ITT9132 Concrete Mathematics
Exercises from Week 8

Silvio Capobianco

The Least Efficient Primality test

Prove *Wilson's theorem:* for every $n \geqslant 2$, n is prime if and only if $(n-1)! \equiv -1 \pmod{n}$.

Solution. First, suppose that n is composite. Let p be a prime factor of n: then $p < n$, so $p \setminus (n-1)!$. If it were $n \setminus (n-1)! + 1$, then it would be $p \setminus 1$ too: which is impossible.

Next, suppose that n is prime. For $n = 2$ the thesis becomes $1! \equiv -1 \pmod{2}$, which is true: we can then suppose that $n \geqslant 3$ is odd. As n is prime, every $j \in [1 : n-1]$ has an inverse modulo n, so:

$$\begin{aligned}
(n-1)! &= \prod_{1 \leqslant j < n} j \\
&= \left(\prod_{1 \leqslant j < n, j = j^{-1} \bmod n} j \right) \cdot \left(\prod_{1 \leqslant j < n, j \neq j^{-1} \bmod n} j \right) \\
&\equiv \left(\prod_{1 \leqslant j < n, j = j^{-1} \bmod n} j \right) \cdot 1 \pmod{n}.
\end{aligned}$$

But $j = j^{-1} \bmod n$ if and only if $j^2 - 1 = (j-1)(j+1) \equiv 0 \pmod{n}$: as n is an odd prime, either $j = 1$ or $j = n-1$. In the end:

$$(n-1)! \equiv 1 \cdot (n-1) \equiv -1 \pmod{n}.$$

Exercise 4.15

The *Euclid numbers* are defined by the recurrence:

$$\begin{aligned} e_1 &= 2\,; \\ e_{n+1} &= e_1 \cdots e_n + 1 \quad \text{for every } n \geqslant 1\,. \end{aligned}$$

For example, $e_2 = 3$, $e_3 = 7$, $e_4 = 43$, while $e_5 = 1807 = 13 \cdot 139$ is the smallest composite Euclid number.

Does every prime occur as a factor of some Euclid number e_n?

Solution. As $e_1 = 2$ and $e_2 = 3$, the number $d_n = e_n - 1$ is a multiple of 6 whenever $n \geqslant 3$. But $6 \equiv 1 \pmod 5$, and as 5 is a prime number, $d_n \equiv -1(\bmod 5)$ (*i.e.*, $5 \backslash e_n$) if and only if $e_3 \cdots e_{n-1} \equiv -1 \pmod 5$: this does not seem to be the case for small n, as $e_3 = 7 \equiv 2 \pmod 5$ and $e_4 = 43 \equiv 3 \pmod 5$.

We may, however, observe a pattern here: for $n \leqslant 4$, $e_n \bmod 5$ is 2 if n is odd, and 3 if n is even, *i.e.*,

$$e_n \bmod 5 = 2 + (n \bmod 2)\,. \tag{1}$$

If (1) holds for every $n \geqslant 1$ (it clearly holds for $n = 1$ and $n = 2$) then no Euclid number can be divisible by 5, and the answer to our original question is negative. We prove by induction that it is so:

Suppose that we have proved (1) for every positive integer up to n. Let us consider $e_{n+1} = e_1 \cdots e_n + 1$: by inductive hypothesis, $e_{n+1} - 1(\bmod 5) = (e_1 \bmod 5) \cdots (e_n \bmod 5)$ is the product of $\lceil n/2 \rceil$ factors equal to 2 and $\lfloor n/2 \rfloor$ equal to 3: hence, it is $2 \pmod 5$ if n is odd, and $1 \pmod 5$ if n is even. Consequently, e_{n+1} is congruent modulo 5 to $2 = 1 + 1$ if $n + 1$ is odd (*i.e.*, n is even) and to $3 = 2 + 1$ if $n + 1$ is even (*i.e.*, n is odd).

Exercise 4.19

Prove the following identities when n is a positive integer:

$$\sum_{1 \leqslant k < n} \left\lfloor \frac{\phi(k+1)}{k} \right\rfloor = \sum_{1 < m \leqslant n} \left\lfloor \left(\sum_{1 \leqslant k < m} \left\lfloor \frac{\frac{m}{k}}{\lceil \frac{m}{k} \rceil} \right\rfloor \right)^{-1} \right\rfloor \tag{2}$$

$$= n - 1 - \sum_{k=1}^{n} \left\lceil \left\{ \frac{(k-1)! + 1}{k} \right\} \right\rceil \tag{3}$$

Hint: This is a trick question and the answer is pretty easy.

Solution. First of all, the summands in the left-hand side of (2) 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 (2), the summand $\lfloor (m/k)/\lceil m/k \rceil \rfloor$ is 1 if $k \setminus m$ 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 (3) 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 4.22

The number 1111111111111111111 is prime. Prove that, in any radix b, $(11\ldots1)_b$ can be prime only if the number of 1's is prime.

Solution. If the number of 1s is $n = qm$ with $q, m \geqslant 2$, then $(11\ldots1)_b$ is the juxtaposition of m sequences of q 1's each: thus,

$$(11\ldots1)_b = \sum_{k=0}^{qm-1} b^k = \left(\sum_{k=0}^{q-1} b^k\right) \cdot \left(\sum_{j=0}^{m-1} b^{qj}\right) ,$$

and both factors are nontrivial.

Exercise 4.30

Prove the following statement (the Chinese Remainder Theorem):

Let $m_1, \ldots, m_r$ be positive integers with $\gcd(m_j, m_k) = 1$ for $1 \leqslant j < k \leqslant r$ let $m = m_1 \cdots m_r$; and let $a_1, \ldots, a_r, A$ be integers. Then there is exactly one integer a such that

$$a \equiv a_k \pmod{m_k} \text{ for } 1 \leqslant k \leqslant r \text{ and } A \leqslant a < A + m\,. \tag{4}$$

Solution. Let

$$U = \{(x \bmod m_1, \ldots, x \bmod m_r) \mid x \in \mathbb{Z}\} \ :$$

then,

$$|U| = \operatorname{lcm}(m_1, \ldots, m_r) = m_1 \cdots m_r = m\,,$$

because the m_k's are pairwise relatively prime. Now, $A + m \equiv A \pmod{m_k}$ for every k, so the set

$$S = \{(x \bmod m_1, \ldots, x \bmod m_r) \mid A \leqslant x < A + m\}\,,$$

actually coincides with U. Then for every $s \in S$ there exists exactly one $x \in \{A, \ldots, A + m - 1\}$ such that $s = (x \bmod m_1, \ldots, x \bmod m_r)$. Given $a_1, \ldots, a_r$, let $s = (a_1 \bmod m_1, \ldots, a_r \bmod m_r)$, and take x accordingly.

Exercise 4.11

Find a function $\sigma(n)$ with the property that

$$g(n) = \sum_{0 \leqslant k \leqslant n} f(k) \quad \Leftrightarrow \quad f(n) = \sum_{0 \leqslant k \leqslant n} \sigma(k) g(n-k) \tag{5}$$

(This is analogous to the Möbius function; see (4.56).)

Solution. As (6) must be true whatever f and g are, let us consider the case $f(n) = \sigma(n)$, $g(n) = [n = 0]$: this surely satisfies the right-hand equation, because

$$\sigma(n) = \sum_{0 \leqslant k \leqslant n} \sigma(k)\,[k = n] = \sum_{0 \leqslant k \leqslant n} \sigma(k)\,[n - k = 0]\ .$$

If we want it to also satisfy the left-hand equation, then we must have $\sum_{0 \leqslant k \leqslant 0} \sigma(k) = [n = 0]$: this is only possible if $\sigma(0) = 1$, $\sigma(1) = -1$, and $\sigma(k) = 0$ for $k > 1$.

Let us now prove that this choice of σ works whatever f and g are. So, suppose $g(n) = \sum_{0 \leqslant k \leqslant n} f(k)$: then

$$\begin{aligned} \sum_{0 \leqslant k \leqslant n} \sigma(k) g(n-k) &= g(n) - g(n-1) \\ &= \sum_{0 \leqslant k \leqslant n} f(k) - \sum_{0 \leqslant k \leqslant n-1} f(k) \\ &= f(n)\,. \end{aligned}$$

Suppose now $f(n) = \sum_{0\leqslant k\leqslant n} \sigma(k)g(n-k)$: this is $g(0)$ if $n=0$, and $g(n) - g(n-1)$ if $n > 0$. In this case we have:

$$\begin{aligned} \sum_{0\leqslant k\leqslant n} f(n) &= f(0) + \sum_{1\leqslant k\leqslant n} f(k) \\ &= g(0) + \sum_{1\leqslant k\leqslant n} (g(k) - g(k-1)) \\ &= g(n)\,. \end{aligned}$$

In the end, $\sigma(n) = [n=0] - [n=1]$.