MATH 8440

Problem Set 1

Due September 2, 2026

Instructions. Turn in at least 30 points worth of problems.

Problem 1. *the profinite (Furstenberg) topology on* $\mathbf{Z}$ (5 points) Look up the condition for a family of subsets of a set X to form a basis for a topology (X, τ). Prove that the sets $U_{a,m} = a + m\mathbf{Z}$, where a, m are integers with $0 \leq a < m$, form a basis for a topology on $\mathbf{Z}$.

Problem 2. (5 points) Euclid's lemma asserts that if p is prime and a, b are integers for which $p \mid ab$, then $p \mid a$ or $p \mid b$. Fill in the details of the following proof, which avoids the (now traditional) use of Bézout's lemma.

(a) Fix a prime p and an $a \in \mathbf{Z}$. Show that $I_{a,p} := \{b \in \mathbf{Z} : p \mid ab\}$ is an ideal of $\mathbf{Z}$ containing p.

(b) Using that $\mathbf{Z}$ is a principal ideal domain, show that $I_{a,p} = \mathbf{Z}$ or $p\mathbf{Z}$.

(c) Conclude.

The usual proof that $\mathbf{Z}$ *is a PID only requires the division algorithm. Hence, this proof — which is essentially Gauss's argument in his 1801* Disquisitiones Arithmeticae *— is not circular!*

Problem 3. (5 points) Show that if p is a prime divisor of the Fermat number $F_n = 2^{2^n} + 1$, where $n \geq 2$, then $2^{n+2} \mid p - 1$. (In class, we showed $2^{n+1} \mid p - 1$.)

This problem assumes you are familiar with one of the classical supplements to the law of quadratic reciprocity: 2 *is a square modulo an odd prime* $p \iff p \equiv \pm 1 \pmod 8$.

Problem 4. *more cases of Dirichlet's theorem* (10 points) Fix a prime p. For each integer $n \geq 0$, define $F_n^{(p)} = \frac{2^{p^{n+1}}-1}{2^{p^n}-1}$.

(a) Show that none of the numbers $F_n^{(p)}$, for $n = 0, 1, 2, \ldots$, are multiples of p.

(b) Show that if q is a prime for which $q \mid F_n^{(p)}$, then $2^{p^{n+1}} \equiv 1 \pmod q$ and $2^{p^n} \not\equiv 1 \pmod q$. Deduce that $p^{n+1} \mid q - 1$.

(c) Show that if m is any fixed power of p, then there are infinitely many primes $q \equiv 1 \pmod m$.

What happens when $p = 2$*?*

Problem 5. (10 points) Let a, m be integers with $m > 0$ and $\gcd(a, m) = 1$. Show that for every $N \in \mathbf{Z}^+$, there are infinitely many positive integers $n \equiv a \pmod m$ with $\gcd(n, N) = 1$. Do **not** assume Dirichlet's theorem on primes in progressions: your proof should use only the toolkit from a first course in number theory.

Problem 6. *Around composites of the form* $2^p - 1$ (10 points)

(a) Suppose p_1 is a prime, $p_1 \equiv 3 \pmod 4$, for which $p_2 = 2p_1 + 1$ is also prime. Prove that $2^{p_1} - 1$ is divisible by p_2. Hence, if there are infinitely many prime pairs p_1, p_2 of this form, then $2^p - 1$ is composite for infinitely many primes p.

(b) Let a and b be integers with $a \geq 2, b \geq 1$. Show that $a^p - b$ assumes infinitely many composite values as p ranges over the primes, except possibly when $a = 2$ and $b = 1$ (the troublesome case!).

You may assume Dirichlet's theorem on primes in arithmetic progressions for this part.

Problem 7. (3 points) Suppose we omit the condition $f(1) = 1$ in our definition of a multiplicative arithmetic function. Then there is precisely one more function that gets admitted to the club: which one?

Problem 8. (3 points) Suppose $f : \mathbf{Z}^+ \to \mathbf{C}$ has the following property:

Whenever $n \in \mathbf{Z}^+$ has canonical prime factorization $p_1^{e_1} \cdots p_k^{e_k}$, we have $f(n) = f(p_1^{e_1}) \cdots f(p_k^{e_k})$.

(Implicit here is the assertion that $f(1) = 1$, the value of the empty product.) Prove that f is multiplicative.

Problem 9. (12 points) Let p be an odd prime, and let G_p be the subgroup of $(\mathbf{Z}/p\mathbf{Z})^\times$ generated by 2. For example, $G_5 = (\mathbf{Z}/5\mathbf{Z})^\times$, while $G_7 = \{1, 2, 4\}$.

(a) Prove that there are infinitely many primes p for which $3 \notin G_p$.

Hint. Quadratic reciprocity and the supplementary laws may be helpful.

(b) Prove that there are infinitely many primes p for which $3 \in G_p$.

Probably $G_p = (\mathbf{Z}/p\mathbf{Z})^\times$ infinitely often, though this is still open. Under the "Generalized Riemann Hypothesis," $G_p = (\mathbf{Z}/p\mathbf{Z})^\times$ for about 37.4% of all primes p.

Problem 10. (5 points)

(a) For $n \in \mathbf{Z}$, define $\chi(n) = 0$ when n is even and $\chi(n) = (-1)^{(n-1)/2}$ when n is odd. Prove that $\chi(ab) = \chi(a)\chi(b)$ for all $a, b \in \mathbf{Z}$.

(b) Assume there are finitely many primes. Show that

$$1 - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} + \cdots = \prod_p \frac{1}{1 - \frac{\chi(p)}{p}}.$$

(c) By identifying the series on the left-hand side, derive a contradiction to the irrationality of π.

The displayed identity in (b) turns out to simply be true; one doesn't need to make a false assumption to derive it. But the proof is nontrivial.

Problem 11. (15 points) In class, we noted that

$$\left(\sum_{p \leq x} \frac{1}{p}\right)^k \leq k! \sum_{n \leq x^k} \frac{1}{n}.$$

By taking $k = \lfloor \log \log x \rfloor$, prove that there is a constant $C > 0$ such that, for all sufficiently large x,

$$\sum_{p \leq x} \frac{1}{p} \leq \log \log x + C \log \log \log x.$$

Start by using the proof of the integral test to show that $\log n! \leq \log n + \int_1^n \log t \, \mathrm{d}t$, for all positive integers n, and deduce an upper bound on $n!$.

Problem 12. (15 points) Let $\mathrm{Dir}(\mathbf{C})$ denote the collection of formal Dirichlet series with the operations of addition and multiplication discussed in class. You may take as known that $\mathrm{Dir}(\mathbf{C})$ is a commutative ring.

(a) Prove that $\mathrm{Dir}(\mathbf{C})$ is an integral domain.

(b) What are the units in $\mathrm{Dir}(\mathbf{C})$? Justify your answer.

(c) Interpret and prove the formal identity $\zeta(s-1) = \zeta(s)\sum_{n\geq 1}\phi(n)n^{-s}$, where ϕ is Euler's ϕ-function.

Problem 13. *(A bit more than) the irrationality of π^2* (20 points) We outline a proof, due to J.D. Dixon, that π is not the root of a polynomial over $\mathbf{Z}$ of degree at most 2. Suppose for the sake of contradiction that π is a root of

$$P(T) = aT^2 + bT + c,$$

where a, b and c are integers, not all vanishing.
Given a polynomial $f(T) \in \mathbf{R}[T]$, define

$$F(T) := f(T) - f^{(2)}(T) + f^{(4)}(T) - f^{(6)}(T) + \cdots. \tag{$\dagger$}$$

Then $F(T) \in \mathbf{R}[T]$. View F as a function of a real variable x.

(a) Check that

$$\frac{\mathrm{d}}{\mathrm{d}x}\big(F'(x)\sin x - F(x)\cos x\big) = f(x)\sin x,$$

and conclude that

$$\int_0^\pi f(x)\sin x\,\mathrm{d}x = F(\pi) + F(0). \tag{$\star$}$$

(b) With n a positive integer to be chosen shortly, let f be the polynomial

$$f(T) := \frac{1}{n!}P(T)^{2n}\big(P(T) - P(0)\big)^{2n}.$$

Show that the left-hand side of ($\star$) is strictly between 0 and 1 if n is sufficiently large.

We now fix such an n and derive a contradiction by showing that the right-hand side of ($\star$) is an integer.

(c) Show that $f^{(r)}(0) = f^{(r)}(\pi) = 0$ for all $0 \leq r < 2n$.

(d) If e and r are nonnegative integers and r is even, show that there is an expansion of the form

$$\frac{\mathrm{d}^r}{\mathrm{d}x^r}\big(P(x)^e\big) = \sum_{j=r/2}^{r} c_j j!\binom{e}{j}P(x)^{e-j}$$

for certain integers c_j.

(e) Use the result of part (d) to show that if e is a nonnegative integer and $r \geq 2n$ is even, then

$$\frac{1}{n!}\frac{\mathrm{d}^r}{\mathrm{d}x^r}\big(P(x)^e\big)$$

is a polynomial in $P(x)$ with integer coefficients. Conclude that $f^{(r)}(0)$ and $f^{(r)}(\pi)$ are integers.

(f) Referring back to definition ($\dagger$), deduce that $F(\pi) + F(0) \in \mathbf{Z}$.