ITT9132 Concrete Mathematics
Exercises from Week 7

Silvio Capobianco

Exercise 4.1

What is the smallest positive integers that has exactly k divisors, for $1 \leqslant k \leqslant 6$?

Solution. Let us just start counting:

1. 1 has only one divisor.
2. 2 has exactly two divisors. This is actually true for every prime number p, of which 2 is the smallest.
3. The only numbers with exactly three divisors, are the squares of primes. (In fact, an nth power of a prime has exactly $n+1$ divisors.) Of these, 4 is the smallest.
4. The only numbers with exactly four divisors, are the cubes of primes and the products of two distinct primes. Of these $6 = 2 \cdot 3$ is the smallest, as $2^3 = 8$.
5. The only numbers with exactly five divisors, are the fourth powers of primes: the smallest one is $2^4 = 16$.
6. A number has six divisors if and only if it is the fifth power of a prime, or the power of a prime and the square of another prime: as $2^5 = 32$ but $3 \cdot 2^2 = 12$, the smallest such number is 12.

Exercise 4.2

Use the identity $\gcd(m,n) \cdot \mathrm{lcm}(m,n) = m \cdot n$ to express $\mathrm{lcm}(m,n)$ in terms of $\mathrm{lcm}(n \bmod m, n)$, when $n \bmod m \neq 0$. *Hint:* Use (4.12), (4.14) and (4.15).

Solution. We have:

$$\begin{aligned}
\mathrm{lcm}(m,n) &= \frac{m \cdot n}{\gcd(m,n)} \\
&= \frac{m \cdot n}{\gcd(n \bmod m, m)} \quad \text{by the Euclidean algorithm} \\
&= \frac{n \cdot (n \bmod m) \cdot m}{(n \bmod m) \gcd(n \bmod m, m)} \\
&= \frac{n}{n \bmod m} \cdot \frac{(n \bmod m) \cdot m}{\gcd(n \bmod m, m)} \\
&= \frac{n}{n \bmod m} \cdot \mathrm{lcm}(n \bmod m, m)\,.
\end{aligned}$$

Exercise 4.13(a)

A positive integer n is called *squarefree* if it is not divisible by m^2 for any $m > 1$. Find a necessary and sufficient condition that n is squarefree, in terms of the prime-exponent representation (4.11) of n.

Solution. By applying the definition of prime number and the fundamental theorem of arithmetic, we see that n is divisible by the square of an integer $m > 1$ if and only if it is divisible by the square of a prime p. Then n is squarefree if and only if $n_p \leqslant 1$ for every prime p.

Exercise 4.14

Prove or disprove:

1. $\gcd(km, kn) = k \gcd(m,n)$;

2. $\mathrm{lcm}(km, kn) = k\mathrm{lcm}(m,n)$.

Solution. The statements are trivially true for $k = 1$. For $k > 1$ they are also true, because for every prime p, $(km)_p = k_p + m_p$ and $(kn)_p = k_p + n_p$, thus

$$\begin{aligned}
\gcd(km, kn) &= \prod_p p^{\min((km)_p, (kn)_p)} \\
&= \prod_p p^{\min(k_p + m_p, k_p + n_p)} \\
&= \prod_p p^{k_p + \min(m_p, n_p)} \\
&= k \gcd(m, n) \,.
\end{aligned}$$

We can reason similarly for the least common multiple, or do as follows:

$$\begin{aligned}
\mathrm{lcm}(km, kn) &= \frac{(km) \cdot (kn)}{\gcd(km, kn)} \\
&= \frac{k^2 mn}{k \gcd(m, n)} \\
&= k \cdot \frac{mn}{\gcd(m, n)} \\
&= k \,\mathrm{lcm}(m, n) \,.
\end{aligned}$$

For $k < 0$ the left-hand sides are positive, but the right-hand sides are negative. But as $\gcd(m, n) = \gcd(|m|, |n|)$ for every two integers $m.n$ not both zero, we can replace k with $|k|$ on the right-hand side, and still get a correct formula. The above work also for $k < 0$.

For $k = 0$ the right-hand sides are 0 but the left-hand sides are undefined. If we use the convention that $a \cdot [\text{False}] = 0$ whenever a is infinite or undefined, then we can summarize the formulas as:

$$\begin{aligned}
\gcd(km, kn)\,[k \neq 0] &= k \gcd(m, n) \\
\mathrm{lcm}(km, kn)\,[k \neq 0] &= k \mathrm{lcm}(m, n)
\end{aligned}$$

Esercise 4.17

Let f_n be the "Fermat number" $2^{2^n} + 1$. Prove that $\gcd(f_m, f_n) = 1$ if $m < n$.

Solution. Let us construct the first Fermat numbers: $f_0 = 3$, $f_1 = 5$, $f_2 = 17$, $f_3 = 257$, $f_4 = 65537$. We observe that $f_0 = 3$ divides $f_1 - 2 = 3$, $f_2 - 2 = 15$, $f_3 - 2 = 255$, $f_4 - 2 = 65535$; and so on. We also observe that

$f_1 = 5$ divides $f_2 - 2$, $f_3 - 2$, and $f_4 - 2$. We thus formulate the following conjecture: if $m < n$ then $f_m \setminus f_n - 2$.

Is this conjecture of any utility for our objective? Yes, it is: if $f_m \setminus f_n - 2$, then $\gcd(f_m, f_n) = \gcd(f_n \bmod f_m, f_m) = \gcd(2, f_m) = 1$ as f_m is odd.

Let us now prove the conjecture. If $m < n$ then 2^{n-m} is even: but $a^{2r} - 1 = (a+1)(a^{2r-1} - a^{2r-2} + \ldots + a - 1)$. Put then $a = 2^{2^m}$ and $2^{n-m} = 2r$: then $f_m = a + 1$ and $f_n - 2 = a^{2r} - 1$.

Exercise 4.18

Show that if $2^n + 1$ is prime then n is a power of 2.

Solution. We reformulate the problem as follows: if n has an odd factor $m > 1$, then $2^n + 1$ has a nontrivial factor. So suppose $n = qm$ with $m > 1$ odd: then

$$2^n + 1 = 2^{qm} + 1 = (2^q + 1)(2^{(m-1)q} - 2^{(m-2)q} + \ldots + 2^{2q} - 2^q + 1) ,$$

and the factor $2^q + 1$ surely is nontrivial.

Exercise 4.20

For every positive integer n there's a prime p such that $n < p \leqslant 2n$. (This is essentially "Bertrand's postulate", which Joseph Bertrand verified for $n < 3000000$ in 1845 and Chebyshev proved for all n in 1850.) Use Bertrand's postulate to prove that there's a constant $b \approx 1.25$ such that the numbers

$$\lfloor 2^b \rfloor \ . \ \left\lfloor 2^{2^b} \right\rfloor \ , \ \left\lfloor 2^{2^{2^b}} \right\rfloor \ , \ \ldots \tag{1}$$

are all prime.

Solution. Call lg the binary (base-2) logarithm. Let us define a "simple" sequence of primes by putting $p_1 = 2$, and p_n as the smallest prime larger than $2^{p_{n-1}}$. By Bertrand's postulate, $2^{p_{n-1}} < p_n < 2^{p_{n-1}+1}$ for every $n \geqslant 2$: we can switch to strict inequality because such p_n are odd. Hence,

$$p_{n-1} < \lg p_n < p_{n-1} + 1 \tag{2}$$

for every $n \geqslant 2$. The left-hand inequality of (2) tells us that the sequence

$$b_n = \lg^{(n)} p_n , \tag{3}$$

where $\lg^{(n)}$ is the nth iteration of lg, is nondecreasing. To prove that it is bounded from above, we set $a_1 = 2$ and $a_n = 2^{a_{n-1}}$ for every $n \geqslant 2$, so that $a_2 = 4$, $a_3 = 16$, and so on: we prove by induction that $p_n < a_{n+1}$ for every $n \geqslant 1$, from which follows $b_n < 2$ for every $n \geqslant 1$ as $\lg^{(n)} a_{n+1} = 2$. This is true for $n = 1$ and $n = 2$ as $p_2 = 5$; for $n \geqslant 3$, if $p_{n-1} < a_n$, then, as p_{n-1} and a_n are both integers, $p_{n-1} + 1 \leqslant a_n$, and the right-hand inequality of (2) tells us that $p_n < 2^{p_{n-1}+1} \leqslant 2^{a_n} = a_{n+1}$. We then set:

$$b = \lim_{n\to\infty} b_n = \sup_{n\geqslant 1} \lg^{(n)} p_n \,. \tag{4}$$

To prove that this is the b we were looking for, we set $u_1 = 2^b$ and $u_n = 2^{u_{n-1}}$ for every $n \geqslant 2$: we will show that $\lfloor u_n \rfloor = p_n$ for every $n \geqslant 1$, which will solve the exercise. Clearly $\lfloor u_n \rfloor \geqslant p_n$ as $b_n < b$; also, as $b = 1.25164\ldots$ and $2^{1.26} < 2.4$, $\lfloor u_1 \rfloor = p_1$. If for some $n > 1$ it is $\lfloor u_n \rfloor > p_n$, let n be the minimum value for which this happens: then $u_n > p_n$, too, and

$$u_{n-1} = \lg u_n > \lg p_n > p_{n-1} \,,$$

against minimality of n.

Factorial factors

For p prime, let $\epsilon_p(n)$ the exponent of p in the prime factorization of n: that is, let $n = p^{\epsilon_p(n)} \cdot m$ with $p \not| m$. For example, $\epsilon_2(20) = 2$, $\epsilon_5(20) = 1$, and $\epsilon_3(20) = 0$. Prove that

$$\epsilon_p(n!) = \sum_{k\geqslant 1} \left\lfloor \frac{n}{p^k} \right\rfloor \tag{5}$$

for every prime p and positive integer n.

Solution. Of the n positive integers from 1 to n, only every pth contributes with one or more factor p. Of those, one in p contribute with *two* or more factors p; of those, one in p contributes with *three* or more factors p; and so on.

We then get an idea about how to compute $\epsilon_p(n!)$. Construct a table A with infinitely many rows and n columns; enumerate the columns from 1 to n, and the rows with the positive integers. Let then:

$$A_{k,m} = \left[p^k \setminus m\right] \quad \forall k \geqslant 1, 1 \leqslant m \leqslant n \,.$$

	1	2	3	4	5	6	7	8	9
1	0	1	0	1	0	1	0	1	0
1	0	0	0	1	0	0	0	1	0
1	0	0	0	0	0	0	0	1	0
1	0	0	0	0	0	0	0	0	0
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$

Figure 1: The table of factorial factors for $n = 9$ and $p = 2$ has 7 entries equal to 1, and indeed, $9! = 362880 = 2^7 \cdot 2385$

The double sum $\sum_{k,m} A_{k,m}$ converges, because only finitely many terms are nonzero. Moreover, the kth row contributes with as many 1s as there are multiples of p^k between 1 and n: there are exactly $\lfloor n/p^k \rfloor$ such 1s. Also, the mth column contributes with a number of 1s equal to (the exponent of) the maximum power of p which divides m. Then the maximum power of p that divides $n!$ is the sum of all the entries of the matrix: by Tonelli's theorem,

$$\begin{aligned} \sum_{k,m} A_{k,m} &= \sum_{k \geqslant 1} \sum_{1 \leqslant m \leqslant n} [p^k \setminus m] \\ &= \sum_{k \geqslant 1} \left\lfloor \frac{n}{p^k} \right\rfloor , \end{aligned}$$

as we wanted to prove.