Calculating $\mathrm{ord}_G g$.

```
/* pseudocode for calculating k=ord_G{g},*/
if g==1, return 1;
else factor n=|G| into prime powers.
/* n=p[1]^a[1]... p[t]^a[t]      */
/* k=p[1]^b[1]... p[t]^b[t], */
/* 0<=b[i]<=a[i],1<=i<=t    */
k=n
for(i=1;i<=t;i++){
   for(j=1;j<=a[i];j++){
      s=k/p[i]
      m=g^s
      if(m!=1) break
             /* out of inner loop */
      else k=s
   }
}
return k
```

EXAMPLE Find $\text{ord}_{433}137$.

SOLUTION. 433 is a prime.
$n = 433 - 1 = 432 = 2^4 3^3$.
$137^{n/2} \equiv 1 \pmod{433}$,
$137^{n/2^2} \equiv 1 \pmod{433}$
$137^{n/2^3} \equiv 1 \pmod{433}$
$137^{n/2^4} \equiv 432 \pmod{433}$. Hence $b_1 = 1$.
$137^{n/2^3 \cdot 3} \equiv 1 \pmod{433}$
$137^{n/2^3 \cdot 3^2} \equiv 198 \pmod{433}$ Hence $b_2 = 2$.

Hence $\text{ord}_{433}137 = 2^1 3^2 = 18$.