Cách 3: Phép cộng các bình phương modulo (Cách dễ hiểu nhất)

Viết biểu thức nhị phân của (6863)2: 1101011001111 (6863 cơ số 2- số nhị phân - binary)

Ta có: (6863)10 = (6863 cơ số 10 - số thập phân – decimal)

= + + + + + + + +

= 4096 + 2048 + 512 + 128 + 64 + 8 + 4 + 2 + 1

* (. . . . . . . .277)mod6863(\*)

Từ quy tắc nhân trong số học modulo, suy ra (\*) như sau:

[( mod 6863) \* ( mod 6863) \* ( mod 6863)

\* ( mod 6863) \* ( mod 6863) \* ( mod 6863)

\* ( mod 6863) \* ( mod 6863) \* (277 mod 6863)] mod 6863 (\*\*)

Tạo bảng sau:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | = | 277 |  |  |  |  |
|  |  | mod 6863 | = | 1236 |  |  |
|  |  | mod 6863 |  | mod 6863 | = | 4110 |
|  |  | mod 6863 |  | mod 6863 | = | 2257 |
|  |  | mod 6863 |  | mod 6863 | = | 1703 |
|  |  | mod 6863 |  | mod 6863 | = | 4023 |
|  |  | mod 6863 |  | mod 6863 | = | 1575 |
|  |  | mod 6863 |  | mod 6863 | = | 3082 |
|  |  | mod 6863 |  | mod 6863 | = | 332 |
|  |  | mod 6863 |  | mod 6863 | = | 416 |
|  |  | mod 6863 |  | mod 6863 | = | 1481 |
|  |  | mod 6863 |  | mod 6863 | = | 4064 |
|  |  | mod 6863 |  | mod 6863 | = | 3718 |

Từ (\*\*)

=> (3718 \* 4064 \* 416 \* 3082 \* 1575 \* 2257 \* 4110 \* 1236 \* 277) mod 6863

= 277 mod 6863 = 277