November 1, 2016 Lecturer Dmitri Zaitsev

Course 1213 - Introduction to group theory 2016

S h e e t 5

Due: at the end of the tutorial

Exercise 1

Prove or disprove:

(i) If $a|b$ (a divides b) and $b|c$, then $a|c$.

(ii) If $a|bc$, then $a|b$ or $a|c$.

(iii) If $a|b$ and $b|a$, then $a = \pm b$.

(iv) If $a|b$, then $a^2|b^2$.

(iv) If $a|b$, then $(a^2 + a)|(b^2 + b)$.

Exercise 2

(i) For each pair a, b, perform the division of a by b with remainder:

$$a = -21,\ b = 5, \quad a = 27,\ b = 7;$$

(ii) Prove that if $m|n$ and $a \equiv b \bmod n$, then $a \equiv b \bmod m$;

(iii) For which n is $29 \equiv -1 \bmod n$?

Exercise 3

Use the Euclidean algorithm to compute the greatest common divisor:

(i) $\gcd(1034, 33)$

(ii) $\gcd(56, 182)$

(iii) $\gcd(234, 2575)$.

Express each greatest common divisor as integer linear combination of the two given integers.

Exercise 4

Use the unique prime factorization to prove:

(i) $\gcd(ac, bc) = c \gcd(a, b)$ for all integers a, b, c.

(ii) If $\gcd(a, c) = \gcd(b, c) = 1$, then $\gcd(ab, c) = 1$.