# MATH10101, optional exercises on proofs in elementary number theory. Will not be discussed in the supervisions — SOLUTIONS

**Opt15.** Let $a, b, c$ be integers. Prove that if $c \mid a$ and $c \nmid b$, then $c \nmid (a+b)$.

**Opt15 - solution.** Assume for contradiction that $c \mid (a+b)$, meaning that $a+b = ck$ for some integer $k$. We are given that $c \mid a$, meaning that $a = c\ell$ for some integer $\ell$. Then $b = (a+b) - a = ck - c\ell = c(k-\ell)$ and, since $k-\ell$ is an integer, $c \mid b$, a contradiction.

Alternatively, write $b = 1(a+b) + (-1)a$ which is a linear combination of $a+b$ and $a$. Assume for contradiction that $c \mid (a+b)$, then since $c$ also divides $a$, by a fact from the course $c$ divides the integral linear combination $1(a+b) + (-1)a$. That is, $c \mid b$, a contradiction.

**Opt16.** Prove that the relation $\mid$ (divides) on $\mathbb{Z}$ is transitive.

**Opt16 - solution.** By definition of transitivity, we need to prove that for all $a, b, c \in \mathbb{Z}$, $(a \mid b) \wedge (b \mid c)$ implies $a \mid c$. Assume that $a$ divides $b$ and $b$ divides $c$. Then by definition $b = ak$ and $c = b\ell$ where $k, \ell$ are integers. Then $c = ak\ell$, and since $k\ell$ is an integer, by definition $a \mid c$.

**Opt17.** Let $a \equiv b \mod m$ and let $n \mid m$. Prove that $a \equiv b \mod n$.

**Opt17 - solution.** By definition of congruence, $a \equiv b \mod m$ means that $m \mid (a-b)$. Also, $n$ divides $m$, so by transitivity of $\mid$ we have $n \mid (a-b)$. By definition of congruence again this means that $a \equiv b \mod n$, as required.

**Opt18.** Let $a, b, c$ be integers, $a \mid c$, $b \mid c$, $\gcd(a, b) = 1$. Prove that $ab \mid c$.

**Opt18 - solution.** By definition $a \mid c$ means that $c = ak$ for some integer $k$. Thus, $b \mid ak$. However, we are given that $b$ is coprime to $a$, so by a fact from the course, $b$ must divide $k$: $k = b\ell$ for some integer $\ell$. Then $c = ak = (ab)\ell$ which is divisible by $ab$ since $\ell$ is an integer.

**Opt19.** Let $a$ be an integer, $p, q$ be primes, $p \neq q$. Prove: $(p \mid a) \wedge (q \mid a) \implies pq \mid a$.

**Opt19 - solution.** Two unequal primes $p, q$ are coprime: indeed, $p$ is not a divisor of $q$ because the only positive divisors of $q$ are $1$ and $q$, none of which is $p$. By a fact from the course, if an integer $q$ is not divisible by a prime $p$, then $q$ is coprime to $p$, as claimed.

Hence, by the previous question, $pq$ divides $a$.

**Opt20.** Let the relation $\sim$ on $\mathbb{Z}$ be defined by $a \sim b$ iff $5 \mid 9a^2 + b^2$.

a) Prove that $\sim$ is an equivalence relation.

b) Show that the equivalence class of $0$ is the set of all integers divisible by $5$.

c) Work out all the other equivalence classes induced by the relation $\sim$.

**Opt20 - solution.** a) See question **Q32**.

b) By definition, the equivalence class of $0$ is the set of all integers $a$ such that $a \sim 0$, which by symmetry of $\sim$ is the same as $0 \sim a$. By definition of $\sim$, $0 \sim a$ means that $5 \,|\, a^2$. Since $5$ is a prime, by Euclid's property of a prime $5 \,|(a \times a)$ implies that $5 \,|\, a$ or $5 \,|\, a$. Thus, every integer $a$ equivalent to $0$ is divisible by $5$.

Vice versa, if $a$ is divisible by $5$, then $5 \,|\, 9 \times 0^2 + a^2$ so $0 \sim a$.

We proved that an integer $a$ belongs to the equivalence class of $0$ with respect to $\sim$, if and only if $5 \,|\, a$, as required.

c) Observe that the integer $1$ does not belong to the equivalence class of $0$, because $1$ is not divisible by $5$. Let us find the equivalence class of $1$. By definition of $\sim$, $1 \sim a$ iff $5 \,|(9 + a^2)$. This is the same as $9 + a^2 \equiv 0 \mod 5$, which can be rewritten as $a^2 \equiv 1 \mod 5$.

By Modular Arithmetic, the remainder of $a^2$ mod $5$ depends only on the remainder of $a$. From the table

| $a \mod 5$ | $0$ | $1$ | $2$ | $3$ | $4$ |
|---|---|---|---|---|---|
| $a^2 \mod 5$ | $0$ | $1$ | $4$ | $4$ | $1$ |

we conclude that $a^2 \equiv 1 \mod 5$ is equivalent to $a \equiv 1$ or $a \equiv 4 \mod 5$. Hence the equivalence class of $1$ induced by $\sim$ is the set $[1]_5 \cup [4]_5$.

We notice that $2$ is neither divisible by $5$ nor in the set $[1]_5 \cup [4]_5$, hence $2$ belongs to an equivalence class which is disjoint from the two equivalence classes found so far. Let us find the equivalence class of $2$. Observe that $2 \sim a$ iff $5 \,|(36 + a^2)$, equivalently $36 + a^2 \equiv 0 \mod 5$, which can be rewritten as $a^2 \equiv 4 \mod 5$. From the table above, $a^2 \equiv 4 \mod 5$ is the same as $a \equiv 2$ or $a \equiv 3 \mod 5$. Hence the equivalence class of $2$ induced by $\sim$ is the set $[2]_5 \cup [3]_5$.

The three equivalence classes $[0]_5$, $[1]_5 \cup [4]_5$ and $[2]_5 \cup [3]_5$ found so far cover the whole set $\mathbb{Z}$, therefore these are all the equivalence classes induced by the relation $\sim$.

**Opt21.** Let the relation $\sim$ on the set $\mathbb{Z}_n$ be defined as follows: $[a]_n \sim [b]_n$ iff $\exists [x]_n \in \mathbb{Z}_n^*$, $[b]_n = [x]_n[a]_n$.

a) Use the properties of $\mathbb{Z}_n^*$, prove that $\sim$ is an equivalence relation on $\mathbb{Z}_n$.

b) Put $n = 14$. Find the equivalence classes induced on the set $\mathbb{Z}_{14}$ by the relation $\sim$.

**Opt21 - solution.** a) We show that $\sim$ is **reflexive**, that is, $[a]_n \sim [a]_n$ for every $[a]_n \in \mathbb{Z}_n$. Indeed, observe that $[1]_n \in \mathbb{Z}_n^*$ because $[1]_n$ is invertible, $[1]_n^{-1} = [1]_n$. We have $[a]_n = [1]_n[a]_n$, so by definition of $\sim$, $[a]_n \sim [a]_n$.

We show that $\sim$ is **symmetric**, that is, $[a]_n \sim [b]_n$ implies $[b]_n \sim [a]_n$. Assume that $[a]_n \sim [b]_n$, meaning that $[b]_n = [x]_n[a]_n$ for some $[x]_n \in \mathbb{Z}_n^*$. Elements of $\mathbb{Z}_n^*$ are invertible, hence there exists $[x]_n^{-1} \in \mathbb{Z}_n^*$. Multiplying the equation $[b]_n = [x]_n[a]_n$ through by $[x]_n^{-1}$, we obtain $[x]_n^{-1}[b]_n =$

$[1]_n[a]_n$, in other words $[a]_n = [x]_n^{-1}[b]_n$, which, since $[x]_n^{-1} \in \mathbb{Z}_n^*$, implies that $[b]_n \sim [a]_n$ as claimed.

We show that $\sim$ is **transitive**, that is, $[a]_n \sim [b]_n$ and $[b]_n \sim [c]_n$ implies $[a]_n \sim [c]_n$. Assume $[a]_n \sim [b]_n$ and $[b]_n \sim [c]_n$, which translates as $[b]_n = [x]_n[a]_n$ and $[c]_n = [y]_n[b]_n$ for some $[x]_n, [y]_n \in \mathbb{Z}_n^*$. Substituting the first equation into the second equation, we obtain $[c]_n = [y]_n[x]_n[a]_n$. The following fact is known from the course: $\mathbb{Z}_n^*$ is multiplicatively closed. This implies that $[y]_n[x]_n \in \mathbb{Z}_n^*$. Hence by definition of $\sim$ we have $[a]_n \sim [c]_n$. Transitivity is proved.

b) We note that $\mathbb{Z}_{14}^* = \{[1]_{14}, [3]_{14}, [5]_{14}, [9]_{14}, [11]_{14}, [13]_{14}\}$.

Let us work out the equivalence class of $[0]_{14} \in \mathbb{Z}_{14}$, induced by the relation $\sim$. Note that $[0]_{14} \sim [a]_{14}$ means that $[a]_{14} = [x]_{14}[0]_{14}$ for some $[x]_{14} \in \mathbb{Z}_{14}^*$. But this implies that $[a]_{14} = [0]_{14}$. We have shown that the equivalence class of $[0]_{14}$ induced by $\sim$ is the single-element set $\{[0]_{14}\}$.

Let us pick an element not equivalent to $[0]_{14}$ — say, $[1]_{14}$ — and work out its equivalence class. Note that $[1]_{14} \sim [a]_{14}$ means that $[a]_{14} = [x]_{14}[1]_{14} = [x]_{14}$ for some $[x]_{14} \in \mathbb{Z}_{14}^*$. This shows that the set of elements equivalent to $[1]_{14}$ in $\mathbb{Z}_{14}$ is exactly the set $\mathbb{Z}_{14}^*$.

Let us pick an element which is in neither equivalence class shown so far, say, $[2]_{14}$. By definition of $\sim$, the set of elements of $\mathbb{Z}_{14}$ equivalent to $[2]_{14}$ is obtained by multiplying $[2]_{14}$ by all elements of $\mathbb{Z}_{14}^*$. We show the results in the following table:

| $[x]_{14} \in \mathbb{Z}_{14}^*$ | $[1]_{14}$ | $[3]_{14}$ | $[5]_{14}$ | $[9]_{14}$ | $[11]_{14}$ | $[13]_{14}$ |
|---|---|---|---|---|---|---|
| $[x]_{14}[2]_{14}$ | $[2]_{14}$ | $[6]_{14}$ | $[10]_{14}$ | $[4]_{14}$ | $[8]_{14}$ | $[12]_{14}$ |

The equivalence class of $[2]_{14}$ is the set of elements of $\mathbb{Z}_{14}$ shown in the second row of this table.

The only element of $\mathbb{Z}_{14}$ which does not appear in the three equivalence classes found so far is $[7]_{14}$. Hence the only option for $[7]_{14}$ is to form an equivalence class by itself. Nevertheless, we check this by finding all possible elements equivalent to $[7]_{14}$, that is, elements of the form $[x]_{14}[7]_{14}$ where $[x]_{14}$ is in $\mathbb{Z}_{14}^*$:

| $[x]_{14} \in \mathbb{Z}_{14}^*$ | $[1]_{14}$ | $[3]_{14}$ | $[5]_{14}$ | $[9]_{14}$ | $[11]_{14}$ | $[13]_{14}$ |
|---|---|---|---|---|---|---|
| $[x]_{14}[7]_{14}$ | $[7]_{14}$ | $[7]_{14}$ | $[7]_{14}$ | $[7]_{14}$ | $[7]_{14}$ | $[7]_{14}$ |

We arrive at the following partition of $\mathbb{Z}_{14}$ into four equivalence classes, induced by the relation $\sim$:

$$\begin{aligned}\mathbb{Z}_{14}/\sim = \big\{\ & \{[0]_{14}\},\\ & \{[1]_{14}, [3]_{14}, [5]_{14}, [9]_{14}, [11]_{14}, [13]_{14}\},\\ & \{[2]_{14}, [6]_{14}, [10]_{14}, [4]_{14}, [8]_{14}, [12]_{14}\},\\ & \{[7]_{14}\}\ \big\}.\end{aligned}$$

**Opt22.** Let $a, b$ be integers. Prove that the following two statements about $a$ and $b$ are equivalent:

(1) $a$ and $b$ are not coprime;
(2) there exists a prime $p$ such that $p \mid a$ and $p \mid b$.

**Opt22 - solution.** To prove that (1) $\implies$ (2), assume that (1) is true, that is, $a$ and $b$ are not coprime. By definition of "coprime", this means that $\gcd(a,b) \neq 1$. There are two cases. First case is $\gcd(a,b) > 1$. By Fundamental Theorem of Arithmetic, every integer greater than $1$ is a product of primes, hence $\gcd(a,b)$ is a product of primes, and it is divisible by a prime $p$. We have $p \,|\, \gcd(a,b)$ and $\gcd(a,b) \,|\, a$, so by transitivity of $|$, $p \,|\, a$. Similarly, $p$ divides $b$.

Second case is $\gcd(a,b) = 0$. Then by definition of $\gcd$ one has $a = b = 0$. Then both $a$ and $b$ are indeed divisible by the same prime $p$, for example $p = 2$.

We now prove that (2) $\implies$ (1). Assume that there exists a prime $p$ such that $p \,|\, a$ and $p \,|\, b$. Recall that by Bezout's Lemma, $\gcd(a,b) = ma + nb$, an integral linear combination of $a$ and $b$. Hence $p$ divides $\gcd(a,b)$. This implies that $\gcd(a,b) \neq 1$, because $1$ is not divisible by any prime. By definition of "coprime", this means that $a$ and $b$ are not coprime.

**Opt23.** Let $[0]_4$, $[1]_4$, $[2]_4$, $[3]_4$ be the congruence classes of the integers modulo $4$; explain why there is only one prime in the set $[0]_4 \cup [2]_4 \subseteq \mathbb{Z}$ and show that $x, y \in [1]_4$ implies $xy \in [1]_4$. By considering integers of the form $4P - 1$, deduce that $[3]_4$ contains infinitely many primes.

**Opt23 - solution.** The integers contained in $[0]_4$ all have positive divisors $1$, $2$ and $4$ and so cannot be prime. The numbers contained in $[2]_4$ are all divisible by $1$ and $2$ and so cannot be prime, apart from $2$ itself. This means that the only primes contained in the union is $2$. If $x, y \in [1]_4$, then $x \equiv 1$ and $y \equiv 1 \mod 4$, so by Modular Arithmetic $xy \equiv 1 \times 1 \equiv 1 \mod 4$ meaning that $xy \in [1]_4$.

Now assume for contradiction that $p_1, \ldots, p_k$ is a finite list of all the primes in $[3]_4$, let $P = p_1 p_2 \ldots p_k$ and consider the integer $N = 4P - 1$. Note that $k \geq 1$ (since the prime $3$ is in $[3]_4$) so that $N > 1$. Furthermore, $N$ is not divisible by $2, p_1, \ldots, p_k$ (because these primes divide $4P$ and do not divide $-1$) and so the unique prime factorisation of $N$ must include only primes in $[1]_4$. However, a product of primes in $[1]_4$ must also lie in $[1]_4$, as shown above. Since $N \in [3]_4$, this is again a contradiction.

**Opt24.** Prove that if $n \in \mathbb{N}$ and $n \geq 3$, then $\phi(n)$ is even. Here $\phi$ is Euler's phi-function.

**Opt24 - solution.** Since $n > 1$, by the Fundamental Theorem of Arithmetic $n$ has prime factorisation. Write it as $n = p_1^{k_1} \ldots p_s^{k_s}$ where $s \geq 1$, $k_i \geq 1$ for all $i$, and $p_1, \ldots, p_s$ are distinct primes. By a formula proved in the course,

$$\phi(n) = \prod_{i=1}^{s} p_i^{k_i - 1}(p_i - 1).$$

If at least one of the primes $p_1, \ldots, p_s$ is odd (that is: any prime except $2$), the factor $(p_i - 1)$ in the formula for $\phi(n)$ is even, hence the whole product is even, and we are done.

It remains to consider the case where the only prime factor of $n$ is 2, that is, $n = 2^k$. Since we are given that $n \geq 3$, we conclude that $k \geq 2$, and so $\phi(n) = \phi(2^k) = 2^{k-1}(2-1)$ which is even as $k - 1 \geq 1$.

Thus, $\phi(n)$ is even in all cases when $n \geq 3$, as required.

**Opt25.** Prove Fermat's Little Theorem using Euler's theorem and properties of Euler's phi-function.

**Opt25 - solution.** Recall that Fermat's Little Theorem claims that if $p$ is a prime, then

(i) $a^p \equiv a \mod p$ for all integers $a$, and

(ii) $a^{p-1} \equiv 1 \mod p$ whenever $a$ is coprime to $p$.

Euler's theorem says that $a^{\phi(n)} \equiv 1 \mod n$ whenever $a$ is coprime to $n$.

Apply Euler's theorem in the case $n = p$. Observe that $\phi(p) = p - 1$ which is the most basic case of the formula $\phi(p^k) = p^{k-1}(p-1)$. We get the following statement: $a^{p-1} \equiv 1 \mod p$ for all $a$ coprime to $p$. We have thus proved statement (ii) of Fermat's Little Theorem.

It remains to prove statement (i). Let $a$ be an integer. We want to prove that $a^p \equiv a \mod p$. There are two cases: first case, $a$ is coprime to $p$. Then by (ii) which is already proved, $a^{p-1} \equiv 1 \mod p$; of course, $a \equiv a \mod p$ by reflexivity of congruence, so, multiplying these congruences, we obtain by Modular Arithmetic the required congruence $a^p \equiv a \mod p$.

Second case: $a$ is not coprime to $p$. By a result from the course, in this case $a$ is divisible by $p$. But then $a \equiv 0 \mod p$ and also $a^p \equiv 0 \mod p$. Hence the congruence $a^p \equiv a \mod p$ trivially holds. Fermat's Little Theorem is proved.