Leonhard Euler
Fall 1737

Math 101 Homework 1

Problem 1.

(a) Prove that there is no rational number whose square is 2.

(b) Let n be an integer greater than 1. Prove that the nth root of any prime number p is irrational.

Solution. (a) Suppose that there is a rational number whose square is 2. Then we can find coprime nonzero integers a and b such that $a^2/b^2 = 2$. Then $a^2 = 2b^2$, so a^2 is even. It follows that a is even, so $a = 2k$ for some integer k. Then $2b^2 = 4k^2$, so $b^2 = 2k^2$, which implies that b^2 is even. But then b itself is even, which is a contradiction since a is even and a and b are coprime. Thus, there is no rational number whose square is 2.

(b) The polynomial $f = x^n - p$ is irreducible over $\mathbb{Z}$ by Eisenstein's criterion. By Gauss's Lemma, f is also irreducible over $\mathbb{Q}$. In particular, f has no roots in $\mathbb{Q}$, so the nth root of p is irreducible.

Problem 2. Let S be a dense subset of $\mathbb{R}$.

(i) Suppose $f : \mathbb{R} \to \mathbb{R}$ is continuous and $f(x) = 0$ for all $x \in S$.

   (A) Prove, using the *definition* of denseness, that $f(x) = 0$ for all $x \in \mathbb{R}$.

   (B) Prove, using the fact that a subset of $\mathbb{R}$ is dense if and only if it is *sequentially dense*, that $f(x) = 0$ for all $x \in \mathbb{R}$.

(ii) Suppose $f, g : \mathbb{R} \to \mathbb{R}$ are continuous and $f(x) = g(x)$ for all $x \in S$. Prove that $f(x) = g(x)$ for all $x \in \mathbb{R}$.

Solution. (i)(A) Let $x \in \mathbb{R}$ be given, and pick any $\varepsilon > 0$. Since f is continuous at x, there exists a $\delta > 0$ such that $|f(x) - f(y)| < \varepsilon$ for all $y \in \mathbb{R}$ such that $|x - y| < \delta$. Since S is dense in $\mathbb{R}$, there exists a number $y \in S \cap (x - \delta, x + \delta)$. Then $f(y) = 0$ and $|x - y| < \delta$. Therefore, $|f(x)| = |f(x) - f(y)| < \varepsilon$. Since $|f(x)| < \varepsilon$ for an arbitrary $\varepsilon > 0$, it follows that $f(x) = 0$. Since x was arbitrary, this shows that $f(x) = 0$ for all $x \in \mathbb{R}$.

(i)(B) Since S is a dense subset of $\mathbb{R}$, it is also sequentially dense (i.e., every real number is a limit of some sequence in S). Let $x \in \mathbb{R}$ be given, and choose a sequence $\{x_n\}$ in S that converges to x. For all $n \in \mathbb{N}$, we have $f(x_n) = 0$ since $x_n \in S$. Thus, $\{f(x_n)\} \to 0$. However, since f is continuous and $\{x_n\} \to x$, it must be the case that $\{f(x_n)\} \to f(x)$, so $f(x) = 0$. Since x was arbitrary, $f(x) = 0$ for all $x \in \mathbb{R}$.

(ii) Define $h : \mathbb{R} \to \mathbb{R}$ by $h(x) = f(x) - g(x)$. Then h is continuous and $h(x) = 0$ for all $x \in S$ (since $f(x) = g(x)$ for all $x \in S$). By part (i), it follows that $h(x) = 0$ for all $x \in \mathbb{R}$, so therefore $f(x) = g(x)$ for all $x \in \mathbb{R}$.

Problem 3 (Ahlfors §4.2.3 #2, p. 123)**.** Prove that a function which is analytic in the whole plane and satisfies an inequality $|f(z)| < |z|^n$ for some n and all sufficiently large $|z|$ reduces to a polynomial.

Solution. Since f is entire, we may write f as a power series centered at 0 which converges for every complex number z:

$$f(z) = \sum_{k=0}^{\infty} a_k z^k.$$

Let $R > 0$ be large enough such that $|f(z)| < |z|^n$ whenever $|z| \geq R$. Let γ be the positively oriented circle of radius R centered at the origin, parametrized as

$$\gamma(t) = Re^{it}, \qquad t \in [0, 2\pi].$$

For each $k \geq 0$ we have

$$\begin{aligned} a_k = \frac{f^{(k)}(0)}{n!} &= \frac{1}{2\pi i} \int_\gamma \frac{f(z)}{z^{k+1}}\, dz = \frac{1}{2\pi i} \int_0^{2\pi} \frac{f(\gamma(t))}{\gamma(t)^{k+1}} \gamma'(t)\, dt \\ &= \frac{1}{2\pi i} \int_0^{2\pi} \frac{f(Re^{it})}{R^{k+1} e^{i(t+1)t}} iRe^{it}\, dt = \frac{1}{2\pi R^k} \int_0^{2\pi} \frac{f(Re^{it})}{e^{ikt}}\, dt, \end{aligned}$$

and hence

$$\begin{aligned} |a_k| &= \frac{1}{2\pi R^k} \left| \int_0^{2\pi} \frac{f(Re^{it})}{e^{ikt}}\, dt \right| \leq \frac{1}{2\pi R^k} \int_0^{2\pi} \frac{|f(Re^{it})|}{|e^{ikt}|}\, dt \\ &= \frac{1}{2\pi R^k} \int_0^{2\pi} |f(Re^{it})|\, dt \leq \frac{1}{2\pi R^k} \int_0^{2\pi} R^n\, dt = \frac{R^n}{R^k} = \frac{1}{R^{k-n}}. \end{aligned}$$

If $k > n$, then letting $R \to \infty$ gives $|a_k| = 0$. Thus, we have $a_k = 0$ for $k > n$, so that

$$f(z) = a_0 + a_1 x + \cdots + a_n x^n.$$

That is, f is a polynomial.

Problem 4. Prove that there are infinitely many prime numbers.

Solution. Let P be the set of prime numbers. To prove that P has infinitely many elements, it suffices to prove that the series

$$\sum_{p \in P} \frac{1}{p} = \lim_{x \to \infty} \sum_{\substack{p \in P \\ p \leq x}} \frac{1}{p} \tag{4.1}$$

diverges. Suppose, for the sake of contradiction, that (4.1) converges. Then there is a positive real number M such that

$$\sum_{\substack{p \in P \\ p > M}} \frac{1}{p} < \frac{1}{2}. \tag{4.2}$$

Let $p_1, \ldots, p_n$ be the distinct prime numbers contained in the interval $[1, M]$, and let $Q = p_1 \cdots p_n$. For every positive integer N, define

$$S(N) = \sum_{n=1}^{N} \frac{1}{1 + nQ}$$

and let $P(N)$ be the finite set of primes q which divide $1 + nQ$ for at least one $n \in \{1, \ldots, N\}$. For each positive integer n, the integers Q and $1 + nQ$ are coprime, so none of the prime numbers $p_1, \ldots, p_n$ divide $1 + nQ$. It follows that

$$P(N) \subseteq P \cap (M, \infty) \tag{4.3}$$

for every positive integer N. If m is another positive integer, then we define $A(N, m)$ to be the set of all integers n such that $1 \leq n \leq N$ and such that $1 + nQ$ has exactly m (not necessarily distinct) prime divisors. Consider the sum

$$S(N, m) = \sum_{n \in A(N, m)} \frac{1}{1 + nQ}.$$

Observe that $S(N, m) = 0$ for m sufficiently large (since $A(N, m)$ is empty for m sufficiently large) and that

$$S(N) = \sum_{m=1}^{\infty} S(N, m). \tag{4.4}$$

If $n \in A(N, m)$, then $1+nQ = (q_1 \cdots q_m)^{-1}$ for some prime numbers $q_1, \ldots, q_m \in P(N)$, so

$$S(N,m) \leq \sum_{q_1,\ldots,q_m \in P(N)} \frac{1}{q_1 \cdots q_m} = \left(\sum_{p \in P(N)} \frac{1}{p} \right)^m.$$

It then follows from (4.2) and (4.3) that

$$S(N,m) \leq \left(\sum_{p \in P(N)} \frac{1}{p} \right)^m \leq \left(\sum_{\substack{p \in P \\ p > M}} \frac{1}{p} \right)^m < \frac{1}{2^m}$$

Now (4.4) implies that

$$S(N) = \sum_{m=1}^{\infty} S(N,m) \leq \sum_{m=1}^{\infty} \frac{1}{2^m} = 1.$$

Thus, the sequence $(S(N))_{N=1}^{\infty}$ is a monotone increasing bounded sequence, so it converges to the limit

$$\lim_{N\to\infty} S(N) = \lim_{N\to\infty} \sum_{n=1}^{N} \frac{1}{1+nQ} = \sum_{n=1}^{\infty} \frac{1}{1+nQ}.$$

However, the series above diverges (e.g., by the integral test), so we have reached a contradiction. It follows that the series (4.1) diverges.

Problem 5 (Atiyah-Macdonald 1.1)**.** Let x be a nilpotent element of a ring A. Show that $1 + x$ is a unit of A. Deduce that the sum of a nilpotent element and a unit is a unit.

Solution. Let $y = -x$. Then y is also nilpotent, so choose a positive integer n such that $y^n = 0$. We have

$$(1-y)(1+y+y^2+\cdots+y^{n-1}) = 1 - y^n = 1$$

which shows that $1 + x = 1 - y$ is a unit.

Next, let $x \in A$ be nilpotent and $u \in A$ a unit. Then $u^{-1}x$ is nilpotent, so $1 + u^{-1}x$ is a unit by the first part. Therefore

$$u + x = u(1 + u^{-1}x).$$

Since it is a product of units, $u + x$ is a unit.