Discrete Mathematics for Part I CST 2018/19
Proofs and Numbers Exercises

Marcelo Fiore   Ohad Kammar

- Suggested supervision schedule
  - On proofs: Basic (§1.1) and core (§1.2) exercises.
    Lectures 3–4 onwards.
  - On numbers: Basic (§2.1) and core (§2.2) exercises.
    Lectures 6–7 onwards.
  - More on numbers: Basic (§3.1) and core (§3.2) exercises.
    Lectures 9–10 onwards.
  - On induction: Basic (§4.1) and core (§4.2) exercises.
    Lectures 11–12 onwards.
- Suggested Xmas-break work
  - 2018 Paper 2 Questions 7 (a), 8 (a) & 9 (a)
  - 2017 Paper 2 Questions 7 (a) & 8 (a)
  - 2016 Paper 2 Questions 7 (a), 8 (a) & (b) , and 9 (a)
  - 2015 Paper 2 Questions 7 (a) & (b), 8 (a) & (b), and 9 (a)
  - 2014 Paper 2 Question 7
  - 2007 Paper 2 Question 3
  - 2006 Paper 2 Questions 3 and 4

1 On proofs

1.1 Basic exercises

The main ***aim*** *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).*

Prove or disprove the following statements.

1. 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.
2. If $x^2 + y = 13$ and $y \neq 4$ then $x \neq 3$.
3. For an integer n, n^2 is even if and only if n is even.
4. For all real numbers x and y there is a real number z such that $x + z = y - z$.
5. For all integers x and y there is an integer z such that $x + z = y - z$.

6. The addition of two rational numbers is a rational number.

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

8. For all integers m and n, if $m \cdot n$ is even, then either m is even or n is even.

1.2 Core exercises

*Having practised how to analyse and understand basic mathematical statements and clearly present their proofs, the **aim** is to get familiar with the basics of divisibility.*

1. Characterise those integers d and n such that:

   (a) $0 \mid n$,

   (b) $d \mid 0$.

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

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

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

4. Prove that for all integers n,

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

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

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

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

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

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

8. Show that for all integers m and n,

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

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

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

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

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

    again for m ranging over the natural numbers.

    (a) Show that, for all natural numbers ℓ, $P^{\#}(\ell) \implies P(\ell)$.

    (b) Exhibit a concrete statement $P(m)$ and a specific natural number n for which the statement

$$P(n) \implies P^{\#}(n)$$

does not hold.

(c) Prove the following:

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

1.3 Optional advanced exercises

Aim: *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

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

   (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 $9 \cdot n + 1$, $25 \cdot n + 3$, $49 \cdot n + 6$, and $81 \cdot n + 10$.

   (f) [Jordan, 1991, attributed to Euler] Prove the generalisation: For all n and k natural numbers, there exists a natural number q such that: $(2n+1)^2\ t_k + t_n = t_q$.

2. 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

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

   holds.

2 On numbers

2.1 Basic exercises

Aim: *To get familiar with the basics of congruences, the division theorem and algorithm, and modular arithmetic.*

1. Let i, j be integers and let m, n be positive integers. Show that:

   (a) $i \equiv i \pmod{m}$

   (b) $i \equiv j \pmod{m} \implies j \equiv i \pmod{m}$

   (c) $i \equiv j \pmod{m} \wedge j \equiv k \pmod{m} \implies i \equiv k \pmod{m}$

2. Prove that for all integers i, j, k, l, m, n with m positive and n nonnegative,

   (a) $i \equiv j \pmod{m} \wedge k \equiv l \pmod{m} \implies i + k \equiv j + l \pmod{m}$

   (b) $i \equiv j \pmod{m} \wedge k \equiv l \pmod{m} \implies i \cdot k \equiv j \cdot l \pmod{m}$

   (c) $i \equiv j \pmod{m} \implies i^n \equiv j^n \pmod{m}$

3. 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) $\mathrm{rem}(k \cdot l, m) = \mathrm{rem}\big(k \cdot \mathrm{rem}(l, m), m\big)$.

4. 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 $[-k]_m$.

2.2 Core exercises

Aim: *To solve problems concerning congruences, the division theorem and algorithm, modular arithmetic, and Fermat's Little Theorem.*

1. 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.

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.

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

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

5. 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?)

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

7. Prove that $n^3 \equiv n \pmod 6$ for all integers n.

8. 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.

9. Prove that $n^7 \equiv n \pmod{42}$ for all integers n.

2.3 Optional advanced exercises

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. [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.

3 More on numbers

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

3.1 Basic exercises

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, and integers k and l,

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

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

5. 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 $\gcd(m, n) = 1$.

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 $n \equiv -1 \pmod p$.

3.2 Core exercises

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

1. Prove that for all positive integers m and n,

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

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

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

3. Prove that for all positive integers m and n, and integers i and j:

$$n \cdot i \equiv n \cdot j \pmod{m} \iff i \equiv j \ (\mathrm{mod}\ \frac{m}{\gcd(m,n)})$$

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

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

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

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

7. (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.

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

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

10. Solve the following congruences:
    (a) $77 \cdot x \equiv 11 \pmod{40}$
    (b) $12 \cdot y \equiv 30 \pmod{54}$
    (c) $\begin{cases} z \equiv 13 \pmod{21} \\ 3 \cdot z \equiv 2 \pmod{17} \end{cases}$

11. What is the multiplicative inverse of: (i) 2 in $\mathbb{Z}_7$, (ii) 7 in $\mathbb{Z}_{40}$, and (iii) 13 in $\mathbb{Z}_{23}$?

12. Prove that $[22^{12001}]_{175}$ has a multiplicative inverse in $\mathbb{Z}_{175}$.

3.3 Optional advanced exercises

1. (a) Let a and b be natural numbers such that $a^2 \mid b(b+a)$. Prove that $a \mid b$.
   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 $a^2 \mid b(b+a)$ implies $a_0 = 1$.
   (b) [49$^{\text{th}}$ Putnam, 1988] Prove the converse to §1.3(1f): For all natural numbers n and s, if there exists a natural number q such that:

   $$(2n+1)^2 s + t_n = t_q$$

   then there exists a natural number k such that $s = t_k$.
   Hint: Recall that if

   $$q = 2nk + n + k \quad , \tag{1}$$

   then $(2n+1)^2\, t_k + t_n = t_q$. Solving for k in (1), we get that $k = \frac{q-n}{2n+1}$; so it would be enough to show that the fraction $\frac{q-n}{2n+1}$ is a natural number.

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.

4 On induction

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

4.1 Basic exercises

1. Prove that for all natural numbers $n \geq 3$, if n distinct points on a circle are joined in consecutive order by straight lines, then the interior angles of the resulting polygon add up to $180 \cdot (n-2)$ degrees.

2. Prove that, for any positive integer n, a $2^n \times 2^n$ square grid with any one square removed can be tiled with L-shaped pieces consisting of 3 squares.

4.2 Core exercises

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 steps for all positive 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.

4.3 Optional advanced exercises

1. Recall the `gcd0` function from §3.3(2). Prove that

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

   by the Principle of Strong Induction from basis 2.

2. The set of *(univariate) polynomials* (over the rationals) on a variable x is defined as that of arithmetic expressions equal to those of the form $\sum_{i=0}^{n} a_i \cdot x^i$, for some $n \in \mathbb{N}$ and some $a_1, \ldots, a_n \in \mathbb{Q}$.

   (a) Show that if $p(x)$ and $q(x)$ are polynomials then so are $p(x) + q(x)$ and $p(x) \cdot q(x)$.

   (b) Deduce as a corollary that, for all $a, b \in \mathbb{Q}$, the linear combination $a \cdot p(x) + b \cdot q(x)$ of two polynomials $p(x)$ and $q(x)$ is a polynomial.

   (c) Show that there exists a polynomial $p_2(x)$ such that $p_2(n) = \sum_{i=0}^{n} i^2 = 0^2 + 1^2 + \cdots + n^2$ for every $n \in \mathbb{N}$.[1]

   Hint: Note that for every $n \in \mathbb{N}$,

   $$(n+1)^3 \quad = \quad \sum_{i=0}^{n}(i+1)^3 - \sum_{i=0}^{n} i^3 \quad . \qquad (\dagger)$$

   (d) Show that, for every $k \in \mathbb{N}$, there exists a polynomial $p_k(x)$ such that, for all $n \in \mathbb{N}$, $p_k(n) = \sum_{i=0}^{n} i^k = 0^k + 1^k + \cdots + n^k$.

   Hint: Generalise

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

   and (†) above.

[1] Chapter 2.5 of *Concrete Mathematics: A Foundation for Computer Science* by R.L. Graham, D.E. Knuth, and O. Patashnik looks at this in great detail.