

### Numbers to a base

We normally write a number to base 10. Thus the number 1234 means  $1 \cdot 10^3 + 2 \cdot 10^2 + 3 \cdot 10 + 4 \cdot 1$ . We write the most significant digit first (the coefficient of the highest power of 10). Also the coefficients of the powers of 10 are 0, 1, 2, 3, 4, 5, 6, 7, 8, 9. If instead of 10 we had chosen to use say 3. Then we assert that any positive number can be expressed as  $a_1 3^{k-1} + a_2 3^{k-2} + \dots + a_{k-1} 3 + a_k$  with  $0 \leq a_i < 3$  and this expression is unique. We can find it as follows: We start with  $n$  and divide by 3. We get a remainder of  $0 \leq b < 3$ . Thus  $n = 3q + b$ . Thus if we can write  $q = a_1 3^{k-1} + a_2 3^{k-2} + \dots + a_{k-1} 3 + a_k$  then

$$\begin{aligned} n &= 3(a_1 3^{k-1} + a_2 3^{k-2} + \dots + a_{k-1} 3 + a_k) + b \\ &= a_1 3^k + a_2 3^{k-1} + \dots + a_{k-1} 3^2 + a_k 3 + a_{k+1} \end{aligned}$$

with  $a_{k+1} = b$ . Thus we can compute the expansion by repeated division by 3.

Example.  $n = 340$  then  $320 = 3(106) + 2$ .  $106 = 3(35) + 1$ .  $35 = 3(11) + 2$ .  $11 = 3(3) + 2$  and thus

$$320 = 1 \cdot 3^5 + 2 \cdot 3^3 + 2 \cdot 3^2 + 1 \cdot 3 + 2.$$

The same argument works to show that any integer can be written to base 2. That is if  $n \geq 0$  then  $n$  can be written uniquely as

$$n = a_1 2^{k-1} + a_2 2^{k-2} + \dots + a_k 1$$

with  $0 \leq a_i < 2$ . We call this the binary expansion of  $n$ .

### Exercises.

1. Calculate  $2^{271} \bmod 251$  using a calculator.
2. Let  $p, q$  be an odd primes and assume that  $2^p - 1 \equiv 0 \pmod q$ . Prove that  $p \mid (q - 1)$ .
3. Use 1. to see that  $2^{11} - 1$  is not prime. (Hint. Problem 1 describes the possible prime divisors.)
4. Show that if  $p$  is an integer such that  $p - 1$  is prime then  $2^p + 1$  cannot be a prime.