Concepts in Abstract Mathematics
MAT246 LEC0101 Winter 2020
Problem Set 2
Solutions

1. (a) Let a and b be relatively prime natural numbers greater than or equal to 2. Prove that $a^{\phi(b)} + b^{\phi(a)} \equiv 1 \pmod{ab}$.

(b) Find the remainder when $47^{144} + 185^{46} \cdot (46! + 2)^{46}$ is divided by 8695.

Solution.

(a) Since a and b are relatively prime, Euler's Theorem implies that $a^{\phi(b)} \equiv 1 \pmod{b}$ and $b^{\phi(a)} \equiv 1 \pmod{a}$. Thus, $b \mid a^{\phi(b)} - 1$ and $a \mid b^{\phi(a)} - 1$, so

$$ab \mid (a^{\phi(b)} - 1)(b^{\phi(a)} - 1),$$

which means that $(a^{\phi(b)} - 1)(b^{\phi(a)} - 1) \equiv 0 \pmod{ab}$. Hence, expanding the left-hand side, we get

$$a^{\phi(b)}b^{\phi(a)} - a^{\phi(b)} - b^{\phi(a)} + 1 \equiv 0 \pmod{ab}.$$

Since $a, b \geq 2$, we have $\phi(a), \phi(b) \geq 1$, so $ab \mid a^{\phi(b)}b^{\phi(a)}$ and hence $a^{\phi(b)}b^{\phi(a)} \equiv 0 \pmod{ab}$. Thus, we get $0 - a^{\phi(b)} - b^{\phi(a)} + 1 \equiv 0 \pmod{ab}$, so $a^{\phi(b)} + b^{\phi(a)} \equiv 1 \pmod{ab}$.

(b) Let $a = 47$ and $b = 185 = 5 \cdot 37$ so that $ab = 8695$. Since for any primes p, q, we have $\phi(p) = p - 1$ and $\phi(pq) = (p-1)(q-1)$, we get that $\phi(a) = 46$ and $\phi(b) = 4 \cdot 36 = 144$. Moreover, the canonical factorizations into primes of a and b are $a = 47$ and $b = 5 \cdot 37$, so they have no prime factor in common, and hence they are relatively prime. Thus, $47^{144} + 185^{46} \equiv 1 \pmod{8695}$ by part (a).

Now, a is prime so $a \mid (a-1)! + 1$ by Wilson's Theorem, and hence

$$ab \mid b \cdot ((a-1)! + 1).$$

In other words, $185 \cdot (46! + 1) \equiv 0 \pmod{8695}$, so

$$185 \cdot (46! + 2) \equiv 185 \cdot (46! + 1) + 185 \equiv 185 \pmod{8695}.$$

Hence,

$$47^{144} + 185^{46} \cdot (46! + 2)^{46} = 47^{144} + \big(185 \cdot (46! + 2)\big)^{46} \equiv 47^{144} + 185^{46} \equiv 1 \pmod{8695},$$

so the remainder is 1.

2. (a) Let p and q be primes. Prove that $\sqrt{pq}$ is rational if and only if $p = q$.

(b) Prove that $\sqrt{57} + \sqrt{n}$ is irrational for all $n \in \mathbb{N}$.

Solution.

(a) If $p = q$ then $\sqrt{pq} = \sqrt{p^2} = p$ is rational. For the converse, we give two different proofs.

Proof 1. Suppose, by contradiction, that $p \neq q$ and $\sqrt{pq} = \frac{a}{b}$ for some relatively prime numbers $a, b \in \mathbb{N}$. Then, $pqb^2 = a^2$, so $p \mid a^2$ and, since p is prime, this implies that $p \mid a$ (Lemma 7.2.2). Similarly, $q \mid a^2$, so $q \mid a$. Since p and q are distinct primes, they are relatively prime, so $pq \mid a$ (this was proved in Lecture 7 and is also a special case Q6 in PS1). Hence, $a = pqk$ for some $k \in \mathbb{N}$, so $pqb^2 = a^2 = p^2q^2k^2$ and hence $b^2 = pqk^2$. Repeating the same argument, we get that $p \mid b$ and $q \mid b$ so $pq \mid b$. Hence, $pq \mid a$ and $pq \mid b$ contradicting that a and b are relatively prime.

Proof 2. Suppose that $\sqrt{pq}$ is rational. Since the square root of a natural number is rational only if the square root is a natural number (Theorem 8.2.8), we have $\sqrt{pq} = n$ for some $n \in \mathbb{N}$. Hence, $pq = n^2$. Let $n = r_1^{\alpha_1} \cdots r_k^{\alpha_k}$ be the canonical factorization of n, so that $pq = r_1^{2\alpha_1} \cdots r_k^{2\alpha_k}$. Then, we must have that $p = q$, as otherwise, we get two canonical factorizations of the same number, where all the exponents of the first one (i.e. pq) are 1 while all the exponents of the second one (i.e. $r_1^{2\alpha_1} \cdots r_k^{2\alpha_k}$) are even, contradicting uniqueness of canonical factorizations.

(b) Note that $57 = 3 \cdot 19$ is the product of two distinct primes. (Side note: although 57 is not prime, it is often jokingly called the *Grothendieck prime*.) Hence, $\sqrt{57}$ is irrational by (a). Suppose, by contradiction, that $\sqrt{n} + \sqrt{57} = r \in \mathbb{Q}$. Then, $\sqrt{n} = r - \sqrt{57}$, so $n = (r - \sqrt{57})^2 = r^2 - 2r\sqrt{57} + 57$ and hence $\sqrt{57} = \frac{r^2+57-n}{2r} \in \mathbb{Q}$, contradicting that $\sqrt{57}$ is irrational. Hence, $\sqrt{n} + \sqrt{57}$ is irrational.

3. (a) Prove that if $z, w \in \mathbb{C}$ then $\overline{z+w} = \bar{z} + \bar{w}$.

(b) Prove that if $z, w \in \mathbb{C}$ then $\overline{zw} = \bar{z}\bar{w}$.

(c) Prove that if $r \in \mathbb{C}$ is a root of a polynomial with real coefficients, then $\bar{r}$ is also a root of that polynomial.

Solution.

(a) Let $z = a + bi$ and $w = c + di$, where $a, b, c, d \in \mathbb{R}$. Then,

$$\begin{aligned}\overline{z+w} &= \overline{(a+bi)+(c+di)} \\ &= \overline{(a+c)+(b+d)i} \\ &= (a+c)-(b+d)i \\ &= (a-bi)+(c-di) \\ &= \bar{z}+\bar{w}.\end{aligned}$$

(b) Let $z = a + bi$ and $w = c + di$, where $a, b, c, d \in \mathbb{R}$. Then,

$$\begin{aligned}\overline{zw} &= \overline{(a+bi)(c+di)} \\ &= \overline{(ac-bd)+(ad+bc)i} \\ &= (ac-bd)-(ad+bc)i \\ &= (ac-(-b)(-d))+(a(-d)+(-b)c)i \\ &= (a-bi)(c-di) \\ &= \bar{z}\bar{w}.\end{aligned}$$

(c) Let $p(z) = a_n z^n + a_{n-1} z^{n-1} + \cdots + a_1 z + a_0$ be a polynomial with $a_n \in \mathbb{R}$ and let $r \in \mathbb{C}$ be a root of $p(z)$, i.e. $p(r) = 0$. We want to show that $p(\bar{r}) = 0$. By (a), we have $\overline{a_1 z + a_0} = \overline{a_1 z} + \overline{a_0}$. Applying (a) again, we get $\overline{a_2 z^2 + a_1 z + a_0} = \overline{a_2 z^2} + \overline{a_1 z + a_0} = \overline{a_2 z^2} + \overline{a_1 z} + \overline{a_0}$. Hence, applying (a) n times, we get

$$\overline{a_n z^n + a_{n-1} z^{n-1} + \cdots + a_1 z + a_0} = \overline{a_n z^n} + \overline{a_{n-1} z^{n-1}} + \cdots + \overline{a_1 z} + \overline{a_0}$$

Now, by (b), we have $\overline{a_i z^i} = \overline{a_i}\overline{z^i} = \overline{a_i}\bar{z}^i$ for all i. But $a_i \in \mathbb{R}$, so $\bar{a}_i = a_i$ and hence we have shown that

$$\overline{a_n z^n + a_{n-1} z^{n-1} + \cdots + a_1 z + a_0} = a_n \bar{z}^n + a_{n-1} \bar{z}^{n-1} + \cdots + a_1 \bar{z} + a_0,$$

or in other words,

$$\overline{p(z)} = p(\bar{z}).$$

In particular, if $p(r) = 0$, then $p(\bar{r}) = \overline{p(r)} = \bar{0} = 0$.

4. Show that $|\mathbb{R}^n| = |\mathbb{R}|$ for all $n \in \mathbb{N}$.

Solution. We first show that $|\mathbb{R}^2| = |\mathbb{R}|$. Since $|\mathbb{R}| = |[0,1]|$ (Theorem 10.3.8), we also have $|\mathbb{R}^2| = |[0,1] \times [0,1]|$. Indeed, the equality $|\mathbb{R}| = |[0,1]|$ implies that there is a bijection $f : \mathbb{R} \to [0,1]$ and hence the function $F : \mathbb{R}^2 \to [0,1] \times [0,1]$ given by $F(x,y) = (f(x), f(y))$ is also a bijection. Now, we also showed that $|[0,1]\times[0,1]| = |\mathbb{R}|$ (Theorem 10.3.33) so we have $|\mathbb{R}^2| = |[0,1] \times [0,1]| = |\mathbb{R}|$. Hence, $|\mathbb{R}^2| = |\mathbb{R}|$ (the fact that if $|S| = |T|$ and $|T| = |U|$ then $|S| = |U|$ follows from the fact that if $f : S \to T$ and $g : T \to U$ are bijections, then $g \circ f : S \to U$ is a bijection since $f^{-1} \circ g^{-1}$ is an inverse).

Now, we show by induction on n that $|\mathbb{R}^n| = |\mathbb{R}|$ for all $n \in \mathbb{N}$. The base case $n = 1$ is trivial, since $\mathbb{R}^1 = \mathbb{R}$. Suppose that $|\mathbb{R}^k| = |\mathbb{R}|$ for some $k \in \mathbb{N}$. We want to show that $|\mathbb{R}^{k+1}| = |\mathbb{R}|$. Since $|\mathbb{R}^k| = |\mathbb{R}|$ we have a bijection $f : \mathbb{R}^k \to \mathbb{R}$. Then, $\mathbb{R}^{k+1} = \mathbb{R}^k \times \mathbb{R}$ and we have a bijection $g : \mathbb{R}^k \times \mathbb{R} \to \mathbb{R} \times \mathbb{R}$ given by $g(x,y) = (f(x), y)$, so $|\mathbb{R}^k \times \mathbb{R}| = |\mathbb{R} \times \mathbb{R}|$. Hence, $|\mathbb{R}^{k+1}| = |\mathbb{R}^k \times \mathbb{R}| = |\mathbb{R} \times \mathbb{R}| = |\mathbb{R}^2| = |\mathbb{R}|$. To show that g is a bijection, we show that it is both surjective and injective. It is injective since if $g(x_1, y_1) = g(x_2, y_2)$ then $(f(x_1), y_1) = (f(x_2), y_2)$ so $f(x_1) = f(x_2)$ and $y_1 = y_2$. Since f is injective, we have $x_1 = x_2$, so $(x_1, y_1) = (x_2, y_2)$. Now, g is also surjective since if $(x,y) \in \mathbb{R} \times \mathbb{R}$ then, since f is surjective, there exists $x_1 \in \mathbb{R}^k$ such that $f(x_1) = x$ so $g(x_1, y) = (f(x_1), y) = (x, y)$.

5. Find the cardinality of each of those sets.

(a) The set of lines in the plane.

(b) The set of circles in the plane whose centre has rational coordinates and whose radius is the square root of a prime number.

Solutions.

(a) We claim that the cardinality is c, the cardinality of $\mathbb{R}$.

First, a vertical line is uniquely determined by its intersection with the x-axis, and hence the set of vertical lines is in bijection with $\mathbb{R}$. A line that is not vertical is of the form $y = ax+b$ for unique $a, b \in \mathbb{R}$, and hence the set of non-vertical lines is in bijection with $\mathbb{R}^2$. Hence, the set of all lines in the plane is in bijection with $\mathbb{R}\cup\mathbb{R}^2$. Now, since $|\mathbb{R}| = |[0,1]|$ (Theorem 10.3.8) we have a bijection $f : \mathbb{R} \to [0,1]$ and since $|\mathbb{R}^2| = |\mathbb{R}|$ (Q5) and $|\mathbb{R}| = |(1,2]|$ (Theorem 10.3.7 and Theorem 10.3.8) we have another bijection $g : \mathbb{R}^2 \to (1,2]$. Hence, we can construct a function $h : \mathbb{R} \cup \mathbb{R}^2 \to [0,2]$ by defining $h(x) = f(x)$ for $x \in \mathbb{R}$ and $h(y,z) = g(y,z)$ for $(y,z) \in \mathbb{R}^2$. Then, h is a bijection since it has an inverse $k : [0,2] \to \mathbb{R}\cup\mathbb{R}^2$ defined by $k(x) = f^{-1}(x)$ if $x \in [0,1]$ and $k(x) = g^{-1}(x)$ if $x \in (1,2]$, where f^{-1} and g^{-1} are the inverses of f and g respectively. Hence, $|\mathbb{R} \cup \mathbb{R}^2| = |[0,2]| = |[0,1]| = |\mathbb{R}|$.

(b) Let C be the set of those circles. We claim that the cardinality of C is $\aleph_0$. Since C is infinite and $\aleph_0$ is the smallest infinite cardinality, we have $\aleph_0 \leq |C|$. Hence, by the Cantor-Bernstein Theorem, it suffices to show that $|C| \leq \aleph_0$. In other words, it suffices to show that C is countable.

A circle in C is uniquely specified by a pair of rational numbers $x, y \in \mathbb{Q}$ and a prime number p, where (x, y) are the coordinates of the centre and $\sqrt{p}$ is the radius. Hence, C is in bijection with $\mathbb{Q}^2 \times \mathbb{P}$, where $\mathbb{Q}^2 = \mathbb{Q} \times \mathbb{Q} = \{(x, y) : x, y \in \mathbb{Q}\}$ and $\mathbb{P} \subseteq \mathbb{N}$ is the set of prime numbers. We begin by proving the following lemma.

Lemma. *If S and T are countable sets, the so is $S \times T$.*

Proof. The set $S \times T$ is the union of the sets $\{s\} \times T$ for $s \in S$. Now, for all $s \in S$, the set $\{s\} \times T$ is in bijection with T, which is countable, so $\{s\} \times T$ is also countable. Since S is countable and the union of a countable number of countable sets is countable (Theorem 10.2.10), we have that $S \times T$ is countable. □

By this lemma, $\mathbb{Q}^2$ is countable. Also $\mathbb{P}$ is countable since $\mathbb{P} \subseteq \mathbb{N}$ and a subset of a countable set is countable. Hence, $\mathbb{Q}^2 \times \mathbb{P}$ by the lemma. So C is countable and infinite, and hence $|C| = \aleph_0$.

6. Show that a set S has infinitely many elements if and only if it has a subset $S_0 \subseteq S$ such that $S_0 \neq S$ and $|S_0| = |S|$.

Solutions. Suppose that S has infinitely many elements. Since $\aleph_0$ is the smallest infinite cardinality, we have $\aleph_0 \leq |S|$, so there is an injection $f : \mathbb{N} \to S$. Let $s_i = f(i)$, so that $s_1, s_2, s_3, \ldots$ is an infinite sequence of distinct elements of S. Let $S_0 = S \setminus \{s_1\}$. Then, $S_0 \neq S$ since $s_1 \notin S_0$. We claim that $|S_0| = |S|$. Define $g : S \to S_0$ by $g(s_i) = s_{i+1}$ for all $i \in \mathbb{N}$ and $g(x) = x$ if $x \neq s_i$ for all i. Then, g is bijective since it has an inverse $h : S_0 \to S$ defined by $h(s_i) = s_{i-1}$ for all $i \geq 2$ and $h(x) = x$ if $x \neq s_i$ for all i. Indeed, if $h(g(s_i)) = h(s_{i+1}) = s_i$ and if $x \neq s_i$ then $h(g(x)) = h(x) = x$. Similarly, $g(h(x)) = x$ for all $x \in S$. Hence, g is a bijection between S and S_0, so $|S| = |S_0|$.

Conversely, if S is finite and $S_0 \subseteq S$ is a subset such that $S_0 \neq S$, then $|S| = n$ for some $n \in \mathbb{N}$ and S_0 has strictly less elements than S, so $|S_0| = k$ for some $k < n$ and hence $|S_0| < |S|$.