

# Elliptic curves over $\mathbf{R}$ and $\mathbf{F}_q$

D. J. Bernstein

University of Illinois at Chicago

## Why elliptic curves?

Can quickly compute

$$4^n \bmod 2^{262} - 5081$$

given  $n \in \{0, 1, 2, \dots, 2^{256} - 1\}$ .

Similarly, can quickly compute

$$4^{mn} \bmod 2^{262} - 5081$$

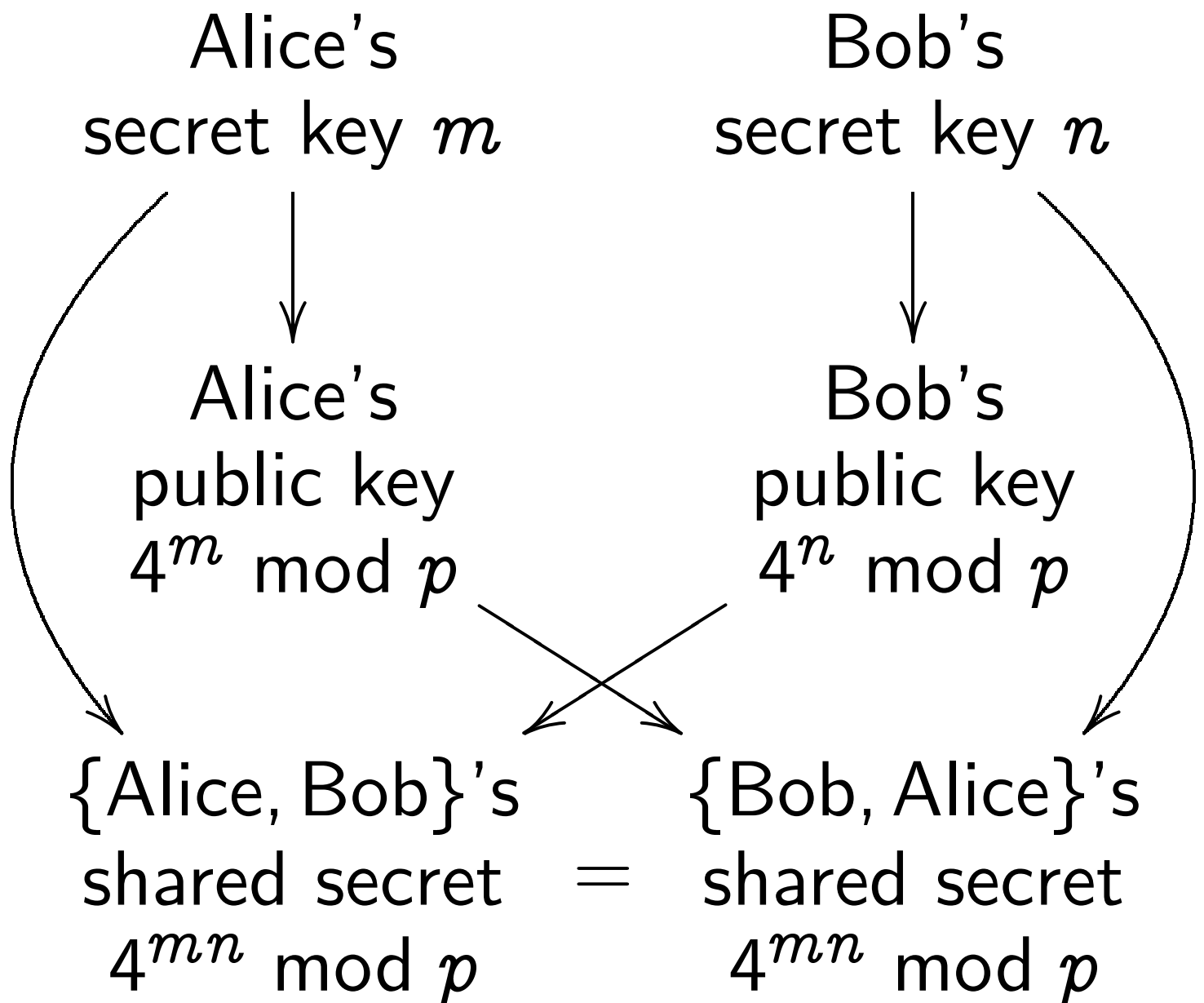
given  $n$  and  $4^m \bmod 2^{262} - 5081$ .

“Discrete-logarithm problem”:

given  $4^n \bmod 2^{262} - 5081$ , find  $n$ .

Is this easy to solve?

Diffie-Hellman secret-sharing  
system using  $p = 2^{262} - 5081$ :



Can attacker find  $4^{mn} \bmod p$ ?

Bad news: DLP can be solved at surprising speed! Attacker can find  $m$  and  $n$  by “index calculus.”

To protect against this attack, replace  $2^{262} - 5081$  with a much larger prime.

*Much* slower arithmetic.

Alternative: Elliptic-curve cryptography. Replace  $\{1, 2, \dots, 2^{262} - 5082\}$  with a comparable-size “safe elliptic-curve group.”

*Somewhat* slower arithmetic.

## An elliptic curve over $\mathbf{R}$

Consider all pairs  
of real numbers  $x, y$   
such that  $y^2 - 5xy = x^3 - 7$ .

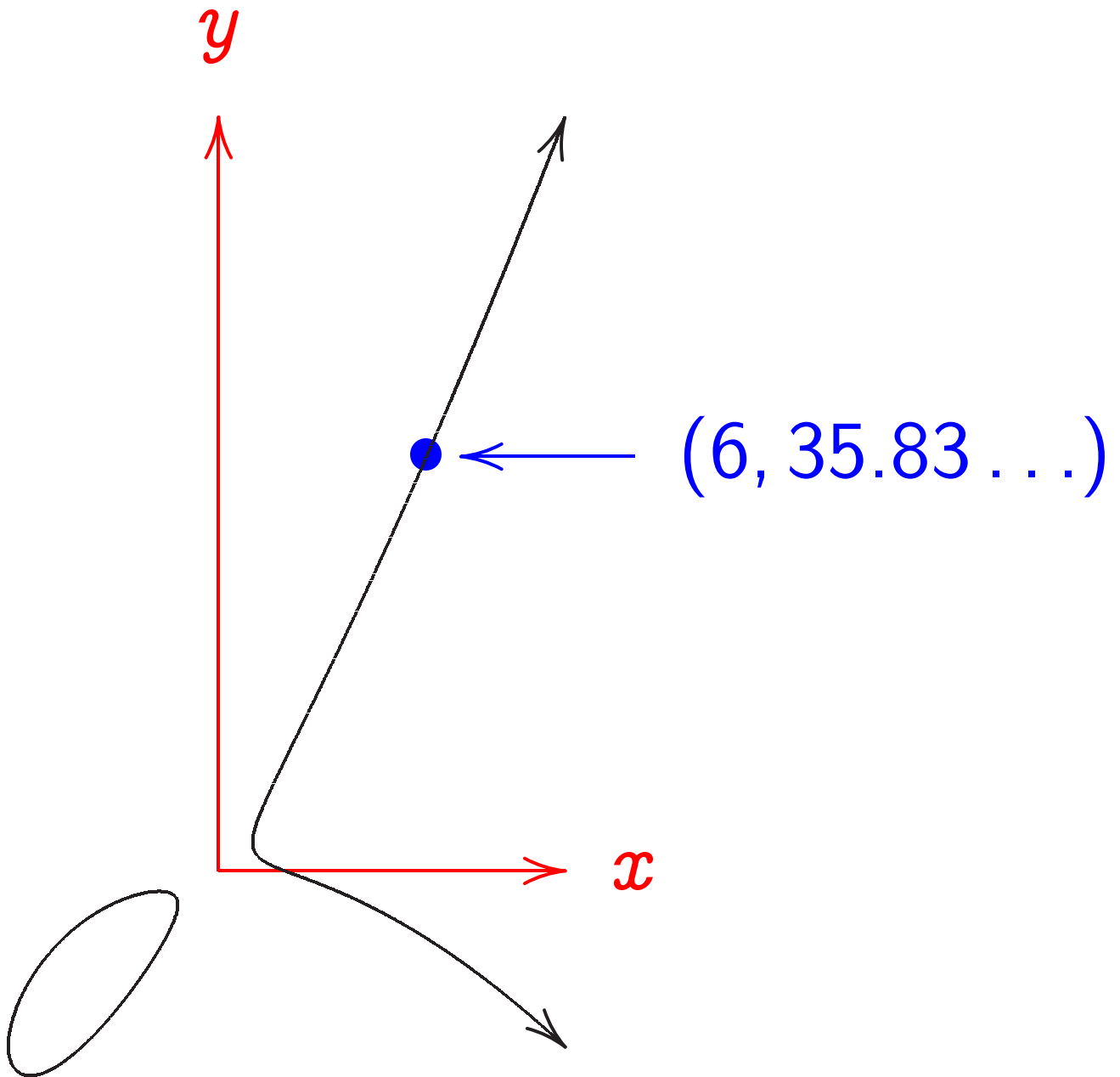
The “points on the elliptic curve  
 $y^2 - 5xy = x^3 - 7$  over  $\mathbf{R}$ ”  
are those pairs and  
one additional point,  $\infty$ .

i.e. The set of points is

$$\{(x, y) \in \mathbf{R} \times \mathbf{R} : \\ y^2 - 5xy = x^3 - 7\} \cup \{\infty\}.$$

( $\mathbf{R}$  is the set of real numbers.)

Graph of this set of points:



Don't forget  $\infty$ .

Visualize  $\infty$  as top of  $y$  axis.

There is a standard definition of  $0, -, +$  on this set of points.

Magical fact: The set of points is a “commutative group”; i.e., these operations  $0, -, +$  satisfy every identity satisfied by  $\mathbf{Z}$ .

e.g. All  $P, Q, R \in \mathbf{Z}$  satisfy  $(P + Q) + R = P + (Q + R)$ , so all curve points  $P, Q, R$  satisfy  $(P + Q) + R = P + (Q + R)$ . ( $\mathbf{Z}$  is the set of integers.)

# Visualizing the group law

$$0 = \infty; -\infty = \infty.$$

Distinct curve points  $P, Q$   
on a vertical line

have  $-P = Q$ ;

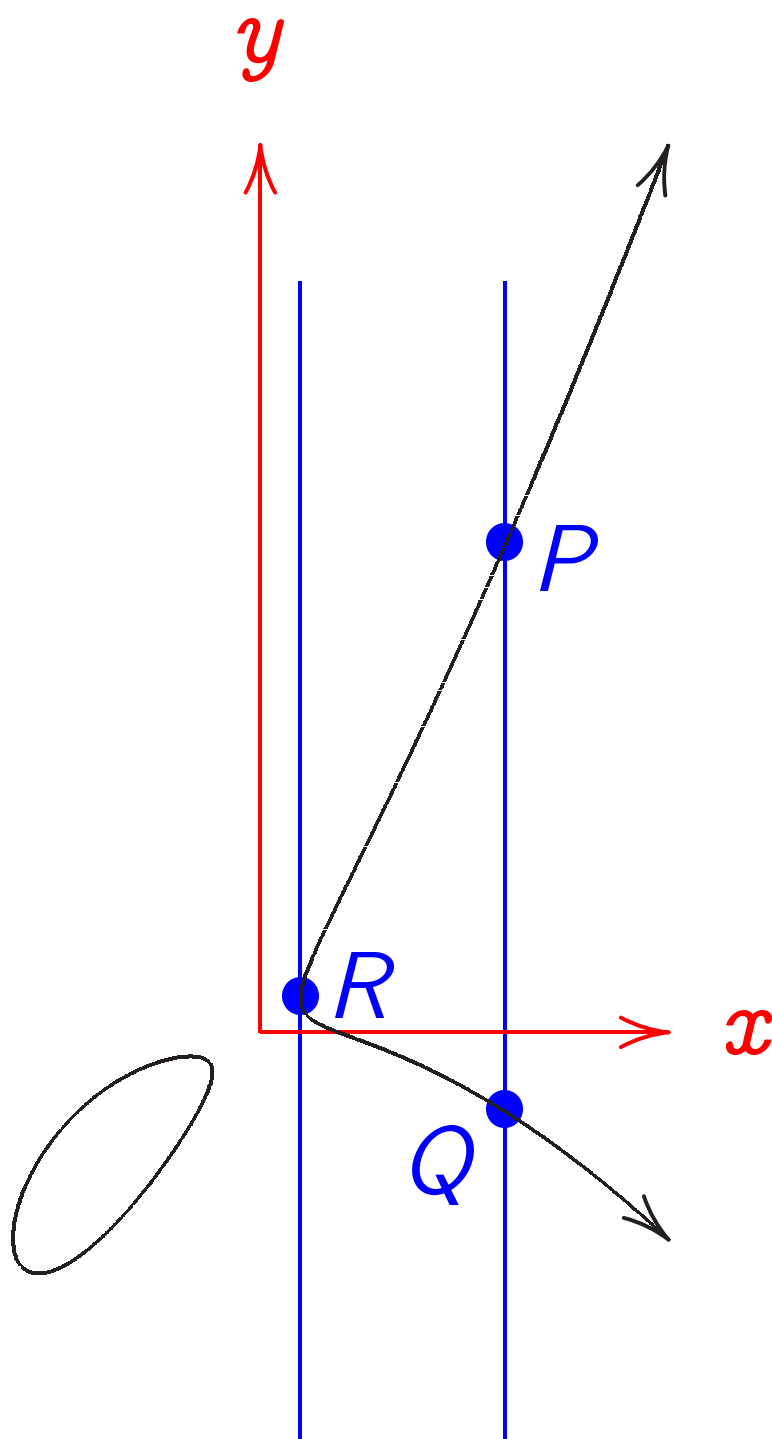
$$P + Q = 0 = \infty.$$

A curve point  $R$   
with a vertical tangent line

has  $-R = R$ ;

$$R + R = 0 = \infty.$$

$$-P = Q, -Q = P, -R = R:$$



Distinct curve points  $P, Q, R$   
on a line

have  $P + Q = -R$ ;

$$P + Q + R = 0 = \infty.$$

Distinct curve points  $P, R$   
on a line tangent at  $P$

have  $P + P = -R$ ;

$$P + P + R = 0 = \infty.$$

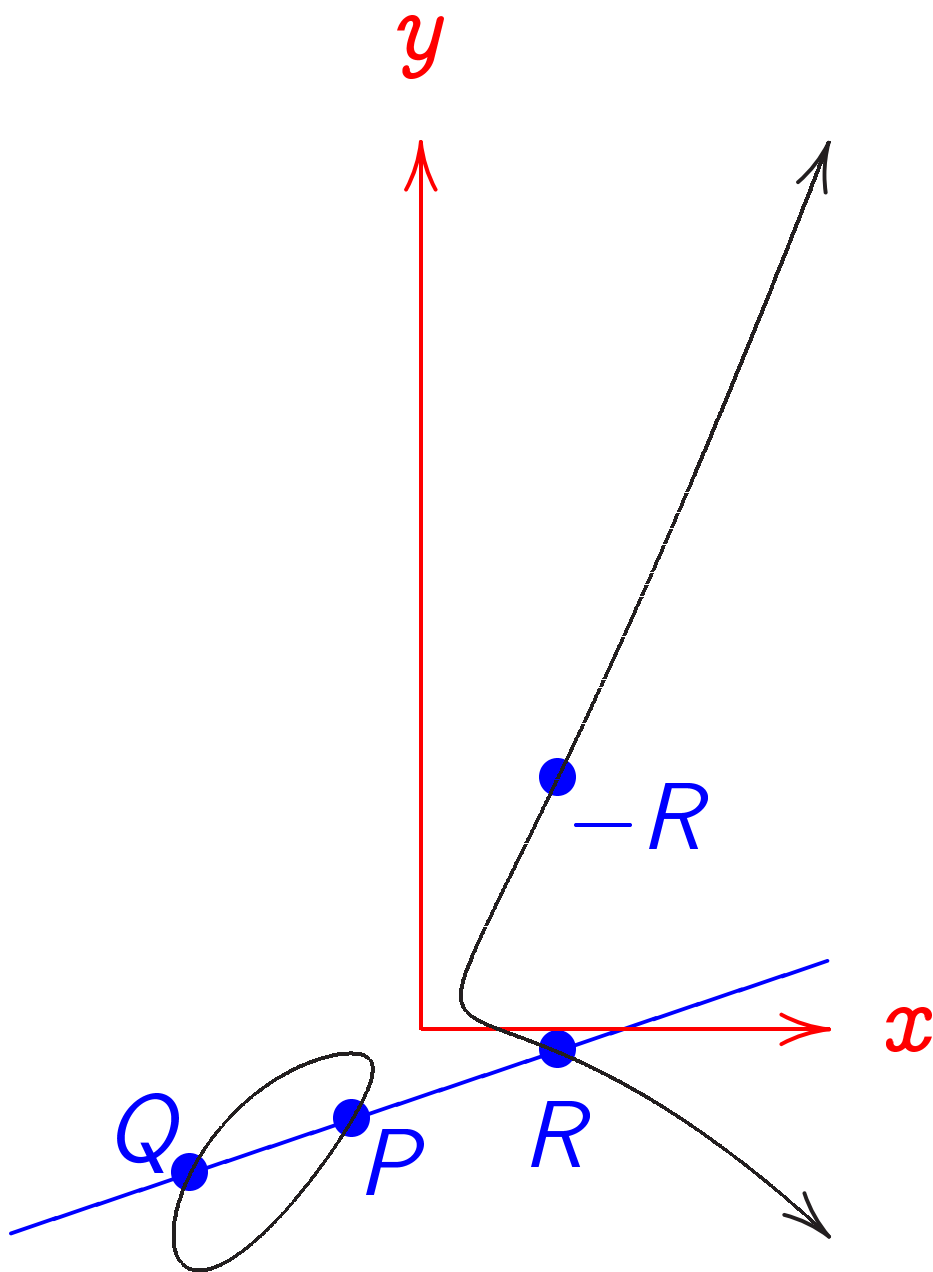
A non-vertical line

with only one curve point  $P$

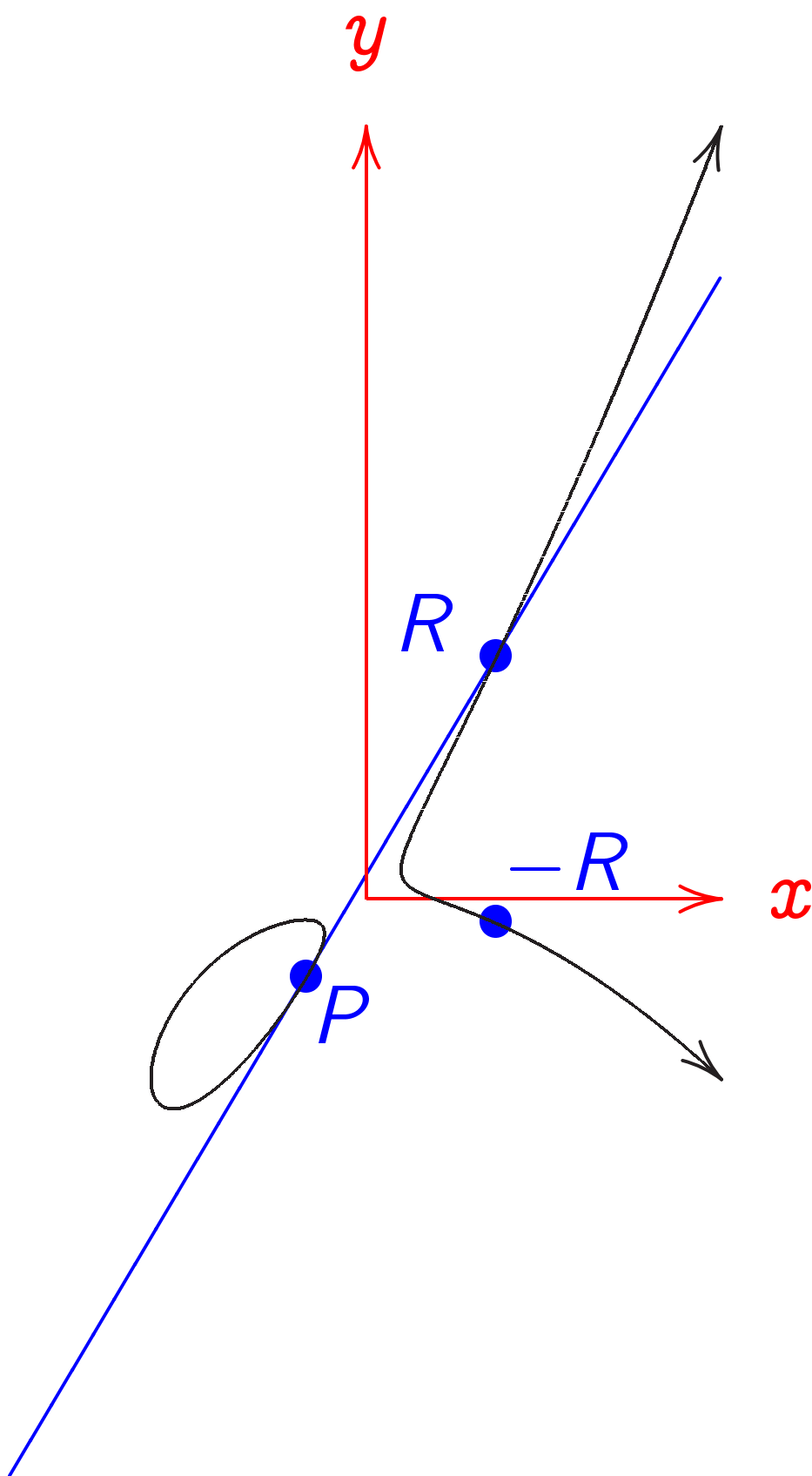
has  $P + P = -P$ ;

$$P + P + P = 0.$$

$$P + Q = -R:$$



$$P + P = -R:$$



# Curve addition formulas

Easily find formulas for  $+$   
by finding formulas for lines  
and for curve-line intersections.

$$x \neq x': (x, y) + (x', y') = (x'', y'')$$

where  $\lambda = (y' - y)/(x' - x)$ ,  
 $x'' = \lambda^2 - 5\lambda - x - x'$ ,  
 $y'' = 5x'' - (y + \lambda(x'' - x))$ .

$$2y \neq 5x: (x, y) + (x, y) = (x'', y'')$$

where  $\lambda = (5y + 3x^2)/(2y - 5x)$ ,  
 $x'' = \lambda^2 - 5\lambda - 2x$ ,  
 $y'' = 5x'' - (y + \lambda(x'' - x))$ .

$$(x, y) + (x, 5x - y) = \infty.$$

## An elliptic curve over $\mathbf{Z}/13$

Consider the prime field

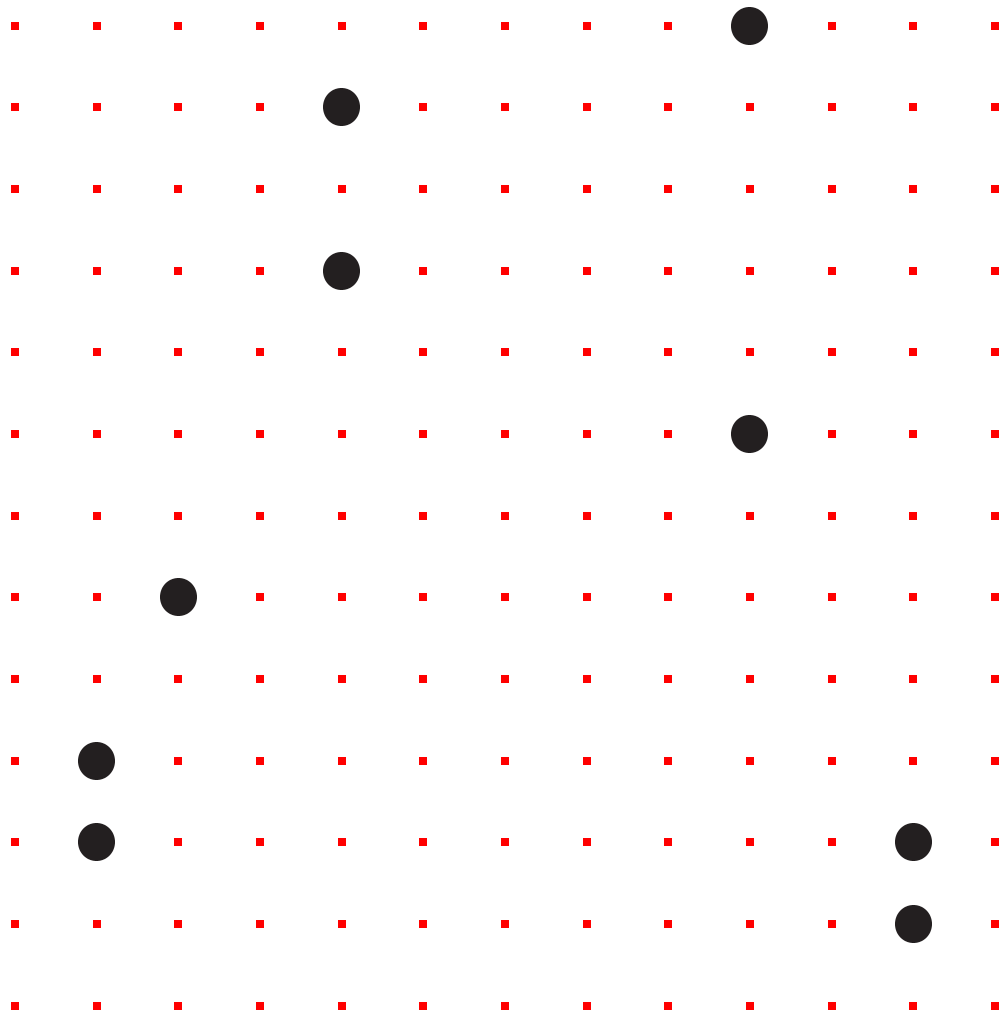
$$\mathbf{Z}/13 = \{0, 1, 2, \dots, 12\}$$

with  $-$ ,  $+$ ,  $\cdot$  defined mod 13.

The “set of points on the elliptic curve  $y^2 - 5xy = x^3 - 7$  over  $\mathbf{Z}/13$ ” is

$$\{(x, y) \in \mathbf{Z}/13 \times \mathbf{Z}/13 : y^2 - 5xy = x^3 - 7\} \cup \{\infty\}.$$

Graph of this set of points:



As before, don't forget  $\infty$ .

The set of curve points  
is a commutative group with  
standard definition of  $0, -, +$ .

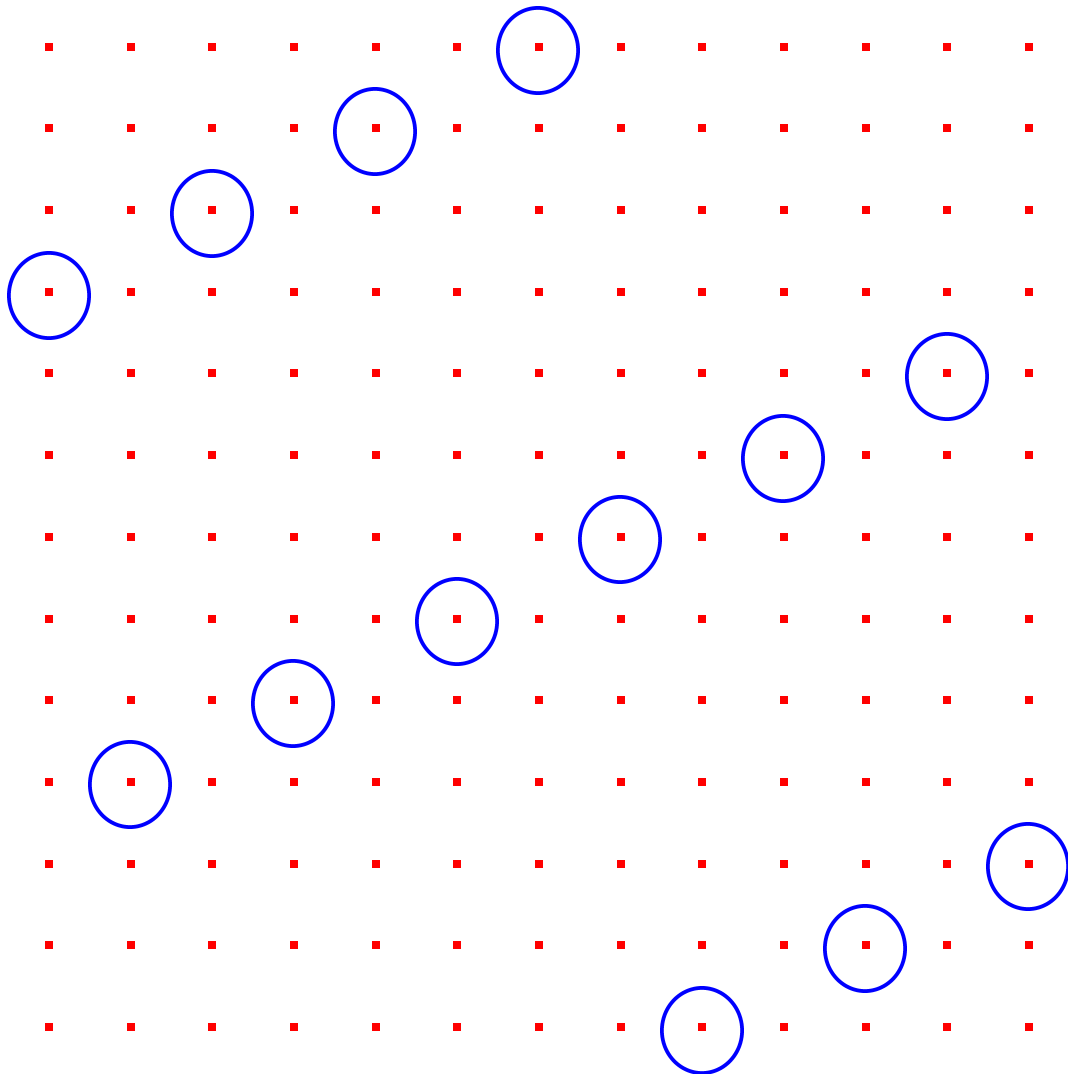
Can visualize  $0, -, +$  as before.

Replace lines over  $\mathbf{R}$   
by lines over  $\mathbf{Z}/13$ .

Warning: tangent is defined by  
derivatives; hard to visualize.

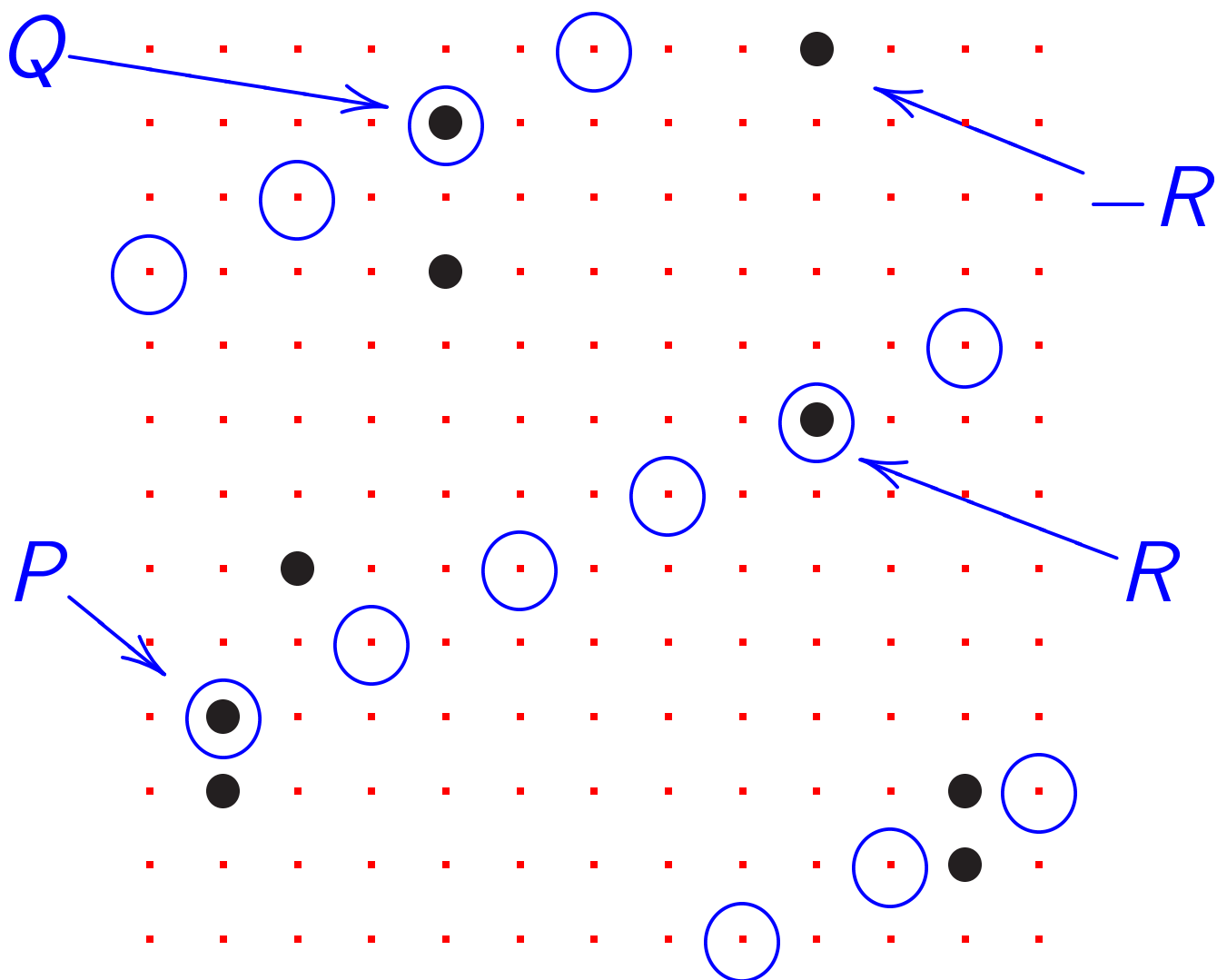
Can define  $0, -, +$   
using same formulas as before.

Example of line over  $\mathbf{Z}/13$ :



Formula for this line:  $y = 7x + 9$ .

$$P + Q = -R:$$



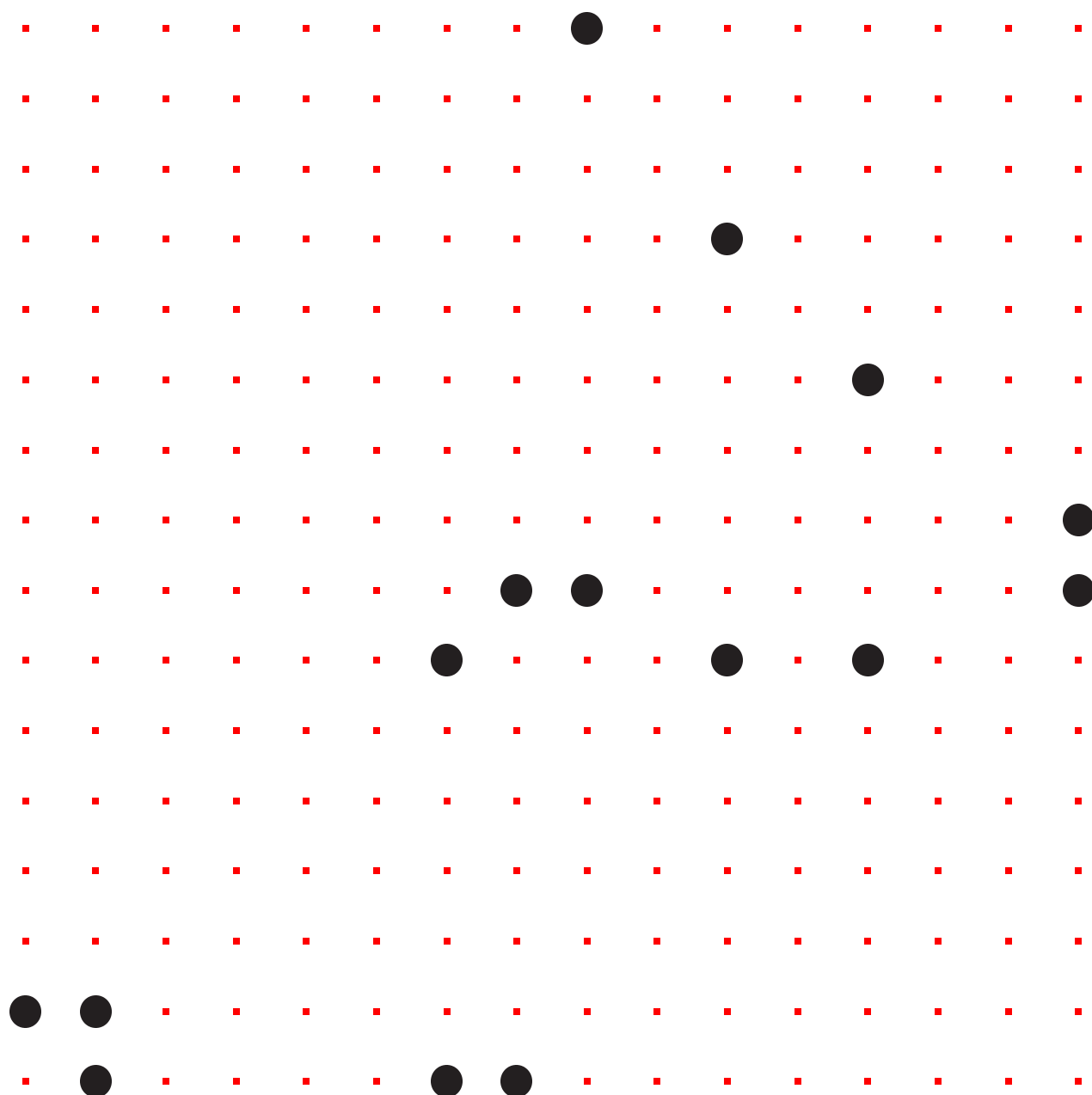
## An elliptic curve over $\mathbf{F}_{16}$

Consider the non-prime field

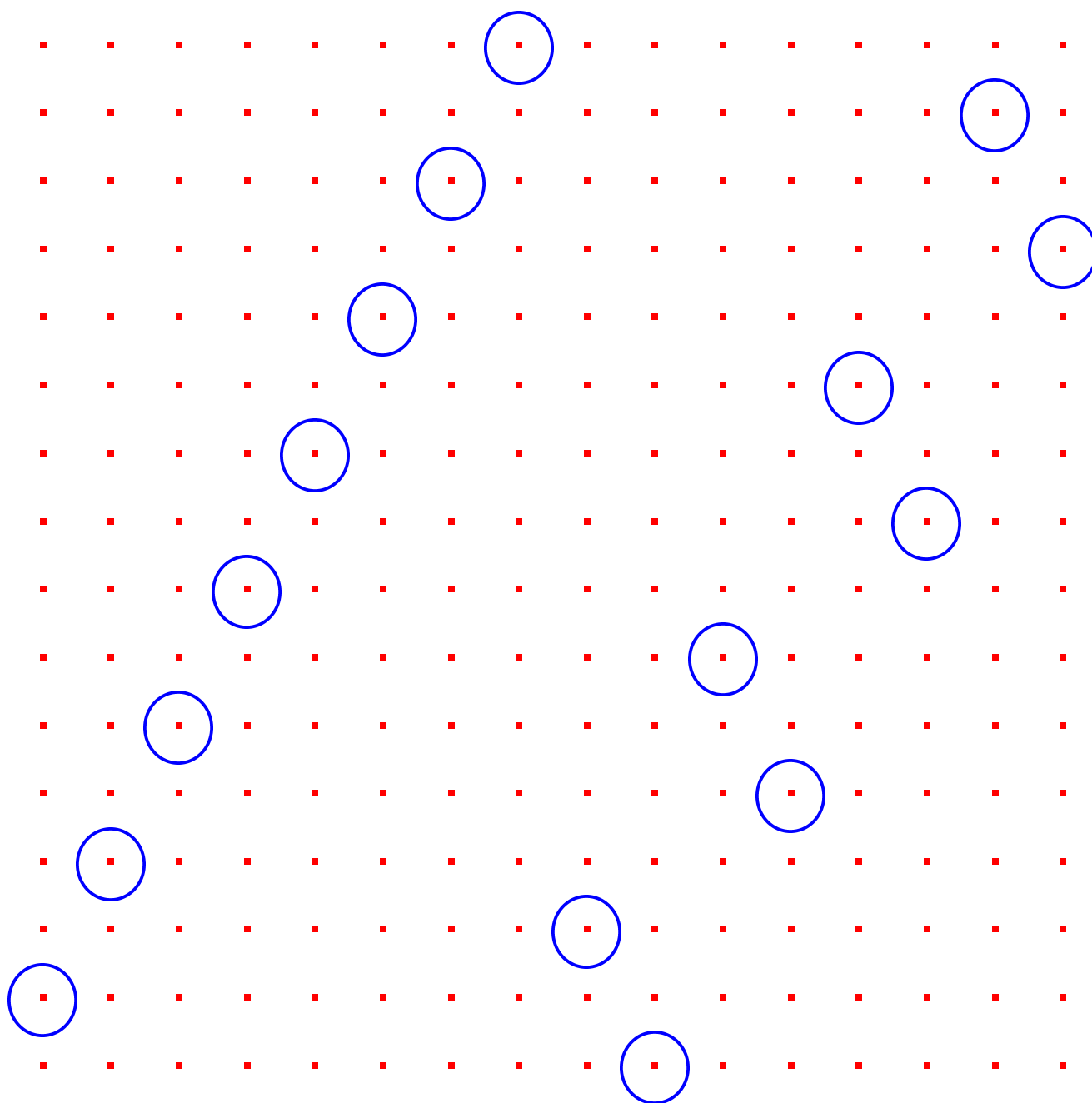
$$(\mathbf{Z}/2)[t]/(t^4 - t - 1) = \{$$
$$\begin{aligned} &0t^3 + 0t^2 + 0t^1 + 0t^0, \\ &0t^3 + 0t^2 + 0t^1 + 1t^0, \\ &0t^3 + 0t^2 + 1t^1 + 0t^0, \\ &0t^3 + 0t^2 + 1t^1 + 1t^0, \\ &0t^3 + 1t^2 + 0t^1 + 0t^0, \\ &\vdots \\ &1t^3 + 1t^2 + 1t^1 + 1t^0 \} \end{aligned}$$

of size  $2^4 = 16$ .

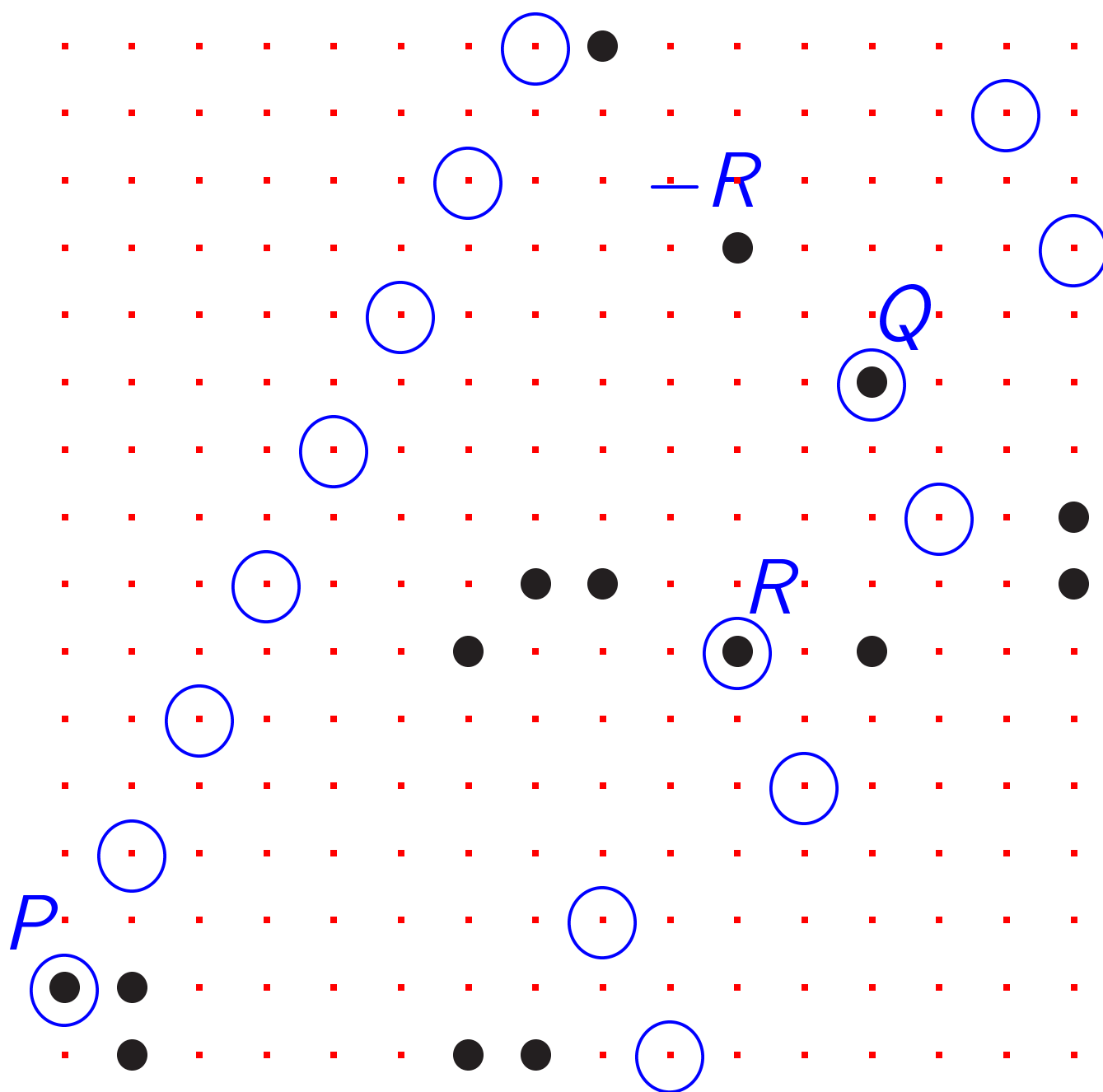
Graph of the “set of points on the elliptic curve  $y^2 - 5xy = x^3 - 7$  over  $(\mathbf{Z}/2)[t]/(t^4 - t - 1)$ ”:



Line  $y = tx + 1$ :



$$P + Q = -R:$$



## More elliptic curves

Can use any field  $k$ .

Can use any nonsingular curve

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

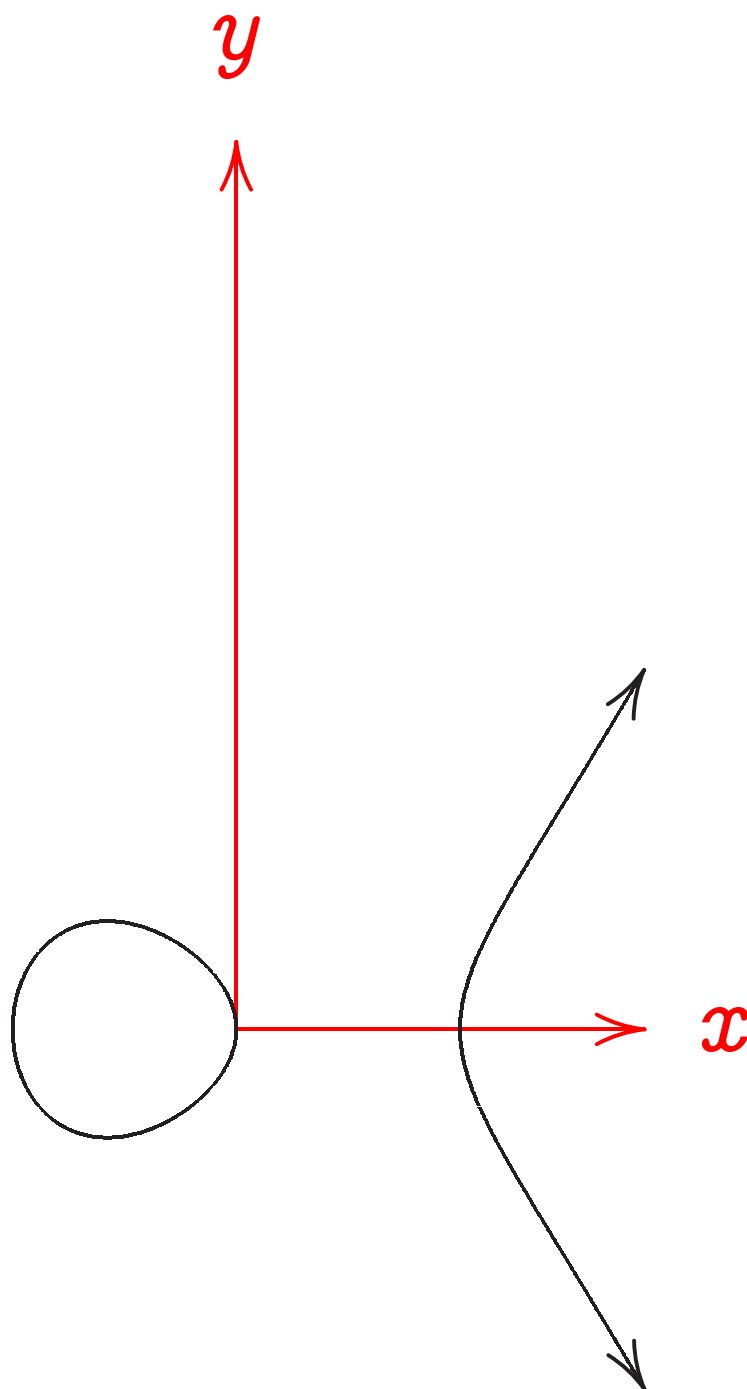
“Nonsingular”: no  $(x, y) \in k \times k$  simultaneously satisfies

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \text{ and } 2y + a_1x + a_3 = 0 \\ \text{and } a_1y = 3x^2 + 2a_2x + a_4.$$

Easy to check nonsingularity.

Almost all curves are nonsingular when  $k$  is large.

e.g.  $y^2 = x^3 - 30x$ :



$$\{(x, y) \in k \times k : \\ y^2 + a_1xy + a_3y = \\ x^3 + a_2x^2 + a_4x + a_6\} \cup \{\infty\}$$

is a commutative group with standard definition of  $0, -, +$ .

Points on line add to  $0$

with appropriate multiplicity.

Group is usually called “ $E(k)$ ” where  $E$  is “the elliptic curve

$$y^2 + a_1xy + a_3y = \\ x^3 + a_2x^2 + a_4x + a_6.”$$

Fairly easy to write down explicit formulas for  $0, -, +$  as before.

If  $\#k$  is finite

then  $\#E(k)$  is finite.

Each  $x$  produces 0, 1, or 2

choices of  $y$  with  $(x, y) \in E(k)$ .

So  $1 \leq \#E(k) \leq 2\#k + 1$ ;

i.e.,  $|\#E(k) - \#k - 1| \leq \#k$ .

Hasse's theorem:

$$|\#E(k) - \#k - 1| \leq 2\sqrt{\#k}.$$

For example, if  $k = \mathbf{Z}/10000003$ ,

then  $\#E(k) \in [998004, 1002004]$ .

Using explicit formulas

can quickly compute

$n$ th multiples in  $E(k)$

given  $n \in \{0, 1, 2, \dots, 2^{256} - 1\}$

and given  $E, k$  with  $\#k \approx 2^{256}$ .

(How quickly?)

See Peter Birkner's talk.)

“Elliptic-curve discrete-log  
problem” (ECDLP):

given points  $P$  and  $nP$ , find  $n$ .

Can find curves where

ECDLP seems extremely difficult:

$\approx 2^{128}$  operations.

See “Handbook of elliptic and hyperelliptic curve cryptography” for much more information.

Two examples of elliptic curves useful for cryptography:

“NIST P-256”:  $E(\mathbf{Z}/p)$

where  $p$  is the prime

$$2^{256} - 2^{224} + 2^{192} + 2^{96} - 1$$

and  $E$  is the elliptic curve  $y^2 = x^3 - 3x + (\text{a particular constant})$ .

“Curve25519”:  $E(\mathbf{Z}/p)$

where  $p$  is the prime  $2^{255} - 19$

and  $E$  is the elliptic curve

$$y^2 = x^3 + 486662x^2 + x.$$