Множення довгих чисел. Модулярний метод (Шенхаге).

Нехай $q_0 = 1,\ q_{k+1} = 3q_k - 1,\ k = 1,2,\ldots$ Тобто $q_k = 3^k - 3^{k-1} - \ldots - 1 = (3^k + 1)/2,\ k = 0,1,2,\ldots$

u, v - p_k-бітові числа, де $p_k = 18q_k + 8$.

Метод зводить множення p_k-бітових чисел до множення p_{k-1}-бітових чисел.

Взаємно прості модулі: $m_1 = 2^{6q_k - 1} - 1$, $m_2 = 2^{6q_k + 1} - 1$, $m_3 = 2^{6q_k + 2} - 1$,

$$m_4 = 2^{6q_k + 3} - 1,\ m_5 = 2^{6q_k + 5} - 1,\ m_6 = 2^{6q_k + 7} - 1.$$

<u>Алгоритм</u> (нехай $k > 0$).

a) Обчислити $u_1 = u \bmod m_1, \ldots, u_6 = u \bmod m_6$ та $v_1 = v \bmod m_1, \ldots, u_6 = v \bmod m_6$.
b) Обчислити добутки $u_1 v_1, \ldots, u_6 v_6$, що мають не більше p_{k-1} біт.
c) Обчислити $w_1 = u_1 v_1 \bmod m_1, \ldots, w_6 = u_6 v_6 \bmod m_6$.
d) Знайти $0 \le w < m$: $w \bmod m_1 = w_1, \ldots, w \bmod m_6 = w_6$.

<u>Деталі.</u>

a) $u = (v_r v_{r-1} \ldots v_0)_{(2)}$, $m = 2^l - 1$. $u = a_t A^t + a_{t-1} A^{t-1} + \ldots + a_1 A + a_0$, де $A = 2^l$, $0 \le a_k < 2^l,\ 0 \le k \le t$. Тоді $u \equiv a_t + a_{t-1} + \ldots + a_1 + a_0 \pmod{(2^l - 1)}$ (аналогічно в 10-й системі числення відбувається процес "відкидання дев'яток" для обчислення $u \bmod 9$).
b) Рекурсивно викликається ця ж процедура обчислення добутку p_{k-1}-бітових чисел.
c) Аналогічно a).
d) Обчислити $w'_1 = w_1 \bmod m_1$ та $w'_j = (\ldots((w_j - w'_1)c_{1j} - w'_2)c_{2j} - \ldots - w'_{j-1})c_{(j-1)j} \bmod m_j$, $j = 2,\ldots,6$.

Далі обчислити $w = (\ldots(w'_6 m_5 + w'_5)m_4 + \ldots + w'_2)m_1 + w'_1$. Тут $c_{ij} : c_{ij} m_i \equiv 1 \pmod{m_j}$.

Враховуючи специфічний вигляд модулів, операція множення на m_j зводиться до побітового зсуву та віднімання.

Пошук $(cu) \bmod (2^f - 1)$, де $0 < l < f$ - цілі, $u < 2^f$ - ціле, $(2^l - 1)c \equiv 1 \pmod{(2^f - 1)}$.

Знайти $b : bl \equiv 1 \pmod f$, тоді $c = c[b] = \left(\sum_{0 \le j < b} 2^{jl} \right) \bmod (2^f - 1)$. Нехай

$b = (b_s b_{s-1} \ldots b_0)_{(2)}$. Обчислити a_k, d_k, u_k, v_k за формулами

$a_0 = l$, $a_k = 2a_{k-1} \bmod f$;

$d_0 = b_0 l$, $d_k = (d_{k-1} + b_k a_k) \bmod f$;

$u_0 = u$, $u_k = (u_{k-1} + 2^{a_{k-1}} u_{k-1}) \bmod (2^f - 1)$;

$v_0 = b_0 u$, $v_k = (v_{k-1} + b_k 2^{d_{k-1}} u_k) \bmod (2^f - 1)$.

В результаті $(c[b]u) \bmod (2^f - 1) = v_s$.

Приклад. Обчислити модулярним методом 123456789*123456789.

u=123456789
v=123456789
11101011011110011010010101
11101011011110011010010101

mdeg:
11 13 14 15 17 19
m[i]=2^(mdeg-1):
2047 8191 16383 32767 131071 524287

c[i,j]= // Не треба обчислювати, тут вони приводяться тільки для контролю/демонстрації/кращого розуміння
11, 13, 0101010101001 2729
11, 14, 10110110110101 11701
13, 14, 11111111111101 16381
11, 15, 110111011101101 28397
13, 15, 010101010101001 10921
14, 15, 111111111111101 32765
11, 17, 11110111110111101 126909
13, 17, 00010001000100001 8737
14, 17, 10110110110110101 93621
15, 17, 01010101010101001 43689
11, 19, 0100100101001001001 150089
13, 19, 0000010000010000001 8321
14, 19, 1110111101111011101 490461
15, 19, 1101110111011101101 454381
17, 19, 0101010101010101001 174761

um[0]=000010101100=172 (11101+01101111001+10100010101=100010101011=2219 mod 2047=172)
vm[0]=000010101100=172
um[1]=00011111110101=2037
vm[1]=00011111110101=2037
um[2]=10101010000100=10884
vm[2]=10101010000100=10884
um[3]=101101111001100=23500
vm[3]=101101111001100=23500
um[4]=11101000011000010=118978
vm[4]=11101000011000010=118978
um[5]=0111100111000000000=249344
vm[5]=0111100111000000000=249344

wm[0]=111001110010000=29584
wm[1]=11111101010000011111001=4149369
wm[2]=11100001111100101010000010000=118461456
wm[3]=10000011101010101010101010010000=552250000
wm[4]=11010010111011111111101001100000100=14155764484
wm[5]=11100111100111000100000000000000000000=62172430336

wm[0] mod m[0] = 01110011110=926
wm[1] mod m[1] = 1001001110011=4723
wm[2] mod m[2] = 11000001001110=12366
wm[3] mod m[3] = 110110001100101=27749

wm[4] mod m[4] = 010111100011100100=96484
wm[5] mod m[5] = 1011100111100111000=380728

w'1=w1 mod m1 = 926 mod 2047
=926
w'2=(w2-w'1)c12 mod m2 = (4723-926)2729 mod 8191
=398
w'3=((w3-w'1)c13-w'2)c23 mod m3 = ((12366-926)11701-398)16381 mod 16383
=12902
w'4=(((w4-w'1)c14-w'2)c24-w'3)c34 mod m4
=(((27749-926)28397-398)10921-12902)32765 mod 32767
=22718
w'5=((((w5-w'1)c15-w'2)c25-w'3)c35-w'4)c45 mod m5
=((((96484-926)126909-398)8737-12902)93621-22718)43689 mod 131071
=1
w'6=(((((w6-w'1)c16-w'2)c26-w'3)c36-w'4)c46-w'5)c56 mod m6
=(((((380728-926)150089-398)8321-12902)490461-22718)454381-1)174761 mod 524287
=0

w=((((w'6*m5+w'5)m4+w'4)m3+w'3)m2+w'2)m1+w'1=
=15241578750190521

Літ. Кнут. Искусство программирования. 2 том, стр. 334