MATHEMATICS OF COMPUTATION
VOLUME 48, NUMBER 177
JANUARY 1987, PAGES S1-S4

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 $(x_i)_{i=0}^{m-1}$, $(y_i)_{i=0}^{m-1}$, $(z_i)_{i=0}^{m-1}$ three elements of $\mathbf{Z}[\zeta_{p^k}]/n\mathbf{Z}[\zeta_{p^k}]$. 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.

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

The following now holds.

$c_0 = a_0 \cdot b_0$,
$c_1 = a_0 \cdot b_1 + a_1 \cdot b_0$,
$c_2 = a_0 \cdot b_2 + a_1 \cdot b_1 + a_2 \cdot b_0$,
$c_3 = a_1 \cdot b_2 + a_2 \cdot b_1$,
$c_4 = a_2 \cdot b_2$.

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.

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

The following now holds:

$c_0 = a_0 \cdot b_0$,
$c_1 = a_0 \cdot b_1 + a_1 \cdot b_0$,
$c_2 = a_0 \cdot b_2 + a_1 \cdot b_1 + a_2 \cdot b_0$,
$c_3 = a_0 \cdot b_3 + a_1 \cdot b_2 + a_2 \cdot b_1 + a_3 \cdot b_0$,
$c_4 = a_1 \cdot b_3 + a_2 \cdot b_2 + a_3 \cdot b_1$,
$c_5 = a_2 \cdot b_3 + a_3 \cdot b_2$,
$c_6 = a_3 \cdot b_3$.

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

©1987 American Mathematical Society
0025-5718/87 $1.00 + $.25 per page

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 $(a_i)_{i=0}^2$, $(b_i)_{i=0}^2$, $(c_i)_{i=0}^4$; $m_0 = a_0+a_3$; $m_1 = a_1+a_4$; $m_2 = b_0+b_3$; $m_3 = b_1+b_4$; $m_4 = a_3+a_4$; $m_5 = b_3+b_4$, apply auxiliary routine 1 with $(a_i)_{i=0}^2$, $(b_i)_{i=0}^2$, $(c_i)_{i=0}^4$ replaced by m_0, m_1, a_2, m_2, m_3, b_2 and $(d_i)_{i=0}^4$, respectively; $d_5 = a_3 \cdot b_3$; $c_8 = a_4 \cdot b_4$; $d_6 = m_4 \cdot m_5$, $d_7 = d_5+c_8$; $c_7 = d_6-d_7$; $d_6 = d_3+d_5$, $c_6 = d_6-c_3$; $d_6 = c_0+d_5$; $d_7 = c_3+d_0$, $c_3 = d_7-d_6$, $d_6 = c_1+c_7$, $d_7 = c_4+d_1$; $c_4 = d_7-d_6$, $d_6 = c_2+c_8$; $c_5 = d_2-d_6$

The following now holds:

$c_0 = a_0 \cdot b_0$,
$c_1 = a_0 \cdot b_1 + a_1 \cdot b_0$,
$c_2 = a_0 \cdot b_2 + a_1 \cdot b_1 + a_2 \cdot b_0$,
$c_3 = a_0 \cdot b_3 + a_1 \cdot b_2 + a_2 \cdot b_1 + a_3 \cdot b_0$,
$c_4 = a_0 \cdot b_4 + a_1 \cdot b_3 + a_2 \cdot b_2 + a_3 \cdot b_1 + a_4 b_0$,
$c_5 = a_1 \cdot b_4 + a_2 \cdot b_3 + a_3 \cdot b_2 + a_4 b_1$,
$c_6 = a_2 \cdot b_4 + a_3 \cdot b_3 + a_4 \cdot b_2$,
$c_7 = a_3 \cdot b_4 + a_4 \cdot b_3$,
$c_8 = a_4 b_4$.

Time $= 15M + 18A_1 + 26A_2$.

Auxiliary routine 4. 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

$m_1 = a_2+a_2$, $m_2 = a_0+a_1$; $m_3 = a_1+m_1$; $m_4 = a_3+a_4$, $m_5 = a_3+m_1$; $m_6 = a_0+a_0$, $m_6 = m_6+m_1$; $m_7 = a_1+a_3$; $m_8 = a_4+a_4$; $m_8 = m_8+m_1$; $m_9 = a_0+a_3$; $m_{10} = a_1+a_4$; $c_0 = a_0 \cdot a_0$; $d_1 = a_0 \cdot a_1$; $c_8 = a_4 \cdot a_4$; $d_2 = a_3 \cdot a_4$; $d_3 = a_1 \cdot m_1$; $d_4 = a_3 \cdot m_1$, $c_1 = d_1+d_1$; $c_7 = d_2+d_2$; $d_5 = m_2 \cdot m_3$, $d_6 = d_1+d_3$; $c_2 = d_5-d_6$; $d_5 = m_4 m_5$; $d_6 = d_2+d_4$; $c_6 = d_5-d_6$; $d_5 = m_6 \cdot m_7$; $d_6 = c_1+d_4$; $c_3 = d_5-d_6$, $d_5 = m_7 \cdot m_8$; $d_6 = c_7+d_3$; $c_5 = d_5-d_6$; $d_5 = m_9 \cdot m_{10}$; $d_6 = d_1+d_2$, $d_5 = d_5-d_6$; $d_6 = d_5+d_5$; $d_5 = a_2 \cdot a_2$, $c_4 = d_5+d_6$.

The following now holds:

$c_0 = a_0^2$,
$c_1 = 2a_0 \cdot a_1$,
$c_2 = 2a_0 \cdot a_2 + a_1^2$,
$c_3 = 2a_0 \cdot a_3 + 2a_1 \cdot a_2$,
$c_4 = 2a_0 \cdot a_4 + 2a_1 \cdot a_3 + a_2^2$,
$c_5 = 2a_1 \cdot a_4 + 2a_2 \cdot a_3$,
$c_6 = 2a_2 \cdot a_4 + a_3^2$,
$c_7 = 2a_3 \cdot a_4$,
$c_8 = a_4^2$.

Time $= 12M + 12A_1 + 14A_2$

Auxiliary routine 5. This routine operates on the variables $(d_{1,i})_{i=0}^8$, $(d_{2,i})_{i=0}^8$, $(d_{3,i})_{i=0}^8$, $(z_i)_{i=0}^9$. The $d_{1,i}$, $d_{2,i}$, and $d_{3,i}$ are input to the routine, and the z_i are output. The $d_{2,i}$ and $d_{3,i}$ will be unaffected, but the values of the $d_{1,i}$ will be changed

$d = d_{2,0}+d_{3,5}$; for $i = 0, 1, \ldots, 7$: $d_{1,i} = d_{1,i}+d_{2,i+1}$; for $i = 0, 1, 2$: $d_{1,i} = d_{1,i}+d_{3,i+6}$, for $i = 5, 6, 7, 8$: $d_{1,i} = d_{1,i}+d_{3,i-5}$; for $i = 0, 1, \ldots, 8$: $z_i = (d_{1,i}-d) \bmod n$; $z_9 = (d_{3,4}-d) \bmod n$.

This routine is used only to do the final reductions mod n in the multiplication and squaring routines for $p = 11$

Time $= 10D + 26A_2$.

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

Multiplication for $p = 3$.

$d_1 = x_0 y_0$; $d_2 = x_1 y_1$; $m_1 = x_0 - x_1$; $m_2 = y_1 - y_0$; $d_3 = m_1 \cdot m_2$, $d_3 = d_3 + d_1$, $z_1 = d_3 \bmod n$; $z_0 = (d_1 - d_2) \bmod n$.

The following now holds modulo n:

$z_0 = x_0 y_0 - x_1 y_1$,
$z_1 = x_0 y_1 + x_1 y_0 - x_1 y_1$.

Time $= 2D + 3M + 2A_1 + 2A_2$. Return $z = x \cdot y$.

Squaring for $p = 3$.

$m_1 = x_0 - x_1$; $m_2 = x_0 + x_1$; $d_1 = m_1 \cdot m_2$; $m_2 = m_1 + x_0$; $y_0 = d_1 \bmod n$; $d_1 = x_1 \cdot m_2$, $y_1 = d_1 \bmod n$.

The following now holds modulo n

$y_0 = x_0^2 - x_1^2$,
$y_1 = 2x_0 \cdot x_1 - x_1^2$.

Time $= 2D + 2M + 3A_1$. Return $y = x^2$

Multiplication for $p^k = 4$.

$m_1 = x_0 + x_1$; $m_2 = y_0 + y_1$; $m_3 = y_1 - y_0$; $d_1 = m_1 y_0$; $d_2 = m_2 \cdot x_1$; $d_3 = m_3 \cdot x_0$; $z_0 = (d_1 - d_2) \bmod n$; $d_2 = d_1 + d_3$; $z_1 = d_2 \bmod n$.

The following now holds modulo n:

$z_0 = x_0 y_0 - x_1 y_1$,
$z_1 = x_0 y_1 + x_1 y_0$.

Time $= 2D + 3M + 3A_1 + 2A_2$. Return $z = x\,y$.

Squaring for $p^k = 4$.

$m_1 = x_0 - x_1$; $m_2 = x_0 + x_1$; $d_1 = m_1 \cdot m_2$; $m_1 = x_0 + x_0$; $y_0 = d_1 \bmod n$, $d_1 = m_1 \cdot x_1$, $y_1 = d_1 \bmod n$.

The following now holds modulo n:

$y_0 = x_0^2 - x_1^2$,
$y_1 = 2x_0 \cdot x_1$

Time $= 2D + 2M + 3A_1$ Return $y = x^2$.

Multiplication for $p = 5$.

$m_1 = x_1 - x_3$; $m_2 = y_1 - y_3$; $m_3 = x_2 - x_3$; $m_4 = y_3 - y_2$; $m_5 = x_0 - x_1$, $m_6 = y_1 - y_0$; $m_7 = x_0 - x_2$; $m_8 = y_2 - y_0$; $d_0 = x_0 y_0$; $d_2 = m_1 \cdot m_2$; $d_1 = d_0 + d_2$; $d_2 = m_3 m_4$, $d_3 = m_5 \cdot m_6$; $d_4 = m_7 \cdot m_8$, $d_5 = x_1 y_1$; $d_6 = x_2 y_2$; $d_7 = x_3 y_3$, $d_8 = d_1 + d_2$, $z_0 = (d_8 - d_5) \bmod n$; $d_8 = d_1 + d_3$; $z_1 = (d_8 - d_6) \bmod n$; $d_8 = d_1 + d_4$, $z_2 = (d_8 - d_7) \bmod n$; $m_3 = m_1 - m_7$; $m_4 = m_2 + m_8$; $d_1 = m_3 \cdot m_4$; $d_8 = d_0 + d_1$, $d_7 = d_8 + d_2$, $d_8 = d_7 + d_3$; $d_7 = d_8 + d_4$; $z_3 = d_7 \bmod n$.

The following now holds modulo n:

$z_0 = x_0 y_0 - x_1 y_3 - x_2 y_2 - x_3 y_1 + x_2 y_3 + x_3 y_2$,
$z_1 = x_0 y_1 + x_1 y_0 - x_1 y_3 - x_2 y_2 - x_3 y_1 + x_3 y_3$,
$z_2 = x_0 y_2 + x_1 y_1 + x_2 y_0 - x_1 y_3 - x_2 y_2 - x_3 y_1$,
$z_3 = x_0 y_3 + x_1 y_2 + x_2 y_1 + x_3 y_0 - x_1 y_3 - x_2 y_2 - x_3 y_1$.

Time $= 4D + 9M + 10A_1 + 11A_2$. Return $z = x \cdot y$.

Squaring for $p = 5$.

$m_1 = x_0 - x_2$, $m_2 = x_0 + x_2$, $m_3 = x_2 - x_1$; $m_4 = x_0 - x_3$; $m_5 = x_1 - x_0$, $m_6 = x_2 - x_3$, $m_7 = x_1 - x_3$; $m_8 = x_3 + x_3$; $d_1 = m_1 \cdot m_2$, $d_2 = m_3 \cdot m_8$, $d_3 = d_1 + d_2$; $m_8 = m_5 + m_7$; $d_2 = m_4 \cdot m_8$, $d_4 = d_1 + d_2$; $m_3 = m_1 + x_0$, $d_1 = x_2 \cdot m_3$, $m_2 = m_7 - x_3$, $d_2 = m_2 x_1$; $y_0 = d_3 \bmod n$; $y_1 = d_4 \bmod n$; $d_3 = d_1 + d_2$, $y_2 = d_3 \bmod n$, $m_7 = m_6 + m_6$, $d_2 = m_7 m_5$; $d_3 = d_1 + d_2$; $y_3 = d_3 \bmod n$

The following now holds modulo n:

$y_0 = x_0^2 - 2x_1 \cdot x_3 - x_2^2 + 2x_2 \cdot x_3$,
$y_1 = 2x_0 \cdot x_1 - 2x_1 \cdot x_3 - x_2^2 + x_3^2$,
$y_2 = 2x_0 \cdot x_2 + x_1^2 - 2x_1 \cdot x_3 - x_2^2$,

$y_3 = 2x_0 \cdot x_3 + 2x_1 \cdot x_2 - 2x_1 \cdot x_3 - x_2^2$

Time $= 4D + 6M + 12A_1 + 4A_2$. Return $y = x^2$

Multiplication for $p = 7$.

Apply auxiliary routine 1 with $(a_i)_{i=0}^2$, $(b_i)_{i=0}^2$, $(c_i)_{i=0}^4$ replaced by $(x_i)_{i=0}^2$, $(y_i)_{i=0}^2$, $(d_i)_{i=0}^4$, respectively; apply auxiliary routine 1 with $(a_i)_{i=0}^2$, $(b_i)_{i=0}^2$, $(c_i)_{i=0}^4$ replaced by $(x_i)_{i=3}^5$, $(y_i)_{i=3}^5$, $(d_i)_{i=6}^{10}$, respectively, $m_1 = x_0 - x_3$; $m_2 = x_1 - x_4$; $m_3 = x_2 - x_5$; $m_4 = y_3 - y_0$; $m_5 = y_4 - y_1$; $m_6 = y_5 - y_2$, apply auxiliary routine 1 with $(a_i)_{i=0}^2$, $(b_i)_{i=0}^2$, $(c_i)_{i=0}^4$ replaced by $(m_i)_{i=1}^3$, $(m_i)_{i=4}^6$, $(d_i)_{i=11}^{15}$, respectively; $d_{18} = d_6 + d_{14}$; $d_{16} = d_{18} + d_3$; $d_{18} = d_7 + d_{15}$; $d_{17} = d_{18} + d_4$; $d_{18} = d_3 + d_{11}$; $d_3 = d_{18} + d_0$; $d_{18} = d_4 + d_{12}$; $d_4 = d_{18} + d_1$, $d_5 = d_2 + d_{13}$; $d_{13} = d_3 + d_6$; $d_{14} = d_4 + d_7$, $d_{15} = d_5 + d_8$; $d_6 = d_{16} + d_9$, $d_7 = d_{17} + d_{10}$; $d_{18} = d_0 + d_7$; $z_0 = (d_{18} - d_6) \bmod n$, $d_{18} = d_1 + d_8$; $z_1 = (d_{18} - d_6) \bmod n$; $d_{18} = d_2 + d_9$; $z_2 = (d_{18} - d_6) \bmod n$; $d_{18} = d_{13} + d_{10}$; $z_3 = (d_{18} - d_6) \bmod n$; $z_4 = (d_{14} - d_6) \bmod n$; $z_5 = (d_{15} - d_6) \bmod n$.

The following now holds modulo n

$z_0 = x_0 \cdot y_0 - x_1 \cdot y_5 - x_2 \cdot y_4 - x_3 \cdot y_3 - x_4 \cdot y_2 - x_5 y_1 + x_2 \cdot y_5 + x_3 \cdot y_4 + x_4 y_3 + x_5 \cdot y_2$,
$z_1 = x_0 \cdot y_1 + x_1 \cdot y_0 - x_1 \cdot y_5 - x_2 \cdot y_4 - x_3 \cdot y_3 - x_4 \cdot y_2 - x_5 \cdot y_1 + x_3 \cdot y_5 + x_4 \cdot y_4 + x_5 \cdot y_3$,
$z_2 = x_0 \cdot y_2 + x_1 \cdot y_1 + x_2 \cdot y_0 - x_1 \cdot y_5 - x_2 \cdot y_4 - x_3 \cdot y_3 - x_4 \cdot y_2 - x_5 \cdot y_1 + x_4 \cdot y_5 + x_5 \cdot y_4$,
$z_3 = x_0 \cdot y_3 + x_1 \cdot y_2 + x_2 \cdot y_1 + x_3 \cdot y_0 - x_1 \cdot y_5 - x_2 \cdot y_4 - x_3 \cdot y_3 - x_4 \cdot y_2 - x_5 \cdot y_1 + x_5 \cdot y_5$,
$z_4 = x_0 \cdot y_4 + x_1 \cdot y_3 + x_2 \cdot y_2 + x_3 \cdot y_1 + x_4 \cdot y_0 - x_1 \cdot y_5 - x_2 \cdot y_4 - x_3 \cdot y_3 - x_4 \cdot y_2 - x_5 \cdot y_1$,
$z_5 = x_0 \cdot y_5 + x_1 \cdot y_4 + x_2 \cdot y_3 + x_3 \cdot y_2 + x_4 \cdot y_1 + x_5 \cdot y_0 - x_1 y_5 - x_2 y_4 - x_3 \cdot y_3 - x_4 \cdot y_2 - x_5 \cdot y_1$.

Time $= 6D + 18M + 24A_1 + 45A_2$. Return $z = x \cdot y$.

Squaring for $p = 7$.

$m_1 = x_0 - x_1$; $m_2 = x_1 - x_2$; $m_3 = x_2 - x_3$; $m_4 = x_3 - x_4$; $m_5 = x_5 - x_4$; $m_6 = m_1 + m_2$; $m_7 = m_2 + m_3$; $m_8 = m_3 + m_4$; $m_9 = x_3 - x_5$; $m_{10} = m_3 + m_6$; $m_{11} = m_4 + m_7$; $m_{13} = m_6 + m_8$; $m_{14} = m_7 + m_9$; $m_{16} = x_0 + x_1$, $m_{17} = x_0 + m_{10}$; $d_1 = x_3 \cdot m_{17}$; $m_{17} = m_{14} - x_4$; $m_{18} = m_{14} + x_4$; $d_2 = m_{17} \cdot m_{18}$, $m_{17} = m_8 - m_2$; $d_3 = m_{11} \cdot m_{17}$; $m_{17} = m_{14} + m_9$; $d_4 = m_{17} \cdot m_7$; $m_{17} = x_1 + x_1$; $d_5 = m_{17} \cdot m_6$; $d_6 = m_1 \cdot m_{16}$; $m_{17} = m_3 + m_3$, $m_2 = x_0 + m_{13}$; $d_7 = m_{17} \cdot m_5$; $d_8 = d_1 + d_2$; $d_1 = d_8 + d_3$; $y_3 = d_1 \bmod n$; $d_8 = d_3 + d_4$; $d_1 = d_8 + d_5$; $y_1 = d_1 \bmod n$; $d_8 = d_4 + d_6$; $d_1 = d_8 + d_7$, $y_0 = d_1 \bmod n$; $m_{17} = m_7 + m_{14}$; $d_1 = m_9 \cdot m_{17}$; $m_{17} = m_8 - x_5$; $m_{18} = x_2 + m_5$; $d_2 = m_{17} \cdot m_{18}$; $d_3 = m_2 \cdot x_4$; $m_{17} = m_3 + m_8$, $d_4 = m_{17} \cdot m_4$; $m_{17} = m_1 + m_1$; $d_5 = m_{17} \cdot m_5$, $m_{17} = m_{14} - m_5$; $d_6 = m_{17} \cdot m_{11}$, $m_{17} = x_2 + x_2$; $d_7 = m_{17} \cdot m_{10}$; $d_8 = d_1 + d_2$; $d_1 = d_8 + d_3$; $y_4 = d_1 \bmod n$; $d_8 = d_3 + d_4$; $d_1 = d_8 + d_5$; $y_5 = d_1 \bmod n$; $d_8 = d_4 + d_6$; $d_1 = d_8 + d_7$, $y_2 = d_1 \bmod n$.

The following now holds modulo n:

$y_0 = x_0^2 - 2x_1 \cdot x_5 - 2x_2 \cdot x_4 - x_3^2 + 2x_2 \cdot x_5 + 2x_3 \cdot x_4$,
$y_1 = 2x_0 \cdot x_1 - 2x_1 \cdot x_5 - 2x_2 \cdot x_4 - x_3^2 + 2x_3 \cdot x_5 + x_4^2$,
$y_2 = 2x_0 \cdot x_2 + x_1^2 - 2x_1 \cdot x_5 - 2x_2 \cdot x_4 - x_3^2 + 2x_4 \cdot x_5$,
$y_3 = 2x_0 \cdot x_3 + 2x_1 \cdot x_2 - 2x_1 \cdot x_5 - 2x_2 \cdot x_4 - x_3^2 + x_5^2$,
$y_4 = 2x_0 \cdot x_4 + 2x_1 \cdot x_3 + x_2^2 - 2x_1 \cdot x_5 - 2x_2 \cdot x_4 - x_3^2$,
$y_5 = 2x_0 \cdot x_5 + 2x_1 \cdot x_4 + 2x_2 \cdot x_3 - 2x_1 \cdot x_5 - 2x_2 \cdot x_4 - x_3^2$.

Time $= 6D + 14M + 29A_1 + 12A_2$. Return $y = x^2$.

Multiplication for $p^k = 8$.

$m_1 = x_1 + x_3$; $m_2 = y_1 + y_3$; $m_3 = x_2 + x_3$; $m_4 = y_2 + y_3$; $m_5 = x_0 + x_1$; $m_6 = y_0 + y_1$; $m_7 = x_0 + x_2$; $m_8 = y_0 + y_2$; $d_0 = x_0 y_0$; $d_1 = x_1 \cdot y_1$; $d_2 = x_2 y_2$; $d_3 = x_3 \cdot y_3$; $d_6 = m_5 \cdot m_6$; $d_7 = m_7 \cdot m_8$; $d_8 = m_1 \cdot m_2$; $d_9 = m_3 \cdot m_4$; $m_3 = m_1 + m_7$; $m_4 = m_2 + m_8$; $d_4 = m_3 \cdot m_4$; $d_{10} = d_0 + d_1$; $d_{11} = d_2 + d_3$; $d_{12} = d_{10} + d_3$; $d_5 = d_8 + d_2$; $z_0 = (d_{12} - d_5) \bmod n$, $d_{12} = d_6 + d_{11}$; $d_5 = d_{10} + d_9$, $z_1 = (d_{12} - d_5) \bmod n$; $d_{12} = d_1 + d_7$; $d_5 = d_0 + d_{11}$; $z_2 = (d_{12} - d_5) \bmod n$; $d_{12} = d_7 + d_6$; $d_5 = d_{12} + d_8$; $d_{12} = d_5 + d_9$; $d_3 = d_{10} + d_{11}$; $d_5 = d_3 + d_4$; $z_3 = (d_5 - d_{12}) \bmod n$.

The following now holds modulo n:

$z_0 = x_0 \cdot y_0 - x_1 \cdot y_3 - x_2 y_2 - x_3 \cdot y_1$,
$z_1 = x_0 y_1 + x_1 \cdot y_0 - x_2 \cdot y_3 - x_3 \cdot y_2$,
$z_2 = x_0 \cdot y_2 + x_1 \cdot y_1 + x_2 y_0 - x_3 \cdot y_3$,
$z_3 = x_0 \cdot y_3 + x_3 \cdot y_0 + x_1 y_2 + x_2 \cdot y_1$

Time $= 4D + 9M + 10A_1 + 17A_2$. Return $z = x \cdot y$.

Squaring for $p^k = 8$.

$m_1 = x_0 - x_2$, $m_2 = x_0 + x_2$; $m_3 = x_1 - x_3$; $m_4 = x_1 + x_3$; $m_5 = x_0 + x_0$; $m_6 = x_1 + x_1$, $m_7 = m_1 + m_3$; $m_8 = m_2 + m_4$, $d_1 = m_1 \cdot m_2$, $d_2 = m_3 m_4$, $d_3 = m_6 x_3$, $d_4 = m_5 \cdot x_2$, $m_2 = x_2 + x_3$, $y_0 = (d_1 - d_3) \bmod n$; $d_6 = d_2 + d_4$, $y_2 = d_6 \bmod n$; $d_5 = m_7 \cdot m_8$, $d_6 = d_1 + d_2$, $y_1 = (d_5 - d_6) \bmod n$; $m_1 = m_5 + m_6$, $d_1 = m_1 \cdot m_2$; $d_6 = d_3 + d_4$; $y_3 = (d_1 - d_6) \bmod n$.

The following now holds modulo n:

$y_0 = x_0^2 - 2x_1 \cdot x_3 - x_2^2$,
$y_1 = 2x_0 \cdot x_1 - 2x_2 x_3$,
$y_2 = 2x_0 x_2 + x_1^2 - x_3^2$,
$y_3 = 2x_0 \cdot x_3 + 2x_1 \cdot x_2$.

Time $= 4D + 6M + 10A_1 + 6A_2$. Return $y = x^2$

Multiplication for $p^k = 9$.

Apply auxiliary routine 1 with $(a_i)_{i=0}^2$, $(b_i)_{i=0}^2$, $(c_i)_{i=0}^4$ replaced by $(x_i)_{i=0}^2$, $(y_i)_{i=0}^2$, $(d_i)_{i=0}^4$, respectively; apply auxiliary routine 1 with $(a_i)_{i=0}^2$, $(b_i)_{i=0}^2$, $(c_i)_{i=0}^4$ replaced by $(x_i)_{i=3}^5$, $(y_i)_{i=3}^5$, $(d_i)_{i=6}^{10}$, respectively; $m_1 = x_0 - x_3$; $m_2 = x_1 - x_4$; $m_3 = x_2 - x_5$, $m_4 = y_3 - y_0$, $m_5 = y_4 - y_1$, $m_6 = y_5 - y_2$; apply auxiliary routine 1 with $(a_i)_{i=0}^2$, $(b_i)_{i=0}^2$, $(c_i)_{i=0}^4$ replaced by $(m_i)_{i=1}^3$, $(m_i)_{i=4}^6$, $(d_i)_{i=11}^{15}$, respectively, $d_{18} = d_6 + d_{14}$, $d_{16} = d_{18} + d_3$; $d_{18} = d_7 + d_{15}$, $d_{17} = d_{18} + d_4$; $d_{18} = d_3 + d_{11}$, $d_3 = d_{18} + d_0$; $d_{18} = d_4 + d_{12}$; $d_4 = d_{18} + d_1$, $d_5 = d_2 + d_{13}$; $z_0 = (d_0 - d_{16}) \bmod n$; $z_1 = (d_1 - d_{17}) \bmod n$; $z_2 = (d_2 - d_8) \bmod n$; $z_5 = d_5 \bmod n$; $d_{18} = d_3 + d_6$; $d_{19} = d_{16} + d_9$, $z_3 = (d_{18} - d_{19}) \bmod n$, $d_{18} = d_4 + d_7$; $d_{19} = d_{10} + d_{17}$; $z_4 = (d_{18} - d_{19}) \bmod n$.

The following now holds modulo n:

$z_0 = x_0 \cdot y_0 - x_1 \cdot y_5 - x_2 \cdot y_4 - x_3 \cdot y_3 - x_4 \cdot y_2 - x_5 \cdot y_1 + x_4 \cdot y_5 + x_5 \cdot y_4$,
$z_1 = x_0 \cdot y_1 + x_1 \cdot y_0 - x_2 \cdot y_5 - x_3 y_4 - x_4 \cdot y_3 - x_5 y_2 + x_5 y_5$,
$z_2 = x_0 \cdot y_2 + x_1 \cdot y_1 + x_2 \cdot y_0 - x_3 \cdot y_5 - x_4 \cdot y_4 - x_5 \cdot y_3$,
$z_3 = x_0 y_3 + x_1 \cdot y_2 + x_2 \cdot y_1 + x_3 y_0 - x_1 \cdot y_5 - x_2 \cdot y_4 - x_3 \cdot y_3 - x_4 \cdot y_2 - x_5 \cdot y_1$,
$z_4 = x_0 \cdot y_4 + x_1 \cdot y_3 + x_2 \cdot y_2 + x_3 \cdot y_1 + x_4 \cdot y_0 - x_2 \cdot y_5 - x_3 \cdot y_4 - x_4 \cdot y_3 - x_5 \cdot y_2$,
$z_5 = x_0 \cdot y_5 + x_1 \cdot y_4 + x_2 \cdot y_3 + x_3 \cdot y_2 + x_4 \cdot y_1 + x_5 \cdot y_0 - x_3 \cdot y_5 - x_4 \cdot y_4 - x_5 y_3$.

Time $= 6D + 18M + 24A_1 + 39A_2$. Return $z = x \cdot y$.

Squaring for $p^k = 9$.

$m_0 = x_0 - x_3$; $m_1 = x_1 - x_4$; $m_2 = x_2 - x_5$; $m_3 = x_0 + x_3$, $m_4 = x_1 + x_4$; $m_5 = x_2 + x_5$, apply auxiliary routine 1 with $(a_i)_{i=0}^2$, $(b_i)_{i=0}^2$, $(c_i)_{i=0}^4$ replaced by $(m_i)_{i=0}^2$, $(m_i)_{i=3}^5$, $(d_i)_{i=0}^4$, respectively; $m_3 = x_0 + m_0$; $m_4 = x_1 + m_1$; $m_5 = x_2 + m_2$; apply auxiliary routine 1 with $(a_i)_{i=0}^2$, $(b_i)_{i=0}^2$, $(c_i)_{i=0}^4$ replaced by $(m_i)_{i=3}^5$, $(x_i)_{i=3}^5$, $(d_i)_{i=5}^9$, respectively; $y_0 = (d_0 - d_8) \bmod n$; $y_1 = (d_1 - d_9) \bmod n$; $y_2 = d_2 \bmod n$; $d_{10} = d_3 + d_5$; $y_3 = (d_{10} - d_8) \bmod n$; $d_{10} = d_4 + d_6$; $y_4 = (d_{10} - d_9) \bmod n$; $y_5 = d_7 \bmod n$.

The following now holds modulo n:

$y_0 = x_0^2 - 2x_1 \cdot x_5 - 2x_2 \cdot x_4 - x_3^2 + 2x_4 \cdot x_5$,
$y_1 = 2x_0 \cdot x_1 - 2x_2 \cdot x_5 - 2x_3 x_4 + x_5^2$,
$y_2 = 2x_0 \cdot x_2 + x_1^2 - 2x_3 \cdot x_5 - x_4^2$,
$y_3 = 2x_0 \cdot x_3 + 2x_1 \cdot x_2 - 2x_1 \cdot x_5 - 2x_2 \cdot x_4 - x_3^2$,
$y_4 = 2x_0 \cdot x_4 + 2x_1 \cdot x_3 + x_2^2 - 2x_2 \cdot x_5 - 2x_3 \cdot x_4$,
$y_5 = 2x_0 \cdot x_5 + 2x_1 \cdot x_4 + 2x_2 \cdot x_3 - 2x_3 \cdot x_5 - x_4^2$.

Time $= 6D + 12M + 21A_1 + 20A_2$. Return $y = x^2$

Multiplication for $p = 11$.

For $i = 0, 1, \ldots, 4$: $a_i = x_i + x_{i+5}$ and $b_i = y_i + y_{i+5}$; apply auxiliary routine 3 with $(a_i)_{i=0}^4$, $(b_i)_{i=0}^4$, $(c_i)_{i=0}^8$ replaced by $(x_i)_{i=0}^4$, $(y_i)_{i=0}^4$, $(d_{1,i})_{i=0}^8$, respectively; apply auxiliary routine 3 with $(a_i)_{i=0}^4$, $(b_i)_{i=0}^4$, $(c_i)_{i=0}^8$ replaced by $(x_i)_{i=5}^9$, $(y_i)_{i=5}^9$, $(d_{2,i})_{i=0}^8$, respectively; apply auxiliary routine 3 with $(a_i)_{i=0}^4$, $(b_i)_{i=0}^4$, $(c_i)_{i=0}^8$ replaced by $(a_i)_{i=0}^4$, $(b_i)_{i=0}^4$, $(d_{3,i})_{i=0}^8$, respectively; for $i = 0, 1, \ldots, 8$: $d_{3,i} = d_{3,i} - d_{1,i} - d_{2,i}$; apply auxiliary routine 5 to $(d_{1,i})_{i=0}^8$,

$(d_{2,i})_{i=0}^{8}$, $(d_{3,i})_{i=0}^{8}$, $(z_i)_{i=0}^{9}$.

The following now holds modulo n:

$z_0 = x_0 y_0 + x_2 y_9 + x_3 y_8 + x_4 y_7 + x_5 y_6 + x_6 y_5 + x_7 y_4 + x_8 y_3 + x_9 y_2 - s,$
$z_1 = x_0 y_1 + x_1 y_0 + x_3 y_9 + x_4 y_8 + x_5 y_7 + x_6 y_6 + x_7 y_5 + x_8 y_4 + x_9 y_3 - s,$
$z_2 = x_0 y_2 + x_1 y_1 + x_2 y_0 + x_4 y_9 + x_5 y_8 + x_6 y_7 + x_7 y_6 + x_8 y_5 + x_9 y_4 - s,$
$z_3 = x_0 y_3 + x_1 y_2 + x_2 y_1 + x_3 y_0 + x_5 y_9 + x_6 y_8 + x_7 y_7 + x_8 y_6 + x_9 y_5 - s,$
$z_4 = x_0 y_4 + x_1 y_3 + x_2 y_2 + x_3 y_1 + x_4 y_0 + x_6 y_9 + x_7 y_8 + x_8 y_7 + x_9 y_6 - s,$
$z_5 = x_0 y_5 + x_1 y_4 + x_2 y_3 + x_3 y_2 + x_4 y_1 + x_5 y_0 + x_7 y_9 + x_8 y_8 + x_9 y_7 - s,$
$z_6 = x_0 y_6 + x_1 y_5 + x_2 y_4 + x_3 y_3 + x_4 y_2 + x_5 y_1 + x_6 y_0 + x_8 y_9 + x_9 y_8 - s,$
$z_7 = x_0 y_7 + x_1 y_6 + x_2 y_5 + x_3 y_4 + x_4 y_3 + x_5 y_2 + x_6 y_1 + x_7 y_0 + x_9 y_9 - s,$
$z_8 = x_0 y_8 + x_1 y_7 + x_2 y_6 + x_3 y_5 + x_4 y_4 + x_5 y_3 + x_6 y_2 + x_7 y_1 + x_8 y_0 - s,$
$z_9 = x_0 y_9 + x_1 y_8 + x_2 y_7 + x_3 y_6 + x_4 y_5 + x_5 y_4 + x_6 y_3 + x_7 y_2 + x_8 y_1 + x_9 y_0 - s,$

where $s = x_1 y_9 + x_2 y_8 + x_3 y_7 + x_4 y_6 + x_5 y_5 + x_6 y_4 + x_7 y_3 + x_8 y_2 + x_9 y_1$.

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

Squaring for $p = 11$.

For $\iota = 0, 1, \ldots, 4$: $a_i = 2x_i$; apply auxiliary routine 4 with $(a_i)_{i=0}^{4}$, $(c_i)_{i=0}^{8}$ replaced by $(x_i)_{i=0}^{4}$, $(d_{1,i})_{i=0}^{8}$, respectively; apply auxiliary routine 4 with $(a_i)_{i=0}^{4}$, $(c_i)_{i=0}^{8}$ replaced by $(x_i)_{i=5}^{9}$, $(d_{2,i})_{i=0}^{8}$, respectively; apply auxiliary routine 3 with $(a_i)_{i=0}^{4}$, $(b_i)_{i=0}^{4}$, $(c_i)_{i=0}^{8}$ replaced by $(x_i)_{i=5}^{9}$, $(a_i)_{i=0}^{4}$, $(d_{3,i})_{i=0}^{8}$, respectively; apply auxiliary routine 5 to $(d_{1,i})_{i=0}^{8}$, $(d_{2,i})_{i=0}^{8}$, $(d_{3,i})_{i=0}^{8}$, and with $(z_i)_{i=0}^{9}$ replaced by $(y_i)_{i=0}^{9}$.

The following now holds modulo n:

$y_0 = x_0^2 + 2x_2 x_9 + 2x_3 x_8 + 2x_4 x_7 + 2x_5 x_6 - s,$
$y_1 = 2x_0 x_1 + 2x_3 x_9 + 2x_4 x_8 + 2x_5 x_7 + x_6^2 - s,$
$y_2 = 2x_0 x_2 + x_1^2 + 2x_4 x_9 + 2x_5 x_8 + 2x_6 x_7 - s,$
$y_3 = 2x_0 x_3 + 2x_1 x_2 + 2x_5 x_9 + 2x_6 x_8 + x_7^2 - s,$
$y_4 = 2x_0 x_4 + 2x_1 x_3 + x_2^2 + 2x_6 x_9 + 2x_7 x_8 - s,$
$y_5 = 2x_0 x_5 + 2x_1 x_4 + 2x_2 x_3 + 2x_7 x_9 + x_8^2 - s,$
$y_6 = 2x_0 x_6 + 2x_1 x_5 + 2x_2 x_4 + x_3^2 + 2x_8 x_9 - s,$
$y_7 = 2x_0 x_7 + 2x_1 x_6 + 2x_2 x_5 + 2x_3 x_4 + x_9^2 - s,$
$y_8 = 2x_0 x_8 + 2x_1 x_7 + 2x_2 x_6 + 2x_3 x_5 + x_4^2 - s,$
$y_9 = 2x_0 x_9 + 2x_1 x_8 + 2x_2 x_7 + 2x_3 x_6 + 2x_4 x_5 - s,$

where $s = 2x_1 x_9 + 2x_2 x_8 + 2x_3 x_7 + 2x_4 x_6 + x_5^2$.

Time $= 10D + 39M + 47A_1 + 80A_2$. Return $y = x^2$.

Multiplication for $p^k = 16$.

$m_1 = x_0 + x_4$; $m_2 = x_1 + x_5$; $m_3 = x_2 + x_6$; $m_4 = x_3 + x_7$; apply auxiliary routine 2 with $(a_i)_{i=0}^{3}$, $(b_i)_{i=0}^{3}$, $(c_i)_{i=0}^{6}$ replaced by $(m_i)_{i=1}^{4}$, $(y_i)_{i=0}^{3}$, $(d_i)_{i=0}^{6}$, respectively; $m_1 = y_0 + y_4$; $m_2 = y_1 + y_5$; $m_3 = y_2 + y_6$; $m_4 = y_3 + y_7$; apply auxiliary routine 2 with $(a_i)_{i=0}^{3}$, $(b_i)_{i=0}^{3}$, $(c_i)_{i=0}^{6}$ replaced by $(m_i)_{i=1}^{4}$, $(x_i)_{i=4}^{7}$, $(d_i)_{i=7}^{13}$, respectively; $m_1 = y_4 - y_0$; $m_2 = y_5 - y_1$; $m_3 = y_6 - y_2$; $m_4 = y_7 - y_3$; apply auxiliary routine 2 with $(a_i)_{i=0}^{3}$, $(b_i)_{i=0}^{3}$, $(c_i)_{i=0}^{6}$ replaced by $(m_i)_{i=1}^{4}$, $(x_i)_{i=0}^{3}$, $(d_i)_{i=14}^{20}$, respectively; $d_{21} = d_4 + d_7$; $d_{22} = d_{21} + d_{18}$; $z_0 = (d_0 - d_{22}) \bmod n$; $d_{21} = d_5 + d_8$; $d_{22} = d_{21} + d_{19}$; $z_1 = (d_1 - d_{22}) \bmod n$; $d_{21} = d_6 + d_9$, $d_{22} = d_{21} + d_{20}$; $z_2 = (d_2 - d_{22}) \bmod n$; $z_3 = (d_3 - d_{10}) \bmod n$; $d_{21} = d_4 + d_0$; $d_{22} = d_{21} + d_{14}$; $z_4 = (d_{22} - d_{11}) \bmod n$; $d_{21} = d_5 + d_1$; $d_{22} = d_{21} + d_{15}$; $z_5 = (d_{22} - d_{12}) \bmod n$; $d_{21} = d_6 + d_2$; $d_{22} = d_{21} + d_{16}$; $z_6 = (d_{22} - d_{13}) \bmod n$; $d_{21} = d_3 + d_{17}$; $z_7 = d_{21} \bmod n$.

The following now holds modulo n:

$z_0 = x_0 y_0 - x_1 y_7 - x_2 y_6 - x_3 y_5 - x_4 y_4 - x_5 y_3 - x_6 y_2 - x_7 y_1,$
$z_1 = x_0 y_1 + x_1 y_0 - x_2 y_7 - x_3 y_6 - x_4 y_5 - x_5 y_4 - x_6 y_3 - x_7 y_2,$
$z_2 = x_0 y_2 + x_1 y_1 + x_2 y_0 - x_3 y_7 - x_4 y_6 - x_5 y_5 - x_6 y_4 - x_7 y_3,$
$z_3 = x_0 y_3 + x_1 y_2 + x_2 y_1 + x_3 y_0 - x_4 y_7 - x_5 y_6 - x_6 y_5 - x_7 y_4,$
$z_4 = x_0 y_4 + x_1 y_3 + x_2 y_2 + x_3 y_1 + x_4 y_0 - x_5 y_7 - x_6 y_6 - x_7 y_5,$
$z_5 = x_0 y_5 + x_1 y_4 + x_2 y_3 + x_3 y_2 + x_4 y_1 + x_5 y_0 - x_6 y_7 - x_7 y_6,$
$z_6 = x_0 y_6 + x_1 y_5 + x_2 y_4 + x_3 y_3 + x_4 y_2 + x_5 y_1 + x_6 y_0 - x_7 y_7,$
$z_7 = x_0 y_7 + x_1 y_6 + x_2 y_5 + x_3 y_4 + x_4 y_3 + x_5 y_2 + x_6 y_1 + x_7 y_0.$

Time $= 8D + 27M + 42A_1 + 62A_2$. Return $z = x \cdot y$.

Squaring for $p^k = 16$.

$m_1 = x_0 + x_4$; $m_2 = x_1 + x_5$; $m_3 = x_2 + x_6$; $m_4 = x_3 + x_7$; $m_5 = x_0 - x_4$; $m_6 = x_1 - x_5$, $m_7 = x_2 - x_6$; $m_8 = x_3 - x_7$; apply auxiliary routine 2 with $(a_i)_{i=0}^{3}$, $(b_i)_{i=0}^{3}$, $(c_i)_{i=0}^{6}$ replaced by $(m_i)_{i=1}^{4}$, $(m_i)_{i=5}^{8}$, $(d_i)_{i=0}^{6}$, respectively; $m_1 = x_0 + x_0$; $m_2 = x_1 + x_1$; $m_3 = x_2 + x_2$; $m_4 = x_3 + x_3$; apply auxiliary routine 2 with $(a_i)_{i=0}^{3}$, $(b_i)_{i=0}^{3}$, $(c_i)_{i=0}^{6}$ replaced by $(m_i)_{i=1}^{4}$, $(x_i)_{i=4}^{7}$, $(d_i)_{i=7}^{13}$, respectively, $y_0 = (d_0 - d_{11}) \bmod n$; $y_1 = (d_1 - d_{12}) \bmod n$; $y_2 = (d_2 - d_{13}) \bmod n$; $y_3 = d_3 \bmod n$; $d_0 = d_4 + d_7$; $y_4 = d_0 \bmod n$; $d_1 = d_5 + d_8$; $y_5 = d_1 \bmod n$; $d_2 = d_6 + d_9$; $y_6 = d_2 \bmod n$; $y_7 = d_{10} \bmod n$

The following now holds modulo n:

$y_0 = x_0^2 - 2x_1 x_7 - 2x_2 x_6 - 2x_3 x_5 - x_4^2,$
$y_1 = 2x_0 x_1 - 2x_2 x_7 - 2x_3 x_6 - 2x_4 x_5,$
$y_2 = 2x_0 x_2 + x_1^2 - 2x_3 x_7 - 2x_4 x_6 - x_5^2,$
$y_3 = 2x_0 x_3 + 2x_1 x_2 - 2x_4 x_7 - 2x_5 x_6,$
$y_4 = 2x_0 x_4 + 2x_1 x_3 + x_2^2 - 2x_5 x_7 - x_6^2,$
$y_5 = 2x_0 x_5 + 2x_1 x_4 + 2x_2 x_3 - 2x_6 x_7,$
$y_6 = 2x_0 x_6 + 2x_1 x_5 + 2x_2 x_4 + x_3^2 - x_7^2,$
$y_7 = 2x_0 x_7 + 2x_1 x_6 + 2x_2 x_5 + 2x_3 x_4$

Time $= 8D + 18M + 32A_1 + 34A_2$. Return $y = x^2$