

## Supplement to Implementation of a New Primality Test

By H. Cohen and A. K. Lenstra

### APPENDIX: MULTIPLICATION AND SQUARING ROUTINES

Here we present the multiplication and squaring routines that are used in the pseudoprime tests with Jacobi sums. For a given prime power  $p^k$  we put  $m = (p-1)p^{k-1}$ , and we denote by  $(x_i)_{i=0}^2$ ,  $(y_i)_{i=0}^m$ ,  $(z_i)_{i=0}^l$  three elements of  $\mathbb{Z}[\zeta_p]/n\mathbb{Z}[\zeta_p]$ . The multiplication routines below have  $x$  and  $y$  as input and compute their product  $x \cdot y$ . On output,  $x$  and  $y$  are unchanged and the product is returned in  $z$ . The squaring routines have  $x$  as input and compute its square  $x^2$ . On output,  $x$  is unchanged and its square is returned in  $y$ . Auxiliary variables whose names begin with a 'c' or a 'd' are 'doubles', the others are 'multiples' (so,  $x_i$ ,  $y_i$ , and  $z_i$  are 'multiples', cf. Section 7).

Let  $D$  be the time to compute the remainder of a 'double' modulo  $n$ , let  $M$  be the time for a 'multiple'-'multiple' multiplication,  $A_1$  for a 'multiple'-'multiple' addition or subtraction, and  $A_2$  for a 'double'-'double' addition or subtraction. At the end of each routine we give the total time expressed in the number of  $D$ 's,  $M$ 's,  $A_1$ 's, and  $A_2$ 's for that routine.

First we present five auxiliary routines.

**Auxiliary routine 1.** This routine operates on the variables  $(a_i)_{i=0}^2$ ,  $(b_i)_{i=0}^2$ ,  $(c_i)_{i=0}^4$ . The  $a_i$  and  $b_i$  are input to the routine and their values are not affected; the  $c_i$  are output variables.

$$\begin{aligned} c_0 &= a_0 \cdot b_0; & d_1 &= a_1 \cdot b_1; & c_4 &= a_2 \cdot b_2; & m_1 &= a_0 + a_1; & m_2 &= b_0 + b_1; & d_3 &= m_1 \cdot m_2; \\ m_1 &= a_0 + a_2; & m_2 &= b_0 + b_2; & d_4 &= m_1 \cdot m_2; & m_1 &= a_1 + a_2; & m_2 &= b_1 + b_2; & d_5 &= m_1 \cdot m_2; \\ d_2 &= c_0 + d_1; & c_1 &= d_3 - d_2; & d_2 &= d_4 + d_1; & d_4 &= c_0 + c_4; & c_2 &= d_2 - d_4; & d_2 &= d_1 + c_4, \\ c_3 &= d_5 - d_2. \end{aligned}$$

The following now holds.

$$\begin{aligned} c_0 &= a_0 \cdot b_0, \\ c_1 &= a_0 \cdot b_1 + a_1 \cdot b_0, \\ c_2 &= a_0 \cdot b_2 + a_1 \cdot b_1 + a_2 \cdot b_0, \\ c_3 &= a_1 \cdot b_2 + a_2 \cdot b_1, \\ c_4 &= a_2 \cdot b_2. \end{aligned}$$

Time =  $6M + 6A_1 + 7A_2$

**Auxiliary routine 2.** This routine operates on the variables  $(a_i)_{i=0}^3$ ,  $(b_i)_{i=0}^3$ ,  $(c_i)_{i=0}^6$ . The  $a_i$  and  $b_i$  are input to the routine and their values are not affected; the  $c_i$  are output variables.

$$\begin{aligned} c_0 &= a_0 \cdot b_0; & d_1 &= a_1 \cdot b_1; & d_2 &= a_2 \cdot b_2; & c_6 &= a_3 \cdot b_3; & m_1 &= a_0 + a_1; & m_2 &= b_0 + b_1; & d_3 &= m_1 \cdot m_2, \\ m_1 &= a_0 + a_2; & m_2 &= b_0 + b_2; & d_4 &= m_1 \cdot m_2; & m_3 &= a_2 + a_3; & m_4 &= b_2 + b_3; & d_5 &= m_3 \cdot m_4; \\ m_3 &= a_1 + a_3; & m_4 &= b_1 + b_3; & d_6 &= m_3 \cdot m_4; & d_7 &= c_0 + d_1; & c_1 &= d_3 - d_7; & d_7 &= c_0 + d_2; \\ d_8 &= d_1 + d_4; & c_2 &= d_8 - d_7; & m_5 &= m_1 + m_3; & m_3 &= m_2 + m_4; & d_7 &= d_2 + c_6; & c_5 &= d_5 - d_7; \\ d_7 &= d_3 + m_5; & d_8 &= c_1 + c_5; & d_9 &= d_8 + d_6; & d_8 &= d_9 + d_4; & c_3 &= d_7 - d_8; & d_7 &= d_6 + d_2; \\ d_8 &= d_1 + c_6; & c_4 &= d_7 - d_8. \end{aligned}$$

The following now holds:

$$\begin{aligned} c_0 &= a_0 \cdot b_0, \\ c_1 &= a_0 \cdot b_1 + a_1 \cdot b_0, \\ c_2 &= a_0 \cdot b_2 + a_1 \cdot b_1 + a_2 \cdot b_0, \\ c_3 &= a_0 \cdot b_3 + a_1 \cdot b_2 + a_2 \cdot b_1 + a_3 \cdot b_0, \\ c_4 &= a_1 \cdot b_3 + a_2 \cdot b_2 + a_3 \cdot b_1, \\ c_5 &= a_2 \cdot b_3 + a_3 \cdot b_2, \\ c_6 &= a_3 \cdot b_3. \end{aligned}$$

Time =  $9M + 10A_1 + 14A_2$

**Auxiliary routine 3.** This routine operates on the variables  $(a_i)_{i=0}^4$ ,  $(b_i)_{i=0}^4$ ,  $(c_i)_{i=0}^8$ . The  $a_i$  and  $b_i$  are input to the routine and their values are not affected; the  $c_i$  are output variables. Apply auxiliary routine 1 to  $(a_i)_{i=0}^2$ ,  $(b_i)_{i=0}^2$ ,  $(c_i)_{i=0}^4$ ;  $m_0 = a_0 + a_1$ ;  $m_1 = a_1 + a_4$ ;  $m_2 = b_0 + b_3$ ;  $m_3 = b_1 + b_4$ ;  $m_4 = e_3 + a_4$ ;  $m_5 = e_2 + b_4$ , apply auxiliary routine 1 with  $(a_i)_{i=0}^2$ ,  $(b_i)_{i=0}^2$ ,  $(c_i)_{i=0}^8$  replaced by  $m_0$ ,  $m_1$ ,  $a_2$ ,  $m_2$ ,  $m_3$ ,  $b_2$  and  $(d_i)_{i=0}^8$ , respectively;  $d_5 = a_3 b_3$ ;  $c_8 = a_4 b_4$ ;  $d_6 = a_0 + a_1$ ;  $d_7 = d_3 + d_4$ ;  $c_7 = d_6 - d_7$ ;  $d_6 = d_3 + d_5$ ;  $c_6 = d_6 - c_3$ ;  $d_6 = c_2 + c_3$ ;  $d_7 = c_3 + d_0$ ;  $c_3 = d_7 - d_6$ ;  $d_6 = c_1 + c_7$ ,  $d_7 = c_4 + d_1$ ;  $c_4 = d_7 - d_6$ ;  $d_6 = c_2 + c_8$ ;  $c_5 = d_2 - d_6$ . The following now holds:

$$\begin{aligned} c_0 &= a_0 b_0, \\ c_1 &= a_0 b_1 + a_1 b_0, \\ c_2 &= a_0 b_2 + a_1 b_1 + a_2 b_0, \\ c_3 &= a_0 b_3 + a_1 b_2 + a_2 b_1 + a_3 b_0, \\ c_4 &= a_0 b_4 + a_1 b_3 + a_2 b_2 + a_3 b_1 + a_4 b_0, \\ c_5 &= a_2 b_4 + a_3 b_3 + a_4 b_2 + a_5 b_1 + a_6 b_0, \\ c_6 &= a_2 b_6 + a_3 b_5 + a_4 b_4 + a_5 b_3, \\ c_7 &= a_5 b_6 + a_6 b_5, \\ c_8 &= a_4 b_4. \end{aligned}$$

Time =  $15M + 18A_1 + 26A_2$ . The following now holds:

$$\begin{aligned} m_1 &= q_2 + a_2, \quad m_2 = a_0 + a_1; \quad m_3 = a_1 + a_3; \quad m_4 = e_3 + a_4; \quad m_5 = a_3 + a_5; \quad m_6 = a_0 + a_6, \\ m_6 &= m_0 + m_1; \quad m_7 = a_1 + a_3; \quad m_8 = a_4 + a_4; \quad m_9 = m_8 + m_1; \quad m_0 = a_0 + a_3; \\ c_0 &= a_0 a_1; \quad d_1 = a_0 a_1; \quad c_8 = a_4 a_4; \quad d_2 = a_1 a_3; \quad d_3 = a_1 a_1; \quad d_4 = a_3 a_1, \\ c_7 &= d_2 + d_2; \quad d_5 = m_2 b_3; \quad d_6 = d_1 + d_3; \quad c_2 = d_5 - d_6; \quad d_5 = m_4 m_5; \quad d_6 = d_2 + d_4; \\ c_6 &= d_5 - d_6; \quad d_5 = m_6 m_7; \quad d_6 = c_1 + d_4; \quad c_3 = d_5 - d_6; \quad d_5 = m_7 m_8; \quad d_6 = c_7 + d_3; \\ c_5 &= d_5 - d_6; \quad d_5 = m_7 m_8; \quad d_6 = d_1 + d_2; \quad d_5 = d_3 - d_6; \quad d_6 = d_4 + d_5; \quad d_5 = a_2 b_2, \\ c_4 &= d_5 + d_6. \end{aligned}$$

The following now holds:

$$\begin{aligned} c_0 &= a_0 b_0, \\ c_1 &= a_0 b_1 + a_1 b_0, \\ c_2 &= a_0 b_2 + a_1 b_1 + a_2 b_0, \\ c_3 &= a_0 b_3 + a_1 b_2 + a_2 b_1 + a_3 b_0, \\ c_4 &= a_0 b_4 + a_1 b_3 + a_2 b_2 + a_3 b_1 + a_4 b_0, \\ c_5 &= a_2 b_4 + a_3 b_3 + a_4 b_2 + a_5 b_1 + a_6 b_0, \\ c_6 &= a_2 b_6 + a_3 b_5 + a_4 b_4 + a_5 b_3, \\ c_7 &= a_5 b_6 + a_6 b_5, \\ c_8 &= a_4 b_4. \end{aligned}$$

Time =  $15M + 18A_1 + 26A_2$ . This routine operates on the variables  $(a_i)_{i=0}^4$ ,  $(c_i)_{i=0}^8$ . The  $a_i$  are input to the routine and their values are not affected; the  $c_i$  are output variables.

$$\begin{aligned} m_1 &= q_2 + a_2, \quad m_2 = a_0 + a_1; \quad m_3 = e_3 + a_4; \quad m_4 = a_3 + a_5; \quad m_5 = a_0 + a_6, \\ m_6 &= m_0 + m_1; \quad m_7 = a_1 + a_3; \quad m_8 = a_4 + a_4; \quad m_9 = m_8 + m_1; \quad m_0 = a_0 + a_3; \\ c_0 &= a_0 a_1; \quad d_1 = a_0 a_1; \quad c_8 = a_4 a_4; \quad d_2 = a_1 a_3; \quad d_3 = a_1 a_1; \quad d_4 = a_3 a_1, \\ c_7 &= d_2 + d_2; \quad d_5 = m_2 b_3; \quad d_6 = d_1 + d_3; \quad c_2 = d_5 - d_6; \quad d_5 = m_4 m_5; \quad d_6 = d_2 + d_4; \\ c_6 &= d_5 - d_6; \quad d_5 = m_6 m_7; \quad d_6 = c_1 + d_4; \quad c_3 = d_5 - d_6; \quad d_5 = m_7 m_8; \quad d_6 = c_7 + d_3; \\ c_5 &= d_5 - d_6; \quad d_5 = m_7 m_8; \quad d_6 = d_1 + d_2; \quad d_5 = d_3 - d_6; \quad d_6 = d_4 + d_5; \quad d_5 = a_2 b_2, \\ c_4 &= d_5 + d_6. \end{aligned}$$

The following now holds:

$$\begin{aligned} c_0 &= a_0 b_0, \\ c_1 &= a_0 b_1 + a_1 b_0, \\ c_2 &= a_0 b_2 + a_1 b_1 + a_2 b_0, \\ c_3 &= a_0 b_3 + a_1 b_2 + a_2 b_1 + a_3 b_0, \\ c_4 &= a_0 b_4 + a_1 b_3 + a_2 b_2 + a_3 b_1 + a_4 b_0, \\ c_5 &= a_2 b_4 + a_3 b_3 + a_4 b_2 + a_5 b_1 + a_6 b_0, \\ c_6 &= a_2 b_6 + a_3 b_5 + a_4 b_4 + a_5 b_3, \\ c_7 &= a_5 b_6 + a_6 b_5, \\ c_8 &= a_4 b_4. \end{aligned}$$

Time =  $12M + 12A_1 + 14A_2$ . This routine operates on the variables  $(d_i)_{i=0}^9$ ,  $(d_{2,i})_{i=0}^8$ ,  $(d_{3,i})_{i=0}^8$ ,  $(d_{4,i})_{i=0}^8$ .

$$\begin{aligned} z_0 &= x_0 y_0 - x_1 y_3 - x_2 y_2 - x_3 y_1 + x_4 y_3 + x_5 y_2, \\ z_1 &= x_0 y_1 + x_1 y_0 - x_1 y_3 - x_2 y_2 - x_3 y_1 + x_4 y_3 + x_5 y_2, \\ z_2 &= x_0 y_2 + x_1 y_1 + x_2 y_0 - x_1 y_3 - x_2 y_2 - x_3 y_1, \\ z_3 &= x_0 y_3 + x_1 y_2 + x_2 y_1 + x_3 y_0 - x_1 y_3 - x_2 y_2 - x_3 y_1. \end{aligned}$$

Time =  $4D + 9M + 10A_1 + 11A_2$ . The following now holds modulo  $n$ :

$$\begin{aligned} m_1 &= x_0 - x_2, \quad m_2 = x_0 + x_2, \quad m_3 = x_2 - x_1; \quad m_4 = x_0 - x_3; \quad m_5 = x_1 - x_0; \quad m_6 = x_2 - x_3, \\ m_7 &= x_1 - x_3; \quad m_8 = x_3 + x_3; \quad d_1 = m_1 m_8, \quad d_2 = m_1 m_2, \quad d_3 = d_1 + d_2; \\ d_2 &= m_1 m_8, \quad d_4 = d_1 + d_3; \quad m_3 = m_1 + x_0, \quad d_1 = x_3 y_2; \\ y_0 = d_3 m_2 n, \quad y_1 = d_4 m_2 n, \quad d_3 = d_1 + d_2, \quad y_2 = d_3 m_2 n, \quad m_7 = m_6 + m_6, \quad d_2 = m_7 m_5; \\ d_3 = d_1 + d_2; \quad z_3 = d_3 \text{ mod } n \end{aligned}$$

The following now holds modulo  $n$ :

$$\begin{aligned} z_0 &= x_0 y_0 - x_1 y_3 - x_2 y_2 - x_3 y_1 + x_4 y_3 + x_5 y_2, \\ z_1 &= x_0 y_1 + x_1 y_0 - x_1 y_3 - x_2 y_2 - x_3 y_1 + x_4 y_3 + x_5 y_2, \\ z_2 &= x_0 y_2 + x_1 y_1 + x_2 y_0 - x_1 y_3 - x_2 y_2 - x_3 y_1, \\ z_3 &= x_0 y_3 + x_1 y_2 + x_2 y_1 + x_3 y_0 - x_1 y_3 - x_2 y_2 - x_3 y_1. \end{aligned}$$

Time =  $4D + 9M + 10A_1 + 11A_2$ . The following now holds modulo  $n$ :

$$\begin{aligned} m_1 &= x_0 - x_2, \quad m_2 = x_0 + x_2, \quad m_3 = x_2 - x_1; \quad m_4 = x_0 - x_3; \quad m_5 = x_1 - x_0; \quad m_6 = x_2 - x_3, \\ m_7 &= x_1 - x_3; \quad m_8 = x_3 + x_3; \quad d_1 = m_1 m_8, \quad d_2 = m_1 m_2, \quad d_3 = d_1 + d_2; \\ d_2 &= m_1 m_8, \quad d_4 = d_1 + d_3; \quad m_3 = m_1 + x_0, \quad d_1 = x_3 y_2; \\ y_0 = d_3 m_2 n, \quad y_1 = d_4 m_2 n, \quad d_3 = d_1 + d_2, \quad y_2 = d_3 m_2 n, \quad m_7 = m_6 + m_6, \quad d_2 = m_7 m_5; \\ d_3 = d_1 + d_2; \quad z_3 = d_3 \text{ mod } n \end{aligned}$$

The following now holds modulo  $n$ :

$$\begin{aligned} z_0 &= x_0^2 - 2x_1 x_3 - x_2^2 + x_2 x_3, \\ z_1 &= 2x_0 x_1 - 2x_1 x_3 - x_2^2 + x_2 x_3, \\ z_2 &= 2x_0 x_2 + x_1^2 - 2x_1 x_3 - x_2^2. \end{aligned}$$

Now we are ready to present the multiplication and squaring routines.

$$y_3 = 2e_0x_3 + 2x_1x_2^2 - 2x_1x_3 - x_2^2$$

Time =  $4D + 6M + 12d_1 + 4d_2$ . Return  $y = x^2$

**Multiplication for  $p = 7$ .**

Apply auxiliary routine 1 with  $(a_i)^2=0$ ;  $(b_i)^2=0$ ;  $(c_i)^4=0$  replaced by  $(x_i)^2=0$ ;  $(y_i)^2=0$ ;  $(d_i)^4=0$ , respectively; apply auxiliary routine 1 with  $(a_i)^2=0$ ;  $(b_i)^2=0$ ;  $(c_i)^4=0$  replaced by  $(x_i)^3=3$ ;  $(y_i)^5=3$ ;  $(d_i)^6=6$ , respectively; apply auxiliary routine 1 with  $(a_i)^2=0$ ;  $(b_i)^2=0$ ;  $(c_i)^4=0$  replaced by  $(m_i)^6=6$ ;  $m_1=x_0-x_1$ ;  $m_2=x_0+x_1$ ;  $m_3=x_1-x_3$ ;  $m_4=x_0+x_3$ ;  $m_5=x_0+x_6$ ;  $m_6=x_1+x_5$ ;  $m_7=x_1+m_3$ ;  $m_8=m_1+m_4$ ;  $d_1=m_1m_2$ ;  $d_2=m_3m_4$ ;  $d_3=m_6m_3$ ;  $d_4=m_5m_2$ ;  $d_5=m_7m_8$ ;  $d_6=d_1+d_3$  mod  $n$ ;  $d_7=d_1+d_4$ ;  $d_8=(d_5-d_6)$  mod  $n$ ;  $d_9=m_5+m_6$ ;  $d_{10}=m_1m_2$ ;  $d_{11}=d_3+d_4$ ;  $d_{12}=d_3-d_6$  mod  $n$ .

The following now holds modulo  $n$ :

$$d_0: d_8 = d_3+d_4; \quad d_1 = d_2+d_3; \quad d_3 = d_3+d_6; \quad d_4 = d_1+d_2; \quad d_5 = d_{18}+d_8; \quad d_6 = d_8+d_9; \quad d_7 = d_9+d_{15}; \quad d_{15} = (d_{18}-d_6) \text{ mod } n; \quad d_{18} = (d_{14}-d_6) \text{ mod } n;$$

$$d_0: d_8 = (d_{18}-d_6) \text{ mod } n; \quad d_8 = d_3+d_{16}; \quad z_3 = (d_{18}-d_6) \text{ mod } n; \quad z_4 = (d_{14}-d_6) \text{ mod } n;$$

$z_5 = (d_{15}-d_6) \text{ mod } n$ .

The following now holds modulo  $n$ :

$$z_6 = x_0x_2 - x_1x_5 - x_2x_4 - x_3x_3 - x_4x_2 - x_5x_1 - x_5x_5 + x_3x_7 + x_4x_3 + x_5x_2 + x_2$$

$$z_1 = x_0x_2x_3 - x_1x_5 - x_2x_4 - x_3x_5 - x_4x_2 - x_5x_1 - x_5x_5 + x_3x_7 + x_4x_3 + x_5x_2 + x_2$$

$$z_2 = x_0x_2x_3x_1 + x_2x_4x_1 + x_3x_5x_1 - x_2x_4 - x_3x_5 + x_4x_2 + x_5x_1 + x_5x_5 + x_5x_4,$$

$$z_4 = x_0x_2 + x_1x_2 + x_2x_3 + x_3x_4 + x_4x_5 - x_2x_4 - x_3x_5 - x_4x_2 - x_5x_1 - x_5x_5 + x_5x_7,$$

$$z_5 = x_0x_2x_3 + x_2x_4x_1 + x_3x_5x_1 + x_4x_5x_2 + x_5x_3 - x_2x_4 - x_3x_5 - x_4x_2 - x_5x_1 - x_5x_5 + x_5x_7,$$

Time =  $6D + 18M + 24d_1 + 54d_2$ . Return  $z = xy$ .

**Squaring for  $p = 7$ .**

$m_1 = x_0-x_1$ ;  $m_2 = x_1-x_2$ ;  $m_3 = x_2-x_3$ ;  $m_4 = x_3-x_4$ ;  $m_5 = x_4-x_5$ ;  $m_6 = x_1+m_2$ ;  $m_7 = m_2+m_3$ ;  $m_8 = m_3+m_4$ ;  $m_9 = m_4+m_5$ ;  $m_{10} = m_5+m_6$ ;  $m_{11} = m_6+m_7$ ;  $m_{12} = m_7+m_8$ ;  $m_{13} = m_8+m_9$ ;  $m_{14} = m_9+m_{10}$ ;  $m_{15} = x_0+x_1$ ;  $m_{16} = x_1+x_2$ ;  $m_{17} = x_2+x_3$ ;  $m_{18} = x_3+x_4$ ;  $m_{19} = x_4+x_5$ ;  $m_{20} = x_5+x_6$ ;  $m_{21} = x_6+x_7$ ;  $m_{22} = x_7+x_8$ ;  $m_{23} = x_8+x_9$ ;  $m_{24} = x_9+x_{10}$ ;  $m_{25} = x_{10}+x_1$ ;  $m_{26} = x_1+x_2$ ;  $m_{27} = x_2+x_3$ ;  $m_{28} = x_3+x_4$ ;  $m_{29} = x_4+x_5$ ;  $m_{30} = x_5+x_6$ ;  $m_{31} = x_6+x_7$ ;  $m_{32} = x_7+x_8$ ;  $m_{33} = x_8+x_9$ ;  $m_{34} = x_9+x_{10}$ ;  $m_{35} = x_{10}+x_1$ ;  $m_{36} = x_1+x_2$ ;  $m_{37} = x_2+x_3$ ;  $m_{38} = x_3+x_4$ ;  $m_{39} = x_4+x_5$ ;  $m_{40} = x_5+x_6$ ;  $m_{41} = x_6+x_7$ ;  $m_{42} = x_7+x_8$ ;  $m_{43} = x_8+x_9$ ;  $m_{44} = x_9+x_{10}$ ;  $m_{45} = x_{10}+x_1$ ;  $m_{46} = x_1+x_2$ ;  $m_{47} = x_2+x_3$ ;  $m_{48} = x_3+x_4$ ;  $m_{49} = x_4+x_5$ ;  $m_{50} = x_5+x_6$ ;  $m_{51} = x_6+x_7$ ;  $m_{52} = x_7+x_8$ ;  $m_{53} = x_8+x_9$ ;  $m_{54} = x_9+x_{10}$ ;  $m_{55} = x_{10}+x_1$ ;  $m_{56} = x_1+x_4$ ;  $m_{57} = x_4+x_5$ ;  $m_{58} = x_5+x_6$ ;  $m_{59} = x_6+x_7$ ;  $m_{60} = x_7+x_8$ ;  $m_{61} = x_8+x_9$ ;  $m_{62} = x_9+x_{10}$ ;  $m_{63} = x_{10}+x_1$ ;  $m_{64} = x_1+x_5$ ;  $m_{65} = x_5+x_6$ ;  $m_{66} = x_6+x_7$ ;  $m_{67} = x_7+x_8$ ;  $m_{68} = x_8+x_9$ ;  $m_{69} = x_9+x_{10}$ ;  $m_{70} = x_{10}+x_1$ ;  $m_{71} = x_1+x_6$ ;  $m_{72} = x_6+x_7$ ;  $m_{73} = x_7+x_8$ ;  $m_{74} = x_8+x_9$ ;  $m_{75} = x_9+x_{10}$ ;  $m_{76} = x_{10}+x_1$ ;  $m_{77} = x_1+x_7$ ;  $m_{78} = x_7+x_8$ ;  $m_{79} = x_8+x_9$ ;  $m_{80} = x_9+x_{10}$ ;  $m_{81} = x_{10}+x_1$ ;  $m_{82} = x_1+x_8$ ;  $m_{83} = x_8+x_9$ ;  $m_{84} = x_9+x_{10}$ ;  $m_{85} = x_{10}+x_1$ ;  $m_{86} = x_1+x_9$ ;  $m_{87} = x_9+x_{10}$ ;  $m_{88} = x_{10}+x_1$ ;  $m_{89} = x_1+x_{10}$ ;  $m_{90} = x_{10}+x_1$ ;  $m_{91} = x_1+x_5$ ;  $m_{92} = x_5+x_6$ ;  $m_{93} = x_6+x_7$ ;  $m_{94} = x_7+x_8$ ;  $m_{95} = x_8+x_9$ ;  $m_{96} = x_9+x_{10}$ ;  $m_{97} = x_{10}+x_1$ ;  $m_{98} = x_1+x_6$ ;  $m_{99} = x_6+x_7$ ;  $m_{100} = x_7+x_8$ ;  $m_{101} = x_8+x_9$ ;  $m_{102} = x_9+x_{10}$ ;  $m_{103} = x_{10}+x_1$ ;  $m_{104} = x_1+x_7$ ;  $m_{105} = x_7+x_8$ ;  $m_{106} = x_8+x_9$ ;  $m_{107} = x_9+x_{10}$ ;  $m_{108} = x_{10}+x_1$ ;  $m_{109} = x_1+x_8$ ;  $m_{110} = x_8+x_9$ ;  $m_{111} = x_9+x_{10}$ ;  $m_{112} = x_{10}+x_1$ ;  $m_{113} = x_1+x_9$ ;  $m_{114} = x_9+x_{10}$ ;  $m_{115} = x_{10}+x_1$ ;  $m_{116} = x_1+x_{10}$ ;  $m_{117} = x_{10}+x_1$ ;  $m_{118} = x_1+x_1$ ;  $m_{119} = x_1+x_2$ ;  $m_{120} = x_2+x_3$ ;  $m_{121} = x_3+x_4$ ;  $m_{122} = x_4+x_5$ ;  $m_{123} = x_5+x_6$ ;  $m_{124} = x_6+x_7$ ;  $m_{125} = x_7+x_8$ ;  $m_{126} = x_8+x_9$ ;  $m_{127} = x_9+x_{10}$ ;  $m_{128} = x_{10}+x_1$ ;  $m_{129} = x_1+x_5$ ;  $m_{130} = x_5+x_6$ ;  $m_{131} = x_6+x_7$ ;  $m_{132} = x_7+x_8$ ;  $m_{133} = x_8+x_9$ ;  $m_{134} = x_9+x_{10}$ ;  $m_{135} = x_{10}+x_1$ ;  $m_{136} = x_1+x_6$ ;  $m_{137} = x_6+x_7$ ;  $m_{138} = x_7+x_8$ ;  $m_{139} = x_8+x_9$ ;  $m_{140} = x_9+x_{10}$ ;  $m_{141} = x_{10}+x_1$ ;  $m_{142} = x_1+x_7$ ;  $m_{143} = x_7+x_8$ ;  $m_{144} = x_8+x_9$ ;  $m_{145} = x_9+x_{10}$ ;  $m_{146} = x_{10}+x_1$ ;  $m_{147} = x_1+x_8$ ;  $m_{148} = x_8+x_9$ ;  $m_{149} = x_9+x_{10}$ ;  $m_{150} = x_{10}+x_1$ ;  $m_{151} = x_1+x_9$ ;  $m_{152} = x_9+x_{10}$ ;  $m_{153} = x_{10}+x_1$ ;  $m_{154} = x_1+x_{10}$ ;  $m_{155} = x_{10}+x_1$ ;  $m_{156} = x_1+x_1$ ;  $m_{157} = x_1+x_2$ ;  $m_{158} = x_2+x_3$ ;  $m_{159} = x_3+x_4$ ;  $m_{160} = x_4+x_5$ ;  $m_{161} = x_5+x_6$ ;  $m_{162} = x_6+x_7$ ;  $m_{163} = x_7+x_8$ ;  $m_{164} = x_8+x_9$ ;  $m_{165} = x_9+x_{10}$ ;  $m_{166} = x_{10}+x_1$ ;  $m_{167} = x_1+x_5$ ;  $m_{168} = x_5+x_6$ ;  $m_{169} = x_6+x_7$ ;  $m_{170} = x_7+x_8$ ;  $m_{171} = x_8+x_9$ ;  $m_{172} = x_9+x_{10}$ ;  $m_{173} = x_{10}+x_1$ ;  $m_{174} = x_1+x_6$ ;  $m_{175} = x_6+x_7$ ;  $m_{176} = x_7+x_8$ ;  $m_{177} = x_8+x_9$ ;  $m_{178} = x_9+x_{10}$ ;  $m_{179} = x_{10}+x_1$ ;  $m_{180} = x_1+x_7$ ;  $m_{181} = x_7+x_8$ ;  $m_{182} = x_8+x_9$ ;  $m_{183} = x_9+x_{10}$ ;  $m_{184} = x_{10}+x_1$ ;  $m_{185} = x_1+x_8$ ;  $m_{186} = x_8+x_9$ ;  $m_{187} = x_9+x_{10}$ ;  $m_{188} = x_{10}+x_1$ ;  $m_{189} = x_1+x_9$ ;  $m_{190} = x_9+x_{10}$ ;  $m_{191} = x_{10}+x_1$ ;  $m_{192} = x_1+x_{10}$ ;  $m_{193} = x_{10}+x_1$ ;  $m_{194} = x_1+x_1$ ;  $m_{195} = x_1+x_2$ ;  $m_{196} = x_2+x_3$ ;  $m_{197} = x_3+x_4$ ;  $m_{198} = x_4+x_5$ ;  $m_{199} = x_5+x_6$ ;  $m_{200} = x_6+x_7$ ;  $m_{201} = x_7+x_8$ ;  $m_{202} = x_8+x_9$ ;  $m_{203} = x_9+x_{10}$ ;  $m_{204} = x_{10}+x_1$ ;  $m_{205} = x_1+x_5$ ;  $m_{206} = x_5+x_6$ ;  $m_{207} = x_6+x_7$ ;  $m_{208} = x_7+x_8$ ;  $m_{209} = x_8+x_9$ ;  $m_{210} = x_9+x_{10}$ ;  $m_{211} = x_{10}+x_1$ ;  $m_{212} = x_1+x_6$ ;  $m_{213} = x_6+x_7$ ;  $m_{214} = x_7+x_8$ ;  $m_{215} = x_8+x_9$ ;  $m_{216} = x_9+x_{10}$ ;  $m_{217} = x_{10}+x_1$ ;  $m_{218} = x_1+x_7$ ;  $m_{219} = x_7+x_8$ ;  $m_{220} = x_8+x_9$ ;  $m_{221} = x_9+x_{10}$ ;  $m_{222} = x_{10}+x_1$ ;  $m_{223} = x_1+x_8$ ;  $m_{224} = x_8+x_9$ ;  $m_{225} = x_9+x_{10}$ ;  $m_{226} = x_{10}+x_1$ ;  $m_{227} = x_1+x_9$ ;  $m_{228} = x_9+x_{10}$ ;  $m_{229} = x_{10}+x_1$ ;  $m_{230} = x_1+x_{10}$ ;  $m_{231} = x_{10}+x_1$ ;  $m_{232} = x_1+x_1$ ;  $m_{233} = x_1+x_2$ ;  $m_{234} = x_2+x_3$ ;  $m_{235} = x_3+x_4$ ;  $m_{236} = x_4+x_5$ ;  $m_{237} = x_5+x_6$ ;  $m_{238} = x_6+x_7$ ;  $m_{239} = x_7+x_8$ ;  $m_{240} = x_8+x_9$ ;  $m_{241} = x_9+x_{10}$ ;  $m_{242} = x_{10}+x_1$ ;  $m_{243} = x_1+x_5$ ;  $m_{244} = x_5+x_6$ ;  $m_{245} = x_6+x_7$ ;  $m_{246} = x_7+x_8$ ;  $m_{247} = x_8+x_9$ ;  $m_{248} = x_9+x_{10}$ ;  $m_{249} = x_{10}+x_1$ ;  $m_{250} = x_1+x_6$ ;  $m_{251} = x_6+x_7$ ;  $m_{252} = x_7+x_8$ ;  $m_{253} = x_8+x_9$ ;  $m_{254} = x_9+x_{10}$ ;  $m_{255} = x_{10}+x_1$ ;  $m_{256} = x_1+x_7$ ;  $m_{257} = x_7+x_8$ ;  $m_{258} = x_8+x_9$ ;  $m_{259} = x_9+x_{10}$ ;  $m_{260} = x_{10}+x_1$ ;  $m_{261} = x_1+x_8$ ;  $m_{262} = x_8+x_9$ ;  $m_{263} = x_9+x_{10}$ ;  $m_{264} = x_{10}+x_1$ ;  $m_{265} = x_1+x_9$ ;  $m_{266} = x_9+x_{10}$ ;  $m_{267} = x_{10}+x_1$ ;  $m_{268} = x_1+x_{10}$ ;  $m_{269} = x_{10}+x_1$ ;  $m_{270} = x_1+x_1$ ;  $m_{271} = x_1+x_2$ ;  $m_{272} = x_2+x_3$ ;  $m_{273} = x_3+x_4$ ;  $m_{274} = x_4+x_5$ ;  $m_{275} = x_5+x_6$ ;  $m_{276} = x_6+x_7$ ;  $m_{277} = x_7+x_8$ ;  $m_{278} = x_8+x_9$ ;  $m_{279} = x_9+x_{10}$ ;  $m_{280} = x_{10}+x_1$ ;  $m_{281} = x_1+x_5$ ;  $m_{282} = x_5+x_6$ ;  $m_{283} = x_6+x_7$ ;  $m_{284} = x_7+x_8$ ;  $m_{285} = x_8+x_9$ ;  $m_{286} = x_9+x_{10}$ ;  $m_{287} = x_{10}+x_1$ ;  $m_{288} = x_1+x_6$ ;  $m_{289} = x_6+x_7$ ;  $m_{290} = x_7+x_8$ ;  $m_{291} = x_8+x_9$ ;  $m_{292} = x_9+x_{10}$ ;  $m_{293} = x_{10}+x_1$ ;  $m_{294} = x_1+x_7$ ;  $m_{295} = x_7+x_8$ ;  $m_{296} = x_8+x_9$ ;  $m_{297} = x_9+x_{10}$ ;  $m_{298} = x_{10}+x_1$ ;  $m_{299} = x_1+x_8$ ;  $m_{300} = x_8+x_9$ ;  $m_{301} = x_9+x_{10}$ ;  $m_{302} = x_{10}+x_1$ ;  $m_{303} = x_1+x_9$ ;  $m_{304} = x_9+x_{10}$ ;  $m_{305} = x_{10}+x_1$ ;  $m_{306} = x_1+x_{10}$ ;  $m_{307} = x_{10}+x_1$ ;  $m_{308} = x_1+x_1$ ;  $m_{309} = x_1+x_2$ ;  $m_{310} = x_2+x_3$ ;  $m_{311} = x_3+x_4$ ;  $m_{312} = x_4+x_5$ ;  $m_{313} = x_5+x_6$ ;  $m_{314} = x_6+x_7$ ;  $m_{315} = x_7+x_8$ ;  $m_{316} = x_8+x_9$ ;  $m_{317} = x_9+x_{10}$ ;  $m_{318} = x_{10}+x_1$ ;  $m_{319} = x_1+x_5$ ;  $m_{320} = x_5+x_6$ ;  $m_{321} = x_6+x_7$ ;  $m_{322} = x_7+x_8$ ;  $m_{323} = x_8+x_9$ ;  $m_{324} = x_9+x_{10}$ ;  $m_{325} = x_{10}+x_1$ ;  $m_{326} = x_1+x_6$ ;  $m_{327} = x_6+x_7$ ;  $m_{328} = x_7+x_8$ ;  $m_{329} = x_8+x_9$ ;  $m_{330} = x_9+x_{10}$ ;  $m_{331} = x_{10}+x_1$ ;  $m_{332} = x_1+x_7$ ;  $m_{333} = x_7+x_8$ ;  $m_{334} = x_8+x_9$ ;  $m_{335} = x_9+x_{10}$ ;  $m_{336} = x_{10}+x_1$ ;  $m_{337} = x_1+x_8$ ;  $m_{338} = x_8+x_9$ ;  $m_{339} = x_9+x_{10}$ ;  $m_{340} = x_{10}+x_1$ ;  $m_{341} = x_1+x_9$ ;  $m_{342} = x_9+x_{10}$ ;  $m_{343} = x_{10}+x_1$ ;  $m_{344} = x_1+x_{10}$ ;  $m_{345} = x_{10}+x_1$ ;  $m_{346} = x_1+x_1$ ;  $m_{347} = x_1+x_2$ ;  $m_{348} = x_2+x_3$ ;  $m_{349} = x_3+x_4$ ;  $m_{350} = x_4+x_5$ ;  $m_{351} = x_5+x_6$ ;  $m_{352} = x_6+x_7$ ;  $m_{353} = x_7+x_8$ ;  $m_{354} = x_8+x_9$ ;  $m_{355} = x_9+x_{10}$ ;  $m_{356} = x_{10}+x_1$ ;  $m_{357} = x_1+x_5$ ;  $m_{358} = x_5+x_6$ ;  $m_{359} = x_6+x_7$ ;  $m_{360} = x_7+x_8$ ;  $m_{361} = x_8+x_9$ ;  $m_{362} = x_9+x_{10}$ ;  $m_{363} = x_{10}+x_1$ ;  $m_{364} = x_1+x_6$ ;  $m_{365} = x_6+x_7$ ;  $m_{366} = x_7+x_8$ ;  $m_{367} = x_8+x_9$ ;  $m_{368} = x_9+x_{10}$ ;  $m_{369} = x_{10}+x_1$ ;  $m_{370} = x_1+x_7$ ;  $m_{371} = x_7+x_8$ ;  $m_{372} = x_8+x_9$ ;  $m_{373} = x_9+x_{10}$ ;  $m_{374} = x_{10}+x_1$ ;  $m_{375} = x_1+x_8$ ;  $m_{376} = x_8+x_9$ ;  $m_{377} = x_9+x_{10}$ ;  $m_{378} = x_{10}+x_1$ ;  $m_{379} = x_1+x_9$ ;  $m_{380} = x_9+x_{10}$ ;  $m_{381} = x_{10}+x_1$ ;  $m_{382} = x_1+x_{10}$ ;  $m_{383} = x_{10}+x_1$ ;  $m_{384} = x_1+x_1$ ;  $m_{385} = x_1+x_2$ ;  $m_{386} = x_2+x_3$ ;  $m_{387} = x_3+x_4$ ;  $m_{388} = x_4+x_5$ ;  $m_{389} = x_5+x_6$ ;  $m_{390} = x_6+x_7$ ;  $m_{391} = x_7+x_8$ ;  $m_{392} = x_8+x_9$ ;  $m_{393} = x_9+x_{10}$ ;  $m_{394} = x_{10}+x_1$ ;  $m_{395} = x_1+x_5$ ;  $m_{396} = x_5+x_6$ ;  $m_{397} = x_6+x_7$ ;  $m_{398} = x_7+x_8$ ;  $m_{399} = x_8+x_9$ ;  $m_{400} = x_9+x_{10}$ ;  $m_{401} = x_{10}+x_1$ ;  $m_{402} = x_1+x_6$ ;  $m_{403} = x_6+x_7$ ;  $m_{404} = x_7+x_8$ ;  $m_{405} = x_8+x_9$ ;  $m_{406} = x_9+x_{10}$ ;  $m_{407} = x_{10}+x_1$ ;  $m_{408} = x_1+x_7$ ;  $m_{409} = x_7+x_8$ ;  $m_{410} = x_8+x_9$ ;  $m_{411} = x_9+x_{10}$ ;  $m_{412} = x_{10}+x_1$ ;  $m_{413} = x_1+x_8$ ;  $m_{414} = x_8+x_9$ ;  $m_{415} = x_9+x_{10}$ ;  $m_{416} = x_{10}+x_1$ ;  $m_{417} = x_1+x_9$ ;  $m_{418} = x_9+x_{10}$ ;  $m_{419} = x_{10}+x_1$ ;  $m_{420} = x_1+x_{10}$ ;  $m_{421} = x_{10}+x_1$ ;  $m_{422} = x_1+x_1$ ;  $m_{423} = x_1+x_2$ ;  $m_{424} = x_2+x_3$ ;  $m_{425} = x_3+x_4$ ;  $m_{426} = x_4+x_5$ ;  $m_{427} = x_5+x_6$ ;  $m_{428} = x_6+x_7$ ;  $m_{429} = x_7+x_8$ ;  $m_{430} = x_8+x_9$ ;  $m_{431} = x_9+x_{10}$ ;  $m_{432} = x_{10}+x_1$ ;  $m_{433} = x_1+x_5$ ;  $m_{434} = x_5+x_6$ ;  $m_{435} = x_6+x_7$ ;  $m_{436} = x_7+x_8$ ;  $m_{437} = x_8+x_9$ ;  $m_{438} = x_9+x_{10}$ ;  $m_{439} = x_{10}+x_1$ ;  $m_{440} = x_1+x_6$ ;  $m_{441} = x_6+x_7$ ;  $m_{442} = x_7+x_8$ ;  $m_{443} = x_8+x_9$ ;  $m_{444} = x_9+x_{10}$ ;  $m_{445} = x_{10}+x_1$ ;  $m_{446} = x_1+x_7$ ;  $m_{447} = x_7+x_8$ ;  $m_{448} = x_8+x_9$ ;  $m_{449} = x_9+x_{10}$ ;  $m_{450} = x_{10}+x_1$ ;  $m_{451} = x_1+x_8$ ;  $m_{452} = x_8+x_9$ ;  $m_{453} = x_9+x_{10}$ ;  $m_{454} = x_{10}+x_1$ ;  $m_{455} = x_1+x_9$ ;  $m_{456} = x_9+x_{10}$ ;  $m_{457} = x_{10}+x_1$ ;  $m_{458} = x_1+x_{10}$ ;  $m_{459} = x_{10}+x_1$ ;  $m_{460} = x_1+x_1$ ;  $m_{461} = x_1+x_2$ ;  $m_{462} = x_2+x_3$ ;  $m_{463} = x_3+x_4$ ;  $m_{464} = x_4+x_5$ ;  $m_{465} = x_5+x_6$ ;  $m_{466} = x_6+x_7$ ;  $m_{467} = x_7+x_8$ ;  $m_{468} = x_8+x_9$ ;  $m_{469} = x_9+x_{10}$ ;  $m_{470} = x_{10}+x_1$ ;  $m_{471} = x_1+x_5$ ;  $m_{472} = x_5+x_6$ ;  $m_{473} = x_6+x_7$ ;  $m_{474} = x_7+x_8$ ;  $m_{475} = x_8+x_9$ ;  $m_{476} = x_9+x_{10}$ ;  $m_{477} = x_{10}+x_1$ ;  $m_{478} = x_1+x_6$ ;  $m_{479} = x_6+x_7$ ;  $m_{480} = x_7+x_8$ ;  $m_{481} = x_8+x_9$ ;  $m_{482} = x_9+x_{10}$ ;  $m_{483} = x_{10}+x_1$ ;  $m_{484} = x_1+x_7$ ;  $m_{485} = x_7+x_8$ ;  $m_{486} = x_8+x_9$ ;  $m_{487} = x_9+x_{10}$ ;  $m_{488} = x_{10}+x_1$ ;  $m_{489} = x_1+x_8$ ;  $m_{490} = x_8+x_9$ ;  $m_{491} = x_9+x_{10}$ ;  $m_{492} = x_{10}+x_1$ ;  $m_{493} = x_1+x_9$ ;  $m_{494} = x_9+x_{10}$ ;  $m_{495} = x_{10}+x_1$ ;  $m_{496} = x_1+x_{10}$ ;  $m_{497} = x_{10}+x_1$ ;  $m_{498} = x_1+x_1$ ;  $m_{499} = x_1+x_2$ ;  $m_{500} = x_2+x_3$ ;  $m_{501} = x_3+x_4$ ;  $m_{502} = x_4+x_5$ ;  $m_{503} = x_5+x_6$ ;  $m_{504} = x_6+x_7$ ;  $m_{505} = x_7+x_8$ ;  $m_{506} = x_8+x_9$ ;  $m_{507} = x_9+x_{10}$ ;  $m_{508} = x_{10}+x_1$ ;  $m_{509} = x_1+x_5$ ;  $m_{510} = x_5+x_6$ ;  $m_{511} = x_6+x_7$ ;  $m_{512} = x_7+x_8$ ;  $m_{513} = x_8+x_9$ ;  $m_{514} = x_9+x_{10}$ ;  $m_{515} = x_{10}+x_1$ ;  $m_{516} = x_1+x_6$ ;  $m_{517} = x_6+x_7$ ;  $m_{518} = x_7+x_8$ ;  $m_{519} = x_8+x_9$ ;  $m_{520} = x_9+x_{10}$ ;  $m_{521} = x_{10}+x_1$ ;  $m_{522} = x_1+x_7$ ;  $m_{523} = x_7+x_8$ ;  $m_{524} = x_8+x_9$ ;  $m_{525} = x_9+x_{10}$ ;  $m_{526} = x_{10}+x_1$ ;  $m_{527} = x_1+x_8$ ;  $m_{528} = x_8+x_9$ ;  $m_{529} = x_9+x_{10}$ ;  $m_{530} = x_{10}+x_1$ ;  $m_{531} = x_1+x_9$ ;  $m_{532} = x_9+x_{10}$ ;  $m_{533} = x_{10}+x_1$ ;  $m_{534} = x_1+x_{10}$ ;  $m_{535} = x_{10}+x_1$ ;  $m_{536} = x_1+x_1$ ;  $m_{537} = x_1+x_2$ ;  $m_{538} = x_2+x_3$ ;  $m_{539} = x_3+x_4$ ;  $m_{540} = x_4+x_5$ ;  $m_{541} = x_5+x_6$ ;  $m_{542} = x_6+x_7$ ;  $m_{543} = x_7+x_8$ ;  $m_{544} = x_8+x_9$ ;  $m_{545} = x_9+x_{10}$ ;  $m_{546} = x_{10}+x_1$ ;  $m_{547} = x_1+x_5$ ;  $m_{548} = x_5+x_6$ ;  $m_{549} = x_6+x_7$ ;  $m_{550} = x_7+x_8$ ;  $m_{551} = x_8+x_9$ ;  $m_{552} = x_9+x_{10}$ ;  $m_{553} = x_{10}+x_1$ ;  $m_{554} = x_1+x_6$ ;  $m_{555} = x_6+x_7$ ;  $m_{556} = x_7+x_8$ ;  $m_{557} = x_8+x_9$ ;  $m_{558} = x_9+x_{10}$ ;  $m_{559} = x_{10}+x_1$ ;  $m_{560} = x_1+x_7$ ;  $m_{561} = x_7+x_8$ ;  $m_{562} = x_8+x_9$ ;  $m_{563} = x_9+x_{10}$ ; <

$$(d_3)_i^8=0, (d_3)_i^9=0, (z_i)_i^9=0.$$

The following now holds modulo  $n$ :

$$\begin{aligned} z_0 &= x_0y + x_1x_2x_3 + x_1x_2y + x_1x_3y + x_1x_2x_3y + x_1x_2x_3y^2 + x_1x_2x_3y^3 + x_1x_2x_3y^4 + x_1x_2x_3y^5 + x_1x_2x_3y^6 + x_1x_2x_3y^7 - 5, \\ z_1 &= x_0y + x_1x_2y + x_1x_3y + x_1x_2x_3y + x_1x_2x_3y^2 + x_1x_2x_3y^3 + x_1x_2x_3y^4 + x_1x_2x_3y^5 - 5, \\ z_2 &= x_0y + x_1x_2y + x_1x_2x_3y + x_1x_2x_3y^2 + x_1x_2x_3y^3 + x_1x_2x_3y^4 + x_1x_2x_3y^5 - 5, \\ z_3 &= x_0y + x_1x_2y + x_1x_2x_3y + x_1x_2x_3y^2 + x_1x_2x_3y^3 + x_1x_2x_3y^4 + x_1x_2x_3y^5 - 5, \\ z_4 &= x_0y + x_1x_2y + x_1x_2x_3y + x_1x_2x_3y^2 + x_1x_2x_3y^3 + x_1x_2x_3y^4 + x_1x_2x_3y^5 - 5, \\ z_5 &= x_0y + x_1x_2y + x_1x_2x_3y + x_1x_2x_3y^2 + x_1x_2x_3y^3 + x_1x_2x_3y^4 + x_1x_2x_3y^5 - 5, \\ z_6 &= x_0y + x_1x_2y + x_1x_2x_3y + x_1x_2x_3y^2 + x_1x_2x_3y^3 + x_1x_2x_3y^4 + x_1x_2x_3y^5 - 5, \\ z_7 &= x_0y + x_1x_2y + x_1x_2x_3y + x_1x_2x_3y^2 + x_1x_2x_3y^3 + x_1x_2x_3y^4 + x_1x_2x_3y^5 - 5, \\ z_8 &= x_0y + x_1x_2y + x_1x_2x_3y + x_1x_2x_3y^2 + x_1x_2x_3y^3 + x_1x_2x_3y^4 + x_1x_2x_3y^5 - 5, \\ z_9 &= x_0y + x_1x_2y + x_1x_2x_3y + x_1x_2x_3y^2 + x_1x_2x_3y^3 + x_1x_2x_3y^4 + x_1x_2x_3y^5 + x_1x_2x_3y^6 + x_1x_2x_3y^7 + x_1x_2x_3y^8 + x_1x_2x_3y^9 + x_1x_2x_3y^{10} - 5, \end{aligned}$$

$$\text{where } s = x_1x_2x_3 + x_1x_2x_3y + x_1x_2x_3y^2 + x_1x_2x_3y^3 + x_1x_2x_3y^4 + x_1x_2x_3y^5 + x_1x_2x_3y^6 + x_1x_2x_3y^7 + x_1x_2x_3y^8 + x_1x_2x_3y^9 + x_1x_2x_3y^{10},$$

Time =  $10D + 45M + 64A_1 + 122A_2$ . Return  $z = x^y$

**Squaring for  $p = 11$ .**

$$\begin{aligned} \text{For } i = 0, 1, \dots, 4, a_i = 2x_i; \text{ apply auxiliary routine 4 with } (a_i)^4_{i=0} = (c_i)^8_{i=0}, \text{ replaced by } (x_i)^9_{i=0}, \text{ respectively; apply auxiliary routine 4 with } (a_i)^4_{i=0} = (c_i)^9_{i=0} \text{ replaced by } (x_i)^9_{i=0}, \text{ respectively; apply auxiliary routine 3 with } (a_i)^4_{i=0} = (b_i)^0_{i=0}, \text{ respectively; apply auxiliary routine 5 to } (d_{1,i})_{i=0}, (d_{2,i})_{i=0}, (d_{3,i})_{i=0}, \text{ and with } (z_i)_{i=0} \text{ replaced by } (y_{1,i})_{i=0}. \\ \text{The following now holds modulo } n. \end{aligned}$$

$$\begin{aligned} j_0 &= x_0^2 + 2x_2x_9 + 2x_3x_6 + 2x_4x_7 + 2x_5x_6^2 - 5, \\ j_1 &= 2x_0x_1 + 2x_3x_9 + 2x_4x_8 + 2x_5x_7 + x_6^2 - 5, \\ j_2 &= 2x_0x_2 + x_3^2 + 2x_4x_9 + 2x_5x_8 + 2x_6x_7 - 5, \\ j_3 &= 2x_0x_3 + 2x_1x_2 + 2x_5x_9 + 2x_6x_8 + x_7^2 - 5, \\ j_4 &= 2x_0x_4 + 2x_1x_3 + x_8^2 + 2x_6x_9 + 2x_7x_8 - 5, \\ j_5 &= 2x_0x_5 + 2x_1x_4 + x_9^2 + 2x_2x_3 + 2x_7x_6 + x_8^2 - 5, \\ j_6 &= 2x_0x_6 + 2x_1x_5 + x_3^2 + 2x_2x_4 + x_8^2 + 2x_8x_9 - 5, \\ j_7 &= 2x_0x_7 + 2x_1x_6 + 2x_2x_5 + 2x_3x_4 + x_9^2 - 5, \\ j_8 &= 2x_0x_8 + 2x_1x_7 + 2x_2x_6 + 2x_3x_5 + x_1x_9 - 5, \\ j_9 &= 2x_1x_9 + 2x_2x_8 + 2x_3x_7 + x_4x_6 + x_5x_3 - 5, \end{aligned}$$

$$\text{where } s = 2x_1x_9 + 2x_2x_8 + 2x_3x_7 + x_4x_6 + x_5x_3 - 5.$$

Time =  $10D + 39M + 47A_1 + 80A_2$ . Return  $y = x^z$ .

**Multiplication for  $p = 16$ .**

$$\begin{aligned} m_1 &= x_0 + x_4; m_2 = x_1 + x_{15}; m_3 = x_2 + x_{15}; m_4 = x_3 + x_{15}; \text{ apply auxiliary routine 2 with } (a_i)^4_{i=0} = (b_i)^0_{i=0}, \text{ respectively; } m_1 = x_0 + x_4, \\ m_2 &= x_1 + x_{15}; m_3 = x_2 + x_{15}; m_4 = x_3 + x_{15}; \text{ apply auxiliary routine 2 with } (a_i)^3_{i=0} = (b_i)^3_{i=0}, \text{ respectively; } m_1 = x_0 + x_4, \\ (c_i)_6 &= y + y_5; m_3 = y + y_6; m_4 = y + y_7; \text{ apply auxiliary routine 2 with } (a_i)^3_{i=0} = (b_i)^3_{i=0}, \text{ respectively; } m_1 = y_4 - x_0, \\ m_3 &= y_6 - y_5; m_4 = y - y_5; \text{ apply auxiliary routine 2 with } (a_i)^3_{i=0} = (b_i)^3_{i=0}, \text{ respectively; } m_1 = d_{21} + d_{19}, \\ \text{replaced by } (m_i)^4_{i=1}, (x_i)_{i=0} = (d_i)_{i=10}, \text{ respectively; } d_{21} = d_4 + d_5; d_{22} = d_{21} + d_{18}; \\ z_0 &= (d_0 - d_{22})\text{mod } n; d_{21} = -d_5 + d_6; d_{22} = -d_1 - d_2; d_{21} = d_6 + d_9, \\ d_{22} &= d_{21} + d_{20}; z_2 = (d_2 - d_{22})\text{mod } n; z_3 = (d_3 - d_{22})\text{mod } n; d_{21} = d_4 + d_6; d_{22} = d_{21} + \\ d_4; z_4 &= (d_{22} - d_1)\text{mod } n; d_{21} = d_5 + d_1; d_{22} = d_{21} + d_{15}; z_5 = (d_{22} - d_1)\text{mod } n; d_{21} = \\ d_6 + d_{21}; d_{22} = d_{21} + d_{16}; z_6 = (d_{22} - d_{13})\text{mod } n; d_{21} = d_3 + d_{17}; z_7 = d_{21} \text{ mod } n. \end{aligned}$$

The following now holds modulo  $n$ :

$$\begin{aligned} z_0 &= x_0y^2 - x_1x_7 - x_2x_6 - x_3x_5 - x_4x_4 - x_5x_3 - x_6x_2 - x_7x_1, \\ z_1 &= -x_0x_1 - x_1x_9 - x_2x_7 - x_3x_6 - x_4x_5 - x_5x_4 - x_6x_3 - x_7x_2 - x_8x_1, \\ z_2 &= x_0x_2 + x_1x_1 + x_2x_9 + x_3x_7 - x_4x_6 - x_5x_5 - x_6x_4 - x_7x_3, \\ z_3 &= x_0x_3 + x_1x_2 + x_2x_8 + x_3x_7 - x_4x_6 - x_5x_6 - x_6x_5 - x_7x_4, \\ z_4 &= x_0x_4 + x_1x_3 + x_2x_9 + x_3x_8 + x_4x_7 - x_5x_7 - x_6x_6 - x_7x_5, \\ z_5 &= x_0x_5 + x_1x_4 + x_2x_9 + x_3x_8 + x_4x_7 + x_5x_7 - x_6x_6 - x_7x_5, \\ z_6 &= x_0x_6 + x_1x_5 + x_2x_9 + x_3x_8 + x_4x_7 + x_5x_8 + x_6x_7, \end{aligned}$$

$$\begin{aligned} z_7 &= x_0y^2 + x_1x_7 + x_2x_6 + x_3x_5 + x_4x_4 + x_5x_3 + x_6x_2 + x_7x_1, \\ \text{Time} &= 8D + 2M + 42A_1 + 62A_2. \text{ Return } z = xy. \end{aligned}$$

**Squaring for  $p^f = 16$ .**

$$\begin{aligned} \text{Time} &= 8D + 2M + 42A_1 + 62A_2. \text{ Return } z = xy, \\ m_1 &= x_0 + x_4; m_2 = x_1 + x_{15}; m_3 = x_2 + x_{15}; m_4 = x_3 + x_{15}; m_5 = x_5 - x_4; m_6 = x_1 - x_7, \\ m_7 &= x_2 - x_6; m_8 = x_3 - x_7; \text{ apply auxiliary routine 2 with } (a_i)^6_{i=0} = (b_i)^6_{i=0}, \text{ respectively; } m_1 = x_0 + x_4, \\ (c_i)_6 &= y + y_5; m_3 = y + y_6; m_4 = y + y_7; \text{ apply auxiliary routine 2 with } (a_i)^6_{i=0} = (b_i)^6_{i=0}, \text{ respectively; } m_1 = x_0 + x_4, \\ m_3 &= x_2 + x_{12}; m_4 = x_3 + x_{13}; m_5 = x_5 + x_{13}; m_6 = x_1 + x_7; \text{ apply auxiliary routine 2 with } (a_i)^6_{i=0} = (b_i)^6_{i=0}, \text{ respectively; } m_1 = (d_1 - d_{12})\text{mod } n; \\ (d_i)_{13} &= (x_i)_{i=1}, (x_i)_{i=0} = (d_i)_{i=7}, \text{ respectively; } d_1 = (d_2 - d_{13})\text{mod } n; y_2 = d_2 - d_{13} \text{ mod } n; y_3 = d_4 - d_7; y_4 = d_0 \text{ mod } n; \\ d'_1 &= d_5 + d_8; y_5 = d_1 \text{ mod } n; d'_2 = d_6 + d_9; y_6 = d_2 \text{ mod } n; y_7 = d_0 \text{ mod } n, \end{aligned}$$

The following now holds modulo  $n$ :

$$\text{Time} = 8D + 16M + 32A_1 + 34A_2. \text{ Return } y = x^2$$