

```
void internal_reduction(uint64_t *rop, int128 *op){
```

```
    uint64_t tmp_q[NB_COEFF];
```

```
    int128 tmp_zero[NB_COEFF];
```

```
    //~ computation of : op*neg_inv_ri_rep_coeff mod((X^n - c), mont_phi)
```

```
    tmp_q[0] = ((uint64_t)op[0] * 14404731248266644585UL) + (((uint64_t)op[1] * 3286953480751773897UL) + ((uint64_t)op[2] * 5408557101331171271UL) + ((uint64_t)op[3] * 6945810801382881972UL)) * 5);
```

```
    tmp_q[1] = ((uint64_t)op[0] * 6945810801382881972UL) + ((uint64_t)op[1] * 14404731248266644585UL) + (((uint64_t)op[2] * 3286953480751773897UL) + ((uint64_t)op[3] * 5408557101331171271UL)) * 5);
```

```
    tmp_q[2] = ((uint64_t)op[0] * 5408557101331171271UL) + ((uint64_t)op[1] * 6945810801382881972UL) + ((uint64_t)op[2] * 14404731248266644585UL) + ((uint64_t)op[3] * 16434767403758869485UL);
```

```
    tmp_q[3] = ((uint64_t)op[0] * 3286953480751773897UL) + ((uint64_t)op[1] * 5408557101331171271UL) + ((uint64_t)op[2] * 6945810801382881972UL) + ((uint64_t)op[3] * 14404731248266644585UL);
```

```
    //~ computation of : tmp_q*red_int_coeff mod(X^n - c)
```

```
    tmp_zero[0] = ((int128)tmp_q[0] * 128659502648371L) + (((int128)tmp_q[1] * 95477151974086L) + ((int128)tmp_q[2] * 95597758307649L) + ((int128)tmp_q[3] * 99992787138717L)) * 5);
```

```
    tmp_zero[1] = ((int128)tmp_q[0] * 99992787138717L) + ((int128)tmp_q[1] * 128659502648371L) + (((int128)tmp_q[2] * 95477151974086L) + ((int128)tmp_q[3] * 95597758307649L)) * 5);
```

```
    tmp_zero[2] = ((int128)tmp_q[0] * 95597758307649L) + ((int128)tmp_q[1] * 99992787138717L) + ((int128)tmp_q[2] * 128659502648371L) + ((int128)tmp_q[3] * 477385759870430L);
```

```
    tmp_zero[3] = ((int128)tmp_q[0] * 95477151974086L) + ((int128)tmp_q[1] * 95597758307649L) + ((int128)tmp_q[2] * 99992787138717L) + ((int128)tmp_q[3] * 128659502648371L);
```

```
    //~ computation of : (op + tmp_zero)/mont_phi
```

```
    rop[0] = (op[0] + tmp_zero[0]) >> WORD_SIZE;
```

```
    rop[1] = (op[1] + tmp_zero[1]) >> WORD_SIZE;
```

```
    rop[2] = (op[2] + tmp_zero[2]) >> WORD_SIZE;
```

```
    rop[3] = (op[3] + tmp_zero[3]) >> WORD_SIZE;
```

```
}
```