Concrete Mathematics
Exercises from Chapter 4

Silvio Capobianco

Wilson's theorem

Prove that an integer $n \geq 2$ is prime if and only if $(n-1)! \equiv -1 \bmod n$.
Solution. If n is composite, let $p < n$ be a prime that divides n. Then p is one of the factors of $(n-1)!$, and cannot be a factor of $(n-1)!+1$: neither can n, which is a multiple of p.

If n is prime, we can suppose it is odd, as $1! = 1 \equiv -1 \bmod 2$. The evenly many numbers $1, 2, \ldots, n-1$ all have a multiplicative inverse modulo n: some coincide with their own multiplicative inverse, and some don't. But i is its own inverse modulo n if and only if $i^2 - 1 \equiv 0 \bmod n$, that is, $n \mid (i+1)(i-1)$: and as n is an odd prime, it must divide either $i-1$ or $i+1$, but cannot divide both, or it would also divide their difference, which is 2. Then the only integers modulo n that are their own inverses modulo n are $i = 1$ and $i = n-1$: and by pairing multiplicative inverses with each other, the product of the numbers from 2 to $n-2$ can be seen to be congruent to 1 modulo n. Then

$$(n-1)! = 1 \cdot (n-1) \cdot \prod_{i=2}^{n-2} i \equiv (n-1) \cdot 1 \equiv -1 \bmod n \,.$$

Exercise 4.19

Prove the following identities when n is a positive integer:

$$\sum_{1 \leq k < n} \left\lfloor \frac{\phi(k+1)}{k} \right\rfloor = \sum_{1 < m \leq n} \left\lfloor \left(\sum_{1 \leq k < m} \left\lfloor \frac{\frac{m}{k}}{\left\lceil \frac{m}{k} \right\rceil} \right\rfloor \right)^{-1} \right\rfloor \tag{1}$$

$$= n - 1 - \sum_{k=1}^{n} \left\lceil \left\{ \frac{(k-1)!+1}{k} \right\} \right\rceil \tag{2}$$

Hint: This is a trick question and the answer is pretty easy.
Solution. First of all, the summands in the left-hand side of (1) are 1 if $k+1$ is prime, and 0 otherwise: thus, that left-hand-side itself is $\pi(n)$, the number of primes not greater than n. Next, in the inner sum of the right-hand side of (1), the summand $\lfloor (m/k)/\lceil m/k \rceil \rfloor$ is 1 if $k \mid m$ and 0 otherwise: the sum itself, where k ranges from 0 to $m-1$, is greater than 1 if and only if m is composite, so the summand a_m in the outer sum is 1 if m is prime and 0 otherwise: the sum itself is again $\pi(n)$. Finally, by Wilson's theorem, the summands in the right-hand side of (2) are 1 if k is greater than 1 and *not* prime, and 0 otherwise: the sum itself is the number of composite numbers from 1 to n, so it yields $n-1$ when added to $\pi(n)$ (remember that 1 itself is neither prime nor composite).

Exercise 4.25

We say that m *exactly divides* n, written $m \parallel n$, if $m \mid n$ and $\gcd(m, n/m) = 1$. Prove or disprove the following:

1. If $\gcd(k, m) = 1$, then $km \parallel n$ if and only if $k \parallel n$ and $m \parallel n$.
2. For all $m, n > 0$, either $\gcd(m, n) \parallel m$ or $\gcd(m, n) \parallel n$.

Solution. To say that $m \parallel n$ is the same as saying that for every prime p, if $p \mid n$, then the maximum power of p that divides n is the same that divides m; to say that $\gcd(k, m) = 1$, is the same as saying that for every prime p, either $p \mid k$ or $p \mid m$, but not both. All this means that point 1 is true.

Point 2, however, is false. To construct a counterexample, suppose that $k = pq$ is the product of two primes: then $m = p^2 q$ and $n = pq^2$ satisfy $\gcd(m, n) = k$, but also $\gcd(k, m/k) = p > 1$ and $\gcd(k, n/k) = q > 1$). The smallest such counterexample is for $p = 2$ and $q = 3$, thus $m = 12$ and $n = 18$.

Exercise 4.33

Show that if $f(m)$ and $g(m)$ are multiplicative functions, then so is $h(m) = \sum_{d \mid m} f(d) g(m/d)$.
Solution.

Recall that a function f, defined on the positive integers, is said to be multiplicative if $\gcd(m, n) = 1$ implies $f(m \cdot n) = f(m) \cdot f(n)$. In this case,

$d \,|\, mn$ if and only if there exist two integers a, b such that $d = ab$, $a \,|\, m$, $\gcd(a, n) = 1$, $b \,|\, n$, and $\gcd(b, m) = 1$: then $\gcd(a, b) = 1$ as well, and

$$\begin{aligned} h(mn) &= \sum_{d \,|\, mn} f(d) g\left(\frac{mn}{d}\right) \\ &= \sum_{a \,|\, m, b \,|\, n} f(ab) g\left(\frac{mn}{ab}\right) \\ &= \sum_{a \,|\, m, b \,|\, n} f(a) f(b) g\left(\frac{m}{a}\right) g\left(\frac{n}{b}\right) \\ &= \left(\sum_{a \,|\, m} f(a) g\left(\frac{m}{a}\right)\right) \cdot \left(\sum_{b \,|\, n} f(b) g\left(\frac{n}{b}\right)\right) \\ &= h(m) \cdot h(n)\,. \end{aligned}$$