Homework set 7 – Solutions
Math 310 – Renato Feres

Note 1. Work on all the problems listed below, but only those marked with an (∗) need to be turned in.
Note 2. The problems marked with (∗) are all worth the same number of points.
Note 3. Chapters and exercise numbers refer to the 4th edition of Liebeck’s text.

1. Read: Chapter 11 and 12 of Liebeck’s textbook.

2. Chapter 11, Exercise 2 (∗)

   (a) Which positive integers have exactly three positive divisors?
   (b) Which positive integers have exactly four positive divisors?

   Solution. Let \( N(n) \) denote the number of positive divisors of \( n \). First observe that if \( n = p_1 \ldots p_k \) is a prime factorization of \( n \) (not all factors distinct), then \( n \) has at least \( k + 1 \) positive divisors, namely \( 1, p_1, p_1 p_2, \ldots, p_1 \ldots p_k \).
   So \( N(n) \geq k + 1 \); and \( N(n) = k + 1 \) if \( n = p^k \), \( p \) a prime.

   (a) If \( N(n) = 3 \), its prime factorization must not contain more than two primes. If \( n \) is itself a prime, \( N(n) = 2 \), so \( n = p_1 p_2 \). And if \( p_1 \neq p_2 \), \( N(n) = 4 \) since \( 1, p_1, p_2, p_1 p_2 \) are the prime factors. Therefore \( N(n) = 3 \) if and only if \( n = p^2 \), where \( p \) is a prime.

   (b) Now suppose \( N(n) = 4 \). Then its prime factorization must contain more than one and less than four prime factors. If it has two prime factors, then these factors must be distinct: \( n = p_1 p_2 \), \( p_1 \neq p_2 \), in which case \( N(n) = 4 \) (the divisors being \( 1, p_1, p_2, p_1 p_2 \)); and if it has three prime factors, with at least two distinct, then \( N(n) \geq 5 \), so it must be \( n = p^3 \), where \( p \) is a prime. We conclude that \( N(n) = 4 \) if and only if \( n = p_1 p_2 \) for distinct primes \( p_1, p_2 \), or \( n = p^3 \) where \( p \) is prime.

3. Chapter 11, Exercise 3. Suppose \( n \geq 2 \) is an integer with the property that whenever a prime \( p \) divides \( n \), \( p^2 \) also divides \( n \) (i.e., all primes in the prime factorization of \( n \) appear at least to the power 2). Prove that \( n \) can be written as the product of a square and a cube.

   Solution. The prime decomposition of \( n \) may, under the stated condition, be written as \( n = p_1^{a_1} \ldots p_k^{a_k} \) where \( a_j \geq 2 \) for \( j = 1, \ldots, k \). Let us split the exponents into two sets consisting of even and odd exponents. More precisely, let us write \( (1, \ldots, k) \) as the union of sets \( I_e \) and \( I_o \), where \( a_i \) is even for \( i \in I_e \) and odd for \( i \in I_o \). For \( i \in I_o \), we may write \( a_i = 3 + b_i \), where \( b_i \) must be even, possibly 0. Now let \( r \) be the product of the \( p_i^{a_i} \) for \( i \in I_e \),
times the product of $p_j^{b_j}$ for $j \in I_o$; and let $s$ be the product of the $p_j^3$ for all $j \in I_o$. Then $n = rs$ where $r$ is a square and $s$ is a cube.

4. **Chapter 11, Exercise 4** (*) Prove that $\text{lcm}(a, b) = ab/hcf(a, b)$ for any positive integers $a, b$ without using the prime factorization.

**Solution.** First note that if positive integers $\alpha, \beta$ are coprimes, than $\text{lcm}(\alpha, \beta) = \alpha \beta$. In fact, let $\gamma = \text{lcm}(\alpha, \beta)$ and note that $\alpha | \gamma$, so $\gamma = ca$ for a positive integer $c$, and since $\beta | \gamma$ and $\alpha, \beta$ are coprimes then $\beta | c$. Therefore $\gamma = r a \beta$ for some positive integer $r$. But $r = 1$ because $\gamma$ is the least common multiple of $\alpha$ and $\beta$.

A second observation is useful: suppose $\alpha, \beta$ are positive integers and $d$ is a positive integer. Then the definition of least common multiple implies $\text{lcm}(\alpha d, \beta d) = \text{lcm}(\alpha, \beta) d$.

Now let $d = \text{hcf}(a, b)$. Then $a/d$ and $b/d$ are coprimes. By the first observation just made, $\text{lcm}(a/d, b/d) = ab/hcf(a, b)$. And by the second observation, $\text{lcm}(a/d, b/d) = \text{lcm}(a, b)/d$. Thus we conclude $\frac{\text{lcm}(a, b)}{d} = \frac{ab}{d^2}$. Cancelling a factor $d$ finally gives $\text{lcm}(a, b) = \frac{ab}{hcf(a, b)}$.

5. **Chapter 11, Exercise 5.**

(a) Prove that $2^{1/3}$ and $3^{1/3}$ are irrational.

(b) Let $m$ and $n$ be positive integers. Prove that $m^{1/n}$ is rational if and only if $m$ is an $n$th power (i.e., $m = c^n$ for some integer $c$).

**Solution.**

(a) Because 2 and 3 are not cubes, their cube roots are irrational by the result of the second part of this exercise.

(b) Suppose $m^{1/n} = \frac{r}{s}$ is rational, where $r, s$ are positive integers. We may assume without loss of generality that the highest common factor of $r$ and $s$ is 1. Raising to the $n$th power gives $m = r^n/s^n$ or, equivalently,

$$s^n m = r^n.$$

This implies that each prime factor of $s^n$ must also be a prime factor of $r^n$. Under the assumption that $\text{hcf}(r, s) = 1$, we must conclude that $s = 1$. Therefore $m = r^n$ as we wanted to show (where $c = r$).

6. **Chapter 11, Exercise 8** (*) Find all solutions $x, y \in \mathbb{Z}$ to the following Diophantine equations:
(a) \(x^2 = y^3\).
(b) \(x^2 - x = y^3\).
(c) \(x^2 = y^4 - 77\).
(d) \(x^3 = 4y^2 + 4y - 3\).

Solution.

(a) If \(x^2 = y^3\), then \(y\) must not be negative. And if \((x, y)\) is a solution, \((-x, y)\) is, too. Thus the solutions will be \((0, 0)\) and \((\pm x, y)\) for any solution \((x, y)\) in which both \(x\) and \(y\) are positive. So let us focus on this last case. Both \(x\) and \(y\) must have the same prime factors, up to powers. That is to say that \(x = p_1^{a_1} \cdots p_k^{a_k}\) and \(y = p_1^{b_1} \cdots p_k^{b_k}\) where the \(a_j\) and \(b_j\) are all greater than or equal to 1 and \(3a_j = 3b_j\) for each \(j\). This implies that \(a_j = 3m_j\) and \(b_j = 2m_j\) for some positive integer \(m_j\), for each \(j\). Thus the positive solutions are all of the form

\[
(p_1^{3m_1} \cdots p_k^{3m_k}, p_1^{2m_1} \cdots p_k^{2m_k})
\]

for arbitrary \(k\), \(m_j\) and distinct primes \(p_j\).

(b) Note that \((0, 0)\) and \((1, 0)\) are solutions. Let us consider solutions such that \(y \neq 0\). We may write \(x^2 - x = y^3\) in the form \(x(x - 1) = y^3\). Observe that \(x\) and \(x - 1\) are coprimes. In fact, their highest positive common factor must also be a factor of \(x - (x - 1) = 1\), so it has to be 1. But we know (Proposition 11.4) that, in this case, both \(x\) and \(x - 1\) must be cubes since their product is a cube. Let us write \(x = a^3\) and \(x - 1 = b^3\) where \(a, b\) are integers. Observe that

\[
1 = x - (x - 1) = a^3 - b^3 = (a - b)(a^2 + ab + b^2).
\]

Therefore \(a - b = a^2 + ab + b^2 = \pm 1\). First consider the negative sign. In this case \(a = b - 1\) and

\[
-1 = (b - 1)^2 + (b - 1)b + b^2 = 3b^2 - 3b + 1 = 3b(b - 1) + 1
\]

or, equivalently,

\[
3b(b - 1) = -2.
\]

But 2 is prime, so this equation cannot have an integer solution in \(b\). Let us now consider the + sign: \(a = b + 1\) and

\[
1 = (b + 1)^2 + (b + 1)b + b^2 = 3b^2 + 3b + 1
\]

or, equivalently,

\[
3b(b + 1) = 0.
\]

This equation implies that \(b = 0\) or \(b = -1\). These correspond to the solutions \((x = 0, y = 0)\) and \((x = 1, y = 0)\).

We conclude that these are the only solutions.

(c) Let us write the equation in the form

\[
(y^2 - x)(y^2 + x) = 77.
\]

If \((x, y)\) is a solution, then \((\pm x, \pm y)\) is also a solution for any combination of signs. So we may focus on positive solutions.
There are a few possibilities to consider, according to the following table:

<table>
<thead>
<tr>
<th>( y^2 - x )</th>
<th>( y^2 + x )</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>77</td>
</tr>
<tr>
<td>7</td>
<td>11</td>
</tr>
<tr>
<td>11</td>
<td>7</td>
</tr>
<tr>
<td>77</td>
<td>1</td>
</tr>
</tbody>
</table>

Since \( y^2 + x \) is greater than \( y^2 - x \), the last two cases cannot happen. If \( y^2 - 1 = 1 \) and \( y^2 + x = 77 \), then \( 2y^2 = 78 \) or \( y = \sqrt{39} \). But the latter number is not an integer, so this case is also not possible. We are left with \( y^2 - x = 7 \) and \( y^2 + x = 11 \). Adding the two equations gives \( 2y^2 = 18 \), hence \( y = 3 \) and \( x = y^2 - 7 = 2 \). In fact, it is easily checked that \( (x = 2, y = 3) \) is indeed a solution. Therefore the solutions are \( (\pm 2, \pm 3) \), where all combinations of signs are possible.

(d) We may write the equation in the form

\[
x^3 = (2y - 1)(2y + 3).
\]

Observe that \( 2y - 1 \) and \( 2y + 3 \) are coprimes. In fact, any common factor must divide \( 4 = 2y + 3 - (2y - 1) \); must the two numbers are odd while 4 does not contain an odd positive divisor other than 1. Proposition 11.4 implies that both \( 2y - 1 \) and \( 2y + 3 \) must be cubes since their product is a cube. Let us then write

\[
2y - 1 = a^3, \ 2y + 3 = b^3
\]

where \( a^3b^3 = x^3 \). Observe that

\[
4 = 2y + 3 - (2y - 1) = b^3 - a^3 = (b - a)(a^2 + ab + b^2).
\]

The two factors on the right-hand side of this equation can only have the values indicated in the following table:

<table>
<thead>
<tr>
<th>( b - a )</th>
<th>( a^2 + ab + b^2 )</th>
</tr>
</thead>
<tbody>
<tr>
<td>( \pm 1 )</td>
<td>( \pm 4 )</td>
</tr>
<tr>
<td>( \pm 2 )</td>
<td>( \pm 2 )</td>
</tr>
<tr>
<td>( \pm 4 )</td>
<td>( \pm 1 )</td>
</tr>
</tbody>
</table>

The two factors must have the same sign. Let \( s \) denote the numbers on the first column, so that \( 4/s \) are the corresponding numbers on the second column. We can then write \( b = a + s \) and

\[
a^2 + a(a + s) + (a + s)^2 = \frac{4}{s}.
\]

After simplification, this gives a quadratic equation for \( a \):

\[
a^2 + sa + \frac{s^3 - 4}{3s} = 0.
\]

The discriminant of this quadratic equation is

\[
\Delta = s^2 - \frac{4}{3} \frac{s^3 - 4}{s}.
\]
In order to have integer solutions in $a$, the discriminant must be an integer squared. But a case by case check shows that in none of the cases is $\Delta$ a square integer. This means that the given Diophantine equation does not have integer solutions.

---

7. **Chapter 12, Exercise 2 (**) Let $n$ be an integer with $n \geq 2$. Suppose for every prime $p \leq \sqrt{n}$, $p$ does not divide $n$.

   (a) Prove that $n$ is prime.

   (b) Is 221 prime? Is 223 prime?

**Solution.**

(a) Let $p$ be the smallest among the prime factors of $n$. By assumption, $p > \sqrt{n}$. If $n$ were not prime, there would be at least one more prime factor, $q$. As $p$ is the smallest, we have $q \geq p$. But then $pq \geq p^2 > n$, which is a contradiction since $pq$ must divide $n$. Therefore $n$ must be prime.

(b) Both 221 and 223 are less than $225 = 15^2$. Thus it suffices to check whether any of the primes 2, 3, 5, 7, 11, 13 divides the given number. By a case by case check we see that 7 divides 221, so 221 is not a prime. On the other hand, none of the primes less than or equal to 13 divides 223, so we can conclude that 223 is a prime.

---

8. **Chapter 12, Exercise 4 (**) Use the idea of the proof of Euclid’s Theorem 12.1 to prove that there are infinitely many primes of the form $4k + 3$ (where $k$ is an integer).

**Solution.** We argue by contradiction. Suppose there are only finitely many primes of this form. Let $p_1, p_2, \ldots, p_n$ denote all of them. Now consider $N = 4p_1 \cdots p_n - 1 = 4(p_1 \cdots p_n - 1) + 3$. If $N$ is prime, we have a contradiction since $N$ is larger than any of the $p_j$. So it must be that $N$ has a prime factor, which must be odd since $N$ is odd.

Observe the following: every odd integer can be written as $4k + 1$ or $4k + 3$ for some integer $k$. If all prime factors of $N$ have the form $4k + 1$ for some integer $k$, then their product must also have this form. In fact, $(4k_1 + 1)(4k_2 + 1) = 4(4k_1k_2 + k_1 + k_2) + 1$. So, in this case, we would have $N = 4\ell + 1$ for some integer $\ell$. But this can’t be since a number cannot be equal to both $4\ell_1 + 1$ and $4\ell_2 + 3$ for integers $\ell_1, \ell_2$. This is because the difference would be $0 = 4(\ell_2 - \ell_1) + 2$, or $1 = 2(\ell_1 - \ell_2)$, which is impossible.

Thus $N$ must have a prime factor of the form $4\ell + 3$. It is, therefore, one of the $p_j$. But then $p_j$ divides both $N$ and $N + 1 = 4p_1 \cdots p_n$. Therefore $p_j$ divides $N + 1 - N = 1$, a contradiction. The conclusion is that there must be infinitely many primes of the form $4k + 3$. 

---
