PROBLEM 1. Let $a, b, c \in \mathbb{Z}$ and suppose that $a|b$ and $b|c$. Prove that $a|c$. (Start by appealing to definition of divisibility to unravel the meaning of $a|b$ and $b|c$.)

SOLUTION: We are given that $b = ak$ and $c = b\ell$ for some integers k and ℓ. Therefore,

$$c = b\ell = (ak)\ell = a(k\ell).$$

Letting $m := k\ell$, we have that m is an integer and $c = am$. Therefore, $a|c$.

PROBLEM 2. Prove that if $a|b$ and $a|c$, then $a|(mb + nc)$ for all $m, n \in \mathbb{Z}$.

SOLUTION: By hypothesis, $b = ak$ and $c = a\ell$ for some integers k, ℓ. Thus $mb + nc = mak + na\ell = a(mk + n\ell)$, and since $mk + n\ell \in \mathbb{Z}$ we have that $a \mid mb + nc$.

PROBLEM 3. Suppose p is prime and that a and k are positive integers. Why is it the case that if $p|a^k$, then $p^k|a^k$?

SOLUTION: Let $a = p_1^{a_1} \cdots p_m^{a_m}$ be the factorization of a into distinct primes. Then the prime factorization of a^k is $p_1^{a_1 k} \cdots p_m^{a_m k}$. Since $p|a^k$, there exists an integer n such that $a^k = pn$. Since p appears in the prime factorization of pn, is must also occur in the prime factorization of a^k. This means that $p = p_i$ for some $i \in \{1, \ldots, m\}$. Note that incidentally this also means that $p|a$. Without loss of generality, we may assume $p = p_1$. Then, $a_1 \geq 1$, and

$$a^k = p_1^{a_1 k} \cdots p_m^{a_m k} = p_1^k \left(p_1^{a_1 k - k} \cdots p_m^{a_m k} \right) = p^k \left(p_1^{(a_1 - 1)k} \cdots p_m^{a_m k} \right).$$

Letting $r := p_1^{(a_1-1)k} \cdots p_m^{a_m k}$, we have $a^k = p^k r$, and hence, $p^k|a^k$.

PROBLEM 4. Prove that if p is a prime number, then $\sqrt{p}$ is irrational.

SOLUTION: We will prove this by contradiction. Say $\sqrt{p} = \frac{a}{b}$ for some integers a, b. By canceling, we may assume $\frac{a}{b}$ is in lowest terms. We have

$$\sqrt{p} = \frac{a}{b} \quad \Rightarrow \quad a^2 = pb^2.$$

Thus, $p|a^2$. By Corollary 197, we have that $p|a$. So we can write $a = pc$. Then,

$$a^2 = pb^2 \Rightarrow (pc)^2 = pb^2 \Rightarrow p^2c^2 = pb^2 \Rightarrow pc^2 = b^2.$$

Hence, $p|b$, as well. This contradicts the fact that $\frac{a}{b}$ is in lowest terms.

PROBLEM 5. Prove that a positive integer n is prime if and only if it is not divisible by any prime p such that $1 < p \leq \sqrt{n}$. What does this say in the case $n = 91$?

SOLUTION: First suppose that n is prime. Then it is not divisible by any positive integer except 1 and n, and thus is not divisible by the prime numbers in question.

Now suppose that n is not prime, in which case it has prime factorization $n = p_1 p_2 \cdots p_k$ with $p_1 \leq \cdots \leq p_k$ all prime. Suppose for contradiction that $\sqrt{n} < p_1$. Then $n = \sqrt{n} \cdot \sqrt{n} < p_1 p_2 \leq n$, i.e., $n < n$, a contradiction.

In the case of $n = 91$, we have $7 < \sqrt{n} < 11$. So to determine whether 91 has a prime factor, we just need to check the primes $2, 3, 5$ and 7. It is clear that $2, 3$ and 5 do not divide 91, but in fact, $91 = 7 \cdot 13$. The number 91 is known as the smallest number that looks like a prime but isn't.

PROBLEM 6. Suppose that a positive integer n has prime factorization $n = p_1^{a_1} \cdots p_k^{a_k}$ with the p_i distinct primes. How many distinct positive integers are divisors of n?

SOLUTION: The divisors of n take the form $p_1^{b_1} \cdots p_k^{b_k}$ with $0 \leq b_i \leq a_i$. Since there are $a_i + 1$ potential values of b_i, we know that n has $(a_1 + 1)(a_2 + 1) \cdots (a_k + 1)$ divisors.