Homework #5 Solutions

Here are a few remarks about the terminology in the next couple of exercises. To be totally clear, an integer n is a *perfect square* if there is an integer m such that $n = m^2$. Note that, according to this definition, a perfect square is nonnegative (because the square of any real number is nonnegative). Also, a "perfect square" is the same thing as a "square." The notion of a square makes sense in any *ring* whatsoever (and the definition is identical to the one for the ring $\mathbf{Z}$ of integers, except that n and m are replaced by elements of the ring), but the use of "perfect square" seems to be mostly restricted to the context of integers. I prefer "square," so that is what I will usually say. (Yes, it is because I am a total square.)

3.5.6. Let $n > 1$ be an integer. (We assume that n is positive because the book only seems to explicitly discuss prime factorizations of positive integers. Of course negative integers have a kind of prime factorization too, preceded by a -1, but they can never be squares. The integers 0 and 1 can reasonably be called squares, but there is no sense in which they have well-defined (unique) prime factorizations, so they should be excluded.) Let $n = p_1^{e_1} \cdots p_r^{e_r}$ be the prime factorization of n. If each multiplicity e_i is even, then for each i there is an integer k_i such that $e_i = 2k_i$. We then have

$$n = p_1^{e_1} \cdots p_r^{e_r} = p_1^{2k_1} \cdots p_r^{2k_r} = (p_1^{k_1} \cdots p_r^{k_r})^2.$$

Thus, if we let $b = p_1^{k_1} \cdots p_r^{k_r}$, we see that $b^2 = n$, so n is a square. Conversely, retaining the notation introduced above for the prime factorization of n, assume there is an integer b (which we may take to be positive) such that $b^2 = n$ (i.e., assume that n is a square). Say b has prime factorization $q_1^{f_1} \cdots q_s^{f_s}$. Assume for convenience that the prime factorizations of n and b have been written with the primes in increasing order (this ensures that the order of each factorization is unique, as opposed to merely unique up to reordering). From $b^2 = a$ we obtain the formula

$$q_1^{2f_1} \cdots q_s^{2f_s} = p_1^{e_1} \cdots p_r^{e_r}.$$

Using the uniqueness of prime factorizations, we may conclude that $r = s$, that $p_i = q_i$, and that $e_i = 2f_i$ for $1 \leq i \leq r$. In particular, we deduce that the multiplicities in the prime factorization of n are all even.

3.5.8. We will give two proofs, one based on playing with multiplicities in prime factorizations, and the other (suggested on the course Piazza site by one of your classmates who should take credit in class for the idea) using induction.

For the first proof, let n be a positive integer with prime factorization $n = p_1^{e_1} \cdots p_g^{e_g}$, where the e_i are positive integers and the p_i are distinct primes, all uniquely determined by n (we are omitting $n = 1$ here, but 1 is $1 \cdot 1$, where 1 is both square-free and, in a paradox of terminology, a square, so the result is true for 1). For each i, write $e_i = 2q_i + r_i$ where q_i and r_i are as in the division algorithm, i.e., q_i and r_i are integers with $0 \leq r_i < 2$ (so $r_i = 0$

Date: February 23, 2018.

or $r_i = 1$). We may then write

$$\begin{aligned} n &= p_1^{e_1} \cdots p_g^{e_g} \\ &= p_1^{2q_1+r_1} \cdots p_g^{2q_g+r_g} \\ &= \left(p_1^{2q_1} \cdots p_g^{2q_g}\right)\left(p_1^{r_1} \cdots p_g^{r_g}\right) = \left(p_1^{q_1} \cdots p_g^{q_g}\right)^2 \left(p_1^{r_1} \cdots p_g^{r_g}\right). \end{aligned}$$

Letting $a = p_1^{q_1} \cdots p_g^{q_g}$ and $b = p_1^{r_1} \cdots p_g^{r_g}$, we see from the formula above that $n = a^2 b$. Of course a^2 is visibly square. Moreover, b is square-free as, according to Exercise 3.5.6, if b were divisible by a square other than 1, the multiplicity of each of the prime divisors of b would be at least 2, but we see above that these multiplicities, if any, are all 1. (Note that all the r_i might be zero, in which case $b = 1$ and $n = a^2$ is itself a square.)

The second proof by induction is somewhat cleaner. The base case $n = 1$ is trivial, as we have already observed. Assume then that $k \geq 1$ is a positive integer such that the assertion in question is true for all integers j with $1 \leq j \leq k$. If $k+1$ is square-free, then we are done, so we will assume that $k+1$ is not square-free. Then, by definition, there is an integer a such that $a^2 > 1$ and a^2 divides $k+1$; say $k+1 = a^2 b$, with b some integer (which is necessarily positive since $k+1$ and a^2 are positive). As $1 < a^2$, we must have $1 < b \leq k$, so we may apply the inductive hypothesis to b to write $b = c^2 d$ where c is an integer and d is a square-free integer. We then have

$$k+1 = a^2 b = a^2(c^2 d) = (a^2 c^2)d = (ac)^2 d.$$

Thus we have expressed $k+1$ as the product of the square $(ac)^2$ and the square-free integer d. By induction, the assertion is true for all integers $n \geq 1$.

Okay, I think I have finally come up with an argument for the next exercise. I do not claim it is optimal or elegant (probably such proofs exist on the internet, but as I have taken the assertion for granted for years (!) I really wanted to try to devise my own). In the proof, I do not directly prove that $v_p(n!)$ (the multiplicity of p in $n!$) is equal to the desired sum of floor values. Instead, I use a straightforward counting argument to obtain a intermediate sum for $v_p(n!)$, and then I show with a similar counting argument that the sum of floor values is in fact equal to the intermediate sum. The key step in the proof that facilitates counting is to list the positive multiples of p not exceeding n in increasing order, arranged in rows corresponding to the multiplicity of p in their prime factorizations. Throughout the proof, I will use the crucial fact (a consequence of Exercise 1.15.29 from Homework 2) that, for any integer $j \geq 1$, $[n/p^j]$ is the number of positive multiples of p^j not exceeding n. I really hope there is not a glitch in this argument, because I just spent an hour-and-a-half typing it. (I am pretty sure it is solid.)

3.5.12. Fix a prime p and let k be the unique nonnegative integer such that $p^k \leq n < p^{k+1}$ (more precisely, $k = [\log_p(n)]$, but this does not matter). Then $[n/p^j] = 0$ for $j > k$, so $\sum_{j=1}^{\infty} [n/p^j] = \sum_{j=1}^{k} [n/p^j]$. (In our notation below, for clarity, it is implicitly assumed that $p > 2$ and that $k > 2$. However, the argument works verbatim even if $p = 2$ or $1 \leq k \leq 2$, and the case in which $k = 0$ is trivial to verify.) The divisors of $n!$ that contribute factors of p are precisely the positive multiples of p not exceeding n. We can list these integers in increasing order, arranged in rows corresponding to the multiplicity of p in their prime

factorizations, as follows:

$$\begin{aligned}
&p, 2p, \ldots, (p-1)p \\
&p^2, 2p^2, \ldots, (p-1)p^2 \\
&\vdots \\
&p^{k-1}, 2p^{k-1}, \ldots, (p-1)p^{k-1} \\
&p^k, \ldots, [n/p^k]p^k.
\end{aligned}$$

We should justify that $[n/p^k]p^k$ really is the largest positive multiple of p not exceeding n. Now we compute $v_p(n!)$ by directly counting, making use of the list of multiples of p above. Each of the first $k-1$ rows has $p-1$ integers. Each integer in the first row contributes one factor of p to $n!$, meaning the integers in the first row contribute a total of $1 \cdot (p-1) = p-1$ factors of p to $n!$. Each integer in the second row contributes two factors of p to $n!$, meaning the integers in the second row contribute a total of $2(p-1)$ factors of p to $n!$. In general, the integers in the j-th row, $1 \leq j \leq k-1$, contribute a total of $j(p-1)$ factors of p to $n!$. Finally, the k-th row contains $[n/p^k]$ integers, each of which contributes k factors of p to $n!$, for a total contribution of $k[n/p^k]$ factors of p. We therefore have

$$v_p(n!) = \left(\sum_{j=1}^{k-1} j(p-1) \right) + k[n/p^k].$$

Now we consider the terms of the sum $\sum_{j=1}^{k}[n/p^j]$. The first summand, $[n/p]$, is the number of positive multiples of p not exceeding n. This is just the total number of integers in the list above, which is $(k-1)(p-1) + [n/p^k]$. The second summand, $[n/p^2]$, is the number of positive multiples of p^2 not exceeding n. This is the total number of integers in rows 2 through k of the list above, which is $(k-2)(p-1) + [n/p^k]$. In general, the j-th summand $[n/p^j]$, $1 \leq j \leq k$, is the total number of integers in rows j through k of the list above, which is $(k-j)(p-1) + [n/p^k]$. We therefore have

$$\sum_{j=1}^{k}[n/p^j] = \sum_{j=1}^{k} \left((k-j)(p-1) + [n/p^k] \right) = \left(\sum_{j=1}^{k} (k-j)(p-1) \right) + k[n/p^k].$$

It remains to observe that the rightmost sums enclosed in parentheses in the previous two displayed equations are in fact equal: the second sum has the same terms as the first, added in reverse order, plus an extra k-th term of $(k-k)(p-1) = 0$. We may therefore finally conclude that $v_p(n!) = \sum_{j=1}^{k}[n/p^k]$.

3.5.28. We will omit the steps of the Euclidean algorithm for computing the greatest common divisor of the given pairs of integers, since in each case it can be determined by inspection.

(a) We have $(8, 12) = 4$, so Theorem 3.16 gives

$$[8, 12] = \frac{8 \cdot 12}{4} = 2 \cdot 12 = 24.$$

(b) We have $(14, 15) = 1$, so Theorem 3.16 gives

$$[14, 15] = \frac{14 \cdot 15}{1} = 14 \cdot 15 = 210.$$

(c) We have $(28, 35) = 7$, so Theorem 3.16 gives

$$[28, 35] = \frac{28 \cdot 35}{7} = 4 \cdot 35 = 140.$$

3.5.38. The lemma that the book suggests can be used to prove the assertion, but the assertion follows more directly from Lemma 3.5. Indeed, our assumption is that $p \mid a^2 = a \cdot a$, so it follows immediately from Lemma 3.5 that $p \mid a$.

3.5.43. Let $\alpha = \sqrt{2} + \sqrt{3}$. Then $\alpha^2 = 2 + 2\sqrt{6} + 3$, so $\alpha^2 - 5 = 2\sqrt{6}$. Squaring both sides of this last equation, we obtain

$$24 = (\alpha^2 - 5)^2 = \alpha^4 - 10\alpha^2 + 25,$$

or equivalently, $\alpha^4 - 10\alpha^2 + 1 = 0$. Thus the real number α is a root of the polynomial $X^4 - 10X^2 + 1$, which has leading coefficient 1 and all other coefficients integral. According to Theorem 3.18, either α is an integer or α is irrational. To see that the former case is impossible, assume that α is in fact an integer. Then α^2 is an integer, and so, by the computation above, $2\sqrt{6} = \alpha^2 - 5$ is also an integer. But since $(2\sqrt{6})^2 = 24$, this would imply, by Exercise 3.5.6, that the multiplicity of each prime divisor of 24 is even, which is not the case (we have $24 = 2^3 \cdot 3$). Therefore α cannot be an integer. So α must be irrational.

3.5.45. We need to assume that b is not any power of p (including $p^0 = 1$). We argue by contradiction, and therefore assume that $\log_p(b)$ is rational, say $\log_p(b) = r/s$ with r and s positive integers ($\log_p(b)$ is positive because b and p are greater than 1). By the definition of the base-p logarithm, we have $p^{\log_p(b)} = b$, i.e., $p^{r/s} = b$. Raising both sides of this equation to the s-th power gives $p^r = b^s$. The lefthand side of this last equation is a power of p, so, by the uniqueness of prime factorizations, p is the only prime divisor of b^s. But then p is also the only prime divisor of b (any divisor of b also divides b^s). Therefore b is a power of p, contrary to assumption. It follows that $\log_p(b)$ must in fact be irrational.

3.5.62. Assume that a^2 divides b^2 and, for the sake of a contradiction, that a does not divide b. The first assumption means that we may write $b^2 = a^2 j$ for some (necessarily positive) integer j. Then $j = b^2/a^2 = (b/a)^2$, so $\sqrt{j} = b/a$. As we have assumed that a does not divide b, $\sqrt{j} = b/a$ is *not* an integer. Because $\sqrt{j}$ is a root of $X^2 - j$, and since $\sqrt{j}$ is real but not an integer, Theorem 3.18 implies that $\sqrt{j}$ is irrational. This contradicts the fact that $\sqrt{j} = b/a$ is visibly rational. Thus it must be that a divides b.

3.5.66. We will use Exercise 3.5.12. More precisely, we will show that, for any prime p, $v_p((m+n)!) \geq v_p(m!n!)$. This implies that the fraction $(m+n)!/(m!n!)$ is an integer (consider prime factorizations of the numerator and denominator). By the aforementioned exercise, we have

$$v_p((m+n)!) = \sum_{j=1}^{\infty} [(m+n)/p^j],$$

$$v_p(m!) = \sum_{j=1}^{\infty} [m/p^j], \text{ and}$$

$$v_p(n!) = \sum_{j=1}^{\infty} [n/p^j].$$

The laws of exponents show that $v_p(m!n!) = v_p(m!) + v_p(n!)$, so, using the second and third formulas above, we conclude that $v_p(m!n!) = \sum_{j=1}^{\infty} ([m/p^j] + [n/p^j])$. By Exercise 1.1.13, $[m/p^j] + [n/p^j] \leq [(m/p^j) + (n/p^j)] = [(m+n)/p^j]$ for any $j \geq 1$. Thus, upon summing over j, we find that $v_p((m+n)!) \geq v_p(m!n!)$, as desired.