### Primality Test: Sieve of Eratosthenes

This procedure, the Sieve of Eratosthenes, is not strictly speaking a test in the sense described above. Rather, the method is used to determine all prime numbers up to a certain limit. From the list of prime numbers determined in this way, however, a randomly chosen value can then be selected. This very simple procedure does not work efficiently for large prime numbers. Therefore, it is not used in cryptography. Nevertheless, it is very well suited for the determination of smaller prime numbers and is especially easy to Choose a maximum value n ∈ ℕ with n ≥ 2 and note all numbers 2, 3, 4, ., n in a list. understand and use. The procedure for this procedure is as follows:

Each number is marked to indicate whether it is a prime number or a composite number.

At first all numbers are unmarked and therefore are potential prime numbers. The proce1. The smallest unmarked number p piis marked as a prime number. < pi dure now runs iteratively as follows: of i, because all smaller multiples are already multiples of numbers pi and there2. Then all multiples of are marked as composite numbers. You start with the square pi) and the procedure aborts. All unmarked numbers are prime numbers and are≤ n pi n < fore already marked as composite numbers.

3. If the square of is greater than the chosen maximum value , all the composite numbers are already marked as such (because they are multiples of numbers marked accordingly.

We choose n := 100 and determine all prime numbers between 2 and n n. To do this, we Example: Sieve of Eratosthenes

enter all numbers 2, 3, ..., into a list. Initially, all entries are unmarked and thus potential prime numbers.

Figure 14: All numbers between 2 and n: = 100 All entries are still unmarked.

The smallest unmarked number is 2, which is obviously a prime number, so we mark it as such. Then we mark all multiples of 2, that is 4, 6, 8, 10, 12, ..., 96, 98, 100, as composite numbers.

Figure 15: The number 2 was marked as a prime number (dark green), all multiples of 2 were marked as composite numbers (light green).

accordingly. Furthermore, we mark all multiples of 3 as composite numbers. We canmultiples have already been considered (because they are always multiples of smallerThe next unmarked number is 3, which is obviously a prime number again, so we mark itactually start with the square of 3, that is, with the number 32 = 96 , because the smaller numbers). In this case the 6 is a multiple of 3, but with 3 · 2 = it is also a multiple of 2 and thus already marked as a composite number. The following figure shows the state of the list after marking 3 as a prime number and marking all multiples of 3, i.e., 9, 12, 15, ..., 93, 96, 99, as composite numbers.

Figure 16: The number 3 was marked as a prime number (dark green), all multiples of 3 were marked as composite numbers (light green).

The next unmarked number we consider to be 5, which is again a prime number. We mark

it as such and then all multiples of 5 as composite numbers. Again, we can start with thesmaller numbers (it is square, i.e., with 52 = 255 · 2 = , because all smaller multiples of 5 are already multiples of10 and 5 · 3 = 15). After marking 5 as a prime number and

all multiples of 5, i.e., 25, 30, 35, ..., 90, 95, 100, as composite numbers, we obtain the state shown below.

Figure 17: The number 5 was marked as a prime number (dark green), all multiples of 5 were marked as composite numbers (light green).

The next unmarked number is the 7, which obviously is a prime number. Therefore, we

mark the 7 accordingly and then mark all multiples of 7 as composite numbers. Again wemultiples of smaller numbers (it is can start with the square, i.e., with = 42 7 · 2 = 72 = 4914, , because the smaller multiples are already7 · 3 = 21, 7 · 4 = 28, 7 · 5 = 35 and 7 · 6

). The following figure shows the list after marking 7 as a prime number and marking the multiples, i.e., 49, 56, 63, ..., 84, 91, 98, as composite numbers.

Figure 18: The number 7 was marked as a prime number (dark green), all multiples of 7 were marked as composite numbers (light green).

The next unmarked number is 11 , again a prime number. Because 112 = 121 > 100, all composite numbers ≤ n have been considered and we can abort the procedure. All numbers not marked so far are obviously prime numbers too. The figure below shows the final list after the end of the procedure.

Figure 19: The number 11 was marked as a prime number (dark green). Since 112 = 121 > 100, all composite numbers have already been found in the area under consideration. All unmarked numbers are therefore prime numbers and can also be marked accordingly

As you can see, the sieve of the Eratosthenes is a very easy to use method, which is especially suitable for the determination of small prime numbers. In practice, however, cryptographic procedures often require enormously large numbers. Therefore, we want to introduce a second primality test in the following section, which is also suitable for very large numbers and is actually used in practice in cryptographic processes. It is, as with most efficient primality tests, a probabilistic test. This means that if the number under consideration does not pass the test, it is certainly composed of factors (but the factors are not determined). Otherwise it is with a certain probability a prime number. By performing the test several times, the probability that the number under consideration is really a prime number can be maximized accordingly. Even if one may not have the impression at first, these types of tests are actually perfectly adequate for practical use.

Before we introduce the actual prime number test, we must first introduce the concept of the Carmichael numbers, which is necessary for further understanding.