Mathematical Foundations for Computer Science – EXCEL

Number Theory (Part 1)
Sun 13 / Mon 14 October 19
Sam Yong [myong]

- One relation practice problem
- Two $\gcd$ practice problems
- Three statements on integers
- Four practice problems on primes
- n mod properties

~ 0.1 Prove the lexicographic ordering on $\mathbb{N}^2$ is a partial order.

$$(a, b)\ R\ (c, d) \Leftrightarrow (a < c) \vee (a = c \wedge b \leq d)$$

~ 1.1 Find

$$\gcd(273, 754)$$

Express it as a linear combination of the two numbers.

~ 1.2 Prove or disprove

a) $\gcd(a, b) = \gcd(a, a + b)$
b) $\gcd(a, b) = \gcd(a, ab)$
c) $\mathrm{lcm}(a, b) = \mathrm{lcm}(a, a + b)$
d) $\mathrm{lcm}(a, b) = \mathrm{lcm}(a, ab)$

~ 2.1 Show that $\forall n \in \mathbb{N}. 42 \mid n^7 - n$

~ 2.2 Show that $\forall n \in \mathbb{Z}. \neg(4 \mid n^2 + 2)$

~ 2.3* Prove that for every positive integer n

$$1^3 + 2^3 + \cdots + n^3 \mid 3(1^5 + 2^5 + \cdots + n^5)$$

Hint: We speculate

$$\sum_{i=1}^{n} i^3 = \frac{1}{4}n^2(n+1)^2, \sum_{i=1}^{n} i^5 = \frac{1}{12}n^2(n+1)^2(2n^2+2n-1)$$

~ 3.1 Show that if p and $p^2 + 2$ are both primes, so is $p^3 + 2$.

~ 3.2 Find the canonical prime factorization of $3628800 = 10!$

~ 3.3* Let $n \in \mathbb{Z}, n > 2$. Prove that $\{k \in \mathbb{Z} : n < k < n!\}$ contains a prime number.

~ 3.4* Prove that the gap between consecutive primes can be arbitrarily large.

~ 4.1 Fix modulus n. Let $a_1, a_2, b_1, b_2 \in \mathbb{Z}$ such that

$$a_1 \equiv b_1 \wedge a_2 \equiv b_2$$

Show

a) $a_1 + a_2 \equiv b_1 + b_2$
b) $a_1 a_2 \equiv b_1 b_2$

~ 4.2 Fix modulus n. Prove or disprove

$$\forall a, b, q \not\equiv 0 \in \mathbb{Z}. qa \equiv qb \Rightarrow a \equiv b$$

Extra Dose of Prime

The Cyclops numbers are binary palindromes with an odd number of digits where every digit is 1 except for the very middle digit – $\{101_2, 11011_2, 1110111_2, \ldots\}$.

Prove 5 is the only Cyclops prime.

[There is also this thing called glitch primes.]