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:

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

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

Solution 1

1. Since $F_{n+1} = F_n + F_{n-1}$, we must have that $\gcd(F_n, F_{n+1})|F_{n-1}$, and furthermore that $\gcd(F_n, F_{n+1}) = \gcd(F_n, F_{n-1})$. Iterating this argument, we find that

$$\begin{aligned}\gcd(F_{n+1}, F_n) &= \gcd(F_n, F_{n-1}) = \gcd(F_{n-1}, F_{n-2}) \\ &= \cdots = \gcd(F_2, F_1) = \gcd(F_1, F_0) = 1.\end{aligned}$$

2. We will give two proofs of this: one by induction, and one by tiling. To establish this identity by induction, we will induct on m. We first check the case of $m = 1$

$$F_0F_n + F_1F_{n+1} = 0(F_n) + 1(F_{n+1}) = F_{n+1},$$

   so the case of $m = 1$ holds for all $n \in \mathbb{N}$. for all $n \in \mathbb{N}$. Now assume $m \geq 2$ and that

$$F_{n+k} = F_{k-1}F_n + F_kF_{n+1}$$

for all $k < m$ and all $n \in \mathbb{N}$. Then, applying this the induction hypothesis to $n + m = (n + 1) + (m - 1)$, we find that

$$\begin{aligned} F_{n+m} &= F_{m-2}F_{n+1} + F_{m-1}F_{n+2} \\ &= F_{m-2}F_{n+1} + F_{m-1}\left(F_{n+1} + F_n\right) \\ &= \left(F_{m-2} + F_{m-1}\right)F_{n+1} + F_{m-1}F_n \\ &= F_mF_{n+1} + F_{m-1}F_n = F_{m-1}F_n + F_mF_{n+1}, \end{aligned}$$

as required. Hence, by induction, Honsberger's identity holds.

A second proof is as follows: Denote by T_n the number of ways of tiling a $2 \times n - 1$ grid with 2×1 dominoes, and set $T_0 = 0$. Note that $T_1 = 1$, since there is only one way to tile an empty grid, and that $T_2 = 1$. We will show that T_n satisfies Honsberger's identity. Note that Honsberger's identity implies, for $m = 2$, that

$$T_{n+2} = T_{n+1} + T_n$$

for all $n \geq 1$. Hence, if T_n satisfies Honsberger's identity, we must have that $T_n = F_n$, as they satisfy the same recurrence and have the same initial terms. We can therefore conclude that F_n satisfies Honsberger's identity.

To see that T_n satisfies Honsberger's identity, consider all the ways of tiling a $2 \times (m + n - 1)$ grid. Consider the $(m - 1)^{\text{th}}$ and m^{th} columns. There are two possibilities. If no domino crosses between the two columns, the tiling is split into a tiling of a $2 \times (m - 1)$ grid and a tiling of a $2 \times n$ grid, contributing a total of T_mT_{n+1} possible tilings. The other possibility is that the $(m-1)^{\text{th}}$ and m^{th} columns are covered by two horizontal dominoes, splitting the tiling into one of a $2 \times (m - 2)$ grid and one of a $2 \times (n - 1)$ grid, contributing a total of $T_{m-1}T_n$ possible tilings. Every possible tiling of a $2 \times (m + n - 1)$ grid is counted between these two cases and hence

$$T_{n+m} = T_{m-1}T_n + T_mT_{n+1}.$$

3. We will proceed by induction, for m non-zero. Clearly, $F_m|F_m$. Suppose $F_m|F_{mk}$ so some $k \geq 1$. Then, by Honsberger's identity

$$F_{m(k+1)} = F_{mk+m} = F_{mk-1}F_m + F_{mk}F_{m+1}.$$

As $F_m|F_m$ and $F_m|F_{mk}$, we must have that

$$F_m| \left(F_{mk-1}F_m + F_{mk}F_{m+1}\right) = F_{m(k+1)}.$$

This completes the induction step, and therefore if $m|n$, $F_m|F_n$. If $m = 0$, then $m|n$ implies $n = 0$ and $F_0|F_0$.

4. The case where $m = 0$ is trivial, so assume $m > 0$ and write $n = mq+r$ with $0 \leq r < m$. It suffices to show that, if $F_m|F_n$, then $r = 0$. By Honsberger's identity

$$F_n = F_{mq+r} = F_{mq-1}F_r + F_{mq}F_{r+1},$$

and so

$$F_{mq-1}F_r = F_n - F_{mq}F_{r+1}.$$

As $F_m|F_n$, by assumption, and $F_m|F_{mq}$ by the previous part of the question, we must have that $F_m|F_{mq-1}F_r$.

We must have $\gcd(F_m, F_{mq-1}) = 1$. If they had a larger common divisor $d > 1$, then d would also be a common divisor of F_{mq} and F_{mq-1}, as $F_m|F_{mq}$. But, from the first part of the question $\gcd(F_{mq}, F_{mq-1}) = 1$, and so d cannot be greater than 1.

Hence, by Gauss' Lemma, we must have that $F_m|F_r$. But $r < m$, and the Fibonacci sequence is strictly increasing from F_2 onwards, so $F_r < F_m$ if $m > 2$. Thus, F_m can only divide F_r if $F_r = 0$, i.e. $r = 0$. Therefore $n = mq$.

5. We assume, without loss of generality, that $n > m$. We have that

$$F_n = F_{m+(n-m)} = F_{m-1}F_{n-m} + F_mF_{n-m+1}$$

and so

$$\mathrm{Div}(F_n, F_m) = \mathrm{Div}(F_m, F_n - F_mF_{n-m+1}) = \mathrm{Div}(F_m, F_{m-1}F_{n-m}).$$

But $\gcd(F_m, F_{m-1}) = 1$, so we must have that

$$\mathrm{Div}(F_n, F_m) = \mathrm{Div}(F_m, F_{m-1}F_{n-m}) = \mathrm{Div}(F_m, F_{n-m}).$$

6. Note that $\gcd(n, m) = \gcd(m, n - m)$. Hence, the greatest common divisor of two numbers may be computed by repeatedly replacing the larger of the pair with their difference. As we have shown that $\mathrm{Div}(F_n, F_m) = \mathrm{Div}(F_m, F_{n-m})$, we can iterate this process to obtain

$$\mathrm{Div}(F_n, F_m) = \mathrm{Div}(F_{\gcd(m,n)}, F_0) = \mathrm{Div}(F_{\gcd(m,n)})$$

from which the claim follows.

Alternatively, writing $n = mq + r_1$ with $0 \leq r < m$, we can iterate the argument to obtain that

$$\mathrm{Div}(F_n, F_m) = \mathrm{Div}(F_m, F_{n-mq}) = \mathrm{Div}(F_m, F_{r_1}).$$

Writing $m = r_1 q_1 + r_2$, the same argument gives that

$$\mathrm{Div}(F_n, F_m) = \mathrm{Div}(F_m, F_{r_1}) = \mathrm{Div}(F_{r_1}, F_{r_2}).$$

Iterating this argument, we see that

$$\mathrm{Div}(F_n, F_m) = \mathrm{Div}(F_{r_k}, F_{r_{k+1}})$$

where $r_1, \ldots, r_{k+1}$ are the remainders in Euclid's algorithm. In particular, we must have that

$$\mathrm{Div}(F_n, F_m) = \mathrm{Div}(F_{\gcd(m,n)}, F_0).$$

Considering the maximum of these sets, we see that

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

Note that to get full points for this equation, one just needs to establish that $\mathrm{Div}(F_n, F_m) = \mathrm{Div}(F_m, F_{n-m})$ *and note that iterating this argument computes the greatest common divisor in the subscripts. Not this much detail is needed.*

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 $k|n + 1$.

Solution 2

(i) Let ℓ be the last digit of n. Then we can write $n = 10m + \ell$ for some integer $m \in \mathbb{Z}$. As $5|10m$, we must have that $5|n = 10m + \ell$ if and only if $5|\ell = n - 10m$. The only one digit numbers divisible by 5 are 0 and 5

(ii) Similarly to the last part, $2|n$ if and only if $2|\ell$ as $2|10m$.

(iii) Let ℓ be integer given by the last two digits of n, so that we can write $n = 100m + \ell$ for some integer m. As $4|100$, $4|100m$, and hence $4|n$ if and only if $4|\ell$.

(iv) Note that $8|1000$, and make the same argument.

(v) If ℓ denotes the integer given by the last k digits of n, then we can write $n = 10^k + \ell$. Since $2^k|10^k$, we can apply the same argument to conclude that $2^k|n$ if and only if $2^k|\ell$.

(vi) Note that $10a - 2 = 10(a+1) - 12$. If $3|a+1$, we must have $3|10a-2$, as $3| - 12$.

(vii) We can factorise $n^2 - 1 = (n-1)(n+1)$. Clearly, if $k|n-1$ or $k|n+1$, then $k|n^2-1$. Since k is prime, if $k|(n-1)(n+1)$, then k divides at least one of the two factors.

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.

Solution 3

(i) Suppose $4n^2 - 2n + 13 = 0$ for some $n \in \mathbb{Z}$. Then $13 = 2(n - 2n^2)$, but $2 \nmid 13$. Therefore no such n exists.

(ii) Note that $3|3$, $3| - 282$, and $3|18$, but $3 \nmid -28$, and so by the same reasoning as the previous question, no integer roots can exist.

(iii) Suppose all of st, $sv + tu$ and uv are odd. Then, since $2 \nmid st$ and $2 \nmid uv$, we must have that s, t, u, v are all odd. Therefore sv and tu are odd, and the sum of two odd numbers is even, so we must have $2|sv + tu$.

If $ax^2 + bx + c$ has a rational root, it can be factorised as $(sx+u)(tx+v)$ for some integers s, t, u, v such that $a = st$, $b = sv + tu$, $c = uv$. As noted above, if a and c are odd, b must be even. Therefore no such factorisation can exist.

Exercise 4 *Applying the algorithm* ★

Compute the following:

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

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

Solution 4

(i) $72 = 4(18)$, so $\gcd(72,18) = 18$.

(ii) $168 = 124+44$, $124 = 2(44)+36$, $44 = 36+8$, $36 = 4(8)+4$, $8 = 2(4)$, so $\gcd(168,124) = 4$.

(iii) $1047 = 3(282)+201$, $282 = 201+81$, $201 = 2(81)+39$, $81 = 2(39)+3$, $39 = 13(3)$, so $\gcd(1047,282) = 3$.

(iv) $2n+1 = 2(n)+1$, so $\gcd(2n+1,n) = 1$.

(v) $21n+4 = 14n+3+7n+1$, $14n+3 = 2(7n+1)+1$, so $\gcd(21n+4,14n+3) = 1$.

Exercise 5 *Bézout's Theorem applied*

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

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

Solution 5

We will apply Euclid's algorithm:

$$\begin{aligned} 2024 &= 7(285)+29 \\ 285 &= 9(29)+24 \\ 29 &= 24+5 \\ 24 &= 4(5)+4 \\ 5 &= 4+1 \end{aligned}$$

and hence $\gcd(2024, 285) = 1$. To determine u and v, we run the algorithm backwards

$$\begin{aligned}
1 &= 5 - 4 \\
&= 5 - (24 - 4(5)) = 5(5) - 24 \\
&= 5(29 - 24) - 24 = 5(29) - 6(24) \\
&= 5(29) - 6(285 - 9(29)) = 59(29) - 6(285) \\
&= 59(2024 - 7(285)) - 6(285) = 59(2024) - 419(285).
\end{aligned}$$

Thus, a solution is given by $(u, v) = (59, -419)$.

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.

Solution 6

The first part of the question is asking us to find the number of non-negative integer solutions to the Diophantine equation

$$10u + 15v = 1073.$$

Note that $\gcd(10, 15) = 5 \nmid 1073$, so there are no integer solutions, let alone non-negative ones.

The second part of the question is asking us to find the number of non-negative integer solutions to the Diophantine equation

$$10u + 15v = 1075.$$

As $5|1075$, we know that infinitely many solutions exist. We can, in fact, reduce the problem to finding non-negative integer solutions to

$$2u + 3v = 215.$$

We will first find an integer solution to

$$2x + 3y = 1$$

which we could solve via the Euclidean algorithm, as in the proof of Bézout's theorem, but there is an obvious solution $(x, y) = (-1, 1)$. Hence, we can take $(u_0, v_0) = (-215, 215)$ as a solution to our main equation. Every other solution is of the form

$$(u, v) = (-215 + 3k, 215 - 2k)$$

as k ranges across $\mathbb{Z}$. In order to obtain a non-negative integer solution, we need that

$$3k \geq 215 \quad \text{and} 215 \geq 2k$$

or equivalently that $107.5 \geq k \geq 71.6666$. Since k must be an integer, we can restrict to $107 \geq k \geq 72$. Every such k gives a non-negative integer solution, and every non-negative integer solution corresponds to such a k, so we must therefore have $107 - 71 = 36$ integer solutions. The easiest solution to count probably corresponds to $k = 107$, giving $(u, v) = (106, 1)$. The solution involving the least number of stamps corresponds to $k = 72$, with $(u, v) = (1, 71)$. Personally, I think $k - 86$, $(u, v) = (43, 43)$ is fun, even if everyone involved in the postage probably disagrees.

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

Solution 7

Suppose $d|a$. Then, as $\gcd(d, b)|d$, we must have that $\gcd(d, b)|a$. By definition $\gcd(d, b)|b$, and so $\gcd(d, b)|\gcd(a, b) = 1$. Hence $\gcd(d, b) = 1$. Now, if $d|a$ and $d|bc$, then by Gauss' Lemma, $d|c$, as $\gcd(d, b) = 1$. But if $d|a$ and $d|c$, then $d|\gcd(a, c) = 1$ and so $d = 1$. Therefore a and bc must be coprime, as 1 is their only common divisor.

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.

Solution 8

(i) We begin by noting that $2024 = 8(253)$: Exercise 2(iv) lets us deduce this quickly. Thus $2024 = 2^3 \cdot 253$. 2 is prime, as there aren't any smaller integers to be non-trivial factors.

To factor 253, we begin dividing by small primes less than or equal to $\sqrt{253} \approx 16$, and find that it is only divisible by 11. Thus

$$2024 = 2^3 \cdot 11 \cdot 23.$$

It is easy to check that 11 is prime, and 23 must be prime, either by direct computation or by noting that 253 would have to have a factor smaller than 11 if 23 we composite.

(ii) Every divisor of 2024 is of the form $2^a \cdot 11^b \cdot 23^c$, where $0 \leq a \leq 3$, and $0 \leq b, c \leq 1$. This gives us $4 \times 2 \times 2 = 16$ divisors. Their sum is given by the product

$$\left(\frac{2^4 - 1}{2 - 1}\right)\left(\frac{11^2 - 1}{11 - 1}\right)\left(\frac{23^2 - 1}{23 - 1}\right) = 4320.$$

(iii) It is currently 15 : 36. Dividing repeatedly by 2, we find $1536 = 2^9 \cdot 3$. This means that 1536 has $10 \cdot 2 = 20$ divisors, and the sum of these divisors is given by

$$\frac{(2^10 - 1)(9 - 1)}{2} = 4092.$$

(iv) From our formula, the sum of divisors of $3^a 5^b$ is given by

$$\left(\frac{3^{a+1} - 1}{2}\right)\left(\frac{5^{b+1} - 1}{4}\right) = (1 + 3 + \cdots + 3^a)\left(1 + 5 + \cdots 5^b\right)$$

Therefore if $\sigma_1(3^a 5^b) = 33883 = 31$, we must have that one of four cases occurs: both prime factors divide the 3-sum, both prime factors divide the 5 sum, 31 divides the 3-sum and 1093 divides the 5-sum, or 31 divides the 5-sum and 1093 divides the 3 sum.

In fact, as there are no other prime factors, we can replace "divides" with "is equal to".

In the first case $b = 0$, and we need

$$1 + 3 + \cdots + 3^a = \frac{3^{a+1} - 1}{2} = 33883$$

and so $3^{a+1} = 2(33883) + 1 = 67767$, which is not a power of three.

In the second case $a = 0$, and we need

$$\frac{5^{b+1} - 1}{4} = 33883$$

and so $5^{b+1} = 4(33883) + 1 = 135533$, which is not even a multiple of 5.

In the third case, we must have

$$\frac{3^{a+1} - 1}{2} = 31 \quad \text{and} \quad \frac{5^{b+1} - 1}{4} = 1093$$

and hence $3^{a+1} = 63$, which is not a power of three.

In the final case, we must have

$$3^{a+1} = 2187 = 3^7 \quad \text{and} \quad 5^{b+1} = 125 = 5^3$$

Hence, $a = 6$ and $b = 2$ is the only possible solution, giving

$$M = 18225.$$

(v) We have that $n^2 - 1 = (n-1)(n+1)$ is a factorisation of $n^2 - 1$, into positive integers, since $n \geq 2$. In order for $n^2 - 1$ to be prime, these two factors must be 1 and $n^2 - 1$. In particular, $n - 1 = 1$ and $n + 1 = n^2 - 1$. This gives $n = 2$, and so 3 is the only prime of the form $n^2 - 1$.

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 $v_p(m+n) > \min(v_p(m), v_p(n))$.

Solution 9

(i) Suppose $m|n$ so that $n = mk$. We can write $k = \prod_i p_i^{c_i}$ for some non-negative integers c_i, using the same set of primes, as if $p|k$ then $p|n$. Thus

$$\prod_i p_i^{b_i} = \left(\prod_i p_i^{a_i}\right)\left(\prod_i p_i^{c_i}\right) = \prod_i p_i^{a_i + c_i}$$

By the uniqueness of prime factorisation, we must have $a_i + c_i = b_i$ for each i, and since $c_i \geq 0$, we must have $a_i = b_i - c_i \leq b_i$.

Conversely, if $b_i \geq a_i$, then $c_i = b_i - a_i \geq 0$, and so

$$k = \prod_i p_i^{c_i}$$

is an integer such that $n = km$. Therefore $m|n$.

(ii) By the previous part of the question, $p^v|n$ if and only if $v \leq v_p(n)$, from which the conclusion is immediate.

(iii) Yes! There is no upper bound on integers v such that $p^v|0$, so declaring the valuation of 0 to be infinite works with this intuition.

(iv) By the definition of $v_p(m)$ we can write $m = p^{v_p(m)}M$ where $p \nmid M$, and similarly for n. Then $mn = p^{v_p(m)+v_p(n)}MN$. Since $p \nmid M$ and $p \nmid N$, $p \nmid MN$ and hence $v = v_p(m) + v_p(n)$ is the maximal integer such that $p^v|mn$, which is to say $v_p(mn) = v_p(m) + v_p(n)$.

This extends to the case where m or n is zero (without loss of generality $m = 0$), as then $mn = 0$, so $v_p(mn) = \infty = \infty + v_p(n)$.

(v) As before, write $m = p^{v_p(m)}M$ and $n = p^{v_p(n)}N$, and without loss of generality assume that $v_p(m) \leq v_p(n)$. We write $v_p(n) = v_p(m) + c$ for some $c \geq 0$. Then

$$m + n = p^{v_p(m)}M + p^{v_p(m)+c}N = p^{v_p(m)}\left(M + p^c N\right)$$

and so $p^{v_p(m)}|m + n$. As $v_p(m + n)$ is the maximal integer v such that $p^v|m + n$, we must have $v_p(m + n) \geq v_p(m) = \min(v_p(m), v_p(n))$.

(vi) Take $m = n = 2$. Then $v_2(m) = v_2(n) = 1$, but $v_2(m + n) = 2$. In general, equality will hold if and only if $v_p(m) \neq v_p(n)$.

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.

Solution 10

Note that $v_p(k^2) = v_p(k) + v_p(k) = 2v_p(k)$ is even, and hence the p-adic valuation of a square number is even for any prime p. Thus, if n is not a square, which is to say $\sqrt{n} \notin \mathbb{N}$, then $v_p(n)$ must be odd for some prime p.

Suppose $\sqrt{n} = \frac{a}{b}$. This implies that

$$a^2 = nb^2.$$

Let p be a prime such that $v_p(n)$ is odd. Then we must have

$$2v_p(a) = v_p(a^2) = v_p(nb^2) = v_p(n) + v_p(b^2) = v_p(n) + 2v_p(b).$$

But this implies $v_p(n)$ must be divisible by 2, a contraction. Therefore $\sqrt{n}$ is irrational if it is not an integer.

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).

Solution 11

1. By the fundamental theorem of arithmetic, we can write $n = 2^a \prod_i p_i^{b_i}$, with $a \geq 1$, since n is even, and where each prime p_i is odd (since non-2 primes are all odd). Since the product of odd numbers is odd, we can take b to be this product.

2. Since b is odd, $2 \nmid b$ and so 2^a and b are coprime, as 2 would divide any common factor larger than 1. We know that σ_1 is weakly multiplicative, so
$$\sigma_1(n) = \sigma_1(2^a b) = \sigma_1(2^a)\sigma_1(b) = (2^{a+1} - 1)\sigma_1(b).$$

3. Since $2^{a+1} - 1$ is odd, we have that
$$\sigma_1(2^a(2^{a+1} - 1)) = (2^{a+1} - 1)\sigma_1(2^{a+1} - 1).$$
   If $2^{a+1} - 1$ is prime, $\sigma_1(2^{a+1} - 1) = 1 + 2^{a+1} - 1 = 2^{a^1}$, and so
$$\sigma_1(2^a(2^{a+1} - 1)) = 2^{a+1}(2^{a+1} - 1) = 2\left(2^a(2^{a+1} - 1)\right)$$
   which is precisely what it means to be perfect.

4. Since n is perfect
$$2n = \sigma_1(n) = (2^{a+1} - 1)\sigma_1(b)$$
   and hence $(2^{a+1} - 1) | 2n$.

5. We have that $(2^{a+1}-1)|2n = 2^{a+1}b$. Since $\gcd(2^{a+1}-1, 2^{a+1}) = 1$, Gauss' Lemma tells us that $(2^{a+1}-1)|b$.

6. We have that

$$(2^{a+1}-1)\sigma_1(b) = 2n = 2^{a+1}(2^{a+1}-1)c$$

and hence

$$\begin{aligned}\sigma_1(b) &= 2^{a+1}c \\ &= (2^{a+1}-1+1)c \\ &= (2^{a+1}-1)c + c = b + c.\end{aligned}$$

7. If $b = (2^{a+1}-1)c$ and $c \neq 1$ then

$$b + c = \sigma_1(b) = b + 2^{a+1} - 1 + c + 1 \cdots \geq b + c + 2^{a+1}$$

which would imply that $2^{a+1} \leq 0$, a clear contraction. Therefore, we must have $c = 1$. Then, since $\sigma_1(b) = b + 1$, we must have b is prime, as we would have other divisors contributing to the sum otherwise.

8. Suppose $q = rs$, $1 < r, s < q$, is composite. Then

$$2^q - 1 = (2^r)^s - 1 = (2^r - 1)(2^{rs-r} + \cdots + 1)$$

is a non-trivial factorisation of $2^q - 1$, as $2^r - 1 \notin \{1, 2^q - 1\}$. Therefore if $2^q - 1$ is prime, q is prime.

9. We need to find a such that $2^{a+1} - 1$ is prime. We know this implies $a + 1$ is prime, so lets try a one less than a prime. If $a = 1$, we get the perfect number 6. If $a = 2$, then $2^3 - 1 = 7$ is prime and so we can say that $2^2(7) = 28$ is perfect. Of $\{4, 6, 10, 12, \ldots\}$, the next value of a for which $2^{a+1} - 1$ is prime is $a = 4$, giving us the perfect number $2^4(2^5 - 1) = 496$.

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.

Solution 12

(i) Clearly $n \in n\mathbb{Z}$, so $n\mathbb{Z}$ is non-empty. If $a, b \in n\mathbb{Z}$, then there exist $k, \ell \in \mathbb{Z}$ such that $a = kn$ and $b = \ell n$. Hence $a + b = n(k + \ell) \in n\mathbb{Z}$. If $a = nk \in n\mathbb{Z}$ and $m \in \mathbb{Z}$, then $ma = n(mk) \in n\mathbb{Z}$. Hence, $n\mathbb{Z}$ is an ideal of $\mathbb{Z}$.

(ii) If $m\mathbb{Z} = n\mathbb{Z}$, then $m \in n\mathbb{Z}$, and so $n|m$. Similarly, we must have $m|n$. But if $m|n$ and $n|m$, we must have $m = \pm n$.

(iii) If $i \in I$, then $(-1)i = -i \in I$, via the multiplicative property of ideals. If $j \in I$, then $-j \in I$, and since ideals are closed under addition $i + (-j) = i - j \in I$. Finally, since I is non-empty, there exists an element $k \in I$, and therefore $0 = 0(k) \in I$.

(iv) If $I = \{0\}$, then $I = 0\mathbb{Z}$, so assume $I \neq \{0\}$. Then, I contains a smallest positive element n, and all multiple of n. Hence $n\mathbb{Z} \subset I$. Now suppose $N \in I$, which we can assume without loss of generality to be positive. Dividing N by n, we get $N = nq + r$, $0 \leq r < n$. Writing $r = N - nq$, we see that $r \in I$ as $N \in I$ and $nq \in I$, But if $r \neq 0$, this contracts the minimality of n. Hence $r = 0$, and $N = nq \in n\mathbb{Z}$. Thus $I \subset n\mathbb{Z}$ and $I = n\mathbb{Z}$.

(v) Since $0 \in I$ and $0 \in J$, $0 \in I + J$, so $I + J$ is non empty. To see that it is closed under addition, suppose $k, \ell \in I + J$. Then there exists $i, i' \in I$ and $j, j' \in J$ such that $k = i + j$ and $\ell = i' + p'$. Hence

$$k + \ell = i + j + i' + j' = (i + i') + (j + j') \in I + J$$

as $(i + i') \in I$ and $(j + j') \in J$). Finally we check the multiplicative property. Suppose $k \in I + J$ and $m \in \mathbb{Z}$. Then $k = i + j$ for some $i \in I$ and $j \in J$, and hence $mk = mi + mj \in I + J$ as $mi \in I$ and $mj \in J$.

(vi) The ideal $a\mathbb{Z} + b\mathbb{Z}$ given as a set is

$$\{au + bv \mid u, v \in \mathbb{Z}\}$$

which by (corollaries to) Bézout's theorem is precisely the set of multiples of $\gcd(a, b)$. Hence $c = \pm \gcd(a, b)$.

(vii) Since $0 \in I$ and $0 \in J$, $0 \in I \cap J$, so it is non-empty. If $i, j \in I \cap J$, then $i + j \in I$ and $i + j \in J$, and so $i + j \in I \cap J$. If $i \in I \cap J$ and $k \in \mathbb{Z}$, then $ki \in I$ and $ki \in J$, so $ki \in I \cap J$.

(viii) $a\mathbb{Z}$ is the set of integers divisible by a. $b\mathbb{Z}$ is the set of integers divisible by b. Their intersection is the set of integers divisible by both a and b. Hence $\operatorname{lcm}(a, b) \in a\mathbb{Z} \cap b\mathbb{Z}$. Furthermore, every such integer is divisible by $\operatorname{lcm}(a, b)$, and so $c = \pm \operatorname{lcm}(a, b)$.