Chapter 0, Problem 20

Let $p_1, \ldots, p_n$ be a collection of primes. We must show that p_i does not divide $p_1 \ldots p_n + 1$.

Method 1: Proof by contradiction

Suppose p_i divides $p_1 \ldots p_n + 1$. Then by definition,

$$p_1 \ldots p_n + 1 = mp_i$$

for some integer m. Note that $p_1 \ldots p_n$ itself is divisible by p_i. We can see this by factoring out p_i:

$$p_1 \ldots p_n = (p_1 \ldots p_{i-1} p_{i+1} \ldots p_n)\, p_i$$

Before continuing, we should note that p_i does not divide 1.

Now let us arrive at a contradiction. Subtract the second equation from the first:

$$p_1 \ldots p_n + 1 - p_1 \ldots p_n = mp_i - (p_1 \ldots p_{i-1} p_{i+1} \ldots p_n)\, p_i$$
$$1 = (m - p_1 \ldots p_{i-1} p_{i+1} \ldots p_n)\, p_i$$

This means that p_i divides 1, which is a contradiction. So p_i does not divide $p_1 \ldots p_n + 1$.

Inspiration for proof: p_i divides $p_1 \ldots p_n$. Can p_i also divide the next consecutive number? What would happen if it did?

Method 2: Division Algorithm

Let us apply the division algorithm on $p_1 \ldots p_n + 1$ with $a = p_1 \ldots p_n + 1$ and $b = p_i$:

$$p_1 \ldots p_n + 1 = (p_1 \ldots p_{i-1} p_{i+1} \ldots p_n)\, p_i + 1$$

We see that dividing $p_1 \ldots p_n + 1$ by p_i will result in a remainder of 1. Therefore, it is not divisible by p_i.

Inspiration: $p_1 \ldots p_n + 1$ already looks like the right side of the division algorithm. We just need to factor out p_i.

Chapter 0, Problem 32

Method 1: Induction on n (note: this only proves the problem for positive integers)

Base case $n = 1$: $1^3 \bmod 6 = 1 \bmod 6$

Suppose the statement is true for $n = k$: $k^3 \bmod 6 = k \bmod 6$ (this is also known as assuming $P(k)$).

We will show that this implies the corresponding equality with $n = k + 1$ is true (we prove $P(k+1)$):

On the left, we start with

$$(k+1)^3 \bmod 6$$

We do not know if this is $k+1 \bmod 6$ yet, so don't set it equal yet! But we can expand:

$$= k^3 + 3k^2 + 3k + 1 \bmod 6$$

$k^3 \bmod 6 = k \bmod 6$, so we can replace the k^3 by k:

$$= k + 3k^2 + 3k + 1 \bmod 6$$

$$= (k+1) + 3k^2 + 3k \bmod 6$$

We want $k+1$ by itself. To do this, we must show that $3k^2+3k \bmod 6 = 0 \bmod 6$. In other words, we must show that $3k^2 + 3k$ is divisible by six. Let us use induction again:

Base case $k = 1$: $3(1^2) + 3(1) = 6$ which is divisible by 6.

Suppose $3j^2 + 3j$ (we need a different variable) is divisible by 6. We need to show that $3(j+1)^2 + 3(j+1)$ is divisible by six.

$$3(j+1)^2 + 3(j+1) = (3j^2 + 6j + 3) + (3j + 3) = 3j^2 + 3j + 6j + 6$$

By the inductive hypothesis, $3j^2 + 3j$ is divisible by six. $6j + 6 = 6(j+1)$ is also divisible by six, so the sum is divisible by six. This proves the inductive step. So $3k^2 + 3k$ is divisible by six for any positive integer k.

Note: you can also factor $3k^2 + 3k$ as $3k(k+1)$ and either use induction, or point that since either k or $k+1$ is divisible by 2, and $3k(k+1)$ is divisible by 3, $3k(k+1)$ must also be divisible by $2 \cdot 3 = 6$. If you try induction and get stuck, expand $3(j+1)(j+2)$ as $3(j+1)j + 3(j+1)2$.

Now let us resume the original induction:

$$(k+1)^3 \bmod 6 = (k+1) + 3k^2 + 3k \bmod 6$$

$$= (k+1) + 0 \bmod 6$$

$$= (k+1) \bmod 6$$

which is what we wanted to show. Therefore, by induction, for any positive integer n, $n^3 \bmod 6 = n \bmod 6$.

Method 2: Divisibility by 2,3, and 6, and Consecutive Integers

Before we start, let us look at the assertion: $n^3 \bmod 6 = n \bmod 6$. This is equivalent to $n^3 - n \bmod 6 = 0 \bmod 6$, which by definition means that $n^3 - n$ is divisible by six. So we will prove that instead.

We can factor $n^3 - n$ as $n(n^2 - 1) = n(n-1)(n+1)$. Rearrange the factors in order:

$$(n-1)(n)(n+1)$$

Now we can determine divisibility by 6. We can split this into two steps:

Step 1: Divisibility by 2

We only need to know if one of the three factors is even. This is guaranteed, because either $n+1$ is divisible by 2, or if not, then $n+1$ has a remainder of 1 when dividing by 2, but that would mean n itself is divisible by 2. Since one of the factors is divisible by 2, the entire product must be divisible by 2.

Step 2: Divisibility by 3

Intuitively, if we have three consecutive numbers, one of them is divisible by 3. Either $n+1$ is divisible by 3, or it has a remainder of 1 or 2, in which case n or $n-1$ is divisible by 3. Thus, the entire product is divisible by 3.

Since $n^3 - n = (n-1)(n)(n+1)$ is divisible by 2 and 3, it must also be divisible by 6, which is what we wanted to show.

Method 3: Reduction to six cases

Let $r \in \{0, 1, 2, 3, 4, 5\}$ (the possible remainders when dividing by 6). If $n \bmod 6 = r \bmod 6$, then $n^3 \bmod 6 = r^3 \bmod 6$, so if we can show

$$r^3 \bmod 6 = r \bmod 6$$

for all possible values of r, we can then conclude

$$n^3 \bmod 6 = r^3 \bmod 6 = r \bmod 6 = n \bmod 6$$

for any integer n.

A direct calculation for each value of r will suffice:

$$0^3 \bmod 6 = 0 \bmod 6$$

$$1^3 \bmod 6 = 1 \bmod 6$$

$$2^3 \bmod 6 = 8 \bmod 6 = 2 \bmod 6 \ (6+2)$$

$$3^3 \bmod 6 = 27 \bmod 6 = 3 \bmod 6 \ (24+3)$$

$$4^3 \bmod 6 = 64 \bmod 6 = 4 \bmod 6 \ (60+4)$$

$$5^3 \bmod 6 = 125 \bmod 6 = 5 \bmod 6 \ (120+5)$$

Note: When choosing values of r, any six integers that are not equal to each other mod 6 will do. A good alternative choice is $r \in \{-2, -1, 0, 1, 2, 3\}$.