MAU22103/33101 - Introduction to Number Theory

Exercise Sheet 1

Trinity College Dublin

Course homepage

Answers are due for September 28th, 2pm.
The use of electronic calculators and computer algebra software is allowed.

Exercise 1 *Divisibility of Fibonacci numbers (100pt)*

Define the Fibonacci numbers numbers by $F_0 = 0$, $F_1 = 1$, and

$$F_{n+1} = F_n + F_{n-1} \quad \text{for all } n \geq 1.$$

The Fibonacci numbers are an example of a *strongly divisible sequence*:

$$\gcd(F_m, F_n) = F_{\gcd(m,n)}.$$

The goal of this problem is to prove this.

1. (10pts) Show that $\gcd(F_n, F_{n+1}) = 1$ for every $n \in \mathbb{N}$.
2. (20pts) By induction, or otherwise, establish Honsberger's Identity:

$$F_{m+n} = F_{m-1}F_n + F_m F_{n+1} \quad \text{for all } m, n \in \mathbb{N}.$$

Hint: If inducting on m, assume the identity holds for all n in your induction hypothesis, or use strong induction with more than one base *case. If trying to prove this otherwise, consider tilings of an $m + n - 1$ grid by dominoes, or derive an explicit formula for the Fibonacci numbers.*

3. (20pts) Using this identity, show that for $n \geq m$, if $m|n$, then $F_m|F_n$.

   Hint: Write $n = mk$ and induct on k.

4. (20pts) Establish the converse for $n \geq m > 2$: if $F_m|F_n$, then $m|n$.

   Hint: Divide n by m with remainder, and apply the results already established.

5. (20pts) Prove that, for $n > m$, $\gcd(F_m, F_n) = \gcd(F_{n-m}, F_m)$.

   Hint: Recall that $\mathrm{Div}(a, b) = \mathrm{Div}(b, a - bk)$ for any integers a, b, k.

6. (10pts) Hence conclude that $\gcd(F_m, F_n) = F_{\gcd(m,n)}$

This was the only exercise that you must submit before the deadline. The following exercises are not mandatory; they are not worth any points, and you do not have to submit them

However, I strongly encourage you to give them a try, as the best way to learn number theory is through practice.

The exercises marked with a star are the exercises I will try to talk about in the tutorial lecture. If there are any exercises would would particularly like to discuss, please let me know

The exercises are arranged by theme, and roughly in order of difficulty within each theme, with the first few working as good warm-ups, and the remainder being of similar difficulty to the main exercise. You are welcome to email me if you have any questions about them. The solutions will be made available with the solution to the main exercise.

Exercise 2 *Divisibility* ★

Prove the following for $n \in \mathbb{N}$:

(i) $5|n$ if and only if the last digit of n (in base 10) is 0 or 5.

(ii) $2|n$ if and only if 2 divides the last digit (in base 10) of n.

(iii) $4|n$ if and only if 4 divides the last two digits (in base 10) of n.

(iv) $8|n$ if and only if 8 divides the last three digits (in base 10) of n.

(v) $2^k|n$ if and only if 2^k divides the last k digits (in base 10) of n.

(vi) $3|10a-2$ if $3|a+1$.

(vii) An prime number k divides n^2-1 if and only if $k|n-1$ or $k|n+1$.

Exercise 3

In the following, try to resolve the question without finding explicitly finding roots of the polynomials.

(i) Prove that $4x^2-2x+13$ has no integer roots.

(ii) Prove that $3x^3-282x^2+18x-28$ has no integer roots.

(iii) Prove that, for any integers s,t,u,v, at least one of st, $sv+tu$, and uv is even. Hence conclude ax^2+bx+c has no rational roots if a,b,c are all odd.

Exercise 4 *Applying the algorithm* ★

Compute the following:

$$i)\,\gcd(72,18),\quad ii)\,\gcd(168,124),\quad iii)\,\gcd(1047,282),$$

$$iv)\,\gcd(n,2n+1),\quad v)\,\gcd(21n+4,14n+3).$$

Exercise 5 *Bézout's Theorem applied*

Prove that 2024 and 285 are coprime and determine integers u and v such that

$$2024u+285v=1.$$

Exercise 6 *Antimatter stamps are forbidden* ★

How many ways are there to pay for exactly €10.73 worth of postage if the post office will only sell you stamps worth 10c and 15c? How many ways are there to pay for exactly €10.75 worth of postage?

Note: The post office will not give change, even in the form of stamps. You cannot give antimatter stamps to cancel out regular stamps. You have to use a non-negative integer number of the stamps available to you.

Exercise 7 *Coprime products*

Let $a, b, c \in \mathbb{N}$. Prove that if a and b are coprime, and a and c are coprime, then a and bc are coprime

Exercise 8 *Primes and factorisations*

(i) Write 2024 as a product of prime factors, and explain why each factor is prime.

(ii) Hence or otherwise, work out the number of divisors of 2024 and their sum.

(iii) Check the time on a 24 hour clock. Do the above computations for the time interpreted as a four digit number.

(iv) Find all integers $M \in \mathbb{N}$ of the form $3^a 5^b$ such that the sum of the positive divisors of M is 33883.

Hint: $33883 = 31 \times 1093$*, and both factors are prime.*

(v) Determine all $n \geq 2$ for which $n^2 - 1$ is prime.

Exercise 9 *Valuations of primes*

(i) Let $m = \prod_i p_i^{a_i}$, $n = \prod_i p_i^{b_i}$ be two integers, where the p_i are pairwise distinct primes. Prove that $m \mid n$ iff. $a_i \leqslant b_i$ for each i.

Hint: If $n = km$*, consider the prime factorisation of* k*.*

(ii) In what follows, let $p \in \mathbb{N}$ be prime. Recall that for nonzero $n \in \mathbb{Z}$, we define $v_p(n)$ as the exponent of p in n. Prove that for all nonzero $n \in \mathbb{Z}$, $v_p(n)$ is the largest integer v such that $p^v \mid n$.

(iii) Recall that we set $v_p(0) = +\infty$ by convention. In view of the previous question, does this convention seem appropriate?

(iv) Let $m, n \in \mathbb{Z}$, both nonzero. Prove that $v_p(mn) = v_p(m) + v_p(n)$. What happens if m or n is zero?

(v) Let $m, n \in \mathbb{Z}$, both nonzero. Prove that $v_p(m+n) \geqslant \min(v_p(m), v_p(n))$. What happens if m or n is zero?

(vi) Let $m, n \in \mathbb{Z}$. Prove that if $v_p(m) \neq v_p(n)$, then $v_p(m+n) = \min(v_p(m), v_p(n))$.

(vii) Give an example where $v_p(m+n) > \min(v_p(m), v_p(n))$.

Exercise 10 *Rational square roots* ★

Prove that for $n \in \mathbb{N}$, either $\sqrt{n} \in \mathbb{N}$ or $\sqrt{n} \notin \mathbb{Q}$ is irrational.

Hint: First show that if $\sqrt{(}n) \notin \mathbb{N}$, then $v_p(n)$ is odd for some prime p. Then suppose $\sqrt{n} = \frac{a}{b}$ for some $a, b \in \mathbb{N}$. Rearrange this into an equality where you can compare valuations.

Exercise 11 *Perfect numbers*

A positive integer n is said to be *perfect* if it agrees with the sum of all of its positive divisors other than itself; in other words, if $\sigma_1(n) = 2n$. For instance, 6 is a perfect number, because its positive divisors other than itself are 1, 2 and 3, and $1 + 2 + 3 = 6$ (and thus $\sigma_1(6) = 1 + 2 + 3 + 6 = 6 + 6$.)

1. Let $n \in \mathbb{N}$ be even. Why may we find integers $a, b \in \mathbb{N}$ such that $n = 2^a b$ and b is odd ?

2. Let $n \in \mathbb{N}$ be even, and write $n = 2^a b$ with b odd as above. Express $\sigma_1(n)$ in terms of a and $\sigma_1(b)$.

   Hint: Prove that 2^a and b are coprime.

3. Let $a \in \mathbb{N}$ be such that $2^{a+1} - 1$ is prime. Prove that $2^a(2^{a+1} - 1)$ is perfect.

   We now want to prove that all **even** perfect numbers are of the above form.

   In this rest of the exercise, we suppose that n is an even perfect number, and as above we write $n = 2^a b$ with b odd.

4. Use the fact that n is perfect to prove that $(2^{a+1} - 1) \mid 2n$.
5. Deduce that $(2^{a+1} - 1) \mid b$.
6. Let thus $c \in \mathbb{N}$ be such that $b = (2^{a+1} - 1)c$. Prove that $\sigma_1(b) = b + c$.
7. Deduce that $c = 1$ and that b is prime.

   Hint: Prove that $c \mid b$. Which other "obvious" divisors does b have?

   Finally, we use the results established above to look for even perfect numbers.

8. Let $q \in \mathbb{N}$. Prove that if $2^q - 1$ is prime, then q is also prime.

   Hint: $x^m - 1 = (x-1)(x^{m-1} + x^{m-2} + \cdots + x + 1)$. Contrapositive.

9. Find two even perfect numbers (apart from 6).

Exercise 12 *Ideals of $\mathbb{Z}$*

In this exercise, we define an *ideal* of $\mathbb{Z}$ to be a subset $I \subseteq \mathbb{Z}$ such that

- I is not empty,
- whenever $i \in I$ and $j \in I$, we also have $i + j \in I$,
- whenever $k \in \mathbb{Z}$ and $i \in I$, we also have $xi \in I$.

(i) Let $n \in \mathbb{Z}$. Prove that $n\mathbb{Z} = \{nk,\ k \in \mathbb{Z}\}$ is an ideal of $\mathbb{Z}$.

(ii) For which $m, n \in \mathbb{Z}$ do we have $m\mathbb{Z} = n\mathbb{Z}$?

(iii) Let $I \subset \mathbb{Z}$ be an ideal. Prove that whenever $i \in I$ and $j \in I$, we also have $-i \in I$, $i - j \in I$, and $0 \in I$.

(iv) Let $I \subset \mathbb{Z}$ be an ideal. Prove that there exists $n \in \mathbb{Z}$ such that $I = n\mathbb{Z}$.

Hint: If $I \neq \{0\}$, let n be the smallest positive element of I, and consider the Euclidean division of the elements of i by n.

(v) Prove that if I and J are ideals of $\mathbb{Z}$, then

$$I + J = \{i + j \mid i \in I, j \in J\}$$

is also an ideal of $\mathbb{Z}$.

Hint: $i + j + i' + j' = i + i' + j + j'$.

(vi) Let now $a, b \in \mathbb{Z}$. By the previous question, $a\mathbb{Z} + b\mathbb{Z}$ is an ideal, so it is of the form $c\mathbb{Z}$ for some $c \in \mathbb{Z}$. Express c in terms of a and b.

Hint: If you are lost, write an English sentence describing the set $a\mathbb{Z} + b\mathbb{Z}$.

(vii) Prove that if I and J are ideals of $\mathbb{Z}$, then so is their intersection $I \cap J$.

(viii) Let now $a, b \in \mathbb{Z}$. By the previous question, $a\mathbb{Z} \cap b\mathbb{Z}$ is an ideal, so it is of the form $c\mathbb{Z}$ for some $c \in \mathbb{Z}$. Express c in terms of a and b.