$q = a \ \mathrm{div} \ d$

$r = a \ \mathrm{mod} \ d$

$d \qquad a$

$7 \,|\, 11 \,|\, 1 \leftarrow q$

$\underline{\ \ 7\ \ }$

$4 \leftarrow r$

$$a \equiv r \pmod{d}$$

$$\left.\begin{aligned} 7 &\equiv 2 \pmod{5} \\ 11 &\equiv 1 \pmod{5} \end{aligned}\right\}$$

$$\left\{\begin{aligned} 7+11 &\equiv 2+1 \pmod{5} \\ 18 &\equiv 3 \pmod{5} \end{aligned}\right.$$

$$\left\{\begin{aligned} 7 \cdot 11 &= 2 \cdot 1 \pmod{5} \\ 77 &= 2 \pmod{5} \end{aligned}\right.$$

$a_1 = r_1 \pmod{d}$

$d_2 = r_2 \pmod{d}$

$a_1 + a_2 = (r_1 + r_2) \pmod{d}$

$a_1 \cdot a_2 = r_1 \cdot r_2 \pmod{d}$

ALGORITHM 5 Modular Exponentiation.

procedure *modular exponentiation*(b: integer, $n = (a_{k-1}a_{k-2}\dots a_1a_0)_2$, m: positive integers)
$x := 1$
$power := b$ **mod** m
for $i := 0$ **to** $k - 1$
  if $a_i = 1$ **then** $x := (x \cdot power)$ **mod** m
  $power := (power \cdot power)$ **mod** m
return x {x equals b^n **mod** m}

$b^n \bmod m = r\ ?$

$3^{644} \bmod 645 = r? = 36$

$n = (644)_{10} = (1010000100)_2$ — a_{k-1} … a_0

$x = 1$ $power = b \bmod m = 3 \bmod 645 = 3$

$a_0 = 0,\ x = 1,\ 3^2 \bmod 645 = 9$

$a_1 = 0,\ x = 1,\ 9^2 \bmod 645 = 81$

$\rightarrow a_2 = 1,\ x = 1 \cdot 81 \bmod 645 = 81,\ 81^2 \bmod 645 = 111$

$a_3 = 0,\ x = 81,\ 111^2 \bmod 645 = 66$

$a_4 = 0,\ x = 81,\ 66^2 \bmod 645 = 486$

$a_5 = 0,\ x = 81\ \ 486^2 \bmod 645 = 126$

$a_6 = 0,\ x = 81\ \ 126^2 \bmod 645 = 396$

$a_7 = 1,\ x = 81 * 396 \bmod 645 = 471$

$396^2 \bmod 645 = 81$

$a_8 = 0,\ x = 471,\ 81^2 \bmod 645 = 111$

$a_9 = 1,\ x = 471 * 111 \bmod 645 = \underline{36}$

$111^2 \bmod 645 = 66$