22. A quick primality test

Prime numbers are one of the most basic objects in mathematics and one of the most basic questions is to decide which numbers are prime (a clearly related problem is to find the prime factorisation of a number). Given a number n one would like a quick way to decide if n is prime, say using a computer. Quick can be given a precise meaning. First one measures the **complexity** by the number of digits, or what comes to the same thing $d = \lceil \log n \rceil$ (we will work base 2, so that this is the same as the number of bits). The larger d the longer it will take to decide if n is prime, in general. We would like an algorithm that runs in **polynomial time**, that is, the algorithm is guaranteed to be over in a time given by a function that is polynomial in d; in essence we are looking for an upper bound for the running time of the form $c \cdot d^m$, where c is some constant and m is an integer.

This very famous problem was solved in 2002 by Manindra Agrawal, Neeraj Kayal and Nitin Saxena, the last two of whom were graduate students, in computer science from India

The basis of their algorithm is the following simple idea. If n is a prime number then

$$a^n = a \mod n,$$

for every integer $1 \leq a \leq n-1$. This at least gives a way to test if a number is not prime.

Definition 22.1. *A natural number n is called a **Carmichael number** if*

$$a^n = a \mod n,$$

for every integer $1 \leq a \leq n-1$ and yet n is not prime.

Unfortunately Carmichael numbers exist; the first such number is $561 = 3 \cdot 11 \cdot 17$. To remedy this, the next idea is that one can test primeness if one works with polynomials, that is, if one works in $\mathbb{Z}_n[x]$ and not just $\mathbb{Z}_n$.

Lemma 22.2. *Let $n \in \mathbb{N}$ be a natural number, $n \geq 2$.*

Assume that a and n are coprime. Then n is prime if and only if

$$(x+a)^n = x^n + a \in \mathbb{Z}_n[x].$$

Proof. If n is prime then the map

$$\phi \colon \mathbb{Z}_n[x] \longrightarrow \mathbb{Z}_n[x] \qquad \text{given by} \qquad \phi(f) = f^n,$$

is a ring homomorphism. In particular

$$(x+a)^n = \phi(x+a) = \phi(x) + \phi(a) = x^n + a^n = x^n + a \in \mathbb{Z}_n[x].$$