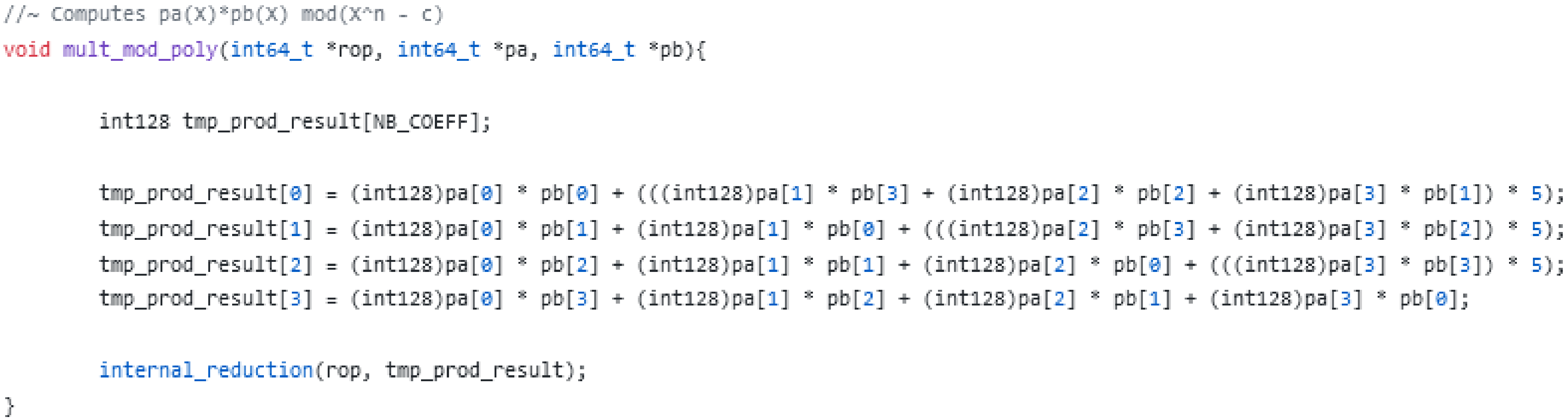

```
//~ Computes pa(X)*pb(X) mod(X^n - c)
void mult_mod_poly(int64_t *rop, int64_t *pa, int64_t *pb){

        int128 tmp_prod_result[NB_COEFF];

        tmp_prod_result[0] = (int128)pa[0] * pb[0] + (((int128)pa[1] * pb[3] + (int128)pa[2] * pb[2] + (int128)pa[3] * pb[1]) * 5);
        tmp_prod_result[1] = (int128)pa[0] * pb[1] + (int128)pa[1] * pb[0] + (((int128)pa[2] * pb[3] + (int128)pa[3] * pb[2]) * 5);
        tmp_prod_result[2] = (int128)pa[0] * pb[2] + (int128)pa[1] * pb[1] + (int128)pa[2] * pb[0] + (((int128)pa[3] * pb[3]) * 5);
        tmp_prod_result[3] = (int128)pa[0] * pb[3] + (int128)pa[1] * pb[2] + (int128)pa[2] * pb[1] + (int128)pa[3] * pb[0];

        internal_reduction(rop, tmp_prod_result);
}
```