1. (§1.3, problem 8) Let \( n \) be a positive integer, and let \( r \) be the integer obtained by removing the last digit from \( n \) and then subtracting two times the digit just removed. (See the hint in NZM for a nice way to formalize this operation.) Prove that \( 7 | n \) if and only if \( 7 | r \).

**Proof:** Let \( u \) be the units digit of \( n \), and write \( n = 10m + u \) for some integer \( m \). Then \( r = m - 2u \).

Observe that

\[
 n - 3r = 7m + 7u
\]

so that \( 7 | (n - 3r) \).

Now suppose \( 7 | n \). Then since \( 7 | (n - 3r) \), it follows by Theorem 1.1(3) that \( 7 | 3r \). Since \((7, 3) = 1\) and \( 7 | 3r \), we get from Theorem 1.10 that \( 7 | r \).

For the converse, suppose \( 7 | r \). Then since \( 7 | (n - 3r) \) also, by Theorem 1.1(3) we get \( 7 | n \). \( \blacksquare \)

2. (Based on §1.3, problem 16) Find a positive integer \( n \) such that \( n/2 \) is a square, \( n/3 \) is a cube, and \( n/5 \) is a fifth power. Have you found the least such positive integer?

**Solution:** Let \( n \) be our integer. Clearly \( n \) must be divisible by 2, 3, and 5, so to get started, let’s write

\[
 n = 2^a3^b5^c
\]

The given conditions tell us that \( a \) must be odd and a multiple of both 3 and 5; \( b \) must be of the form \( 3k + 1 \) and must be a multiple of both 2 and 5; and \( c \) must be of the form \( 5k + 1 \) and must be a multiple of both 2 and 3.

That is, the number \( a \) must satisfy

\[
 a \equiv 1 \pmod{2}, \quad a \equiv 0 \pmod{3}, \quad a \equiv 0 \pmod{5}.
\]

Any positive solution to this system must be divisible by \([3, 5] = 15\), and the least such number is \( a = 15 \).

The number \( b \) must satisfy

\[
 b \equiv 0 \pmod{2}, \quad b \equiv 1 \pmod{3}, \quad b \equiv 0 \pmod{5}.
\]
Again, any positive solution to this system must be divisible by \([2, 5] = 10\), and the number 10 happens to be a solution.

Finally, the number \(c\) must satisfy
\[
c \equiv 0 \pmod{2}, \quad c \equiv 0 \pmod{3}, \quad c \equiv 1 \pmod{5}.
\]
That is, \(c\) must be a multiple of \([2, 3] = 6\), and it happens that \(c = 6\) satisfies all three congruences.

Taking \(a = 15\), \(b = 10\), and \(c = 6\), we get
\[
n = 2^{15}3^{10}5^6 = 30,233,088,000,000.
\]

This is the smallest such number because the three exponents we chose were all the least positive integers satisfying their respective criteria.

3. (Based on §1.3, problem 17)

Let \(P\) be the set of pairs of twin primes greater than 2. That is, let
\[
P = \{(3, 5), (5, 7), (11, 13), (17, 19), \ldots\}.
\]

Let \(N\) be the set of positive integers \(n > 3\) such that \(n^2 - 1\) has exactly four positive divisors. Prove that there is a one-to-one correspondence between \(P\) and \(N\).

**Proof:**

For each pair \((p, p + 2) \in P\), let \(\Phi(p, p + 2) = p + 1\). Then if \(n = \Phi(p, p + 2)\), we have
\[
n^2 - 1 = (p + 1)^2 - 1
= ((p + 1) - 1)((p + 1) + 1)
= p(p + 2),
\]
the product of two distinct primes. Thus there are exactly four positive divisors of \(n^2 - 1\), namely, 1, \(p\), \(p + 2\), and \(p(p + 2)\). To see that these divisors are all distinct, we need only point out that \(p > 1\) and \(2 > 0\). Together these imply that
\[
1 < p < p + 2 < p(p + 2).
\]
Furthermore, since \(p \geq 3\), we have \(p + 1 > 3\). Therefore, \(n \in N\). This shows that the range of \(\Phi\) is a subset of \(N\).
The map $\Phi$ is clearly one-to-one, because if $\Phi(p, p+2) = \Phi(q, q+2)$, then $p+1 = q+1$, from which it follows that $(p, p+2) = (q, q+2)$.

The map $\Phi$ is also onto. Let $n \in \mathbb{N}$. Write

$$n^2 - 1 = (n-1)(n+1).$$

Since $n > 3$, we have $n - 1 > 1$. Multiply both sides by the positive integer $n + 1$ to get

$$n^2 - 1 > n + 1.$$

This establishes that

$$1 < n - 1 < n + 1 < n^2 - 1,$$

so that these four integers are all distinct and positive. They are also all divisors of $n^2 - 1$, and since $n \in \mathbb{N}$, they must be the only four positive divisors of $n^2 - 1$.

It follows that $n - 1$ must be prime, for otherwise it would have a prime divisor $p$ between 1 and $n - 1$, and then $p$ would be a fifth positive divisor of $n^2 - 1$.

Similarly, $n + 1$ can have no proper divisors other than $n - 1$, because any such divisor would be a fifth positive divisor of $n^2 - 1$. If $(n - 1)|(n + 1)$ for positive $n$, we must have $2(n - 1) \leq n + 1$, from which it follows that $n \leq 3$. But we know $n > 3$, so $n - 1$ cannot be a factor of $n + 1$, and thus $n + 1$ is prime.

We have shown that if $n \in \mathbb{N}$, then $n - 1$ and $n + 1$ are both primes, and since $n > 3$, we have $n - 1 \geq 3$, so the pair $(n - 1, n + 1)$ is an element of $\mathcal{P}$. Finally, we have

$$\Phi(n - 1, n + 1) = n,$$

and since $n$ was an arbitrary element of $\mathbb{N}$, we have shown that $\Phi$ is onto.

Thus the map $\Phi$ is the desired one-to-one correspondence between $\mathcal{P}$ and $\mathbb{N}$.

4. (Part of §1.3, problem 19.) Let $a$ and $b$ be positive integers such that $(a, b) = 1$ and $ab$ is a perfect square. Prove that $a$ and $b$ are perfect squares.

**Proof:** By the Fundamental Theorem of Arithmetic, we may write

$$a = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k} \cdots$$

$$b = p_1^{f_1} p_2^{f_2} \cdots p_k^{f_k} \cdots$$
where \( p_1, p_2, \ldots \) is the sequence of primes, and all exponents are zero once we get far enough out in the sequence.

Since \( ab \) is a perfect square, we know that \( e_i + f_i \) is even for every \( i \).

Since \( (a, b) = 1 \), we know that, for each \( i \), only one of \( e_i \) and \( f_i \) is non-zero.

Now for each \( i \), we have that \( e_i + f_i \) is even, and either \( e_i = 0 \) (in which case \( f_i \) must be even) or \( f_i = 0 \) (in which case \( e_i \) must be even). In either case, both \( e_i \) and \( f_i \) are even (the number 0 is even, despite the deeply-held beliefs of certain calculus students), and it follows that \( a \) and \( b \) are both perfect squares. \( \square \)

5. (§1.3, problem 31 – also read problem 30 and the remarks following problem 31) Prove that no polynomial \( f(x) \) of degree greater than (or equal to) 1 with integral coefficients can represent a prime for every positive integer \( x \).

**Proof:** Write

\[
f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n.
\]

Suppose \( f(x) \) is prime for every positive integer \( x \). Let \( p = f(1) \). Then \( p \) is prime. Now let \( k \) be a positive integer, and consider

\[
f(1 + kp) = a_0 + a_1 (1 + kp) + a_2 (1 + kp)^2 + \cdots + a_n (1 + kp)^n.
\]

Note that for each \( j \geq 1 \),

\[
(1 + kp)^j = 1 + \binom{j}{1} kp + \binom{j}{2} (kp)^2 + \cdots + \binom{j}{j-1} (kp)^{j-1} + (kp)^j
\]

where \( N_j \) is the integer given by

\[
N_j = \binom{j}{1} k + \binom{j}{2} k^2 p + \cdots + \binom{j}{j-1} k^{j-1} p^{j-2} + k^j p^{j-1}.
\]

Thus we may write

\[
f(1 + kp) = (1 + pN_0)a_0 + (1 + pN_1)a_1 + \cdots + (1 + pN_n)a_n
\]

\[
= a_0 + a_1 + \cdots + a_n + a_0(pN_0) + a_1(pN_1) + a_2(pN_2) + \cdots + a_n(pN_n)
\]

\[
= f(1) + p(N_0 + N_1 + \cdots + N_n).
\]
In fact, since \( f(1) = p \), we have

\[
f(1 + kp) = p(1 + N_0 + N_1 + \cdots + N_n)
\]

so that \( p | f(1 + kp) \) for all integers \( k \geq 0 \).

Now by hypothesis, \( f(1 + kp) \) is prime for every \( k \geq 0 \), so it follows that \( f(1 + kp) = p \) for every \( k \geq 0 \).

Consider \( g(x) = f(x) - p \). Then \( g(x) \) is a polynomial and \( g(1 + kp) = 0 \) for every \( k \geq 0 \). That is, \( g \) has infinitely many roots. So \( g \) must be identically 0. Thus \( f \) must be identically equal to \( p \). But this contradicts the assumption that the degree of \( f \) is greater than or equal to 1.

6. (Part of §1.3, problem 53) Let \( \pi(x) \) denote the number of primes not exceeding \( x \). Show that

\[
\sum_{p \leq x} \frac{1}{p} = \frac{\pi(x)}{x} + \int_{2}^{x} \frac{\pi(u)}{u^2} \, du
\]

where the sum is taken over all primes \( p \) less than or equal to \( x \).

**Proof:** First we note that for a positive integer \( k > 1 \),

\[
\pi(k) - \pi(k - 1) = \begin{cases} 
1 & \text{if } k \text{ is prime} \\
0 & \text{if } k \text{ is composite}.
\end{cases}
\]

Next we observe that \( \pi(u) \) is constant in any interval \([n - 1, n)\) where \( n \) is an integer. Thus we get

\[
\int_{n-1}^{n} \frac{\pi(u)}{u^2} \, du = \pi(n - 1) \int_{n-1}^{n} \frac{du}{u^2} = \pi(n - 1)\left[ \frac{1}{n - 1} - \frac{1}{n} \right].
\]

We write

\[
\int_{2}^{x} \frac{\pi(u)}{u^2} \, du = \int_{2}^{3} \frac{\pi(u)}{u^2} \, du + \int_{3}^{4} \frac{\pi(u)}{u^2} \, du + \cdots + \int_{[x]-1}^{[x]} \frac{\pi(u)}{u^2} \, du + \int_{[x]}^{x} \frac{\pi(u)}{u^2} \, du
\]

\[
= \pi(2)\left[ \frac{1}{2} - \frac{1}{3} \right] + \pi(3)\left[ \frac{1}{3} - \frac{1}{4} \right] + \cdots + \pi([x] - 1)\left[ \frac{1}{[x] - 1} - \frac{1}{[x]} \right] + \pi([x])\left[ \frac{1}{[x]} - \frac{1}{x} \right],
\]
where the factor $\pi([x])$ comes out of the final integral because $\pi(u)$ is constant on $[[x], x)$.

We collect multiples of each reciprocal $1/n$ to get

$$
\int_2^x \frac{\pi(u)}{u^2} \, du = \frac{1}{2}\pi(2) + \frac{1}{3}(\pi(3) - \pi(2)) + \frac{1}{4}(\pi(4) - \pi(3)) + \cdots + \frac{1}{[x]}(\pi([x]) - \pi([x] - 1)) - \frac{1}{x}\pi([x]).
$$

Next we use the fact that $\pi(2) = 1$ and $\pi(n) - \pi(n - 1)$ is 1 if $n$ is prime and 0 if $n$ is composite to write

$$
\int_2^x \frac{\pi(u)}{u^2} \, du = \sum_{p \leq x} 1 - \frac{\pi([x])}{x}
$$

where the sum is taken only over the primes.

Finally, we note that $\pi([x]) = \pi(x)$ and move the rightmost term to the left side of the equation to conclude that

$$
\int_2^x \frac{\pi(u)}{u^2} \, du + \frac{\pi(x)}{x} = \sum_{p \leq x} \frac{1}{p}
$$

as required.