# herm1t 🇺🇦: Multiplicative PRIDE

herm1tvx.blogspot.com/2025/07/multiplicative-pride.html

Friday, July 4, 2025

## Multiplicative PRIDE

Last time, I explored how PRIDE works. It turned out that the initial value and the generator in the group Zn under addition are simply split into two variables. Can we do something similar with multiplication? Let's try the following example:

pride-mul.c

```
        for (a = 1; a < n; a++)
        for (b = 1; b < n; b++) {
                /* GCD(b, n)       A062955 phi(n^2) - phi(n)
                   GCD(a * b, n)   A127473 phi(n)^2 */
                if (gcd(b, n) != 1)
                        continue;
                bzero(o, sizeof(o));
                for (y = 0, i = 0; i < n; i++) {
                        /* x = (a + b * i) % n; */
                        x = (y + a) % n;
                        y = (y + b) % n;
                }
        }
```

Although it looks very similar to the previous one, this is not group addition, but an affine transformation in the *ring* Zn, of the form x = a + b * i, where GCD(b, n) == 1.

If you calculate the number of possible permutations for different n, you get sequence A062955 in OEIS:

```
for a in `seq 1 16`; do ./a.out $a|sort|uniq|wc -l; done|xargs
0 1 4 6 16 10 36 28 48 36 100 44 144 78 112 120
```

That is: $\phi(n2)-\phi(n)=(n-1)\times\phi(n)$, where $\phi$ is Euler's totient function.