Examen19

```
pr.<x,y>=PolynomialRing(QQ,order='lex')
```

```
f1=x^2+y^2-4
```

```
f2=x^3-x*y-4*x+y^2+2*y
```

```
I=ideal([f1,f2])
```

```
G=I.groebner_basis()
```

```
G
```

```
    [x^2 + y^2 - 4, x*y + y^4 + y^3 - 3*y^2 - 2*y, y^5 + 2*y^4 - 2*y^3 -
    4*y^2]
```

```
len(G)
```

```
    3
```

```
factor(G[2])
```

```
    (y + 2) * y^2 * (y^2 - 2)
```

```
def TEST1(n,P):
    for p in P:
        b=1
        while b==1:
            a=ZZ.random_element(1,n)
            b=mod(a,n)^((n-1)/p)
        if mod(b,n)^p<>1 :
            return 0
    return 1
```

```
TEST1(10^10+33,[2,3,11,17,557041])
```

```
    1
```

```
def TEST2(n,F,P):
    U=(n-1)//F
    for p in P:
        d=0
        while d<>1:
            a=ZZ.random_element(1,n)
            b=mod(a,n)^((n-1)//p)
            d=gcd(b-1,n)
        if mod(b,n)^p<>1 :
            return 0
    d=0
    while d<>1:
        a=ZZ.random_element(1,n)
        b=mod(a,n)^F
        d=gcd(b-1,n)
    if mod(b,n)^U<>1 :
            return 0
    return 1
```

```
n=10^20+207
```

```
factor(n-1)
```

```
    2 * 3^2 * 811 * 1531 * 161521 * 27701447
```

```
F=2*3^2*811*1531
```

```
TEST2(n,F,[2,3,811,1531])
```

```
    1
```

```
F
```

```
    22349538
```

```
(F*1532)^2-n
```

```
    1072342827209524590449
```