Week 1 Problem Sheet
Group Theory and Linear algebra
Semester II 2011

Arun Ram
Department of Mathematics and Statistics
University of Melbourne
Parkville, VIC 3010 Australia
aram@unimelb.edu.au

Last updates: 1 July 2011

1. Week 1: Vocabulary

(1) Define set, subset and equal sets and give some illustrative examples.

(2) Define union of sets, intersection of sets, and product of sets and give some illustrative examples.

(3) Define partition of a set and give some illustrative examples.

(4) Define relation, symmetric relation, reflexive relation and transitive relation and give some illustrative examples.

(5) Define equivalence relation and equivalence class and give some illustrative examples.

(6) Define the order $\le$ on $\mathbb{Z}$ and give some illustrative examples.

(7) Define well ordered set and give some illustrative examples.

(8) Let $d \in \mathbb{Z}$. Define the ideal generated by d and give some illustrative examples.

(9) Let $d, a \in \mathbb{Z}$ and define

(i) d divides a,
(ii) d is a factor of a,
(iii) a is a multiple of d,

and give some illustrative examples.

(10) Let $a, b \in \mathbb{Z}$. Define greatest common divisor of a and b and give some illustrative examples.

(11) Define relatively prime integers and give some illustrative examples.

(12) Define prime integer and give some illustrative examples.

(13) Let $m \in \mathbb{Z}$. Define congruence modulo m and give some illustrative examples.

(14) Let $m \in \mathbb{Z}$. Define congruence class modulo m and give some illustrative examples.

(15) Define $\mathbb{Z}_{>0}$ and give some illustrative examples.

(16) Define $\mathbb{Z}_{>0}$ and the operations of addition and multiplication on $\mathbb{Z}_{>0}$ and give some illustrative examples.

(17) Define $\mathbb{Z}_{\geq 0}$ and give some illustrative examples.

(18) Define $\mathbb{Z}_{\geq 0}$ and the operations of addition and multiplication on $\mathbb{Z}_{\geq 0}$ and give some illustrative examples.

(19) Define $\mathbb{Z}$ and give some illustrative examples.

(20) Define $\mathbb{Z}$ and the operations of addition and multiplication on $\mathbb{Z}$ and give some illustrative examples.

(21) Let $m \in \mathbb{Z}$. Define $\mathbb{Z}/m\mathbb{Z}$ and give some illustrative examples.

(22) Let $m \in \mathbb{Z}$. Define $\mathbb{Z}/m\mathbb{Z}$ and the operations of addition and multiplication on $\mathbb{Z}/m\mathbb{Z}$ and give some illustrative examples.

(23) Let $m \in \mathbb{Z}$. Define multiplicative inverse in $\mathbb{Z}/m\mathbb{Z}$ and give some illustrative examples.

(24) Which sets are the three elements of $\mathbb{Z}/3\mathbb{Z}$?

2. Week 1: Results

(1) (Division with remainder) Show that if $a, d \in \mathbb{Z}$ and $d > 0$ then there exist unique integers q and r such that $0 \leq r < d$ and $a = qd + r$.

(2) Let $a, b, c \in \mathbb{Z}$. Show that if $a|b$ and $b|c$ then $a|c$.

(3) Let a, b, and c be integers. Show that if $a|b$ and $a|c$ then $a^2|(b^2 + 3c^2)$.

(4) Show that if a, b, c, d are integers such that $a|b$ and $c|d$ then $ac|bd$.

(5) Prove that if a, b, c, d, x, y are integers such that $a|b$ and $a|c$ then $a|(xb + yc)$.

(6) Prove that if a, b are positive integers such that $a|b$ and $b|a$ then $a = b$.

(7) Show that if $a, d \in \mathbb{Z}$ and $q_1, r_1, q_2, r_2 \in \mathbb{Z}$ and $0 \leq r_1 < d$ and $0 \leq r_2 < d$ and $a = q_1 d + r_1$ and $a = q_2 d + r_2$ then $q_1 = q_2$ and $r_1 = r_2$.

(8) Let $a, b \in \mathbb{Z}$. Show that

(a) $\gcd(a, b) = \gcd(b, a) = \gcd(-a, b)$,
(b) $\gcd(a, 0) = a$,
(c) If q and r are integers such that $a = bq + r$ then $\gcd(a, b) = \gcd(b, r)$.

(9) Let $a, b \in \mathbb{Z}$ and let d be the greatest common divisor of a and b. Show that there exist integers x and y such that $ax + by = d$.

(10) Let $a, b \in \mathbb{Z}$ and let d be the greatest common divisor of a and b. Show that d is the largest integer that divides both a and b.

(11) Let $d, a, b \in \mathbb{Z}$. Show that if $d|ab$ and $\gcd(a, d) = 1$ then $d|b$.

(12) Let $p, a, b \in \mathbb{Z}$. Show that if p is prime and $p|ab$ then $p|a$ then or $p|b$.

(13) Give an example of positive integers a, b, c such that $a|c$ and $b|c$ but $ab \nmid c$.

(14) Let $a, b, c \in \mathbb{Z}$ be integers with $\gcd(a, b) = 1$. Prove that if $a|c$ and $b|c$ then $ab|c$.

(15) Let $m \in \mathbb{Z}_{\geq 0}$. Prove that congruence mod m is an equivalence relation.

(16) Let $m \in \mathbb{Z}_{\geq 0}$. Prove that the operation of addition on $\mathbb{Z}/m\mathbb{Z}$ is well defined.

(17) Let $m \in \mathbb{Z}_{\geq 0}$. Prove that the operation of multiplication on $\mathbb{Z}/m\mathbb{Z}$ is well defined.

(18) Let $m \in \mathbb{Z}_{\geq 0}$ and let $a \in \mathbb{Z}$. Prove that $[a]$ has a multiplicative inverse in $\mathbb{Z}/m\mathbb{Z}$ if and only if $\gcd(a, m) = 1$.

(19) Let $p \in \mathbb{Z}$ be prime. Show that every non-zero element of $\mathbb{Z}/p\mathbb{Z}$ has a multiplicative inverse.

(20) Prove that if $a = b \bmod m$ and $b = c \bmod m$ then $a = c \bmod m$

(21)

(a) Prove that if a, b, c are integers with $ac = bc \bmod m$ and $\gcd(c, m) = 1$ then $a = b$ mod m.
(b) Give an example to show that this result fails if we drop the condition that $\gcd(c, m) = 1$.
(c) What can you conclude if $\gcd(c, m) = d$?

(22)

(a) Show that if p is prime, then p divides the binomial coefficient $\binom{p}{k} = \frac{p!}{p!(p-k)!}$, for $0 < k < p$.

(b) Deduce, using induction on n and the binomial theorem, that if p is prime then $n^p = n \bmod p$, for all natural numbers n ("Fermat's Little Theorem").

3. Week 1: Examples and Calculations

(1)
(a) Find the quotient and remainder when 25 is divided by 3.
(b) Find the quotient and remainder when 68 is divided by 7.
(c) Find the quotient and remainder when -33 is divided by 7.
(d) Find the quotient and remainder when -25 is divided by 3.

(2)
(a) Find the quotient and remainder when 25 is divided by -3.
(b) Find the quotient and remainder when -25 is divided by -3.
(c) Find the quotient and remainder when 25 is divided by 0.
(d) Find the quotient and remainder when 0 is divided by 25.

(3) Show that $\gcd(4, 6) = 2$.

(4) Show that $\gcd(10, -20) = 10$.

(5) Show that $\gcd(7, 3) = 1$.

(6) Show that $\gcd(0, 5) = 5$.

(7) Show that 12 and 35 are relatively prime.

(8) Show that 12 and 34 are not relatively prime.

(9) Find $\gcd(4163, 8869)$.

(10) Solve the equation $131x + 71y = 1$. Explain why this question is not well stated. Fix up the question and solve it.

(11) Using Euclid's Algorithm find $\gcd(14, 35)$.

(12) Using Euclid's Algorithm find $\gcd(105, 165)$.

(13) Using Euclid's Algorithm find $\gcd(1287, 1144)$.

(14) Using Euclid's Algorithm find $\gcd(1288, 1144)$.

(15) Using Euclid's Algorithm find $\gcd(1287, 1145)$.

(16) Find $d = \gcd(27, 33)$ find integers x and y such that $d = x27 + y33$.

(17) Find $d = \gcd(27, 32)$ find integers x and y such that $d = x27 + y32$.

(18) Find $d = \gcd(312, 377)$ find integers x and y such that $d = x312 + y377$.

(19)

(a) Show that $3 = 1 \bmod 2$.

(b) Show that $3 = 17 \bmod 17$.

(20)

(a) Show that $3 = -15 \bmod 9$.

(b) Show that $4 = 0 \bmod 2$.

(21) Show that $6 \neq 1 \bmod 4$.

(22) Explain the most efficient way to calculate 29^4 modulo 12.

(23) Show that $3 + 4 = 1, 3 \cdot 5 = 3$, and $3 - 5 = 4$ in $\mathbb{Z}/6\mathbb{Z}$.

(24) Write down the addition and multiplication tables for $\mathbb{Z}/5\mathbb{Z}$ and $\mathbb{Z}/6\mathbb{Z}$.

(25) Show that 2 has no multiplicative inverse in $\mathbb{Z}/4\mathbb{Z}$.

(26) Find the multiplicative inverse of 71 in $\mathbb{Z}/131\mathbb{Z}$.

(27)

(a) Decide whether $3 = 42 \pmod{13}$.
(b) Decide whether $2 = -20 \pmod{11}$.
(c) Decide whether $26 = 482 \pmod{14}$.

(28)

(a) Decide whether $-2 = 933 \pmod{5}$.
(b) Decide whether $-2 = 933 \pmod{11}$.
(c) Decide whether $-2 = 933 \pmod{55}$.

(29)

(a) Simplify $482 \pmod{14}$.
(b) Simplify $511 \pmod{9}$.
(c) Simplify $-374 \pmod{11}$.

(30)

(a) Simplify $933 \pmod{55}$.
(b) Simplify $102725 \pmod{10}$.
(c) Simplify $57102725 \pmod{9}$.

(31) Calculate $24 \cdot 25 \pmod{21}$.

(32) Calculate $84 \cdot 125 \pmod{210}$.

(33) Calculate $25^2 + 24 \cdot 3 - 6 \pmod{9}$.

(34) Calculate $36^3 - 3 \cdot 19 + 2 \pmod{11}$.

(35) Calculate $1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \pmod{7}$,

(36) Calculate $1 \cdot 2 \cdot 3 \cdots 20 \cdot 21 \pmod{22}$.

(37) Use congruences modulo 9 to show that the following multiplication in $\mathbb{Z}$ is incorrect: $326 \cdot 4471 = 1357546$.

(38) Determine the multiplicative inverses in $\mathbb{Z}/7\mathbb{Z}$.

(39) Determine the multiplicative inverses in $\mathbb{Z}/8\mathbb{Z}$,

(40) Determine the multiplicative inverses in $\mathbb{Z}/12\mathbb{Z}$,

(41) Determine the multiplicative inverses in $\mathbb{Z}/13\mathbb{Z}$,

(42) Determine the multiplicative inverses in $\mathbb{Z}/15\mathbb{Z}$,

(43) If it exists, find the multiplicative inverse of 32 in $\mathbb{Z}/27\mathbb{Z}$.

(44) If it exists, find the multiplicative inverse of 32 in $\mathbb{Z}/39\mathbb{Z}$.

(45) If it exists, find the multiplicative inverse of 17 in $\mathbb{Z}/41\mathbb{Z}$.

(46) If it exists, find the multiplicative inverse of 18 in $\mathbb{Z}/33\mathbb{Z}$.

(47) If it exists, find the multiplicative inverse of 200 in $\mathbb{Z}/911\mathbb{Z}$.

(48) Write down all the common divisors of 56 and 72.

(49)

- (a) Use Euclid's algorithm to find $d = \gcd(323, 377)$.
- (b) Find integers x, y such that $323x + 377y = d$.

(50) Simplify the following, giving your answers in the form $a \bmod m$, where $0 \leq a < m$.

- (a) $14 \cdot 13 - 67 + 133 \pmod{10}$,
- (b) $53 \pmod{7}$,
- (c) $53 + 2 \cdot 4 \pmod{7}$,
- (d) $21 \cdot 22 \cdot 23 \cdot 24 \cdot 25 \pmod{20}$.

(51) For the following, write your answers in the form $0, 1, \ldots, 18 \pmod{19}$.

- (a) Calculate $3^2, 3^4, 3^8, 3^{16}, 3^{32}, 3^{64}, 3^{128}$ and 3^{256} modulo 19.
- (b) Use (a) to calculate 3^{265} modulo 19. (Hint: $265 = 256 + 8 + 1$.)

(52) (A test for divisibility by 11.) Let $n = a_d a_{d-1} \cdots a_2 a_1 a_0$ be a positive integer written in base 10, i.e. $n = a_0 + 10a_1 + 10^2 a_2 + \cdots + 10^d a_d$, where $a_0, a_1, \ldots a_d$, are the digits of the number n read from right to left.

(a) Show that $n = a_0 - a_1 + a_2 - a_3 + \cdots + (-1)^d a_d$ mod 11. Hence n is divisible by 11 exactly when $a_0 - a_1 + a_2 - a_3 + \cdots + (-1)^d a_d$ is divisible by 11.
(b) Use this test to decide if the following numbers are divisible by 11: (i) 123537, (ii) 30639423045.

(53)

(a) Write down the addition and multiplication tables for $\mathbb{Z}/7\mathbb{Z}$.
(b) Find the multiplicative inverse of 2 in $\mathbb{Z}/7\mathbb{Z}$.

(54) Find the smallest positive integer in the set $\{6u + 15v \mid u, v \in \mathbb{Z}\}$. Always justify your answers.

4. References

[GH] J.R.J. Groves and C.D. Hodgson, *Notes for 620-297: Group Theory and Linear Algebra*, 2009.