In[22]:= **punktAdd[1, 6, 11, 8, 3, 8, 3];**

```
E(x) = x^3 + 1 x + 6 mod 11

P = (xp, yp) = (8, 3)

Q = (xq, yq) = (8, 3)

P == Q: Tangente am Punkt (8, 3 )
Anstieg s der Tangenten ermitteln
s = (3 xp^2 + a) / (2 yp) mod p
  = (3 8^2 + 1) (2 3)^(-1) mod 11
  = (193) (6)^(-1) mod 11
  = (6) (2) mod 11
  = 1

xr = s^2 - 2 xp mod p
   = 1^2 - 2 8 mod 11
   = -15 mod 11
   = 7

yr = -yp + s (xp - xr) mod p
   = -3 + 1 (8 - 7) mod 11
  = -2 mod 11
  = 9

neuer Punkt R = (xr, yr) = (7, 9)
```

```
In[23]:= punktAdd[1, 6, 11, 2, 7, 5, 2];
```

```
E(x) = x^3 + 1 x + 6 mod 11

P = (xp, yp) = (2, 7)

Q = (xq, yq) = (5, 2)

P ≠ Q: Gerade durch P und Q
Anstieg s der Geraden ermitteln
s = (yq - yp) / (xq - xp) mod p
  = (2 - 7) (5 - 2)^(-1) mod 11
  = (-5) (3)^(-1) mod 11
  = (6) (4) mod 11
  = 2

xr = s^2 - xp - xq mod p
   = 2^2 - 2 - 5 mod 11
   = -3 mod 11
   = 8

yr = -yp + s (xp - xr) mod p
   = -7 + 2 (2 - 8) mod 11
  = -19 mod 11
  = 3

neuer Punkt R = (xr, yr) = (8, 3)
```

```
(* Vielfache des Punktes (2,7) zum Vergleich für nachfolgendes Beispiel *)
In[28]:= vielfPunktoA[1, 6, 11, 2, 7];
E(x) = x^3 + 1 x + 6 mod 11
Startpunkt: (2, 7)
2 P = (5, 2)
3 P = (8, 3)
4 P = (10, 2)
5 P = (3, 6)
6 P = (7, 9)
7 P = (7, 2)
8 P = (3, 5)
9 P = (10, 9)
10 P = (8, 8)
11 P = (5, 9)
12 P = (2, 4)
Ende: 13 P = (2, 7)
In[30]:= punktMul[1, 6, 11, 3 , 2, 7];
E(x) = x^3 + 1 x + 6 mod 11
Startpunkt: (2, 7)
Faktor: 3
3 (2, 7) = (8, 3)
```

```
(* kleines Beispiel zum ECDH

  mit p = 11, a = 1, b = 6, P = (2,7);
xA = 4, xB = 3 *)
```

```
(* öffentlicher Wert von A *)
```

In[32]:=
```
QA = punktMul[1, 6, 11, 4, 2, 7];
```

```
E(x) = x^3 + 1 x + 6 mod 11

Startpunkt: (2, 7)

Faktor: 4

4 (2, 7) = (10, 2)
```

```
(* öffentlicher Wert von B *)
```

In[33]:=
```
QB = punktMul[1, 6, 11, 3, 2, 7];
```

```
E(x) = x^3 + 1 x + 6 mod 11

Startpunkt: (2, 7)

Faktor: 3

3 (2, 7) = (8, 3)
```

```
(* gemeinsamer Schluessel, von A berechnet *)
```

In[34]:=
```
AkAB = punktMul[1, 6, 11, 4, 8, 3];
```

```
E(x) = x^3 + 1 x + 6 mod 11

Startpunkt: (8, 3)

Faktor: 4

4 (8, 3) = (2, 4)
```

```
(* gemeinsamer Schluessel, von B berechnet *)
```

In[35]:=
```
RB = punktMul[1, 6, 11, 3, 10, 2];
```

```
E(x) = x^3 + 1 x + 6 mod 11

Startpunkt: (10, 2)

Faktor: 3

3 (10, 2) = (2, 4)
```

```
(* kleines Beispiel zu ElGamal

  mit p = 11, a = 1, b = 6, P = (2,7);
P = (2,7);
n = 13;
kd = 2        *)
```

In[36]:=
```
QA = punktMul[1, 6, 11, 2, 2, 7];
```

```
E(x) = x^3 + 1 x + 6 mod 11

Startpunkt: (2, 7)

Faktor: 2

2 (2, 7) = (5, 2)
```

```
(* Verschluesselung von m = 8 fuer r = 3 *)
```

In[37]:=
```
c1 = punktMul[1, 6, 11, 3, 2, 7];
```

```
E(x) = x^3 + 1 x + 6 mod 11

Startpunkt: (2, 7)

Faktor: 3

3 (2, 7) = (8, 3)
```

In[38]:=
```
(* tmp = r QA mod p *)
tmp = punktMul[1, 6, 11, 3, 5, 2];
```

```
E(x) = x^3 + 1 x + 6 mod 11

Startpunkt: (5, 2)

Faktor: 3

3 (5, 2) = (7, 9)
```

In[39]:=
```
(* m = 8 --> M = (8,3) *)
c2 = punktAdd[1, 6, 11, 8, 3, 7, 9];
```

```
E(x) = x^3 + 1 x + 6 mod 11

P = (xp, yp) = (8, 3)

Q = (xq, yq) = (7, 9)

P ≠ Q: Gerade durch P und Q
Anstieg s der Geraden ermitteln

s = (yq - yp) / (xq - xp) mod p

  = (9 - 3) (7 - 8)^(-1) mod 11

  = (6) (10)^(-1) mod 11

  = (6) (-1) mod 11

  = 5

xr = s^2 - xp - xq mod p
   = 5^2 - 8 - 7 mod 11

   = 10 mod 11

   = 10

yr = -yp + s (xp - xr) mod p
   = -3 + 5 (8 - 10) mod 11

  = -13 mod 11

  = 9

neuer Punkt R = (xr, yr) = (10, 9)
```

```
(* Ergebnis: (c1, c2) = ((8,3),(10,9)) *)

(* Entschluesselung *)
(* tmpd = kd c1 mod p *)
```

In[40]:=
```
tmpd = punktMul[1, 6, 11, 2, 8, 3];
```

```
E(x) = x^3 + 1 x + 6 mod 11

Startpunkt: (8, 3)

Faktor: 2

2 (8, 3) = (7, 9)
```

```
(* M = c2 - kd c1 mod p   *)
```

In[41]:=
```
punktAdd[1, 6, 11, 10, 9, 7, -9];
```

```
E(x) = x^3 + 1 x + 6 mod 11
P = (xp, yp) = (10, 9)
Q = (xq, yq) = (7, -9)

P ≠ Q: Gerade durch P und Q
Anstieg s der Geraden ermitteln
s = (yq - yp) / (xq - xp) mod p
  = (-9 - 9) (7 - 10)^(-1) mod 11
  = (-18) (8)^(-1) mod 11
  = (4) (-4) mod 11
  = 6

xr = s^2 - xp - xq mod p
   = 6^2 - 10 - 7 mod 11
   = 19 mod 11
   = 8

yr = -yp + s (xp - xr) mod p
   = -9 + 6 (10 - 8) mod 11
  = 3 mod 11
  = 3

neuer Punkt R = (xr, yr) = (8, 3)
      (* M = (8,3)  --> m = 8 *)
```