Week 2: Number Theory

Instructions: This handout is meant to go over some basic Number Theoretic techniques and skills. The problems covered here are meant to be of the same level as the NMTC descriptive questions and above that. Problems marked at the end with (*) are a bit more tough (and fun!).
The problems covered here are meant to build your problem-solving skills, and as such, they are open-book. You are encouraged to use any textbook, video, or other online or offline resource as long as it doesn't give away the complete solution.
For each section, there are some worked examples. These examples are meant to show the applications of various techniques and how to approach more difficult problems. It is recommended that you try to attempt all the example problems before reading the solution.

1. Divisibility

This section is concerned with the basics of Number Theory. Surprisingly, the things considered 'basic' here are quite varied. We assume the reader is familiar with the concepts of greatest common divisors, divisibility and divisibility rules, the extremal principle, and some algebraic manipulation skills. It is **heavily** recommended that you consult a standard textbook along with this handout, as the theory covered is a bit expansive for newcomers. We have chosen to take the following lemmas/theorems as true without proof. If you wish, you can find elementary proofs online.
You will need the following for this handout:

1. Fundamental Theorem of Arithmetic: If a is a natural number, we can write $a = p_1^{r_1} p_2^{r_2} \cdots p_k^{r_k}$, where each p_k is a prime dividing a, and this expression is unique.

2. For p prime, if $p \mid ab$, then either $p \mid a$ or $p \mid b$, or both.

3. $a \mid b \iff p \mid b$, for all primes p such that $p \mid a$.

4. We say two numbers a, b are relatively prime, or coprime, if we have $gcd(a, b) = 1$, where the $gcd(a, b)$ represents their greatest common divisor.

5. If we have $gcd(a, b) = d$, then there exist integers x, y (not necessarily unique) such that $ax + by = d$.

6. We have that $gcd(a, b) = gcd(a + kb, b)$ for any integer k

7. Euclidean Algorithm: If we have 2 numbers a, b then there exist a unique pair of integers (q, r) such that $a = bq + r$, where we have $0 \leq r < b$.
   Additionally, we have that $gcd(a, b) = gcd(b, r)$

8. Let $p \mid a$. We say p^t *fully divides* a if we have $p^t \mid a$, but $p^{t+1} \nmid a$. We write this as $p^t \mid\mid a$.

Example 1.1 Find all positive integers n such that $n(n+1)$ is a perfect square.

Solution. We write $n(n+1) = k^2$ for some integer k. If p is a prime such that $p^t \mid\mid n$ OR $p^t \mid\mid n+1$, then $p^t \mid\mid k^2$, and so t is even. Thus, any prime in the prime factorization of either n or $n+1$ must have an even exponent. This implies that n and $n+1$ are both perfect squares, which is impossible unless n=0. Since this is not a positive integer, then our original question has no solutions.
Note: It is a common idea to work with the prime divisors of a number as they have nice properties.

Example 1.2 (IMO 1959 P1) Prove that, for all positive integers n, the fraction $\dfrac{21n+4}{14n+3}$ is irreducible.

Solution. The fraction being irreducible simply means that the numerator and denominator have no common factors, so it suffices to prove that their *gcd* is 1. We write:

$$\begin{aligned} &21n+4 = (14n+3) + (7n+1) \implies \\ &14n+3 = 2(7n+1) + 1 \end{aligned}$$

By the euclidean algorithm, we have

$$gcd(21n+4, 14n+3) = gcd(14n+3, 7n+1) = gcd(7n+1, 1) = 1$$

Example 1.3 Prove that for all integers n:

(a) $n^5 - 5n^3 + 4n$ is divisible by 120

(b) $n^2 + 3n + 5$ is not divisible by 121

Solution.

(a) We factor and get $n^5 - 5n^3 + 4n = n(n-1)(n+1)(n-2)(n+2)$.
The above expression is the product of 5 consecutive integers. One of these is divisible by 5, one is divisible by 4, at least one these is divisible by 3, and at least 2 are divisible by 2. This tells us that the expression is divisible by $2 * 3 * 4 * 5 = 120$.

(b) Observe that $n^2 + 3n + 5 = (n+7)(n-4) + 33$.
For it to be divisible by 121, it must be divisible by 11. Since 33 is divisible by 11, we must have that $11 \mid (n+7)(n-4)$. Hence, $11 \mid (n+7)$ or $11 \mid (n-4)$.
Note that $7 \equiv -4 \mod 11$, so $n+7 \equiv n-4 \mod 11$. Thus 11 divides both $(n+7)$ and $(n-4)$. Thus the original expression is congruent to 33 mod 11, and so is not divisible by 121.

Note: The main idea here consists of various factorizations. Indeed, these can be very useful, and the techniques covered in last week's Algebra handout can come in useful here.

Example 1.4 Find all primes a, b, c such that $ab + bc + ac > abc$

Solution. Notice that since the ordering does not matter, we may assume that $a \leq b \leq c$.
We thus get

$$\begin{aligned} &abc < ab + bc + ac \leq bc + bc + bc = 3bc \implies \\ &abc < 3bc \implies \\ &a < 3 \implies \\ &a = 2 \end{aligned}$$

The original equation now reduces to $2b + 2c > bc$. Dividing both sides by $2bc$ gives

$$\frac{1}{b} + \frac{1}{c} > \frac{1}{2}$$

It is easy to see that if $b \geq 5$, then the inequality is violated. Thus, $b < 5$, so $b = 2$ or $b = 3$. Plugging these values into the original equation and solving for c gives us the solutions $(a, b, c) = (2, 2, p), (2, 3, 3), (2, 3, 5)$ where p is any prime.
Note: The main idea here consists of bounding the variables via approximate inequalities.

Example 1.5 Let p be a prime number. Find all $k \in \mathbb{Z}$ such that $\sqrt{k^2 - pk}$ is a positive integer.

Solution. In cases involving prime numbers, it is useful to consider $p = 2$ separately, since 2 is the only even prime. If $p = 2$, then:

$$k^2 - 2k = (k - 1)^2 - 1$$

must be a perfect square, which is impossible.
Thus we assume that p is odd.
If $p \mid k$, then we write $k = np$, which tells us that $np(np - p) = p^2 n(n - 1)$ is a perfect square. For this to be true, n and $n - 1$ must both be perfect squares, which is impossible.
We thus know that $p \nmid k$. Hence, $gcd(k, k - p) = 1$, and by Example Problem 1.1, we know that both these numbers must be perfect squares. We now write $k = m^2, k - p = n^2$ for some natural n, m, and so

$$p = m^2 - n^2 = (m + n)(m - n)$$

Since p is prime, this implies

$$m + n = p, m - n = 1$$

Solving for m gives $m = \frac{p+1}{2}$. Plugging in for k gives $k = \frac{(p+1)^2}{4}$, where p is odd. It must also be checked that this solution works, but it's easy to verify in this case and so we omit it.

Example 1.6 (EGMO 2025 P1) For a positive integer N, let $c_1 < c_2 < \cdots < c_m$ be all positive integers smaller than N that are coprime to N. Find all $N \geq 3$ such that

$$\gcd(N, c_i + c_{i+1}) \neq 1$$

for all $1 \leq i \leq m-1$

Solution. One should start by trying to understand the statement and working with some small values of N to get a idea of what numbers work. For $N = 3$, we have $gcd(3, 1+2) = 3$ so it works.
$N = 4$ has $gcd(4, 1+3) = 4$ so it too works but $N = 5$ doesn't as $gcd(5, 1+2) = 1$.
We have that only $N = 6, 8, 9, 10, 12, 14, 16$ work for $N \leq 16$.
This leads us to believe that only N which are even or powers of 3 work. Trying $N = 27$ seems to suggest this even more.
To show that all even N work, we simply note that all the numbers coprime to it are odd and the sum of any two odd numbers is even. Hence, $2 \mid gcd(N, c_i + c_{i+1})$
To show that all N which are powers of 3 work. We notice that any number coprime to it is of the form $3k+1$, or $3k+2$ for some natural k. Further, note that depending on wether $c_i \equiv 1, 2 \bmod 3$, we have:

$$\begin{aligned} c_i + c_{i+1} &= (3k+1) + (3k+2) \qquad or \qquad (3k+2) + (3k+4) \\ &= 6k+3 \qquad or \qquad 6k+6 \end{aligned}$$

Hence, we must have $3 \mid gcd(N, c_i + c_{i+1})$
All that's left is to show that no other odd N work...but how?
After some tinkering, we make the observation that we must have

$$\begin{aligned} 1 &\neq gcd(N, (N-1) + (N-2)) \\ &= gcd(N, 2N-3) \\ &= gcd(N, 3) \end{aligned}$$

Since $N-1$ and $N-2$ are coprime with N. Hence, $3 \mid N$

It is now natural to write $N = 3^k m$ where m is the odd part of N and k is a natural number with $3 \nmid m$. We should now analyze m as this factor somehow makes odd N not work.
The key step is now to realize that we must have one of $3 \mid m+1, m-1$. For the first case, it follows that $m-1$ and $m+2$ are coprime with N whilst m and $m+1$ are not. It follows that we must have

$$gcd(N, (m-1)+(m+2)) = gcd(3^k m, 2m+1)$$

But

$$gcd(m, 2m+1) = gcd(3^k, m+1) = 1$$

It follows that $gcd(3^k m, 2m+1) = 1$. We can do a similar argument for the case $3 \mid m-1$. Hence, no N of the form $3^k m$ for natural k and odd m work and we're done.
Note: The above problem was indeed a bit challenging, it is covered here so that the reader can get some experience on how to approach and think about such problems.

Problems

The problems are ordered roughly in order of difficulty though it may or may not be accurate. You can ask us for hints in the gc or ask for more problems if you aren't satisfied with the ones provided! The last few problems are a bit tough!

Problem 1.1 Prove that the fraction

$$\frac{n^5+n+1}{n^2+2n+1}$$

Is irreducible for any natural number n.

Problem 1.2 Find all natural numbers n such that the numbers $4n-3$, $5n+3$, $3n-4$ are all prime.

Problem 1.3 Let a, b, x, y be natural numbers.

(a) Prove that $7 \mid 3a+2b$ if, and only if, $7 \mid 4a+5b$.

(b) Prove that $11 \mid 7x-3y$ if, and only if, $11 \mid 4x+14y$

Problem 1.4 Find all natural numbers a, b with $gcd(a, b) = 1$ such that

$$a + b \mid b^2 - 3ab$$

Problem 1.5 (AHSME 1976) Suppose p and q are primes, and that $x^2+q = px$ has distinct, integral roots. Find p and q.

Problem 1.6 For any positive integral a, b, and c, prove that the number $ab + bc + ca + b^2$ is never prime.

Problem 1.7 Let a and b be positive integers.

(a) Show that if $gcd(a, b) = 1$, then $gcd(a + b, ab) = 1$.

(b) Show that if $gcd(a, b) = 1$, then $gcd(a + b, a^2 - ab + b^2) = 1$ or 3.

Problem 1.8 (Quite Useful) Show that for any natural a, b, we have that $gcd(a, b) \cdot lcm(a, b) = ab$

Problem 1.9 Prove that any two consecutive Fibonacci numbers are co-prime

Problem 1.10 (All Russia Mathematics Olympiad 1995) Ler m, n be positive integers such that

$$gcd(m, n) + lcm(m, n) = m + n$$

Show that either $m \mid n$ or $n \mid m$

Problem 1.11 Let a be a natural number and let p be a prime. Show that for all natural k with $0 < k < p$ we have that $\binom{p^a}{k}$ is a multiple of p.

Problem 1.12 (2010 BAMO P1) We write $S = \{a, b, c\}$ for the set of three distinct positive integers a, b, c. For each possible subset of S, we consider the sum of the elements of that subset. For example, if $S = \{2, 3, 4\}$, then possible sums include $2, 3, 4, 5, 6, 7, 9$. Note that 4 of these sums are prime. Find the maximal numbers of such sums which can be prime.

Problem 1.13 Show that for all natural $n > 1$, the number $n^4 + 4^n$ is composite.

Problem 1.14 Let n be a non-negative integer. For what values of n is the number $4^{2n} + 4^n + 1$ prime?

Problem 1.15 (2026 Spanish Girls MO P2) Determine all integers $d \geqslant 1$ such that there exist positive integers $a \neq b$ satisfying $gcd(a, b) = d$ and $a + b \mid a^2 + b^2$

Problem 1.16 (Quite Useful) Let a, m, n be positive integers. Prove that

$$gcd(a^m - 1, a^n - 1) = a^{gcd(m,n)} - 1$$

A Hint[1]

Problem 1.17 (2022 Turkey JBMO TST P1) Let a, b be positive integers. Suppose that $(a - b)^2 \mid a^2 + b^2$. Prove that $(a - b)^3 \mid a^3 + b^3$.

Problem 1.18 Find all positive integers a, b, c which satisfy the equation:

$$a!b! = a! + b! + c!$$

Problem 1.19 (2009 Japan MO Finals P1) Find all positive integers n such that $8^n + n$ is divisible by $2^n + n$.

Problem 1.20 (2023 Kazakhstan District Olympiad 11th Grade) Find all natural numbers a, b, c such that

$$a + (b, c) = b + (c, a) = c + (a, b).$$

Where $(x, y) = gcd(x, y)$.

Problem 1.21 (1995 Russian MO) Suppose an infinite sequence of positive integers a_1, $a_2, \cdots$ satisfies the condition

$$gcd(a_i, a_j) = gcd(i, j)$$

for any natural numbers $i \neq j$. Show that $a_n = n$ for all natural numbers n.

[1] Suppose $m \geq n$. Use the Euclidean Algorithm to reduce m into a smaller integer.

Problem 1.22 (APMO) Are there distinct prime numbers a, b, and c which satisfy

$$a \mid bc + b + c, \quad b \mid ca + c + a, \quad c \mid ab + a + b$$

Problem 1.23 (2022 USAMO P4)(*) Find all pairs of primes (p, q) for which $p - q$ and $pq - q$ are both perfect squares.

Problem 1.24 (2012 EGMO P5)(*) The numbers p and q are prime and satisfy

$$\frac{p}{p+1} + \frac{q+1}{q} = \frac{2n}{n+2}$$

for some positive integer n. Find all possible values of $q - p$.

Problem 1.25 (2020 USEMO P1)(*) Which positive integers can be written in the form

$$\frac{\operatorname{lcm}(x, y) + \operatorname{lcm}(y, z)}{\operatorname{lcm}(x, z)}$$

for positive integers x, y, z?

2. Modular Arithmetic and Euler's Theorem

This section will go over modular arithmetic. It is assumed that the reader is familiar with the following results and definitions.

1. We denote by $\phi(n)$ the number of integers less than n, that are relatively prime to n. For example $\phi(2) = 1, \phi(3) = 2, \phi(10) = 4$.
2. We have that $\phi(n) = n \times \prod_{p,p|n} \left(1 - \frac{1}{p}\right)$.
3. For any two coprime integers a, n, we have $a^{\phi(n)} \equiv 1 \mod n$. As a corollary we have $a^t \mod n \equiv a^{t \mod \phi(n)} \mod n$.
4. Wilson's Theorem: Let n be an integer. We have $(n-1)! \equiv 1 \mod n$ if and only if n is prime.

Example 2.1 For how many integer values of i, $1 \leq i \leq 1000$, does there exist an integer j, $1 \leq j \leq 1000$, such that i is a divisor of $2^j - 1$?

Solution. Notice that if i is even, it can not divide $2^j - 1$, and hence i is odd. By Euler's Theorem, it is easy to see that if $j = \phi(i)$, then

$$2^j \equiv 1 \mod i$$

Since $\phi(i) < i$, it follows that a value of j satisfying the equation always holds if i is odd. Thus, there are 500 such values of i.

Example 2.2 How many prime numbers p are there such that $29^p + 1$ is a multiple of p?

Solution. Notice that $p = 29$ does not work. Hence, $p \neq 29$ and so $\gcd(p, 29) = 1$. By Fermat's Little Theorem(A special case of Euler's Theorem), we have

$$29^p + 1 \equiv 29 + 1 \equiv 30 \mod p$$

This implies $p \mid 30$, so $p = 2, 3, 5$. So there are a total of 3 numbers satisfying the equation.

Example 2.3 Find all primes p and q such that $p + q = (p - q)^3$

Solution. We notice that if $p = q$, then $p = 0$ which is a contradiction. Hence $p \neq q$ and $\gcd(p, q) = 1$.
If we try reducing the equation mod p and mod q and rearranging, we get

$$\begin{aligned} q + q^3 &\equiv 0 \mod p \\ p - p^3 &\equiv 0 \mod q \end{aligned}$$

Since q and p are both prime, this tells us that $p \mid q^2 + 1$ and $q \mid 1 - p^2$. If you try to play around with this information, you won't find it too useful. Instead, notice that the RHS is equal to $p + q$ and since any number divides itself, we must have that $p + q \mid RHS = (p - q)^3$. We thus reduce the given equation $\mod p + q$. We have first:

$$\begin{aligned} &p + q \equiv 0 \mod p + q \implies \\ &p - q \equiv -2q \mod p + q \implies \\ &0 \equiv (p - q)^3 \equiv (-2q)^3 \equiv 8q^3 \mod p + q \end{aligned}$$

Thus $p + q \mid 8q^3$, but we also have that $\gcd(p + q, q) = 1$(since p and q are both primes) and so $p+q$ and q^3 *also* have no common factors. Thus $p+q \mid 8$ and so $p + q \in \{1, 2, 4, 8\}$.
Since p, q are both primes, we must have $p + q = 8$(You can see the other 3 possibilities don't work simply by listing them out) so the only possible solutions are $(p, q) = (3, 5)$ or $(p, q) = (5, 3)$

Note While doing this problem, you also could have reduced both sides mod $p - q$ and gotten $p - q \mid 2q$ which tells you that $p - q \mid 2$ and hence $p - q = 1, 2$. Plugging these into the original equation would have given you $p + q = 8$, just as we got above.

Example 2.4 Prove the following statement: Let p be a prime. There exists an x with $x^2 \equiv -1 \mod p$ if and only if $p \equiv 1 \mod 4$

Solution. We start by proving the forward direction. We would like to use the fact that p is prime somehow, so Euler's Theorem is the most obvious

place to start. We want to get a $p-1$ in the exponent so we proceed as follows. Suppose there is an x such that $x^2 \equiv -1 \mod p$. This gives us:

$$(x^2)^{\frac{p-1}{2}} \equiv (-1)^{\frac{p-1}{2}} \mod p \implies$$
$$1 \equiv x^{p-1} \equiv (-1)^{\frac{p-1}{2}} \mod p$$

which is possible only if $\frac{p-1}{2}$ is even, which is equivalent to saying $p \equiv 1 \mod 4$.
For the reverse direction, we must prove that if $p \equiv 1 \mod 4$ then there exists an x satisfying the equation in the problem statement. If p is prime, then by Wilson's Theorem, this reduces to finding an x such that:

$$x^2 \equiv (p-1)! \mod p$$

Notice that we have

$$\begin{aligned}(p-1)! &\equiv [(1)(p-1)][(2)(p-2)]\cdots[(\frac{p-1}{2})(\frac{p+1}{2})] \mod p \\ &\equiv [(1)(-1)][(2)(-2)]\cdots[(\frac{p-1}{2})(-\frac{p-1}{2})] \mod p \\ &\equiv (-1)^{\frac{p-1}{2}}[(\frac{p-1}{2}!)]^2 \mod p\end{aligned}$$

Thus $x = (\frac{p-1}{2})!$ solves the equation(Why? Where did we use the condition that $p \equiv 1 \mod 4$?) and we are done.

Problems

The problems are ordered roughly in order of difficulty though it may or may not be accurate. You can ask us for hints in the gc or ask for more problems if you aren't satisfied with the ones provided! The last few problems are a bit tough!

Problem 2.1 Let $a_n = 6^n + 8^n$. Find the remainder on dividing a_{83} by 49.

Problem 2.2 Calculate the last 3 digits of $2008^{2007^{\cdots^{2^1}}}$ (*)

Problem 2.3 Find all primes that can be written as both the sum of two primes and as the difference of two primes.

Problem 2.4

(a) Let a be a positive integer. Prove that any prime factor > 2 of $a^2 + 1$ is of the form $4m + 1$

(b) Prove that there are infinitely many primes of the form $4m + 1$

Problem 2.5 Let p be a prime such that $p \equiv 2 \mod 3$.
Prove:
If $a^3 \equiv b^3 \mod p$, then $a \equiv b \mod p$

Problem 2.6 Let $p > 2$ be a prime number such that $3 \mid p - 2$.
Let $S = \{y^2 - x^3 - 1 : 0 \leq x, y \leq p - 1 \cap x, y \in \mathbb{Z}\}$.
Prove that there are at most p elements of S that are divisible by p. (Hint: Use the previous problem).

Problem 2.7 Prove that there are no positive integers x, k and $n \geq 2$ such that $x^2 + 1 = k(2^n - 1)$. (Hint: Do you notice any similarities with Example 2.4?)

Problem 2.8 Let a, b be positive integers and p, q be prime numbers for which $p \nmid q - 1$ and $q \mid a^p - b^p$. Prove that $q \mid a - b$.

Problem 2.9 Let a be a positive integer and p a prime such that $GCD(a, p!) = 1$. Prove that

$$p! \mid a^{(p-1)!} - 1$$

Disclaimer You will need the following definition for Problems 2.10-2.14 and 2.16.

Definition The order of $a \mod m$ is the smallest positive integer x such that $a^x \equiv 1 \mod m$. We denote this by $ord_m a$. Note that the order exists only if a, m are coprime.

Problem 2.10 Prove that the order of $a \mod m$ is less than or equal to $\phi(m)$

Problem 2.11 Let a, m be coprime integers. Prove the following statement:
$a^n \equiv 1 \mod m$ if and only if $ord_m a \mid n$.

Problem 2.12 Prove that if p is prime, then every prime divisor of $2^p - 1$ is greater than p.(Hint: You will need the previous 2 exercises)

Problem 2.13 Let n be an integer with $n \geq 2$. Prove that n does not divide $2^n - 1$.

Problem 2.14 Prove that for all positive integers $a > 1$ and n, we have $n \mid \phi(a^n - 1)$.

Problem 2.15 If p is an odd prime, and a, b are coprime, show that

$$\gcd(\frac{a^p + b^p}{a + b}, a + b) \in \{1, p\}$$

Hint: Consider the expansion of $\dfrac{a^p + b^p}{a + b}$

Problem 2.16 (2014 Cyprus IMO TST3 P1) Given a natural number $n \geq 2$, such that $n|3^n + 4^n$. Prove that $7|n$.