Solutions to Homework #6

1. Each of the following statements is an identically true implication (as proved in class) depending on some free variables with values in $\mathbb{Z}$:

(i) Let $a, b, c \in \mathbb{Z}$. If $c \mid a$ and $c \mid b$, then $c \mid (a + b)$ (here a, b and c are free variables)

(ii) Let $a, b \in \mathbb{Z}$. If $a \mid b$, then $a \mid bd$ for all $d \in \mathbb{Z}$ (here a and b are free variables and d is a bound variable)

(iii) Let $a, b \in \mathbb{Z}$, and let $p \in \mathbb{P}$ where $\mathbb{P}$ is the set of all prime numbers. If $p \mid ab$, then $p \mid a$ or $p \mid b$ (here p, a, b are free variables)

Solution: (i) The converse says: Let $a, b, c \in \mathbb{Z}$. If $c \mid (a+b)$, then $c \mid a$ and $c \mid b$. This is false: for instance, take $a = b = 1$ and $c = 2$. Then $c \mid (a + b)$, but $c \nmid a$.

(ii) The converse says: Let $a, b \in \mathbb{Z}$. If $a \mid bd$ for all $d \in \mathbb{Z}$, then $a \mid b$. This is true: if $a \mid bd$ for all $d \in \mathbb{Z}$, in particular, we have $a \mid bd$ for $d = 1$, which is equivalent to saying $a \mid b$.

(iii) The converse says: Let $a, b \in \mathbb{Z}$, and let $p \in \mathbb{P}$. If $p \mid a$ or $p \mid b$, then $p \mid ab$. This is true by the statement (ii) above (not the converse of (ii)). Note that we do not have to use the fact that p is prime.

2. Let $n \in \mathbb{N}$ with $n \geq 2$, and write $n = p_1^{a_1} \dots p_k^{a_k}$ where $p_1, \dots, p_k$ are distinct primes and each $a_i \in \mathbb{N}$. Prove that n is a perfect square $\iff$ each a_i is even. Recall that we proved the "$\Leftarrow$" direction in Lecture 12, so you only need to prove the "$\Rightarrow$" direction. **Warning/Hint:** If you did not refer to the uniqueness factorization, your argument is likely incomplete.

Solution: Let $n = p_1^{a_1} \dots p_k^{a_k}$ where $p_1, \dots, p_k$ are distinct primes and each $a_i \in \mathbb{N}$, and suppose that $n = m^2$. Since $n > 1$, we have $m > 1$ as well, so by FTA (the fundamental theorem of arithmetic) we can write $m = q_1^{b_1} \dots q_l^{b_l}$ where $q_1, \dots, q_l$ are distinct primes and each $b_i \in \mathbb{N}$.

Substituting these factorizations into the equality $n = m^2$, we get $\prod_{i=1}^{k} p_i^{a_i} = \prod_{i=1}^{l} q_j^{2b_j}$. The uniqueness part of FTA implies that $k = l$ (two factorizations of the same number must involve the same number of primes) and $\{p_1, \dots, p_k\} = \{q_1, \dots, q_k\}$ as sets. WOLOG we can assume that $q_i = p_i$ for each i. Replacing q_i by p_i in the above equation, we get

$$\prod_{i=1}^{k} p_i^{a_i} = \prod_{i=1}^{k} p_i^{2b_i}$$

Again by the uniqueness part of FTA, the exponents with which each prime appears in both factorizations must be the same, so $a_i = 2b_i$ for each i. Thus each a_i is even, which is precisely what we wanted to prove.

3. Prove Corollary 3.3.4 from the book which can be restated as follows: Let $m, n \in \mathbb{N}$ with $n \geq 2$, and write $n = p_1^{a_1} \dots p_k^{a_k}$ where $p_1, \dots, p_k$ are distinct primes and each $a_i \in \mathbb{N}$. Then $m \mid n \iff$ there exist $b_1, \dots, b_k \in \mathbb{Z}_{\geq 0}$ such that $m = p_1^{b_1} \dots p_k^{b_k}$ and $b_i \leq a_i$ for each i. **Note:** The goal of this problem is to give a completely formal proof (a sketch is already given in the book).

Solution: "$\Leftarrow$" Suppose that $m = p_1^{b_1} \dots p_k^{b_k}$ where $b_i \in \mathbb{Z}_{\geq 0}$ and $b_i \leq a_i$ for each i. Define $d = p_1^{a_1 - b_1} \dots p_k^{a_k - b_k}$. Then $d \in \mathbb{N}$ since by assumption $a_i - b_i$ is a non-negative integer for each i and $md = \prod_{i=1}^k p_i^{b_i} \cdot \prod_{i=1}^k p_i^{a_i - b_i} = \prod_{i=1}^k p_i^{a_i} = n$, so $m \mid n$.

"$\Rightarrow$" Suppose now that $m \mid n$. If $m = 1$, then $m = \prod_{i=1}^k p_i^0$, so m has the required form. Thus, for now on we can assume that $m \geq 2$. We first claim that any prime p which appears in the prime factorization of m must equal to p_i for some i. Indeed, if p is a prime appearing in the prime factorization of m, then $p \mid m$. Since we also have $m \mid n$ and the divisibility relation is transitive (by Corollary 3.1.5(d) in the book), we have $p \mid n$. Since $n = \prod_{i=1}^k p_i^{a_i}$, by the generalized Euclid's lemma we must have $p \mid p_i$ for some i, and finally since p and p_i are both prime, we must have $p = p_i$ for some i.

Thus, we proved that each prime in the prime factorization of m is equal to p_i for some i, so we can write $m = \prod_{i=1}^k p_i^{b_i}$ for some $b_i \in \mathbb{Z}_{\geq 0}$ (we set $b_i = 0$ if p_i does not occur in the factorization of m). It remains to show that $b_i \leq a_i$ for each i. Since $m \mid n$, we have $n = md$ for some $d \in \mathbb{Z}$; moreover, $d > 0$ since $m > 0$ and $n > 0$. Applying the argument from the previous paragraph to d instead of m, we get that $d = \prod_{i=1}^k p_i^{c_i}$ for some $c_i \in \mathbb{Z}_{\geq 0}$.

Substituting the prime factorizations for n, m and d into the equation $n = md$, we get $\prod_{i=1}^k p_i^{a_i} = \prod_{i=1}^k p_i^{b_i} \cdot \prod_{i=1}^k p_i^{c_i} = \prod_{i=1}^k p_i^{b_i + c_i}$, and by the uniqueness part of FTA we get $a_i = b_i + c_i$ for each i. Since $c_i \geq 0$, we deduce that $b_i = a_i - c_i \leq a_i$, as desired.

4. Problem 2 in Section 3.3.

Solution: Recall the setup of the problem: we are given $m, n \in \mathbb{N}$ written in the form $m = \prod_{i=1}^k p_i^{m_i}$ and $n = \prod_{i=1}^k p_i^{n_i}$ where $p_1, \dots, p_k$ are distinct primes and $m_i, n_i \in \mathbb{Z}_{\geq 0}$. We need to prove that

(a) $gcd(m, n) = \prod_{i=1}^k p_i^{\min(m_i, n_i)}$

(b) $lcm(m,n) = \prod_{i=1}^{k} p_i^{\max(m_i,n_i)}$

We will give a proof of (a); the proof of (b) is similar. To prove (a) define $d = \prod_{i=1}^{k} p_i^{\min(m_i,n_i)}$. Thus we need to prove that $d = gcd(m,n)$. By the definition of *gcd* this amounts to checking two conditions:

(i) $d \mid m$ and $d \mid n$

(ii) If c is any integer such that $c \mid m$ and $c \mid n$, then $c \leq d$

Condition (i) follows immediately from the "$\Leftarrow$" direction of Problem 3 since $\min(m_i, n_i) \leq m_i$ and $\min(m_i, n_i) \leq n_i$ for each i.

To prove (ii) take any $c \in \mathbb{Z}$ such that $c \mid m$ and $c \mid n$. If $c \leq 0$, then we definitely have $c \leq d$ (since $d > 0$), so assume that $c > 0$. Then c is a positive divisor of m and c is a positive divisor of n, so by the "$\Rightarrow$" direction of Problem 3 we have $c = \prod_{i=1}^{k} p_i^{c_i}$ where for each i we have $c_i \in \mathbb{Z}_{\geq 0}$, $c_i \leq m_i$ and $c_i \leq n_i$. Combining the two inequalities, we get $c_i \leq \min(m_i, n_i)$ for each i. But then $p_i^{c_i} \leq p_i^{\min(m_i,n_i)}$ for each i and hence $c = \prod_{i=1}^{k} p_i^{c_i} \leq \prod_{i=1}^{k} p_i^{\min(m_i,n_i)} = d$.

5. Given an integer n and a prime p, define $\mathrm{ord}_p(n)$ to be the multiplicity with which p occurs in the prime factorization of n. If p does not occur in the prime factorization of n at all, set $\mathrm{ord}_p(n) = 0$. For instance,

$$\mathrm{ord}_p(45) = \begin{cases} 2 & \text{if } p = 3 \\ 1 & \text{if } p = 5 \\ 0 & \text{if } p \neq 3, 5. \end{cases}$$

Note that the results of Problems 2 and 3 can be restated as follows in terms of the ord_p function:

(2) Let $n \in \mathbb{N}$. Then n is a perfect square if and only if $\mathrm{ord}_p(n)$ is even for each prime p

(3) Let $m, n \in \mathbb{N}$. Then $m \mid n$ if and only if $\mathrm{ord}_p(m) \leq \mathrm{ord}_p(n)$ for each prime p.

Prove the following properties:

(a) $\mathrm{ord}_p(mn) = \mathrm{ord}_p(m) + \mathrm{ord}_p(n)$ for each prime p and for all $m, n \in \mathbb{N}$

(b) $\mathrm{ord}_p(m+n) \geq \min(\mathrm{ord}_p(m), \mathrm{ord}_p(n))$ for each prime p and for all $m, n \in \mathbb{N}$. Give an example showing that the inequality may be strict.

(c) Let $m, n \in \mathbb{N}$. Then m and n are relatively prime $\iff$ for each prime p we have $\mathrm{ord}_p(n) = 0$ or $\mathrm{ord}_p(m) = 0$.

Solution: (a) As explained at the beginning of Lecture 16, we can always write $m = \prod_{i=1}^{k} p_i^{m_i}$ and $n = \prod_{i=1}^{k} p_i^{n_i}$ where $p_1, \ldots, p_k$ are distinct primes and $m_i, n_i \in \mathbb{Z}_{\geq 0}$. By definition of the ord_p function we have $\mathrm{ord}_{p_i}(m) = m_i$

and $\text{ord}_{p_i}(n) = n_i$ for each $1 \leq i \leq k$ and $\text{ord}_p(m) = \text{ord}_p(n) = 0$ for each prime $p \notin \{p_1, \ldots, p_k\}$.

Now $mn = \prod_{i=1}^k p_i^{m_i} \prod_{i=1}^k p_i^{n_i} = \prod_{i=1}^k p_i^{m_i+n_i}$. Take any prime p. If $p = p_i$ for some $1 \leq i \leq k$, then from the above factorization we have $\text{ord}_p(mn) = m_i + n_i = \text{ord}_p(m) + \text{ord}_p(n)$. And if $p \notin \{p_1, \ldots, p_k\}$, then p does not appear in the prime factorization of mn, so $\text{ord}_p(mn) = 0 = 0 + 0 = \text{ord}_p(m) + \text{ord}_p(n)$.

(b) Let p be any prime. If p does not appear in the prime factorization of m or n, then $\text{ord}_p(m) = 0$ or $\text{ord}_p(n) = 0$. Hence $\min(\text{ord}_p(m), \text{ord}_p(n)) = 0$ and the inequality $\text{ord}_p(m+n) \geq \min(\text{ord}_p(m), \text{ord}_p(n))$ is automatically true since $\text{ord}_p(m+n) \geq 0$ by definition.

Thus, we can assume that p appears in the prime factorization of both m and n. Define $a = \text{ord}_p(m)$ and $b = \text{ord}_p(n)$. By definition of the ord_p function we can write $m = p^a u$ and $n = p^b v$ for some $u, v \in \mathbb{N}$ (the numbers u and v are the products of prime powers of primes different from p in the prime factorizations of m and n respectively; if there are no other primes in one or both of those factorizations, we set u and/or v equal to 1).

WOLOG assume that $a \leq b$, so that $\min(\text{ord}_p(m), \text{ord}_p(n)) = a$. Then we can write $m + n = p^a u + p^a(p^{b-a}v) = p^a w$ with $w = u + p^{b-a}v$. Since $w \in \mathbb{N}$ by construction, applying the result of part (1), we get $\text{ord}_p(m+n) = \text{ord}_p(p^a w) = \text{ord}_p(p^a) + \text{ord}_p(w) = a + \text{ord}_p(w) \geq a$ since $\text{ord}_p(w) \geq 0$.

Thus, we proved that $\text{ord}_p(m+n) \geq a = \min(\text{ord}_p(m), \text{ord}_p(n))$, as desired.

It remains to produce an example where the above inequality is strict. We let p be any prime, take $m = 1$ and $n = p - 1$. Then p does not divide m or n, so $\text{ord}_p(m) = \text{ord}_p(n) = 0$ and $\min(\text{ord}_p(m), \text{ord}_p(n)) = 0$ while $\text{ord}_p(m+n) = \text{ord}_p(p) = 1$.

(c) "$\Rightarrow$" Assume that m and n are relatively prime. Take any prime p. Since m and n are relatively prime, p cannot be a common divisor of m and n. Thus, $p \nmid m$ or $p \nmid n$ and hence $\text{ord}_p(m) = 0$ or $\text{ord}_p(n) = 0$.

"$\Leftarrow$" We prove this direction by contrapositive. The contrapositive asserts: if m and n are NOT relatively prime, then there exists a prime p such that $\text{ord}_p(m) > 0$ and $\text{ord}_p(n) > 0$.

So assume m and n are NOT relatively prime. This means that $gcd(m, n) > 1$, so $gcd(m, n)$ is divisible by at least one prime p. Then this prime p divides both m and n and hence $\text{ord}_p(m) \geq 1$ and $\text{ord}_p(n) \geq 1$, as desired.

6. Problem 17 in 3.3.

Solution: See Lecture 16.

7. Problem 3 in 3.4.

Let $a_k a_{k-1} \dots a_0$ be the decimal expansion of a natural number n. Thus by definition $n = a_0 + 10a_1 + \dots + 10^k a_k$.

Let $s = a_0 - a_1 + a_2 - \dots = \sum_{i=0}^{k} (-1)^i a_i$ be the alternating sum of the digits of n. We need to show that $11 \mid n \iff 11 \mid s$. Similarly to the proof of the criteria of divisibility by 3 and 4, it suffices to show that $11 \mid (n - s)$.

Note that $n - s = \sum_{i=0}^{k} 10^i a_i - \sum_{i=0}^{k} (-1)^i a_i = \sum_{i=0}^{k} (10^i - (-1)^i) a_i$. To prove that this number is divisible by 11, it suffices to check that $10^i - (-1)^i$ is divisible by 11 for each $i \in \mathbb{Z}_{\geq 0}$. We prove this separately for i even and i odd.

Case 1: i is even, so $i = 2j$ for some $j \in \mathbb{Z}_{\geq 0}$. Then $10^i - (-1)^i = 10^{2j} - 1$. If $j = 0$, then $10^{2j} - 1 = 0$ and there is nothing to prove. If $j > 0$, using the identity $x^{2j} - 1 = (x^2 - 1)(1 + x^2 + x^4 + \dots + x^{2j-2})$, we get that $10^{2j} - 1$ is divisible by $10^2 - 1 = 99 = 9 \cdot 11$, so in particular divisible by 11.

Case 2: i is odd, so $i = 2j + 1$ for some $j \in \mathbb{Z}_{\geq 0}$. Then $10^i - (-1)^i = 10^{2j+1} + 1$. This time we use the identity

$$x^{2j+1} + 1 = (x + 1)(1 - x + x^2 - x^3 + \dots - x^{2j-1} + x^{2j})$$

to conclude that $11 = 10 + 1$ divides $10^{2j+1} + 1$.