HW 5

March 30, 2023

Problem 0.1 (Chapter 11, problem 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.

Proof. By the fundamental theorem of arithmetic, we can write

$$n = p_1^{\alpha_1} \cdots p_m^{\alpha_m}$$

for some primes $p_1 < \cdots < p_m$ and integers $\alpha_i \geq 1$. In our case, we are assuming that in fact $\alpha_i \geq 2$ for all $1 \leq i \leq m$.

I claim that if a is an integer and $a \geq 2$, then we can write $a = 2s + 3t$ for some non–negative integers s, t. Here is one way to prove this. It is definitely true if a is even, because then $a = 2k$ for some $k \geq 1$. If a is odd, then $a = 2k + 1$ for some $k \geq 1$, and so $a = 2k + 1 = 2(k - 1) + 3$ (and $k - 1 \geq 0$!). (2 points)

Now, for each i, write $\alpha_i = 2s_i + 3t_i$ for some non–negative integers s_i, t_i. We have

$$\begin{aligned} n = p_1^{\alpha_1} \cdots p_m^{\alpha_m} &= p_1^{2s_1+3t_1} \cdots p_m^{2s_m+3t_m} \\ &= \left(p_1^{2s_1} \cdots p_m^{2s_m}\right)\left(p_1^{3t_1} \cdots p_m^{3t_m}\right) \\ &= \left(p_1^{s_1} \cdots p_m^{s_m}\right)^2 \left(p_1^{t_1} \cdots p_m^{t_m}\right)^3 \end{aligned}$$

Therefore n is the product of a square and a cube. □

Problem 0.2 (Chapter 12, problem 4)**.** Prove that there are infinitely many primes of the form $4k+3$ (where k is an integer).

Proof. We claim that, for every $k \geq 1$, the number $4k + 3$ has a prime factor which is of the form $4l + 3$. We will prove this by total induction on k. It is definitely true if $k = 1$ (base case). Suppose we know it is true for $4 \cdot 1 + 3, 4 \cdot 2 + 3, \ldots, 4 \cdot k + 3$. Consider the number $4(k + 1) + 3$. This number is odd, so we can write it as the product of two odd numbers, say x and y.

$$4(k + 1) + 3 = xy$$

Furthermore, we must have that one of x and y is of the form $4a + 1$ and the other is of the form $4a + 3$. This is because the product of two numbers of the form $4a + 1$ is again of the form $4a + 1$, and the product of two numbers of the form $4a + 3$ is of the form $4a + 1$ (because $3^2 = 9 = 4 \cdot 2 + 1$). Therefore we have

$$4(k + 1) + 3 = (4a + 1)(4b + 3)$$

By our induction hypothesis, $4b + 3$ has a prime factor of the form $4c + 1$. Hence so does $4(k + 1)$

Now we prove the statement of the problem. Let $p_1, \ldots, p_m$ be a collection of distinct prime numbers. We might as well assume that $p_1 = 3$. Suppose that $p_i = 4k_i + 3$ for some integer k_i. Consider the product

$$N = 3 + \prod_{i=1}^{m} p_i = 3 + \prod_{i=1}^{m} (4k_i + 3)$$

Let q be a prime factor of N such that $q > 3$. If q were equal to any of the p_i, then q would divide 3, a contradiction. So q is not equal to any of the p_i. Furthermore, by the claim we proved above, we can find a prime factor q of N such that q is of the form $q = 4k + 3$. Therefore there is a prime of this form which is not on our list. We conclude that there are infinitely many primes of the form $4k + 3$. □

Problem 0.3 (Chapter 13, problem 4a)**.** Prove the "rule of 9": an integer is divisible by 9 if and only if the sum of its digits is divisible by 9.

Proof. We observe that

$$10 \equiv 1 \pmod 9$$

Therefore

$$10^k \equiv 1 \pmod 9$$

for every integer $k \geq 1$. (2 points)

Now suppose n is an integer, and let

$$n = a_r \ldots a_1 a_0$$

be its digit expansion. We have

$$n = 10^r a_r + \cdots + 10^1 a_1 + a_0$$

Reduce modulo 9 to get

$$\begin{aligned} n &\equiv 10^r a_r + \cdots + 10^1 a_1 + a_0 \pmod 9 \\ &\equiv 1 \cdot a_r + \cdots + 1 \cdot a_1 + a_0 \pmod 9 \\ &\equiv a_r + \cdots + a_1 + a_0 \pmod 9 \end{aligned}$$

(3 points) □