Worksheet 7: Induction, Prime Factorization

Problem 1. Prove that
$$\frac{(2n)!}{2^n \cdot n!}$$
is an integer for all $n \geqslant 0$.

Solution. We induct on n. When $n = 0$, we have
$$\frac{(2n)!}{2^n \cdot n!} = \frac{0!}{2^0 \cdot 0!} = 1$$
which is in fact an integer. For the inductive step, suppose we know that
$$\frac{(2k)!}{2^k \cdot k!}$$
is an integer. Observe that
$$\begin{aligned}\frac{(2(k+1))!}{2^{k+1} \cdot (k+1)!} &= \frac{(2k+2)(2k+1) \cdot (2k)!}{2 \cdot (k+1) \cdot 2^k \cdot k!} \\ &= (2k+1) \cdot \frac{(2k)!}{2^k \cdot k!}.\end{aligned}$$
Since $2k+1$ is an integer, and since $(2k)!/(2^k \cdot k!)$ is an integer by our inductive hypothesis, it follows that $(2(k+1))!/(2^{k+1} \cdot (k+1)!)$ is also an integer.

Problem 2. Prove that $15 \mid 2^{4n} - 1$ for all non-negative integers n.

Solution. The $n = 0$ case is clear, since $2^{4 \cdot 0} - 1 = 0$. Suppose that $15 \mid 2^{4k} - 1$. Then
$$2^{4(k+1)} - 1 = 2^{4k+4} - 1 = 2^{4k} \cdot 2^4 - 1 = (2^{4k} - 1) \cdot 2^4 + 2^4 - 1 = (2^{4k} - 1) \cdot 2^4 + 15.$$
Since $15 \mid 15$ and $15 \mid (2^{4k} - 1)$, we see that $15 \mid 2^{4(k+1)} - 1$ as well, completing the induction.

Problem 3. Let $F_1 = F_2 = 1$ and $F_n = F_{n-1} + F_{n-2}$ for all $n \geqslant 3$. Show that F_n is even if and only if $3 \mid n$.

Solution. We use strong induction. The base cases are easy: since $F_1 = 1$ and $F_2 = 1$ are both odd, the statement is true for $n \leqslant 2$. For the inductive step, suppose $k \geqslant 2$ and that F_m is even if and only if $3 \mid m$ for all $1 \leqslant m \leqslant k$. We prove that F_{k+1} is even if and only if $3 \mid k+1$ using cases:

- Suppose $k \equiv 0 \bmod 3$. By our inductive hypothesis, we know that F_k is even and F_{k-1} is odd, so $F_{k+1} = F_k + F_{k-1}$ is odd.
- Suppose $k \equiv 1 \bmod 3$. By our inductive hypothesis, we know that F_k is odd and F_{k-1} is even, so $F_{k+1} = F_k + F_{k-1}$ is odd.
- Suppose $k \equiv 2 \bmod 3$. By our inductive hypothesis, we know that F_k and F_{k-1} are both odd, so $F_{k+1} = F_k + F_{k-1}$ is even.

This completes the induction.

Problem 4. Suppose $p_1, \ldots, p_n$ are distinct primes. Show that $\sqrt{p_1 \cdots p_n}$ is irrational.

Solution. Suppose for a contradiction that its square root is rational. Then there exist integers a and b such that $\gcd(a, b) = 1$ and $\sqrt{p_1 \cdots p_n} = a/b$. This means that $p_1 \cdots p_n b^2 = a^2$. Notice that $p_1 \mid a^2$, so by Euclid's lemma, $p_1 \mid a$. Thus there exists an integer x such that $a = p_1 x$, so then
$$p_1 \cdots p_n b^2 = a^2 = (p_1 x)^2 = p_1^2 x^2.$$
Dividing through by p_1, we see that
$$p_2 \cdots p_n b^2 = p_1 x^2.$$
Thus $p_1 \mid p_2 \cdots p_n b^2$. But $p_1 \neq p_2, \cdots, p_n$, so by Euclid's lemma, we must have $p_1 \mid b^2$, and by Euclid's lemma again, this means that $p_1 \mid b$. This p_1 is a common divisor of a and b, contradicting our choice that $\gcd(a, b) = 1$.

Problem 5. Let $p_1, p_2, p_3, \ldots$ be a list of the primes in increasing order. Prove that $p_n \leqslant p_1 \cdots p_{n-1} - 1$ for all $n \geqslant 3$.

Solution. Let $a = p_1 \cdots p_{n-1} - 1$. Since $n \geqslant 3$ and we have $p_1 = 2$ and $p_2 = 3$, we have $a \geqslant 2 \cdot 3 - 1 \geqslant 5$. In particular, it has some prime factor q by the fundamental theorem of arithmetic. This means means that $q \leqslant a$. Since $a \equiv -1 \not\equiv 0 \mod p_i$ for $i = 1, \ldots, n-1$, we know that $q \neq p_i$ for all $i = 1, \ldots, n-1$. Since $p_1, p_2, \ldots$ is a list of the primes in order, we must have $q \geqslant p_n$. Thus we have

$$p_n \leqslant q \leqslant a = p_1 \cdots p_{n-1} + 1,$$

completing the proof.

Problem 6. Let $a \geqslant 2$ be an integer. By the fundamental theorem of arithmetic, there exist distinct primes $p_1, \ldots, p_n$ and positive integers $e_1, \ldots, e_n \in \mathbb{N}$ such that $a = p_1^{e_1} \cdots p_n^{e_n}$. Show that a is a perfect square if and only if e_i is even for all $i = 1, \ldots, n$.

Solution. By the division algorithm, we can write $e_i = 2f_i + r_i$ where $r_i \in \{0, 1\}$ for all i, and e_i is even if and only if $r_i = 0$. Moreover, a is a perfect square if and only if $\sqrt{a}$ is an integer. Thus, we are trying to show that $\sqrt{a}$ is an integer if and only if $r_i = 0$ for all i. Observe that

$$\sqrt{a} = \sqrt{p_1^{e_1} \cdots p_n^{e_n}} = \sqrt{p_1^{2f_1 + r_1} \cdots p_n^{2f_n + r_n}} = p_1^{f_1} \cdots p_n^{f_n} \sqrt{p_1^{r_1} \cdots p_n^{r_n}}.$$

If all of the r_i are 0, then the part under the square root is just 1 and $\sqrt{a}$ is an integer. Conversely, if even one of the r_i is not 1, then the square root above is irrational by problem 4, so $\sqrt{a}$ is not an integer.