

**Definition 1 (Least Common Multiple)**  $\text{lcm}\{x_1, \dots, x_n\}$  is the smallest number  $M$  such that  $x_i | M$  for all  $i = 1, \dots, n$ .

**Definition 2 (Carmichael Lambda Function)** Let  $N = \prod_{i=1}^l p_i^{e_i}$ . The Carmichael lambda function is  $\lambda(N) = \text{lcm}\{p_i^{e_i-1}(p_i - 1) : i = 1, \dots, l\}$ .

**Exercise 1** Give an example of a number  $N$  for which  $\lambda(N) \neq \varphi(N)$ . Then, prove that, for every  $N \in \mathbb{N}$ ,  $\lambda(N) | \varphi(N)$ . What does this tell you about RSA?

**Exercise 2** Show that all Carmichael numbers are odd. Show that  $N$  is a Carmichael number if and only if  $\lambda(N) | (N - 1)$ . Show that a composite number  $N \in \mathbb{N}$  is a Carmichael number if and only if  $N = \prod_{i=1}^l p_i$  is a product of distinct primes such that  $(p_i - 1) | (N - 1)$  for  $i = 1, \dots, l$ .

**Exercise 3** Recall Pollard's  $p - 1$  method for factorizing  $N = pq$ . Prove that if  $L$  is such that  $(p - 1) | L$  and  $(q - 1) \nmid L$ , then  $a^L \equiv 1 \pmod{p}$  for randomly chosen  $a$ .

**Exercise 4** Let  $N, B \in \mathbb{N}$ . Show that  $N$  is  $B$ -powersmooth if and only if  $N | \text{lcm}\{1, \dots, B\}$ .

**Definition 3 (Hensel Lifting)** Let  $f$  be a polynomial and  $r$  be a root of  $f$  modulo  $p^k$ . Then there exists root  $s$  modulo  $p^{k+m}$ , with  $m \leq k$ , such that  $r \equiv s \pmod{p^k}$ .

**Exercise 5** Let  $N$  be an odd composite integer and  $m$  be the number of distinct primes dividing  $N$ . Show that the equation  $x^2 \equiv 1 \pmod{N}$  has  $2^m$  solutions modulo  $N$ .

*Hint: use Hensel Lifting.*

**Exercise 6** Recall the random squares method for factoring. How many relations are needed to be sure that there is a non-trivial exponent vector  $\eta$ ? What's the probability that computing  $(a - b, N)$  factors  $N$ ?