1 Exercises

1.1

How many even primes are there? How many whose last digit is 5?

2 is the only even prime; any other even number is divisible by 2, and thus not prime. 5 is the only number whose last digit is 5; any other number in base 10 whose last digit is 5 is divisible by 5.

1.2

Prove by induction: $\forall n \in \mathbb{Z}^+$, n can be written as a product of primes.

We know this holds for $n = 1$ and $n = 2$, both of which are simple products of 1 and a prime. Assume now that the property holds for $n \leq k$. If $k+1$ is prime, then it is clearly a product of 1 and a prime (like 1 and 2). Otherwise, $k+1 = ab$, with $a, b \leq k$. But, by the inductive assumption, a and b can be written as products of primes, so $k+1$ is itself a product of primes.

1.3

Write prime decompositions for 72 and 480.

$72 = 2 * 2 * 2 * 3 * 3 = 2^3 * 3^2$.
$480 = 2 * 2 * 2 * 2 * 2 * 3 * 5 = 2^5 * 3 * 5$.

1.4

Which members of the set less than 100 are not prome?

All members of the set less than 100 are as follows:
1, 5, 9, 13, 17, 21, 25, 29, 33, 37, 41, 45, 49, 53, 57, 61, 65, 69, 73, 77, 81, 85, 89, 93, 97
Eliminating prome members, have:
1, 5, 9, 13, 17, 21, 29, 33, 37, 41, 49, 53, 57, 61, 69, 73, 77, 89, 93, 97

1.5

What is the prime-power decomposition of 7950?

$2 * 3 * 5^2 * 53$

2 Problems

2.1

Find the prime-power decompositions of 1234, 34560, and 111111.

2 * 617
$2^8 * 3^3 * 5$
3 * 7 * 11 * 13 * 37

2.2

Find the prime-power decompositions of 2345, 45670, and 999999999999.

5 * 7 * 67
2 * 5 * 4567
$3^3 * 7 * 11 * 13 * 37 * 101 * 9901$

2.3

Tartaglia (1556) claimed that the sums

$$1 + 2 + 4, \quad 1 + 2 + 4 + 8, \quad 1 + 2 + 4 + 8 + 16, \quad ... \tag{1}$$

are alternately prime and composite. Show that he was wrong.

The sums are of the form $f(n) = \Sigma_{k=0}^{n} 2^k$. This holds until $f(7) = 255$, which is composite. However $f(8) = 511$ is divisible by 7, so it is not prime.

2.4

(a) DeBouvelles (1509) claimed that one or both of $6n+1$ and $6n-1$ are primes for all $n \geq 1$. Show that he was wrong.
(b) Show that there are infinitely many n such that both $6n-1$ and $6n+1$ are composite.

(a) When $n = 24$, $6n + 1 = 145$, which is divisible by 5, and $6n - 1 = 143$, which is divisble by 11.
(b) Already know that this property holds for some n, namely $n = 24$. Suppose $\exists n' \ni n'$ is the greatest n for which the property holds. Observe that $6(n' + k) - 1 = (6n' - 1) + 6k$ and $6(n' + k) + 1 = (6n' + 1) + 6k$. We know that both $(6n' - 1)$ and $(6n' + 1)$ are composite, so can be written as $p_1 * p_2 * ... * p_n$ and $q_1 * q_2 * ... * q_n$. So, if we pick $k \ni k$ shares a divisor with both $(6n' - 1)$ and $(6n' + 1)$, we know that the property won't hold for $n' + k$. Even with no $p_i = q_j \forall i, j$, we can manufacture such a k by picking an arbitrary product of any combination of p_is and p_qs. So, n' is not the greatest n for which the property holds.

2.5

Prove that if n is a square, then each exponent in its prime-power decomposition is even.

If n is a square, we know that $\exists k \ni k^2 = n$. Let $k = p_1^{e_1} * p_2^{e_2} * ... * p_k^{e_k}$. Then $k^2 = p_1^{2e_1} * p_2^{2e_2} * ... * p_k^{2e_k}$. By **Theorem 2**, this is the unique prime decomposition of n, and all e_i are even.

2.6

Prove that if each exponent in the prime-power decomposition of n is even, then n is a square.

We write $n = p_1^{2e_1} * p_2^{2e_2} * ... * p_k^{2e_k}$. This can be rewritten as $p_1^{e_1} * p_1^{e_1} * p_2^{e_2} * p_2^{e_2} * ... * p_k^{e_k} * p_k^{e_k} = (p_1^{e_1} * p_2^{e_2} * ... * p_k^{e_k})^2$. So, $\exists k = p_1^{e_1} * p_2^{e_2} * ... * p_k^{e_k} \ni k^2 = n$.

2.7

Find the smallest integer divisble by 2 and 3 which is simultaneously a square and a fifth power.

We can show analogously to the previous exercise that if each exponent in the prime-power decomposition of n is divisible by d, then $\exists k \ni k^d = n$. The smallest d' for which this holds for both $d_1 = 2$ and $d_2 = 5$ is 10. So $2^{10} * 3^{10} = 60466176$ is the smallest integer with such a property.

2.8

If $d|ab$, does it follow that $d|a$ or $d|b$?

No, for example if $d = ab$ and $a, b > 1$, then $d|ab$, but $d \nmid a$, $d \nmid b$.

2.9

Is it possible for a prime p to divide both n and $n+1$ ($n \geq 1$)?

$p|n \Rightarrow \exists k \ni n = pk$. Then $n+1 = pk+1$. If $p|pk+1$, then $p|pk$ and $p|1$. But there is no prime that divides 1.

2.10

Prove that $n(n+1)$ is never a square for $n > 0$.

$n(n+1) = n^2 + n$. The number n^2 is certainly a square. Since $n^2 + n > n^2$, if $n^2 + n$ is a square, it must be of some $k > n$. The smallest such $k \in \mathbb{Z}$ is $n+1$. However, $(n+1)^2 = n^2 + 2n + 1 > n^2 + n$. The inequality will hold for any other $k > n+1$ as well, so there is no such k.

2.11

(a) Verify that $2^5 * 9^2 = 2592$.
(b) Is $2^5 * a^b = [25ab]$ possible for other a, b? (Here, $[25ab]$ denotes the digits of $2^5 * a^b$ and not a product.)

(a) Sure.
(b) $2^5 = 32$. Let's examine the range in which a^b must fall to produce a 4 digit $[25ab]$. The ceiling of $2510/32$ is 79 (never will $a = 0$ have the desired property, since $32 * 0^b = 0$, or at best, and debatedly so, 32 when $b = 0$; this hardly makes a difference for what follows). The floor of $2599/32$ is 81, a number we're familiar with as 9^2. So $a^b \in \{79, 80, 81\}$. Let's write the prime-power decompositions of each:

$$79 = 79^1 \tag{2}$$
$$80 = 2^4 * 5 \tag{3}$$
$$81 = 3^4 \tag{4}$$

79 can be written as 79^1, but then $[25ab] \geq 25000 > 2599$.
80 can be written as 80^1, but then $[25ab] \geq 25000 > 2599$.
81 can be written as 3^4 as well as 9^2, but since $32 * 81 = 2592$, this alternative representation of 81 does not have the desired property. 81^1, like the previous $b = 1$ cases, will also not fulfill the property.

2.12

Let p be the least prime factor of n, where n is composite. Prove that if $p > n^{1/3}$, then n/p is prime.

n/p can only be prime if $n = p * z$ for some prime z. We have $p > n^{1/3} \Rightarrow p^3 = p * p^2 > p * z$. So we know that $z < p^2$. Suppose z is composite. Then, by **Lemma 3**, it must have a divisor $d \ni 1 < d \leq z^{1/2} < p$. But, if there were such a d, then p would not be the least prime factor of n.

2.13

True or false? If p and q divide n, and each is greater than $n^{1/4}$, then n/pq is prime.

TODO, author gives example to show this is false, but I wish there was a more elegant way than guessing.

2.14

Prove that if n is composite, then $2^n - 1$ is composite.

Observe that $2^n - 1 = (2-1)(2^{n-1} + 2^{n-2} + ... + 1)$. If n is composite, than it can be written as ab for some $a, b \in \mathbb{Z}$. So, $(2^a)^b - 1 = (2^a - 1)(2^{a(b-1)} + 2^{a(b-2)} + ... + 1)$. This is composite by definition.

2.15

Is it true that if $2^n - 1$ is composite, then n is composite?

$2^{11} - 1 = 2047 = 23 * 89$ is apparently the famous counterexample... Dunno if there is a good (feasible for me) "analytic" way to show this.