



and the second is a power of 2, hence they are relatively prime.

d) The number  $2^n$  has  $n + 1$  binary digits while  $2^n - 1$  has  $n$  binary digits; therefore  $d_1$  has 241 binary digits and  $d_2$  has 120 binary digits. Of course  $d_3 = 1$  has a single one.

Since  $2^{10} = 1024$  is close to  $10^3$ , the number  $2^{240} = (2^{10})^{24}$  is approximately  $(10^3)^{24}$ , hence has about 73 decimal digits. *The exact number of decimal digits of  $d_1$  is the integer  $n$  such that  $10^{n-1} \leq 2^{240} < 10^n$ ; since*

$$240 \cdot \frac{\log 2}{\log 10} = 72, 24 \dots$$

*the exact number of decimal digits of  $d_1$  is in fact 73.*

Similarly,  $d_2$  is close to  $(10^3)^{12}$ , hence has about 37 decimal digits; *in fact*

$$120 \cdot \frac{\log 2}{\log 10} = 36, 12 \dots$$

*and the exact number of decimal digits of  $d_2$  is indeed 37.*

For  $n \geq 1$  the last decimal digit of  $2^n$  is 2, 4, 8 or 6 according to  $n \equiv 1, 2, 3$  or  $0 \pmod{4}$  respectively. Since 240 and 120 are multiple of 4, the last decimal digit of  $d_1$  is 6, for  $d_2$  it is 5. For  $d_1$  it is 1.

**6.** For each of the four prime numbers 37, 41, 43, 47,

- 1 and 4 are quadratic residues since they are squares in  $\mathbf{Z}$ ,
- $-1$  is a quadratic residue when  $p$  is congruent to 1 modulo 4, which is the case of 37 and 41, it is nonresidue for the two others.
- 2 is a quadratic residue when  $p$  is congruent to 1 or 3 modulo 8, hence for 41 and 47, it is nonresidue for the two others.
- From the multiplicativity of Legendre symbol, we deduce that  $-2$  is a quadratic residue when  $p$  is congruent to 1 or 3 modulo 8, hence for 41 and 43, it is nonresidue for the two others:

	$41 \equiv 1$	$43 \equiv 3$	$37 \equiv 5$	$47 \equiv 7$	$(\text{mod } 8)$
$\left(\frac{-1}{p}\right)$	1	-1	1	-1	
$\left(\frac{2}{p}\right)$	1	-1	-1	1	
$\left(\frac{-2}{p}\right)$	1	1	-1	-1	

According to the law of quadratic reciprocity,

$$\left(\frac{3}{p}\right) = \begin{cases} \left(\frac{p}{3}\right) & \text{if } p \equiv 1 \pmod{4}, \\ -\left(\frac{p}{3}\right) & \text{if } p \equiv 3 \pmod{4}. \end{cases}$$

Therefore

$$\begin{aligned} \left(\frac{3}{37}\right) &= \left(\frac{37}{3}\right) = \left(\frac{1}{3}\right) = 1, \\ \left(\frac{3}{41}\right) &= \left(\frac{41}{3}\right) = \left(\frac{-1}{3}\right) = -1, \\ \left(\frac{3}{43}\right) &= -\left(\frac{43}{3}\right) = -\left(\frac{1}{3}\right) = -1, \\ \left(\frac{3}{47}\right) &= -\left(\frac{47}{3}\right) = -\left(\frac{2}{3}\right) = 1. \end{aligned}$$

**7.** Consider a finite field with  $q = 64$  elements.

a) Since 64 is a power of 2, the characteristic of this field is 2.

b) The multiplicative group of the field is cyclic of order  $q - 1 = 63$ . The integers  $n$  for which there exists a subgroup of order  $n$  are the divisors of  $q - 1$ . Hence the integers  $n \geq 1$  for which there exists at least a primitive  $n$ -th root of unity in this field are the divisors of  $q - 1 = 63$ , namely 1, 3, 7, 9, 21 and 63. When  $n$  divides  $q - 1$ , there are exactly  $\varphi(n)$  elements of order  $n$  in the cyclic group of order  $q - 1$ , hence there is one element of order 1, there are 2 of order 3, 6 of order 9, 6 of order 7, 12 of order 21 and 36 of order 63. The total  $1 + 2 + 6 + 6 + 12 + 36$  is 63, as it should.

**8.** The generators of the cyclic group  $(\mathbf{Z}/7\mathbf{Z})^\times$  (that is the elements of order 6) are the classes of 3 and 5 modulo 7.

The prime numbers  $p$  such that the cyclotomic polynomial  $\Phi_7(X)$  is irreducible over the finite field  $\mathbf{F}_p$  with  $p$  elements are the prime numbers  $p$  whose class modulo 7 generate  $(\mathbf{Z}/7\mathbf{Z})^\times$ , hence they are the prime numbers which are congruent to 3 or 5 modulo 7.

The question was not asked, but we may add that the classes of 2 and 4 modulo 7 have order 3, the class of 6 (which is also the class of  $-1$ ) has order 2 and the class of 1 has order 1 (as always).

For a prime number  $p$  congruent to 2 or 4 modulo 7, the polynomial  $\Phi_7$  splits into a product of two irreducible polynomials over  $\mathbf{F}_p$  of degree 3, while for  $p$  congruent to 6 modulo 7, the polynomial  $\Phi_7$  splits into a product of three irreducible polynomials over  $\mathbf{F}_p$  of degree 2. For  $p$  congruent to 1 modulo 7, the polynomial  $\Phi_7$  splits completely over  $\mathbf{F}_p$ , which means that  $\mathbf{F}_p^\times$  contains the 6 primitive 7th roots of

unity (for  $p - 1$  multiple of 7, any cyclic group of order  $p - 1$  contains a unique subgroup of order 7, this subgroup is cyclic with 6 generators). Finally for  $p = 7$  the polynomial  $\Phi_7$  splits completely over  $\mathbf{F}_7$  as  $\Phi_7 = (X - 1)^6$ .

**9.** Let  $f \in \mathbf{F}_p[X]$  be an irreducible polynomial of degree  $d$ ,  $K$  a finite field of characteristic  $p$  and  $\alpha \in K$  a root of  $f$ . The roots of  $f$  in  $K$  are

$$\alpha, \alpha^p, \alpha^{p^2}, \dots, \alpha^{p^{d-1}}.$$

Hence the polynomial  $f$  splits completely in  $K$ .

**10.** The cyclic code over  $\mathbf{F}_2$  of length 7 with generating polynomial

$$1 + X + X^2 + X^3 + X^4 + X^5 + X^6$$

has dimension 1, it contains exactly two elements, namely

$$(0, 0, 0, 0, 0, 0, 0) \quad \text{and} \quad (1, 1, 1, 1, 1, 1, 1).$$

**11.** Let  $n \geq 2$  be an integer,  $F_n$  the  $n$ th Fermat number  $2^{2^n} + 1$ ,  $p$  a prime divisor of  $F_n$ .

a) The order of 2 divides  $2^{n+1}$  because  $2^{n+1} \equiv 1 \pmod{p}$ , but it does not divide  $2^n$  because  $2^n \equiv -1 \pmod{p}$ . Hence it is  $2^{n+1}$ .

b) The order of 2 modulo  $p$  divides  $p - 1$ , hence  $p$  is congruent to 1 modulo  $2^{n+1}$ .

c) The number 2 is a quadratic residue modulo  $p$  because  $p$  is congruent to 1 modulo 8 (recall the assumption  $n \geq 2$ ).

d) Since 2 is a quadratic residue modulo  $p$  and since the Legendre symbol  $\left(\frac{2}{p}\right)$  is congruent to  $2^{(p-1)/2}$  modulo  $p$ , it follows that the number  $2^{(p-1)/2}$  is congruent to 1 modulo  $p$ . This means that the order of 2 modulo  $p$  divides  $(p - 1)/2$ . Since this order is  $2^{n+1}$ , it follows that  $2^{n+1}$  divides  $(p - 1)/2$ , which means that  $p$  is congruent to 1 modulo  $2^{n+2}$ .