Discrete Mathematics for Part I CST 2014/15
Proofs, Numbers, and Sets
Michaelmas Supervision Exercises

Marcelo Fiore   Ohad Kammar

November 6, 2014

Suggested supervision schedule:

- §1 On proofs (basic exercises).
- §2 On proofs (advanced exercises) and §3 On numbers (basic exercises).
- §4 On numbers (advanced exercises) and §5 More on numbers (basic exercises).
- §6 More on numbers (advanced exercises) and §7 On induction (basic exercises).

1 On proofs (basic exercises)

The main ***aim*** *here is to practice the analysis and understanding of mathematical statements (e.g. by isolating the different components of composite statements), and exercise the art of presenting a logical argument in the form of a clear proof (e.g. by following proof strategies and patterns).*

1. Prove or disprove the following statements.

   (a) Suppose n is a natural number larger than 2, and n is not a prime number. Then $2 \cdot n + 13$ is not a prime number.

   (b) If $x^2 + y = 13$ and $y \neq 4$ then $x \neq 3$.

   (c) For an integer n, n^2 is even if and only if n is even.

2. Characterise those integers d and n such that:

   (a) $0 \mid n$,

   (b) $d \mid 0$.

3. Let k, m, n be integers with k positive. Show that:

   $$(k \cdot m) \mid (k \cdot n) \iff m \mid n \quad .$$

4. Prove or disprove that: For all natural numbers n, $2 \mid 2^n$.

5. Prove that for all integers n,

$$30 \mid n \iff \big(2 \mid n \,\wedge\, 3 \mid n \,\wedge\, 5 \mid n\big) \quad .$$

6. Find a counterexample to the statement: For all positive integers k, m, n,

$$\text{if } (m \mid k \,\wedge\, n \mid k) \text{ then } (m \cdot n) \mid k \ .$$

7. Show that for all integers l, m, n,

$$l \mid m \,\wedge\, m \mid n \implies l \mid n \ .$$

8. Prove that for all integers d, k, l, m, n,

   (a) $d \mid m \,\wedge\, d \mid n \implies d \mid (m+n)$,

   (b) $d \mid m \implies d \mid k \cdot m$,

   (c) $d \mid m \,\wedge\, d \mid n \implies d \mid (k \cdot m + l \cdot n)$.

9. Prove or disprove the following statements.

   (a) For all real numbers x and y there is a real number z such that $x + z = y - z$.

   (b) For all integers x and y there is an integer z such that $x + z = y - z$.

   (c) For every real number x, if $x \neq 2$ then there is a unique real number y such that $2 \cdot y/(y + 1) = x$.

   (d) The addition of two rational numbers is a rational number.

10. Prove or disprove that: For all integers m and n, if $m \cdot n$ is even, then either m is even or n is even.

11. Show that for all integers m and n,

$$(\, m \mid n \,\wedge\, n \mid m \,) \implies (\, m = n \,\vee\, m = -n \,) \ .$$

12. Prove or disprove that: For all positive integers k, m, n,

$$\text{if } k \mid (m \cdot n) \text{ then } k \mid m \text{ or } k \mid n \ .$$

2 On proofs (advanced exercises)

*Having practised how to analyse and understand basic mathematical statements and clearly present their proofs in the previous supervision, the **aim** here is to prove some more challenging mathematical statements that further require thinking about how to tackle and solve the problems.*

1. [Adapted from David Burton]

   (a) A natural number is said to be *triangular* if it is of the form $\sum_{i=0}^{k} i = 0+1+\cdots+k$, for some natural number k. For example, the first three triangular numbers are $t_0 = 0$, $t_1 = 1$, and $t_2 = 3$. Find the next three triangular numbers t_3, t_4, and t_5.

   (b) Find a formula for the k-th triangular number t_k.
   Hints:

- Geometric approach: Observe that

$$\begin{array}{ccc} \circ & & \\ \circ & \circ & \\ \circ & \circ & \circ \end{array} \quad + \quad \begin{array}{ccc} \bullet & \bullet & \bullet \\ & \bullet & \bullet \\ & & \bullet \end{array} \quad = \quad \begin{array}{cccc} \circ & \bullet & \bullet & \bullet \\ \circ & \circ & \bullet & \bullet \\ \circ & \circ & \circ & \bullet \end{array}$$

- Algebraic approach: Note that

$$(n+1)^2 \;=\; \textstyle\sum_{i=0}^{n}(i+1)^2 - \sum_{i=0}^{n} i^2 \;.$$

(c) A natural number is said to be *square* if it is of the form k^2 for some natural number k.

[Plutarch, circ. 100BC] Show that n is triangular iff $8 \cdot n + 1$ is square.

(d) [Nicomachus, circ. 100BC] Show that the sum of every two consecutive triangular numbers is square.

(e) [Euler, 1775] Show that, for all natural numbers n, if n is triangular, then so are $9 \cdot n + 1$, $25 \cdot n + 3$, and $49 \cdot n + 6$.

2. Formalise [and prove] the following statement: A natural number is a multiple of 3 iff so is the number obtained by summing its digits. Do the same for analogous criteria for multiples of 9 and for multiples of 11.

   Prove the following statement: A natural number is a multiple of 3 iff so is the number obtained by summing its digits. Do the same for analogous criteria for multiples of 9 and for multiples of 11.

3. Let $P(m)$ be a statement for m ranging over the natural numbers, and consider the derived statement

$$P^{\#}(m) \;=\; \forall \text{ natural } k.\; 0 \leq k \leq m \implies P(k)$$

   again for m ranging over the natural numbers.

   Prove the following equivalences:

   - $P^{\#}(0) \iff P(0)$
   - $\big(P^{\#}(n) \implies P^{\#}(n+1)\big) \iff \big(P^{\#}(n) \implies P(n+1)\big)$
   - $\forall$ natural number $m.\, P^{\#}(m) \iff \forall$ natural number $m.\, P(m)$

4. Let $P(x)$ be a predicate on a variable x and let Q be a statement not mentioning x. (For instance, $P(x)$ could be the predicate "programmer x found a software bug" and Q could be the statement "all the code has to be rewritten".)

   Show that the equivalence

$$\Big((\exists x.\, P(x)) \implies Q\Big) \iff \Big(\forall x.\, \big(P(x) \implies Q\big)\Big)$$

   holds.

3 On numbers (basic exercises)

Aim: *To get familiar with the basics of: divisibility and congruences, the division theorem and algorithm, modular arithmetic, and Fermat's Little Theorem.*

1. Let i, j be integers and let m be a positive integer. Show that:
   (a) $i \equiv i \pmod{m}$
   (b) $i \equiv j \pmod{m} \implies j \equiv i \pmod{m}$
   (c) $i \equiv j \pmod{m} \implies i^2 \equiv j^2 \pmod{m}$

2. Find an integer i, natural numbers k, l, and a positive integer m for which $k \equiv l \pmod{m}$ holds while $i^k \equiv i^l \pmod{m}$ does not.

3. Prove that for all integers i, j, k, l, m, n with m positive and n nonnegative,
   (a) $i \equiv j \pmod{m} \wedge j \equiv k \pmod{m} \implies i \equiv k \pmod{m}$
   (b) $i \equiv j \pmod{m} \wedge k \equiv l \pmod{m} \implies i + k \equiv j + l \pmod{m}$
   (c) $i \equiv j \pmod{m} \wedge k \equiv l \pmod{m} \implies i \cdot k \equiv j \cdot l \pmod{m}$
   (d) $i \equiv j \pmod{m} \implies i^n \equiv j^n \pmod{m}$

4. Prove the following statement: A natural number is a multiple of 3 iff so is the number obtained by summing its digits. Do the same for analogous criteria for multiples of 9 and for multiples of 11.

5. Show that for every integer n, the remainder when n^2 is divided by 4 is either 0 or 1.

6. Prove that for all natural numbers k, l, and positive integer m,
   (a) $\mathrm{rem}(k \cdot m + l, m) = \mathrm{rem}(l, m)$
   (b) $\mathrm{rem}(k + l, m) = \mathrm{rem}\big(\mathrm{rem}(k, m) + l, m\big)$, and
   (c) $\mathrm{rem}(k \cdot l, m) = \mathrm{rem}\big(k \cdot \mathrm{rem}(l, m), m\big)$.

7. What are $\mathrm{rem}(55^2, 79)$, $\mathrm{rem}(23^2, 79)$, $\mathrm{rem}(23 \cdot 55, 79)$, and $\mathrm{rem}(55^{78}, 79)$?

8. Calculate that $2^{153} \equiv 53 \pmod{153}$.

   (Btw, at first sight this seems to contradict Fermat's Little Theorem, why isn't this the case though?)

9. Let m be a positive integer.
   (a) Prove the associativity of the addition and multiplication operations in $\mathbb{Z}_m$; that is, that for all i, j, k in $\mathbb{Z}_m$,
   $$(i +_m j) +_m k = i +_m (j +_m k) \quad \text{and} \quad (i \cdot_m j) \cdot_m k = i \cdot_m (j \cdot_m k) \quad .$$
   (b) Prove that the additive inverse of k in $\mathbb{Z}_m$ is $[-k]_m$.

10. Calculate the addition and multiplication tables, and the additive and multiplicative inverses tables for $\mathbb{Z}_3$, $\mathbb{Z}_6$, and $\mathbb{Z}_7$.

4 On numbers (advanced exercises)

*Modular arithmetic is a corner stone of number theory, an area of mathematics in which one very easily hits very hard problems. The **aim** here is to solve problems on congruences that are more challenging than those of the previous supervision and will give you a taste of this.*

1. Prove that for all integers n, there exist natural numbers i and j such that $n = i^2 - j^2$ iff either $n \equiv 0 \pmod 4$, or $n \equiv 1 \pmod 4$, or $n \equiv 3 \pmod 4$.
2. Prove that $n^3 \equiv n \pmod 6$ for all integers n.
3. Let i and n be positive integers and let p be a prime. Show that if $n \equiv 1 \pmod{p-1}$ then $i^n \equiv i \pmod p$ for all i not multiple of p.
4. Prove that $n^7 \equiv n \pmod{42}$ for all integers n.
5. [Adapted from David Burton]

   A *decimal (respectively binary) repunit* is a natural number whose decimal (respectively binary) representation consists solely of 1's.

   (a) What are the first three decimal repunits? And the first three binary ones?

   (b) Show that no decimal repunit strictly greater than 1 is square, and that the same holds for binary repunits. Is this the case for every base?

   Hint: Use Lemma 26 of the notes.

5 More on numbers (basic exercises)

Aim: *To get familiar with the basics of: the greatest common divisor, (the Extended) Euclid's Algorithm, and Euclid's Theorem.*

1. Calculate the set $\mathrm{CD}(666, 330)$ of common divisors of 666 and 330.
2. Find the gcd of 21212121 and 12121212.
3. Prove that for all positive integers m and n,

$$\gcd(m, n) = m \iff m \mid n \ .$$

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

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

5. Prove that for all positive integers m and n, and integers k and l,

$$\gcd(m, n) \mid (k \cdot m + l \cdot n) \ .$$

6. Find integers x and y such that $x \cdot 30 + y \cdot 22 = \gcd(30, 22)$. Now find integers x' and y' with $0 \le y' < 30$ such that $x' \cdot 30 + y' \cdot 22 = \gcd(30, 22)$.

7. Let m and n be positive integers with $\gcd(m,n) = 1$. Prove that for every natural number k,

$$m \mid k \wedge n \mid k \iff (m \cdot n) \mid k \quad .$$

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

9. Prove that for all positive integers m, n, p, q such that $\gcd(m,n) = \gcd(p,q) = 1$, if $q \cdot m = p \cdot n$ then $m = p$ and $n = q$.

6 More on numbers (advanced exercises)

> ***Aim:*** *To consolidate your knowledge and understanding of the basic number theory that has been covered in the course.*

1. Prove that, for all positive integers m and n, there exist integers k and l such that $k \cdot m + l \cdot n = 1$ iff $\gcd(m,n) = 1$.

2. Show the correctness of the following algorithm

```
fun gcd0( m , n )
  = if m = n then m
    else
      let
        val p = min(m,n) ; val q = max(m,n)
      in
        gcd0( p , q - p )
      end
```

   for computing the gcd of two positive integers.

3. Prove that for all positive integers a and b,

$$\gcd\big(\, 13 \cdot a + 8 \cdot b \,,\, 5 \cdot a + 3 \cdot b \,\big) \;=\; \gcd(a,b) \quad .$$

4. (a) Prove that if an integer n is not divisible by 3, then $n^2 \equiv 1 \pmod{3}$.
   (b) Show that if an integer n is odd, then $n^2 \equiv 1 \pmod{8}$
   (c) Conclude that if p is a prime greater than 3, then $p^2 - 1$ is divisible by 24.

5. Prove that $n^{13} \equiv n \pmod{10}$ for all integers n.

6. Prove that for all positive integers l, m, and n, if $\gcd(l, m \cdot n) = 1$ then $\gcd(l,m) = 1$ and $\gcd(l,n) = 1$.

7. Solve the following congruences:
   (a) $77 \cdot x \equiv 11 \pmod{40}$
   (b) $12 \cdot y \equiv 30 \pmod{54}$

(c) $\begin{cases} z \equiv 13 \pmod{21} \\ 3 \cdot z \equiv 2 \pmod{17} \end{cases}$

8. What is the multiplicative inverse of: (i) 2 in $\mathbb{Z}_7$, (ii) 7 in $\mathbb{Z}_{40}$, and (iii) 13 in $\mathbb{Z}_{23}$?
9. Prove that $[22^{12001}]_{175}$ has a multiplicative inverse in $\mathbb{Z}_{175}$.

7 On induction (basic exercises)

Aim: *To practise proofs by the mathematical Principle of Induction.*

1. Establish the following:
   (a) For all positive integers m and n,
   $$(2^n - 1) \cdot \sum_{i=0}^{m-1} 2^{i \cdot n} = 2^{m \cdot n} - 1 \quad .$$
   (b) Suppose k is a positive integer that is not prime. Then $2^k - 1$ is not prime.
2. Prove that
   $$\forall\, n \in \mathbb{N}.\ \forall\, x \in \mathbb{R}.\ x \geq -1 \implies (1 + x)^n \geq 1 + n \cdot x \quad .$$
3. Recall that the Fibonacci numbers F_n for n ranging over the natural numbers are defined by $F_0 = 0$, $F_1 = 1$, and $F_n = F_{n-1} + F_{n-2}$ for $n \geq 2$.
   (a) Prove Cassini's Identity: For all natural numbers n,
   $$F_n \cdot F_{n+2} = {F_{n+1}}^2 + (-1)^{n+1} \quad .$$
   (b) Prove that for all natural numbers k and n,
   $$F_{n+k+1} = F_{k+1} \cdot F_{n+1} + F_k \cdot F_n \quad .$$
   (c) Deduce that $F_n \mid F_{l \cdot n}$ for all natural numbers n and l.
   (d) Prove that $\texttt{gcd}(F_{n+2}, F_{n+1})$ terminates with output 1 in $n+1$ steps for all natural numbers n.
   (e) Deduce also that,
   (i) for positive integers $n < m$, $\gcd(F_m, F_n) = \gcd(F_{m-n}, F_n)$
   and hence that,
   (ii) for all positive integers m and n, $\gcd(F_m, F_n) = F_{\gcd(m,n)}$.
   (f) Show that for all positive integers m and n, $(F_m \cdot F_n) \mid F_{m \cdot n}$ if $\gcd(m, n) = 1$.
   (g) Conjecture and prove theorems concerning the sums
   (i) $\sum_{i=0}^{n} F_{2 \cdot i}$, and
   (ii) $\sum_{i=0}^{n} F_{2 \cdot i+1}$
   for n any natural number.
4. Prove that

   For all natural numbers $l \geq 2$, we have that for all positive integers m, n, if $m + n = l$ then $\texttt{gcd0}(m, n)$ terminates.

   by the Principle of Strong Induction from basis 2.