- Recall that, in contrast to DES, the operations of AES have very simple (though somewhat advanced) mathematical descriptions.

  No mysteriously constructed S-boxes and P-boxes as in DES.

ByteSub (continued)

Each of the 16 bytes gets substituted as follows.

- Interpret the input byte $(b_7b_6...b_0)_2$ as the element $b_7x^7+...+b_1x+b_0$ of $\mathrm{GF}(2^8)$.
- Compute $s^{-1}=c_0+c_1x+...+c_7x^7$ (with 0^{-1} interpreted as 0).

  Important comment. This inversion is what makes AES highly nonlinear.

  If the ByteSub substitution was linear, then all of AES would be linear (because all other layers are linear; assuming we adjust the key schedule accordingly).

- Then the output bits $(d_7d_6...d_1d_0)_2$ are

$$\begin{bmatrix} d_0 \\ d_1 \\ \vdots \\ d_7 \end{bmatrix} = \begin{bmatrix} 1&0&0&0&1&1&1&1 \\ 1&1&0&0&0&1&1&1 \\ 1&1&1&0&0&0&1&1 \\ 1&1&1&1&0&0&0&1 \\ 1&1&1&1&1&0&0&0 \\ 0&1&1&1&1&1&0&0 \\ 0&0&1&1&1&1&1&0 \\ 0&0&0&1&1&1&1&1 \end{bmatrix} \begin{bmatrix} c_0 \\ c_1 \\ \vdots \\ c_7 \end{bmatrix} + \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{bmatrix}.$$

Comment. The particular choice of matrix and vector has the effect that no ByteSub output equals the ByteSub input (or its complement).

Example 124. Invert x^2+1 in $\mathrm{GF}(2^8)$, constructed as in AES. [Example 120, again]

Solution. Recall that for AES, $\mathrm{GF}(2^8)$ is constructed using $x^8+x^4+x^3+x+1$.

We use the extended Euclidean algorithm for polynomials, and reduce all coefficients modulo 2:

$$\boxed{x^8+x^4+x^3+x+1} \equiv (x^6+x^4+x)\cdot\boxed{x^2+1}+1$$

Hence, $(x^2+1)^{-1}=x^6+x^4+x$ in $\mathrm{GF}(2^8)$.

Example 125. (homework) What happens to the byte $(0000\ 0101)_2$ during ByteSub?

Solution. $(0000\ 0101)_2$ represents the polynomial x^2+1.

By the previous example, its inverse is $(x^2+1)^{-1}=x^6+x^4+x$ in $\mathrm{GF}(2^8)$, which is $\boldsymbol{c}=(0101\ 0010)_2$.

$$\begin{bmatrix} 1&0&0&0&1&1&1&1 \\ 1&1&0&0&0&1&1&1 \\ 1&1&1&0&0&0&1&1 \\ 1&1&1&1&0&0&0&1 \\ 1&1&1&1&1&0&0&0 \\ 0&1&1&1&1&1&0&0 \\ 0&0&1&1&1&1&1&0 \\ 0&0&0&1&1&1&1&1 \end{bmatrix} \underbrace{\begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 1 \\ 0 \end{bmatrix}}_{\boldsymbol{c}} + \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 1 \\ 0 \end{bmatrix} + \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \end{bmatrix} + \begin{bmatrix} 1 \\ 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 1 \end{bmatrix} + \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 1 \\ 1 \\ 0 \\ 1 \\ 0 \\ 1 \\ 1 \\ 0 \end{bmatrix}$$

[This is just the usual matrix-vector product modulo 2. The highlighted columns are the ones which get added up during this matrix-vector product.]

Hence, the output of ByteSub is the byte $(0110\ 1011)_2$.

Comment. To check, this indeed matches the value $107=(0110\ 1011)_2$ in the lookup table given in Table 5.1 of our book (row 0, column $(0101)_2=5$).

Review: multiplicative order and primitive roots

Definition 126. The **multiplicative order** of an invertible residue a modulo n is the smallest positive integer k such that $a^k \equiv 1 \pmod{n}$.

Lemma 127. If $a^r \equiv 1 \pmod{n}$ and $a^s \equiv 1 \pmod{n}$, then $a^{\gcd(r,s)} \equiv 1 \pmod{n}$.

Proof. By Bezout's identity, there are integers x, y such that $xr + ys = \gcd(r, s)$.
Hence, $a^{\gcd(r,s)} = a^{xr+ys} = a^{xr}a^{ys} = (a^r)^x(a^s)^y \equiv 1 \pmod{n}$. □

Corollary 128. The multiplicative order of a modulo n divides $\phi(n)$.

Proof. Let k be the multiplicative order, so that $a^k \equiv 1 \pmod{n}$. By Euler's theorem $a^{\phi(n)} \equiv 1 \pmod{n}$. The previous lemma shows that $a^{\gcd(k,\phi(n))} \equiv 1 \pmod{n}$. But since the multiplicative order is the smallest exponent, it must be the case that $\gcd(k, \phi(n)) = k$. Equivalently, k divides $\phi(n)$. □

Definition 129. If the multiplicative order of an residue a modulo n equals $\phi(n)$ [in other words, the order is as large as possible], then a is said to be **primitive root** modulo n.

A primitive root is also referred to as a **multiplicative generator** (because the products of a, that is, $1, a, a^2, a^3, \ldots$, produce all invertible residues).

Example 130. Compute the multiplicative order of 2 modulo $7, 11, 9, 15$. In each case, is 2 a primitive root?

Solution.

- $2 \pmod{7}$: $2^2 \equiv 4, 2^3 \equiv 1$. Hence, the order of 2 modulo 7 is 3.
  Since the order is less than $\phi(7) = 6$, 2 is not a primitive root modulo 7.
- $2 \pmod{11}$: Since $\phi(11) = 10$, the only possible orders are $2, 5, 10$. Hence, checking that $2^2 \not\equiv 1$ and $2^5 \not\equiv 1$ is enough to conclude that the order must be 10.
  Since the order is equal to $\phi(11) = 10$, 2 is a primitive root modulo 11.
  Brute force approach (too much unnecessary work). Just for comparison, $2^0 = 1, 2^1 = 2, 2^2 = 4, 2^3 = 8, 2^4 \equiv 5, 2^5 \equiv 2 \cdot 5 = 10, 2^6 \equiv 2 \cdot 10 \equiv 9, 2^7 \equiv 2 \cdot 9 \equiv 7, 2^8 \equiv 2 \cdot 7 \equiv 3, 2^9 \equiv 2 \cdot 3 = 6, 2^{10} \equiv 2 \cdot 6 \equiv 1$. Thus, the order of 2 mod 11 is 10.
- $2 \pmod{9}$: Since $\phi(9) = 6$, the only possible orders are $2, 3, 6$. Hence, checking that $2^2 \not\equiv 1$ and $2^3 \not\equiv 1$ is enough to conclude that the order must be 6. (Indeed, $2^2 \equiv 4$, $2^3 \equiv 8$, $2^4 \equiv 7$, $2^5 \equiv 5$, $2^6 \equiv 1$.)
  Since the order is equal to $\phi(9) = 6$, 2 is a primitive root modulo 9.
- The order of $2 \pmod{15}$ is 4 (a divisor of $\phi(15) = 8$).
  2 is not a primitive root modulo 15. In fact, there is no primitive root modulo 15.

Comment. It is an open conjecture to show that 2 is a primitive root modulo infinitely many primes. (This is a special case of Artin's conjecture which predicts much more.)

Advanced comment. There exists a primitive root modulo n if and only if n is of one of $1, 2, 4, p^k, 2p^k$ for some odd prime p.