Calculator Program Notes

Pohlig-Hellman on calculator:

- First, factor the group order yourself!
- Then start the program, and input your h, g (generator) and modulus
- Now QS is the number of factors
- Now input the factors, and after that, input the powers of the factors

Fermat test.

TRIVIAAL. Gebruik programma ervoor niet! (doet namelijk iets raars met square and multiply).

Take an a, and check if:

$$a^{n-1} \equiv 1 \mod n$$

Example, $a = 2$ and $n = 4891$:

$$2^{4890} \equiv 3950 \not\equiv 1 \mod 4891$$

```
Mod(2^4890,4891)
```

```
Mod(3950, 4891)
```

Since $2^{4890} \not\equiv 1 \mod 4891$, thus n is not prime.

Calculate lcm of multiple numbers

$\text{lcm}(\{1,2,3,4\}) = \text{lcm}(\text{lcm}(1,2), \text{lcm}(3,4))$

```
lcm([1,2,3,4])
lcm(lcm(1,2), lcm(3,4))
```

```
12
12
```

Inverse of a number modulo n

Inverse of g, modulo n. First calculate the XGCD, with $xg + yn = 1$ (otherwise it is not invertible). Then, x is the inverse. If x is negative, do modulo n to obtain positive.

Example: $g = 7, n = 34567$. Calculate $g^{-1} \mod n$. First calculate the XGCD, which gives $-4938 \cdot 7 + 1 \cdot 34567 = 1$ $g^{-1} \equiv -4938 \equiv 29629 \mod 34567$

```
gcdext(7, 34567)
Mod(-4938, 34567)
Mod(7^-1, 34567)
```

```
[-4938, 1, 1]
Mod(29629, 34567)
Mod(29629, 34567)
```

Order of a point in Edwards curve

Given a point P, calculate $2P, 3P, 4P, \ldots$ until $n \cdot P = P$ with $n \in \mathbb{N}$.

The order of P is the smallest $n \in \mathbb{N}, n \neq 1$ such that $n \cdot P = P$

```

```