

METODO delle CURVE ELLITTICHE: fase 1

ESERCIZIO 1. Sia $n=589=(19 \cdot 31)$. Fattorizzare n usando la curva ellittica E :
 $Y^2=X^3+4X+9$ e il punto $P=(2,5)$ su E .

Qui sotto scegliamo $B=10$, costruiamo il grosso intero B -smooth K e calcoliamo $K \cdot P$,
usando l'espansione binaria di K etc...
In questo modo si vede esattamente il momento in cui compare un denominatore d
non invertibile modulo n
e $\gcd(d,n)$ individua un fattore non banale di n .

```
n=589
B=10
K=2^3*3^2*5*7
binary(K)
E=ellinit([0,0,0,4,9]*mod(1,n),1);
P=[2,5]
ellpow(E,P,K)
P0=P
P1=ellpow(E,P0,2)
P2=ellpow(E,P1,2)
P3=ellpow(E,P2,2)
P4=ellpow(E,P3,2)
P5=ellpow(E,P4,2)
P6=ellpow(E,P5,2)
P7=ellpow(E,P6,2)
P8=ellpow(E,P7,2)
P9=ellpow(E,P8,2)
P10=ellpow(E,P9,2)
P11=ellpow(E,P10,2)
Q4=elladd(E,P3,P4)
Q6=elladd(E,Q4,P6)
Q7=elladd(E,Q6,P7)
Q8=elladd(E,Q7,P8)
Q11=elladd(E,Q8,P11)
```

$Q6+P7$ impossibile

```
x1=241
y1=262
x2=564
y2=156
gcd(x2-x1,n)

m=(y2-y1)*(x2-x1)^-1
```

ESERCIZIO 2. Sia $n=26167=(137*191)$. Fattorizzare n usando la curva ellittica E :
 $Y^2=X^3+4X+128$ e il punto $P=(2,12)$ su E .

Qui sotto scegliamo $B=10$, costruiamo il grosso intero B -smooth K e calcoliamo $K*P$,
usando l'espansione binaria di K etc...
In questo modo si vede esattamente il momento in cui compare un denominatore d
non invertibile modulo n
e $\gcd(d,n)$ individua un fattore non banale di n .

```
n=26167
B=10
K=2^3*3^2*5*7
binary(K)
E=ellinit([0,0,0,4,128]*mod(1,n),1);
P=[2,12]
ellpow(E,P,K)
```

```
P0=P
P1=ellpow(E,P0,2)
P2=ellpow(E,P1,2)
P3=ellpow(E,P2,2)
P4=ellpow(E,P3,2)
P5=ellpow(E,P4,2)
P6=ellpow(E,P5,2)
P7=ellpow(E,P6,2)
P8=ellpow(E,P7,2)
P9=ellpow(E,P8,2)
P10=ellpow(E,P9,2)
P11=ellpow(E,P10,2)
Q4=elladd(E,P3,P4)
Q6=elladd(E,Q4,P6)
Q7=elladd(E,Q6,P7)
Q8=elladd(E,Q7,P8)
Q11=elladd(E,Q8,P11)
```

```
x1=18446
y1=5959
x2=8705
y2=23264
gcd(x2-x1,n)
```

ESERCIZIO 3. Sia $n=1386493=(1069*1297)$. Fattorizzare n usando la curva ellittica

E: $Y^2=X^3+3X-3$ e il punto $P=(1,1)$ su E.

Qui sotto scegliamo $B=20$, costruiamo il grosso intero B-smooth K e calcoliamo $K \cdot P$,

usando l'espansione binaria di K etc...

In questo modo si vede esattamente il momento in cui compare un denominatore d non invertibile modulo n

e $\gcd(d,n)$ individua un fattore non banale di n.

$n=1069 \cdot 1297$

$B=20$

$K=2^4 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19$

$\text{binary}(K)$

$E=\text{ellinit}([0,0,0,3,-3] \cdot \text{mod}(1,n),1);$

$P=[1,1]$

$\text{ellpow}(E,P,K)$

$P_0=P$

$P_1=\text{ellpow}(E,P_0,2)$

$P_2=\text{ellpow}(E, P_1,2)$

$P_3=\text{ellpow}(E,P_2,2)$

$P_4=\text{ellpow}(E,P_3,2)$

$P_5=\text{ellpow}(E,P_4,2)$

$P_6=\text{ellpow}(E,P_5,2)$

$P_7=\text{ellpow}(E,P_6,2)$

$P_8=\text{ellpow}(E,P_7,2)$

$P_9=\text{ellpow}(E,P_8,2)$

$P_{10}=\text{ellpow}(E,P_9,2)$

$P_{11}=\text{ellpow}(E,P_{10},2)$

$P_{12}=\text{ellpow}(E,P_{11},2)$

$P_{13}=\text{ellpow}(E,P_{12},2)$

$P_{14}=\text{ellpow}(E,P_{13},2)$

$P_{15}=\text{ellpow}(E,P_{14},2)$

$P_{16}=\text{ellpow}(E,P_{15},2)$

$P_{17}=\text{ellpow}(E,P_{16},2)$

$P_{18}=\text{ellpow}(E,P_{17},2)$

$P_{19}=\text{ellpow}(E,P_{18},2)$

$P_{20}=\text{ellpow}(E,P_{19},2)$

$P_{21}=\text{ellpow}(E,P_{20},2)$

$P_{22}=\text{ellpow}(E,P_{21},2)$

$P_{23}=\text{ellpow}(E,P_{22},2)$

$P_{24}=\text{ellpow}(E,P_{23},2)$

$P_{25}=\text{ellpow}(E,P_{24},2)$

$P_{26}=\text{ellpow}(E,P_{25},2)$

$P_{27}=\text{ellpow}(E,P_{26},2)$

```

Q5=elladd(E,P4,P5)
Q6=elladd(E,Q5,P6)
Q7=elladd(E,Q6,P7)
Q8=elladd(E,Q7,P8)
Q13=elladd(E,Q8,P13)
Q21=elladd(E,Q13,P21)
Q22=elladd(E,Q21,P22)
Q23=elladd(E,Q22,P23)
Q24=elladd(E,Q23,P24)
Q26=elladd(E,Q24,P26)
Q27=elladd(E,Q26,P27)

```

```

x1=533649
y1=65400
x2=533649
y2=1321093
gcd(x2-x1,n)

```

METODO delle CURVE ELLITTICHE: fase 1

ESERCIZIO 4. Sia $n=1386493=1069 \cdot 1297$, $p=1069$, $q=1297$.
 Queste righe di programma mostrano la fase 1 dell'algoritmo delle curve ellittiche:
 farlo girare diverse volte e osservare
 sia in caso di successo che di insuccesso le proprietà di B-smoothness degli
 ordini di $E(\mathbb{Z}_p)$ e di $E(\mathbb{Z}_q)$.

```

n =1386493
B=20
K=2^4*3^2*5*7*11*13*17*19
x=random(n);
y=random(n);
b=y^2-x^3-x;
E=ellinit([0,0,0,1,b]*mod(1,n),1);
P=[x,y]
lift(ellpow(E,P,K))
p=1069
F=ellinit([0,0,0,1,b]*mod(1,p),1);
N=p+1-ellap(F,p)
factor(N)
q=1297
G=ellinit([0,0,0,1,b]*mod(1,q),1);
M=q+1-ellap(G,q)
factor(M)

```

ESERCIZIO 5. Sia $n=p*q=28102844557$, $p=117763$, $q=238639$.

Queste righe di programma mostrano la fase 1 dell'algoritmo delle curve ellittiche: farlo girare diverse volte e osservare sia in caso di successo che di insuccesso le proprietà di B-smoothness degli ordini di $E(\mathbb{Z}_p)$ e di $E(\mathbb{Z}_q)$.

```
n=28102844557
B=100
K=2^6*3^4*5^2*7^2*11*13*17*19*23*29*31*37*41*43*47*53*59*61*67*71*73*79*83
*89*97*101
x=random(n);
y=random(n);
b=y^2-x^3-x;
E=ellinit([0,0,0,1,b]*mod(1,n),1);
gcd(lift(E.disc),n)
P=[x,y]
lift(ellpow(E,P,K))
p=117763
F=ellinit([0,0,0,1,b]*mod(1,p),1);
N=p+1-ellap(F,p)
factor(N)
q=238639
G=ellinit([0,0,0,1,b]*mod(1,q),1);
M=q+1-ellap(G,q)
factor(M)
```