Discrete Mathematics 1 Supervisior: Marton Havasi
Lectures 7-9 19/11/2017

Topics modular arithmetic; sets; membership; comprehension; gcd; Euclid's Algorithm; properties of gcds; Euclid's Theorem; fields of modular arithmetic; extended Euclid's Algorithm; integer linear combinations; Diffie-Hellman cryptographic method: shared secret key, key exchange.

Core questions (everyone is expected to solve these exercises)

1. Exercise sheet 3.1.1

   Calculate the set CD(666, 330) of common divisors of 666 and 330.

2. Exercise sheet 3.1.6

   Prove that for all integers n and primes p, if $n^2 \equiv 1 \pmod{p}$ then either $n \equiv 1 \pmod{p}$ or $n \equiv -1 \pmod{p}$

3. Exercise sheet 3.2.2

   Prove that for all positive integers a, b, c,

   $$gcd(a, c) = 1 \implies gcd(ab, c) = gcd(b, c)$$

4. Exercise sheet 3.2.6

   Prove that for all positive integers a and b,

   $$gcd(13a + 8b, 5a + 3b) = gcd(a, b)$$

5. 2007 Paper 2 Question 3 link

Tryhard questions (recommended)

1. Exercise sheet 3.3.1.a

   Let a and b be natural numbers such that $a^2|b(b + a)$. Prove that a — b.

   Hint: For positive a and b, consider $a_0 = \frac{a}{gcd(a,b)}$ and $b_0 = \frac{b}{gcd(a,b)}$ so that $gcd(a_0, b_0) = 1$, and show that $a^2|b(b + a) \implies a_0 = 1$.

2. 2015 Paper 2 Question 9, Part A link