A divisor of a non-zero integer a is at least 1 but not greater than |a|.
- 1, 0, all negative integers are neither prime nor composite
- P928 Theorem 31.1 (Division theorem)
- P928 circled paragraph

P929 Common divisors and greatest common divisors

- P929 1 is a common divisor of any two integers.
- P929 circled paragraph
- P930-932 Theorem 31.2, corollary 31.3, corollary 31.4, corollary 31.5, theorem 31.6, theorem 31.7, theorem 31.8

Relatively prime integers

- Two integers a and b are **relatively prime** if their only common divisor is 1, that is, if gcd(a,b) = 1.
- P931 If two integers are each relatively prime to an integer p, then their product is relatively prime to p.
- A consequence of Theorem 31.7 is that we can uniquely factor any composite integer into a product of primes.

31.2 Greatest common divisor

- P934 theorem 31.9 (GCD recursion theorem)
- P935 EUCLID -> first argument is larger than the second argument
  ➔ The number of recursive call in EUCLID is O(lg b)
- P935-936 Lemma 31.10, Theorem 31.11

The extended form of Euclid’s algorithm

- We now rewrite Euclid’s algorithm to computer additional useful information. Specifically, we extend the algorithm to compute the integer coefficients x and y such that d = gcd(x,y) = ax + by. Note that x and y may be zero or negative.
- P937 EXTENDED-EUCLID -> number of recursive call is also O(lg b)
- P938 circled paragraph

31.3 Modular arithmetic

- P940-941 circled paragraph
- The additive group modulo n (the group operation is addition modulo n) & the multiplicative group modulo n (the group operation is multiplication modulo n)
- P940 - 942 theorem 31.12, theorem 31.13
- P942-943 circled paragraph (pay attention to the calculation of the multiplicative inverse and Euler's phi function)
- P944-945 Theorem 31.14(a non-empty closed subset of a finite group is a subgroup), theorem 31.15(Lagrange's theorem), corollary 31.16, theorem 31.17, corollary 31.18, corollary 31.19
- P944-945 circled paragraph

31.4

- P946 circled paragraph
- P947-949 Theorem 31.20, corollary 31.21, corollary 31.22, theorem 31.23, theorem 31.24, corollary 31.25, corollary 31.26

31.5-7: read all