ECDLP course

Other curves and choice of curves

Daniel J. Bernstein

University of Illinois at Chicago

Tanja Lange

Technische Universiteit Eindhoven

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

Easy to check nonsingularity.
Almost all curves are nonsingular when k is large.

An example over **R**

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

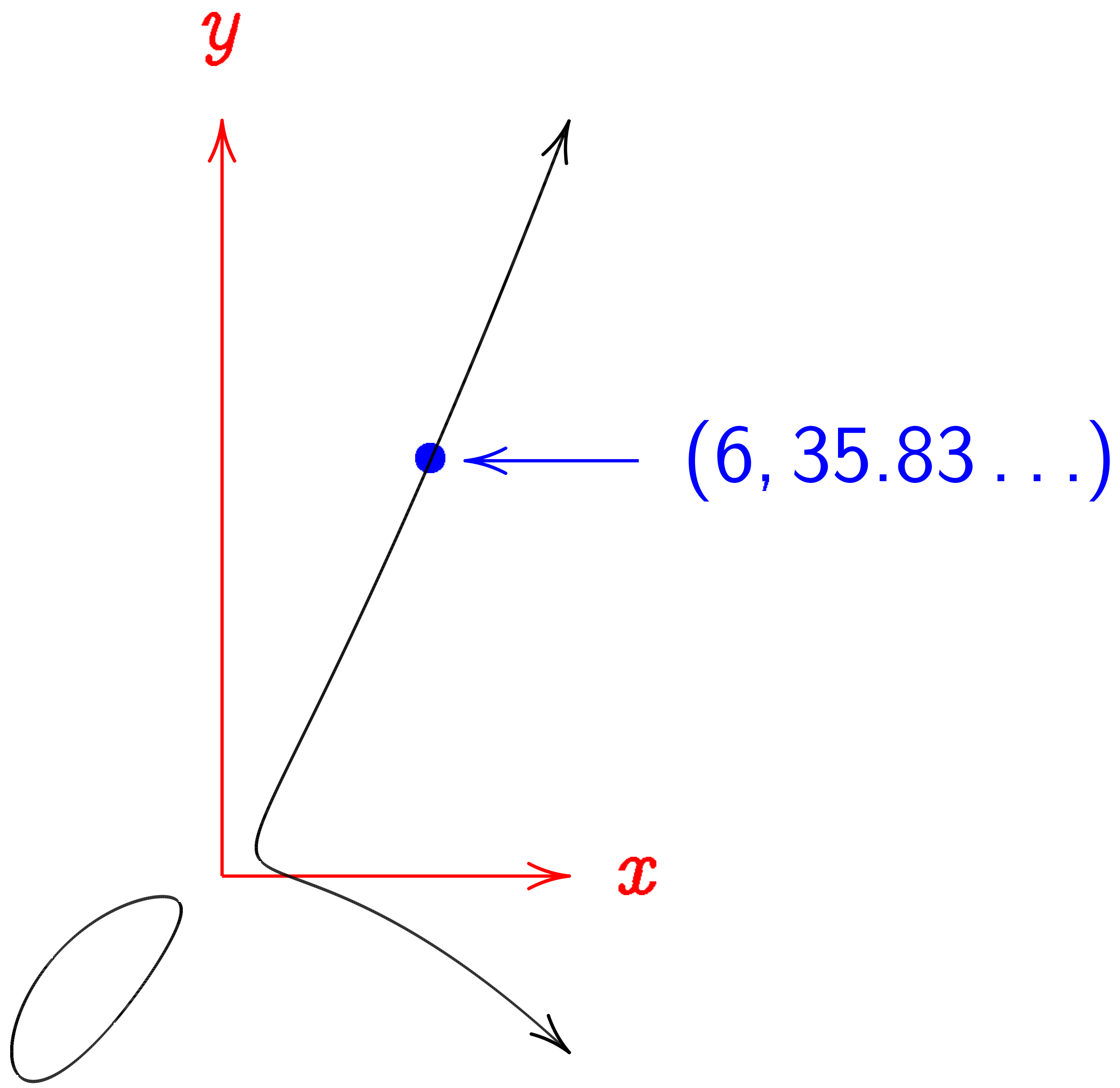
The "points on the elliptic curve
$y^2 - 5xy = x^3 - 7$ over **R**"
are those pairs and
one additional point, ∞.

i.e. The set of points is

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

(**R** is the set of real numbers.)

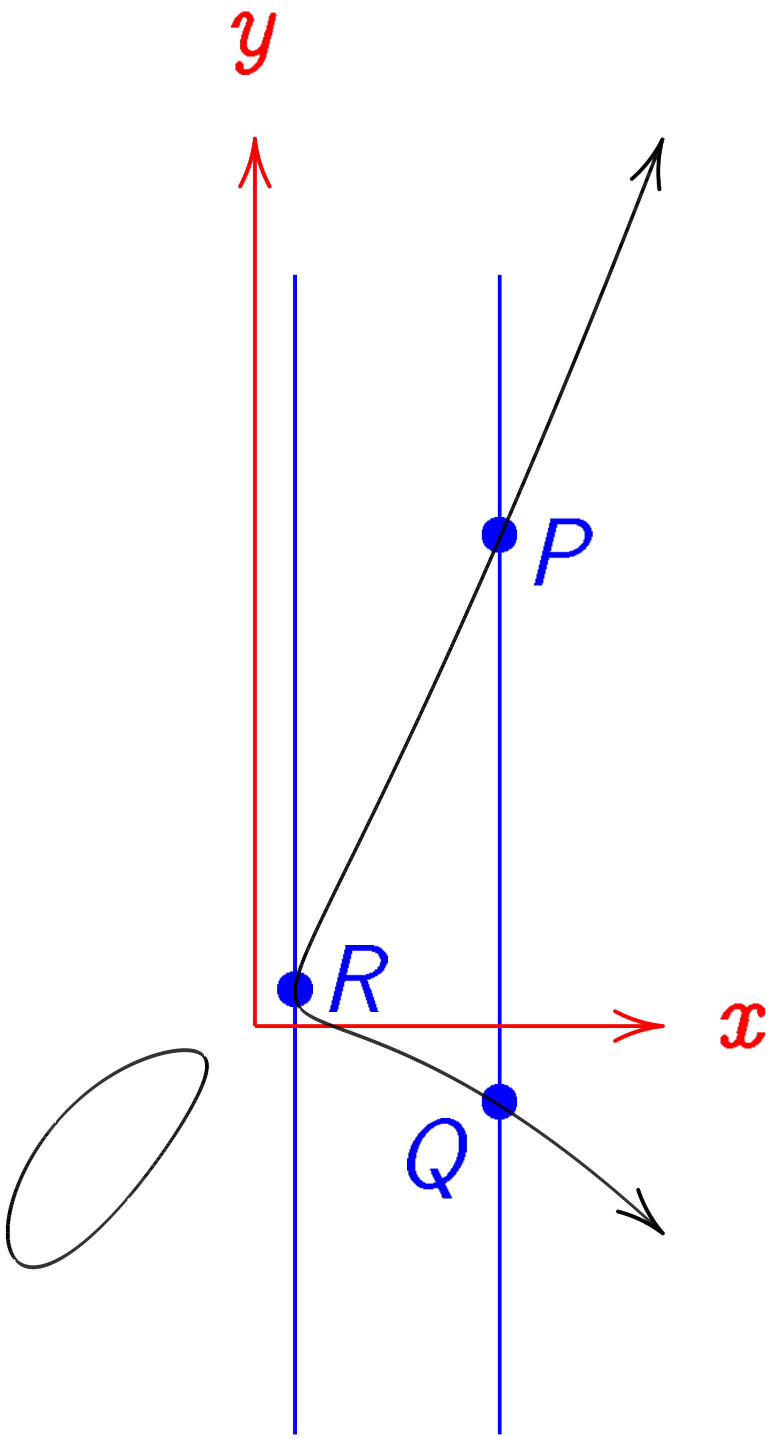
Graph of this set of points:



Don't forget ∞.

Visualize ∞ as top of y axis.

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

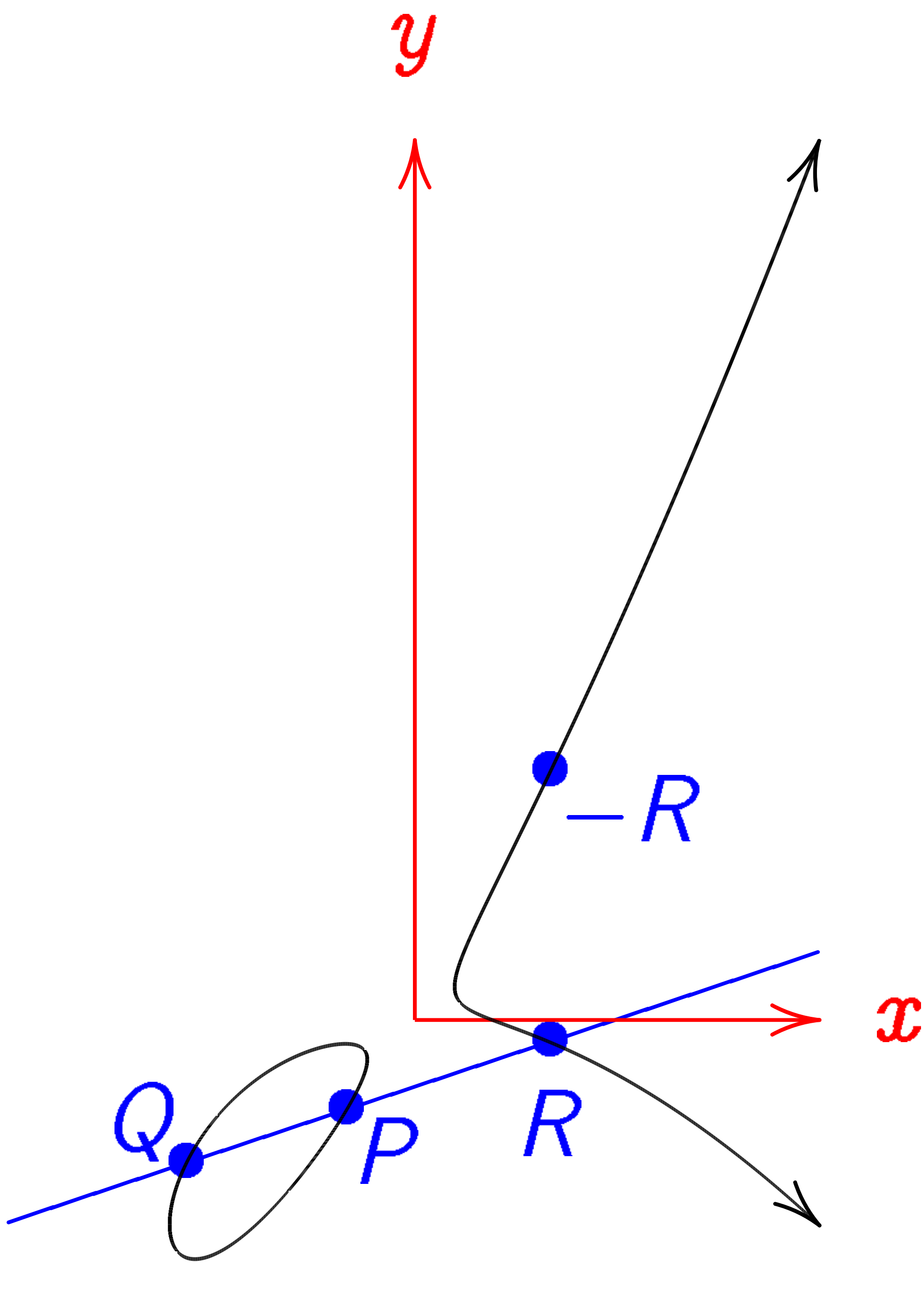


Distinct curve points P, Q, R
on a line
have $P + Q = -R$;
$P + Q + R = \infty$.

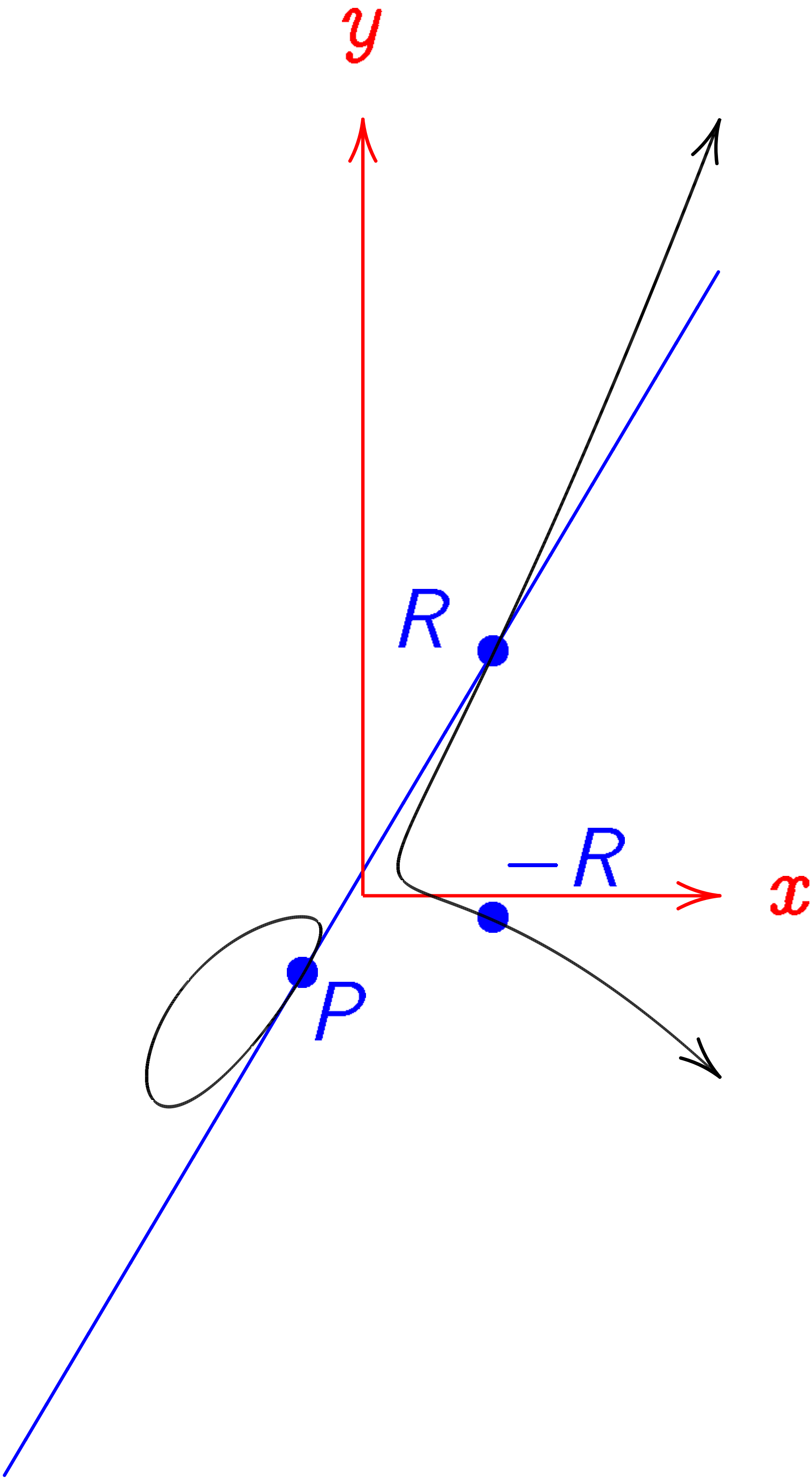
Distinct curve points P, R
on a line tangent at P
have $P + P = -R$;
$P + P + R = \infty$.

A non-vertical line
with only one curve point P
(a flex of the curve)
has $P + P = -P$;
$P + P + P = \infty$.

Here $P + Q = -R$:



Here $P + P = -R$:



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

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

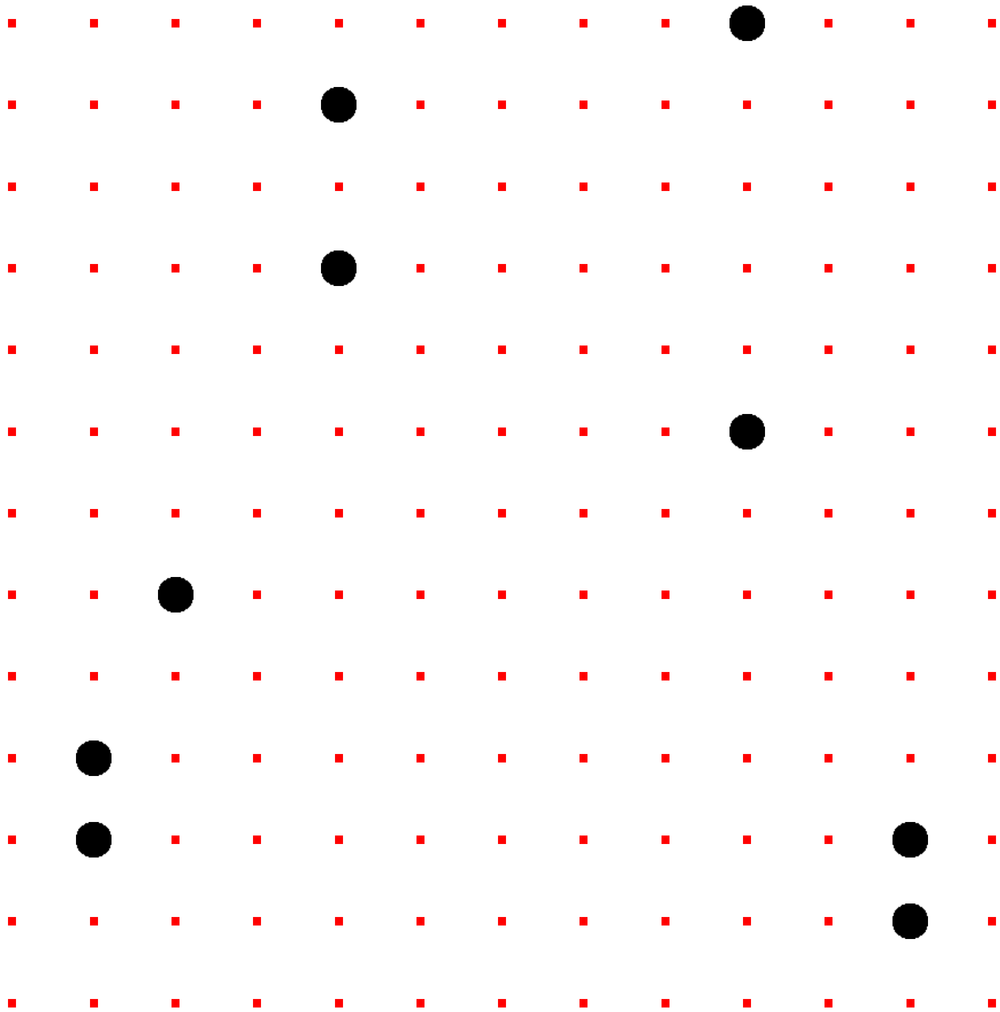
An elliptic curve over $\mathbf{Z}/13$

Consider the prime field
$\mathbf{Z}/13 = \{0, 1, 2, \ldots, 12\}$
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 ∞.

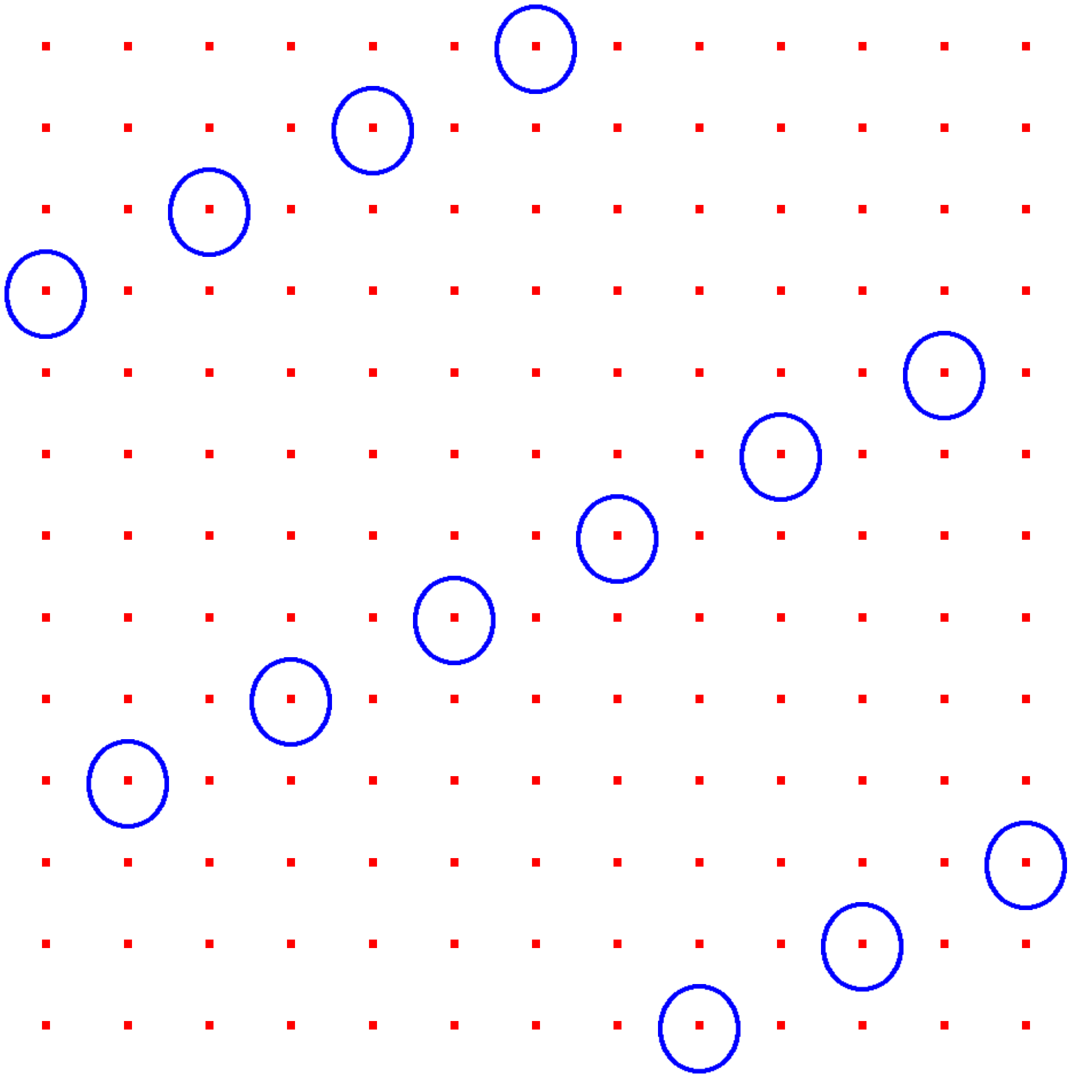
The set of curve points
is a commutative group with
standard definition of $\infty, -, +$.

Can visualize $\infty, -, +$ as before.
Replace lines over $\mathbf{R}$
by lines over $\mathbf{Z}/13$.

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

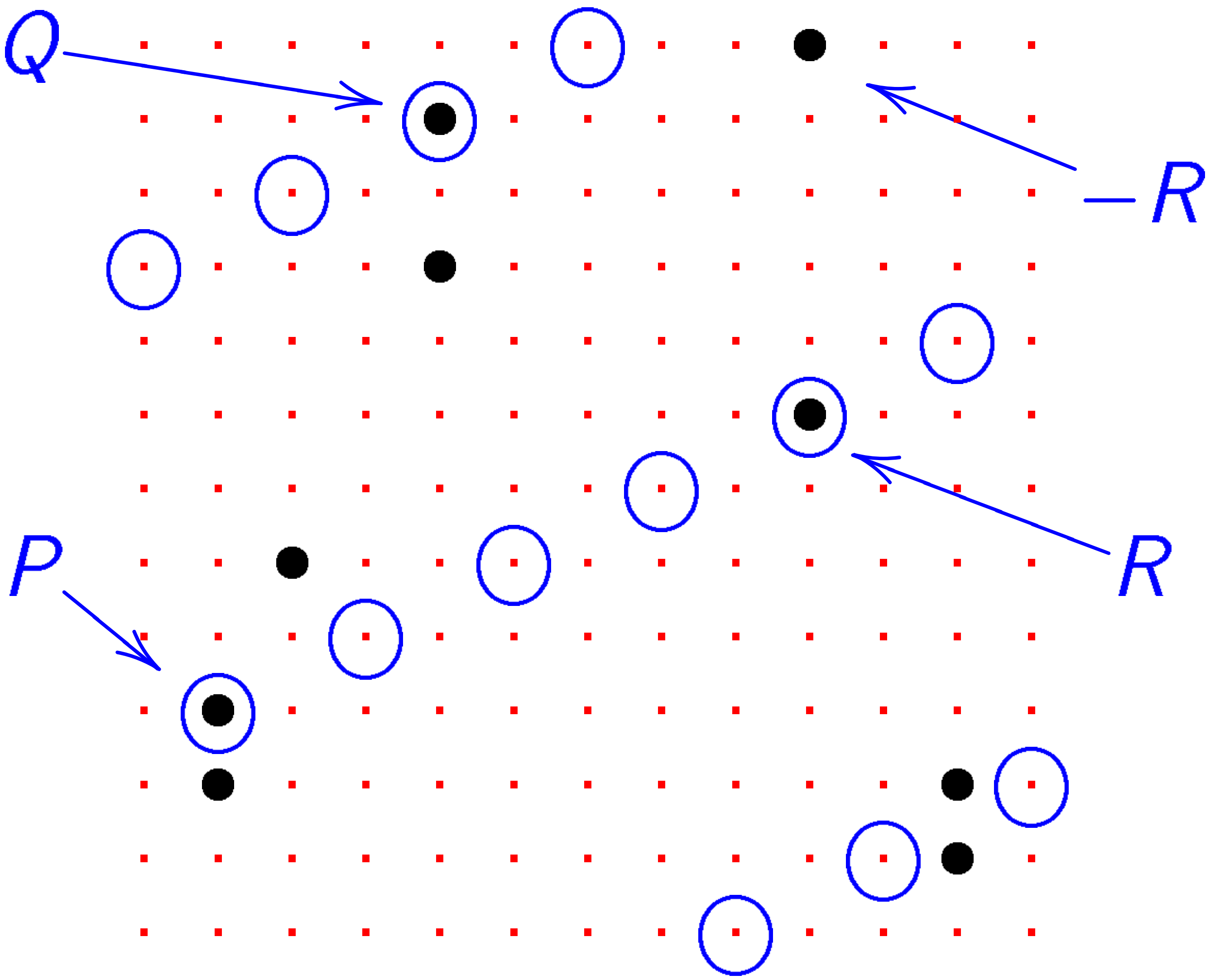
Can define $\infty, -, +$
using same formulas as before.

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



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

$P + Q = -R$:



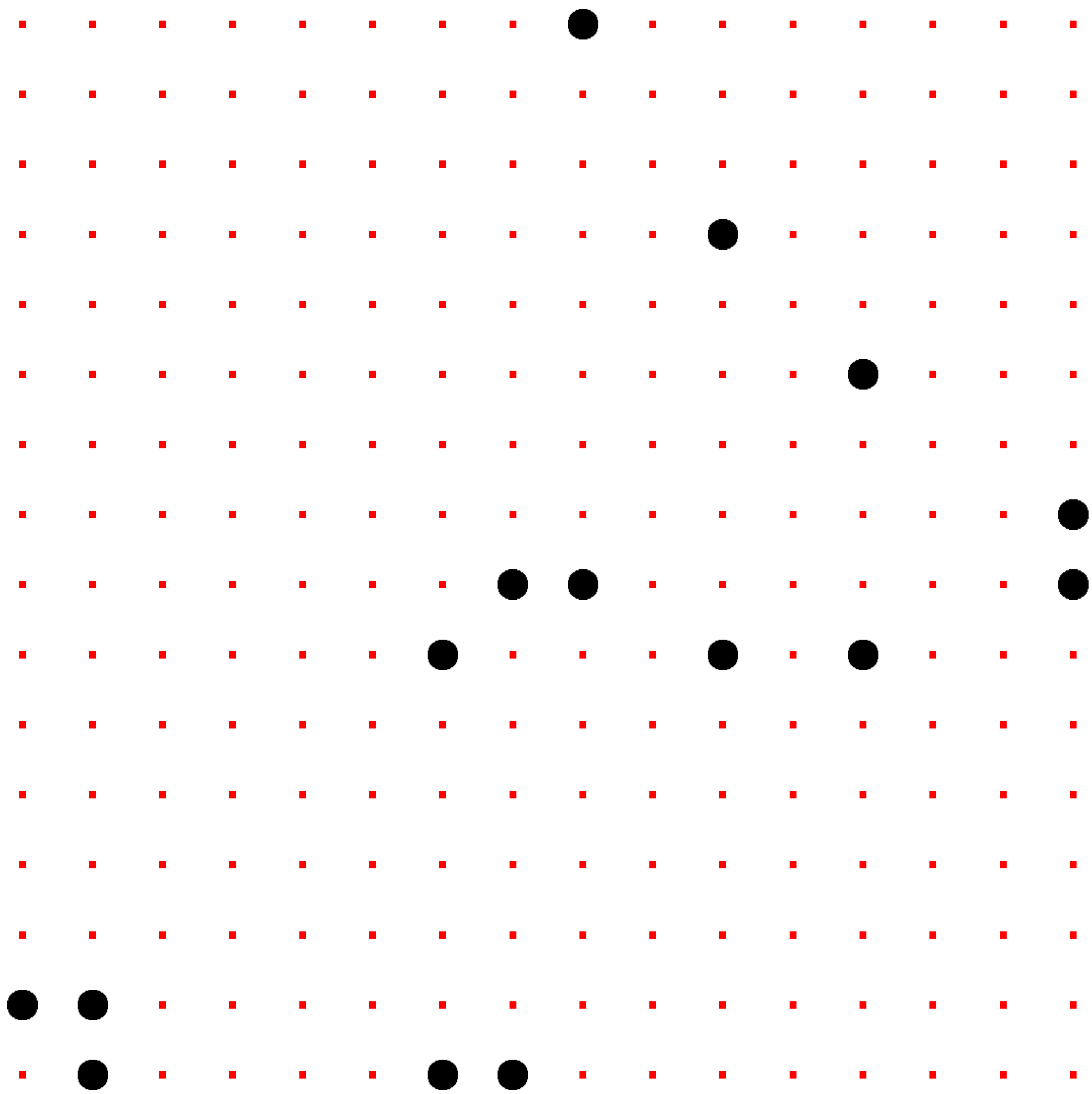
An elliptic curve over $\mathbf{F}_{16}$

Consider the non-prime field

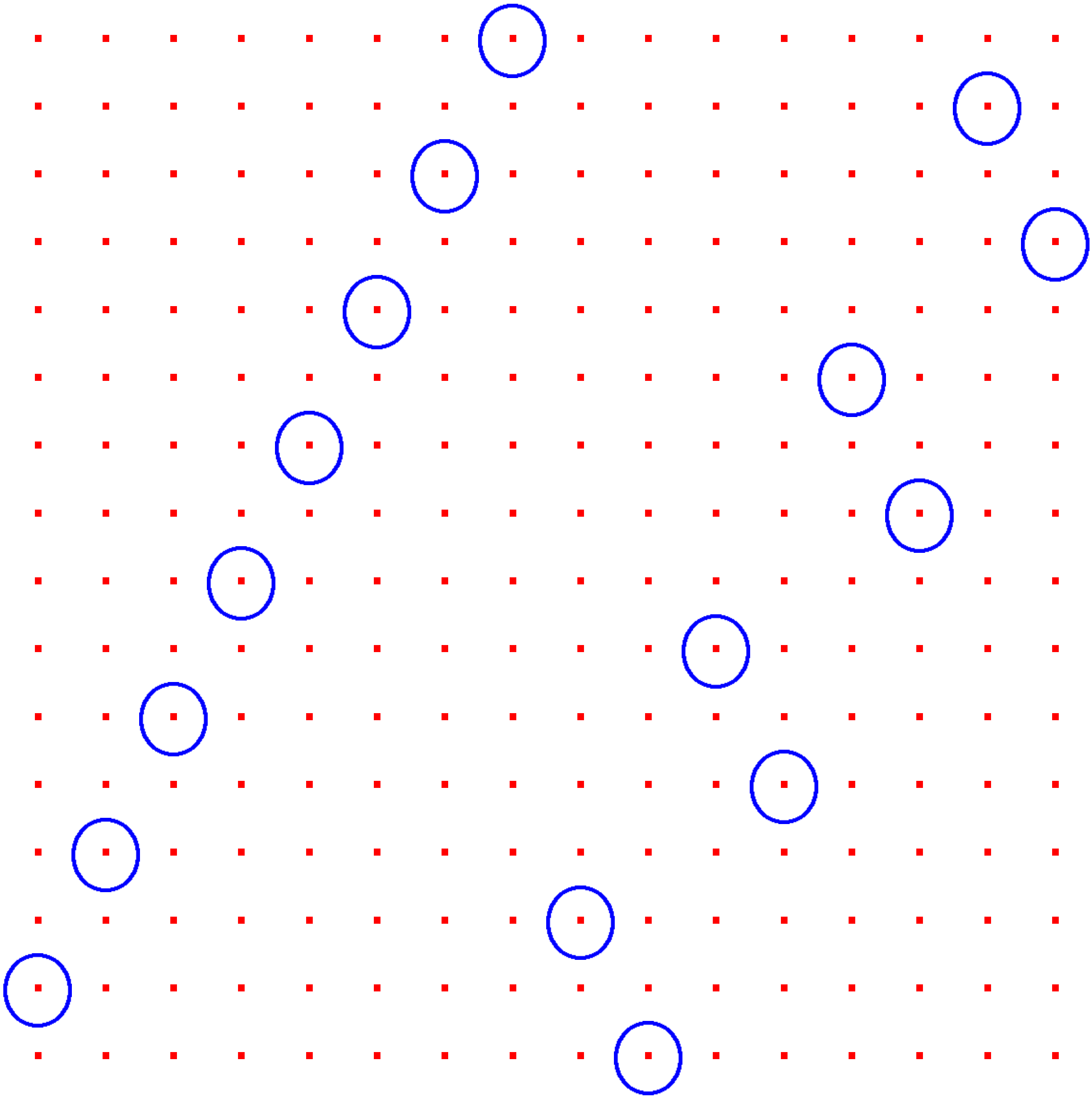
$$(\mathbf{Z}/2)[t]/(t^4 - t - 1) = \{$$
$$0t^3 + 0t^2 + 0t^1 + 0t^0,$$
$$0t^3 + 0t^2 + 0t^1 + 1t^0,$$
$$0t^3 + 0t^2 + 1t^1 + 0t^0,$$
$$0t^3 + 0t^2 + 1t^1 + 1t^0,$$
$$0t^3 + 1t^2 + 0t^1 + 0t^0,$$
$$\vdots$$
$$1t^3 + 1t^2 + 1t^1 + 1t^0\}$$

of size $2^4 = 16$.

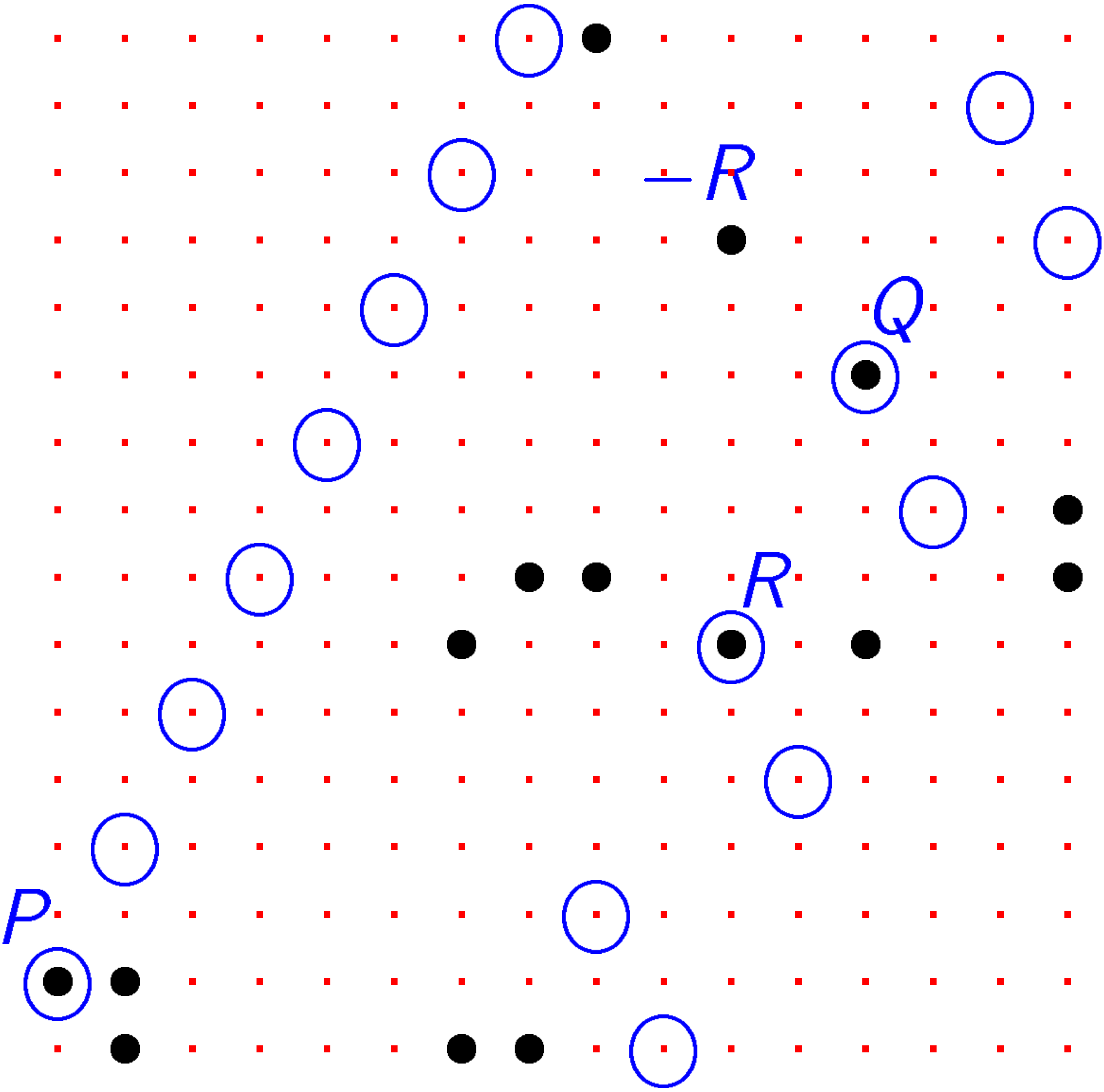
Graph of the "set of points on the elliptic curve $y^2 - 5xy = x^3 - 7$ over $(\mathbf{Z}/2)[t]/(t^4 - t - 1)$":



Line $y = tx + 1$:



$P + Q = -R$:



Why more coefficients?

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

"Nonsingular": no $(x, y) \in k \times k$ simultaneously satisfies $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ and $2y + a_1x + a_3 = 0$ and $a_1y = 3x^2 + 2a_2x + a_4$.

Easy to check nonsingularity.
Almost all curves are nonsingular when k is large.

Why more coefficients?

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

"Nonsingular": no $(x, y) \in k \times k$ simultaneously satisfies $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ and $2y + a_1x + a_3 = 0$ and $a_1y = 3x^2 + 2a_2x + a_4$.

$k = \mathbf{F}_{2^n}$, then partial derivatives become: $a_1x + a_3 = 0$ and $a_1y = x^2 + a_4$. Monday's curve shape had $a_1 = a_3 = 0$
$\Rightarrow$ only condition $x^2 = a_4$ and every element is a square in $\mathbf{F}_{2^n}$.

Isomorphic transformations

Elliptic curves over $\mathbf{F}_{2^n}$ need to have at least one of a_1 and a_3 non-zero.
Do *isomorphic transformations* linear transformations $y \mapsto a^3 y + bx + c$, $x \mapsto a^2 x + d$ to simplify curve equation.

If $a_1 \neq 0$ use a and d to map to $y^2 + xy = x^3 + a_2' x^2 + a_4' x + a_6'$ and c to achieve $a_4' = 0$.
b appears as $b^2 + b + a_2'$, can restrict coefficient of x^2 to two choices.

If $a_1 = 0$, put $b = 0$, $d = a_2$ to map to
$y^2 + a_3 y = x^3 + a'_4 x + a'_6$
c appears as $c^2 + a_3 c + a'_6$, can restrict constant term; can use a to restrict choice of a_3; if n odd can get $a_3 = 1$.

If $\mathrm{char}(k) \neq 2$ put $b = -a_1/2$ and $c = -a_3/2$ to map to
$y^2 = x^3 + a'_2 x^2 + a'_4 x + a'_6$.
If $\mathrm{char}(k) \neq 3$ can additionally remove a'_2 using d. Can use a to restrict a'_4 or a'_6.

Short Weierstrass forms

Over $\mathbf{F}_{2^n}$ can map to one of
$y^2 + xy = x^3 + a_2x^2 + a_6$
$y^2 + a_3y = x^3 + a_4x + a_6$
with $a_2, a_4, a_6 \in \mathbf{F}_{2^n}$;
$a_3 = 1$ for n odd.

Over $\mathbf{F}_q$, $q = p^n$, $p > 3$ can map
to $y^2 = x^3 + a_4x + a_6$
with $a_4, a_6 \in \mathbf{F}_q$.

Nice for proofs but arithmetic
might prefer other choices,
e.g. Montgomery curves
$y^2 = x^3 + a_2x^2 + x$ over $\mathbf{F}_q$
are faster than above form.

Quadratic twists

Over $\mathbf{F}_q$, $q = p^n$, $p > 3$
still have freedom to map
$E : y^2 = x^3 + a_4 x + a_6$ to
$E' : y^2 = x^3 + a_4/c^4 x + a_6/c^6$
using $y \mapsto c^3 y$, $x \mapsto c^2 x$, $c \in \mathbf{F}_q$.

For $d \in \mathbf{F}_q$, curve
$\tilde{E} : y^2 = x^3 + a_4/d^2 x + a_6/d^3$
is defined over $\mathbf{F}_q$ but
isomorphism is defined over $\mathbf{F}_q$
only if d is a square in $\mathbf{F}_q$.
$\tilde{E}$ is a *quadratic twist* of E. This
concept includes isomorphisms.
Only *one* non-isomorphic class.

General addition law

$$E : y^2 + \underbrace{(a_1 x + a_3)}_{h(x)} y =$$

$$\underbrace{x^3 + a_2 x^2 + a_4 x + a_6}_{f(x)}, h, f \in \mathbf{F}_q[x].$$

$$-(x_P, y_P) = (x_P, -y_P - h(x_P)).$$

$$(x_P, y_P) + (x_R, y_R) = (x_3, y_3) =$$
$$= (\lambda^2 + a_1\lambda - a_2 - x_P - x_R,$$
$$\lambda(x_P - x_3) - y_P - a_1 x_3 - a_3),$$

where $\lambda =$

$$\begin{cases} (y_R - y_P)/(x_R - x_P) & x_P \neq x_R, \\ \frac{3x_P^2 + 2a_2 x_P + a_4 - a_1 y_P}{2y_P + a_1 x_P + a_3} & P = R \neq -R \end{cases}$$

Number of points

Number of points over finite field is finite.

Hasse's theorem:

$$\#E(\mathbf{F}_q) = q + 1 - t,$$

with $|t| \le 2\sqrt{q}$.

t is called the trace of E.

Each point has finite order dividing $\#E(\mathbf{F}_q)$.

Want to work in (sub-)group of prime order ℓ (Pohlig-Hellman attack).

Why characteristic 2?

Large char is slower in hardware than char 2, but char 2 is slower in software than large char.

Typical CPU includes circuits for integer multiplication, not for poly mult mod 2.

Situation somewhat improved with latest generation of processors having PCLMULQDQ (Carry-Less Multiplication) instructions.

System might focus on hardware users (low power devices need every speedup they can get; server can handle slowdown).

Doubling somewhat easier:
On $y^2 + xy = x^3 + ax^2 + b$ have
$\lambda = (x^2 + y)/x = x + y/x$,
so ADD and DBL each take
$1\mathbf{I} + 2\mathbf{M} + 1\mathbf{S}$.

If computing square-roots is fast (normal-basis representation) can improve speed using *halving*.

$1\mathbf{I}/\mathbf{M}$ smaller than in odd characteristic fields.

Other curve shapes

The EFD features 3 curve shapes in characteristic 2:

Binary Edwards curves:
$d_1(x+y) + d_2(x^2+y^2) =$
$(x+x^2)(y+y^2)$

Hessian curves:
$x^3 + y^3 + 1 = dxy$

Short Weierstrass curves:
$y^2 + xy = x^3 + a_2x^2 + a_6$

For reasons stated later skips
$y^2 + y = x^3 + a_4x + a_6$.

Koblitz curves

Let $q = p^n$ for small p and big n.
$y^2 + h(x)y = f(x)$
over $\mathbf{F}_q$ is called a *Koblitz curve*
if it is defined over $\mathbf{F}_p$, i.e., if
$h(x), f(x) \in \mathbf{F}_p[x]$.

p need not be prime; $p = 4$ is also small.

Typical case: $p = 2$. This is the case proposed by Koblitz; also called *anomalous binary curves*.

Frobenius map

Take $E_a : y^2 + xy = x^3 + ax^2 + 1$, with $a \in \{0, 1\}$ as curve over $\mathbf{F}_{2^n}$ and let $P = (x_P, y_P) \in E_a(\mathbf{F}_{2^n})$.

Then $\sigma(P) = (x_P^2, y_P^2)$ is also a point in $E_a(\mathbf{F}_{2^n})$:

$$y_P^2 + y_P = x_P^3 + ax_P^2 + 1 \Leftrightarrow$$
$$(y_P^2 + y_P)^2 = (x_P^3 + ax_P^2 + 1)^2 \Leftrightarrow$$
$$(y_P^2)^2 + y_P^2 = (x_P^3)^2 + a^2(x_P^2)^2 + 1^2$$
$$\Leftrightarrow$$
$$(y_P^2)^2 + y_P^2 = (x_P^2)^3 + a(x_P^2)^2 + 1$$

since $a^2 = a$.

This means (x_P^2, y_P^2) satisfies the curve equation.

Take $E : y^2 + h(x)y = f(x)$,
with $h(x), f(x) \in \mathbf{F}_p[x]$ as curve over $\mathbf{F}_{p^n}$
and let $P = (x_P, y_P) \in E(\mathbf{F}_{p^n})$.

Then $\sigma(P) = (x_P^p, y_P^p)$ is also a point in $E_a(\mathbf{F}_{p^n})$:

Proof uses that Frobenius automorphism is linear
$(a + b)^p = a^p + b^p$
and that $c^p = c$ for $c \in \mathbf{F}_p$.

The map σ is called the *Frobenius endomorphism* of E.

Properties of Koblitz curves

Let $\#E(\mathbf{F}_p) = p + 1 - t$ and let $T^2 - tT + p = (T - \tau)(t - \bar{\tau})$ then

$$\#E(\mathbf{F}_{p^n}) = (1 - \tau^n)(1 - \bar{\tau}^n).$$

Easy computation of number of points – but shows restriction: if $m|n$ then $\#E(\mathbf{F}_{p^m})|\#E(\mathbf{F}_{p^n})$, so require *prime* n to have large prime order subgroup.

$$\chi(T) = T^2 - tT + p$$

called *characteristic polynomial of the Frobenius endomorphism*.

Each $P \in E(\mathbf{F}_{p^n})$ satisfies
$\sigma^2(P) - t\sigma(P) + pP = \infty$.

Each $P \in E(\mathbf{F}_{p^n})$ satisfies
$\sigma^2(P) - t\sigma(P) + pP = \infty$.

This means
$pP = t\sigma(P) - \sigma^2(P)$
for $t \in [-2\sqrt{p}, 2\sqrt{p}]$.

Each $P \in E(\mathbf{F}_{p^n})$ satisfies
$\sigma^2(P) - t\sigma(P) + pP = \infty$.

This means
$pP = t\sigma(P) - \sigma^2(P)$
for $t \in [-2\sqrt{p}, 2\sqrt{p}]$.

Expand integer k in base τ
$k = \sum k_i \tau^i$, with
$k_i \in [-\lfloor (p-1)/2 \rfloor, \lceil (p-1)/2 \rceil]$
and compute
$kP = \sum k_i \sigma^i(P)$.

Each $P \in E(\mathbf{F}_{p^n})$ satisfies
$\sigma^2(P) - t\sigma(P) + pP = \infty$.

This means
$pP = t\sigma(P) - \sigma^2(P)$
for $t \in [-2\sqrt{p}, 2\sqrt{p}]$.

Expand integer k in base τ
$k = \sum k_i \tau^i$, with
$k_i \in [-\lfloor (p-1)/2 \rfloor, \lceil (p-1)/2 \rceil]$
and compute
$kP = \sum k_i \sigma^i(P)$.
Density of expansion similar to base p expansion, same set of coefficients – but computing $\sigma(P)$ is much cheaper than pP.

Case $p = 2$: $T^2 + (-1)^a T + 2 = 0$

DBL costs $1\mathbf{I} + 2\mathbf{M} + 1\mathbf{S}$.

σ costs $2\mathbf{S}$.

Few tricks (Meier-Staffelbach, Solinas)

$kP = \sum_{i=0}^{n} k_i \sigma^i(P)$,
$k_i \in \{0, 1\}$ for $P \in E(\mathbf{F}_{2^n})$
has average density $1/2$.

$kP = \sum_{i=0}^{n+1} k_i \sigma^i(P)$,
$k_i \in \{-1, 0, 1\}$ for $P \in E(\mathbf{F}_{2^n})$
has average density $1/3$.

Similar to binary and NAF expansion; generalizations of other methods exist.

General case:
Frobenius endomorphism makes scalar multiplications faster.

Optimal extension fields – medium size p and n – get some benefit, too.
OEF assumes p fits word size.

Most extreme cases:
Prime order subgroup $\leq p^{n-1}$.
$n = 3$ or 5: *trace-zero varieties*
$n = 2$: not worthwhile.

Some attacks – see tomorrow – but not devastating, except for some bad choices.

Other curves with endomorphisms

Gallant-Lambert-Vanstone:

When E has equation
$y^2 = x^3 + ax$ over $\mathbf{F}_p$
with $p \equiv 1 \pmod 4$.
$\phi\colon E \to E$, $(x, y) \mapsto (-x, \sqrt{-1}y)$
Note that $\phi^2 + 1 = 0$.

When E has equation
$y^2 = x^3 + b$ over $\mathbf{F}_p$
with $p \equiv 1 \pmod 3$.
Let $\xi_3 = (1 - \sqrt{-3})/2$.
$\phi\colon E \to E$, $(x, y) \mapsto (\xi_3 x, y)$
Note that $\phi^2 + \phi + 1 = 0$.

Bigger example of GLV method:

When E has equation

$y^2 = x^3 - 3x^2/4 - 2x - 1$ over $\mathbf{F}_p$

with $p \equiv 1, 2$ or $4 \pmod 7$.

Denote $\xi = (1 + \sqrt{-7})/2$ and

$a = (\xi - 3)/4$.

ϕ: $E \to E$,

$$(x, y) \mapsto \left(\frac{x^2 - \xi}{\xi^2(x-a)}, \frac{y(x^2 - 2ax + \xi)}{\xi^3(x-a)^2} \right)$$

Note that $\phi^2 - \phi + 2 = 0$.

Computation of $Q = kP$

Gallant-Lambert-Vanstone method, where endomorphism ϕ is different from the Frobenius σ.

Write
$kP = k^{(0)}P + k^{(1)}\phi(P)$,
$\max\left\{|k^{(0)}|, |k^{(1)}|\right\} = O(\sqrt{\ell})$

Key points:
Each $k^{(i)}$ is half as long as $k \in [1, \ell]$.
Computing $\phi(P)$ is easy.
Use Joint Sparse Form to quickly evaluate double scalar multiplication.

Combination

GLV curves are rare.

Galbraith-Lin-Scott (GLS)
use Frobenius σ with $n = 2$
– and avoids having big subgroup!

Let E be an elliptic curve defined over $\mathbf{F}_{p^2}$.
Quadratic twist of
$E : y^2 = x^3 + a_4 x + a_6$ is
$\tilde{E} : y^2 = x^3 + a_4/c^2 x + a_6/c^3$,
$c \in \mathbf{F}_{p^2}$ and $c \neq \blacksquare$ over $\mathbf{F}_{p^2}$.
Start with $\tilde{E}$ over $\mathbf{F}_p$.
(Aha, the subfield idea comes in!)
and pick nonsquare $c \in \mathbf{F}_{p^2}$.

$\tilde{E} : y^2 = x^3 + b_4 x + b_6$; $b_4, b_6 \in \mathbf{F}_p$.

Gets E over $\mathbf{F}_{p^2}$:

$E : y^2 = x^3 + b_4 c^2 x + b_6 c^3$,

$b_4 c^2, b_6 c^3 \in \mathbf{F}_{p^2}$.

No reason that E cannot have (almost) prime order.

Yet E closely related to curve with Frobenius endomorphism.

Define $\psi : E \to E$ as map from E to $\tilde{E}$, followed by p-th power Frobenius on $\tilde{E}$, followed by map back to E.

ψ satisfies $\psi^2 + 1 = 0$ on points of order $\geq 2p$ on E. Can use all GLV tricks; many more curves.

Interlude:

Index calculus in prime fields

Index calculus is a method to compute discrete logarithms. Works in many situations but depends on group (not generic attack)

p prime, elements of $\mathbf{F}_p$ represented by numbers in $\{0, 1, \ldots, p-1\}$;
g generator of multiplicative group.

If $h \in \mathbf{F}_p$ factors as
$h = h_1 \cdot h_2 \cdots h_n$ then

$$h = g^{a_1} \cdot g^{a_2} \cdots g^{a_n}$$
$$= g^{a_1 + a_2 + \ldots + a_n},$$

with $h_i = g^{a_i}$.

Knowledge of the a_i,
i.e., of the discrete logarithms of h_i to base g,
gives knowledge of the discrete logarithm of h to base g.

If h factors appropriately . . .

If h factors appropriately?!

Ensure by finding h' s.t. $h \cdot h'$ and h' factor over the h_i.
So far: instead of finding *one* DL we have to find *many* DLs *and* they have to fit to h *and* we have to find a suitable h' *and* factor numbers.

Two different settings –
the integers modulo p and
the integers themselves.
Factorization takes place over **Z**, while the left hand side is reduced modulo p.

Select $F = \{g_1, g_2, \ldots, g_m\}$
so that $\bar{h} < p$ is likely to factor
into powers of g_i.
F called *factor base*.

An equation of form
$\bar{h} = g_1^{n_1} \cdot g_2^{n_2} \cdots g_m^{n_m}$,
with $n_i \in \mathbf{Z}$ is called a *relation*.
Choose F as small primes , e.g.
$g_1 = 2, g_2 = 3, g_3 = 5, \ldots$

Generate many relations with
known DL of $\tilde{h}_j = g^{k_j}$
$\tilde{h}_j = g^{k_j} = g_1^{n_{j1}} \cdot g_2^{n_{j2}} \cdots g_m^{n_{jm}}$.
(This means discarding
g^{k_j} if it does not factor .)

Matrix of relations

For each relation
$\tilde{h}_j = g^{k_j} = g_1^{n_{j1}} \cdot g_2^{n_{j2}} \cdots g_m^{n_{jm}}$

enter the row

$$(n_{j1} n_{j2} \ldots n_{jm} | k_j)$$

into a matrix $M =$

$$\begin{pmatrix} n_{11} & \ldots & n_{1i} & \ldots & n_{m1} & k_1 \\ n_{21} & \ldots & n_{2i} & \ldots & n_{m2} & k_2 \\ \vdots & & \vdots & & \vdots & \vdots \\ n_{l1} & \ldots & n_{li} & \ldots & n_{lm} & k_l \end{pmatrix}$$

The i-th column

corresponds to the unknown a_i

so that $g_i = g^{a_i}$.

Computing DLPs

Use linear algebra to solve for a_is.
This step does not depend on the target DLP $h = g^a$.
A single relation $h \cdot g^k$ factoring over F gives the DLP.

Running time (with much more clever way of finding relations)
$O(\exp(c \log p^{1/3} \log(\log p)^{2/3}))$
for some c.
This is subexponential in $\log p$!

Similar for $\mathbf{F}_{2^n}$

Elements of $\mathbf{F}_{2^n}$ are represented as $\mathbf{F}_{2^n} = \{\sum_{i=0}^{n-1} c_i x^i | c_i \in \mathbf{F}_2, 0 \leq i < n\}$, i.e. polynomials of degree less than n modulo an irreducible polynomial $f(x) \in \mathbf{F}_2[x]$.

Factoring into powers of small primes is replaced by factoring into irreducible polynomials of small degree.

Same approach works; even somewhat faster
$O(\exp(c' \log p^{1/3} \log(\log p)^{2/3}))$
for some smaller c'.

Same approach works; even somewhat faster
$O(\exp(c' \log p^{1/3} \log(\log p)^{2/3}))$
for some smaller c'.

More recent result (2006):
For $\mathbf{F}_q = \mathbf{F}_{p^n}$ use mix of both approaches
$O(\exp(c'' \log p^{1/3} \log(\log p)^{2/3}))$
for some c''.

Very small factorbase

Restrict F to linear polynomials.
So $|F| = p$.
Number of $f \in \mathbf{F}_p[x]$, $\deg(f) < n$ splitting over $F \approx \frac{1}{n!}p^n$.
$\#\{f \in \mathbf{F}_p[x] | \deg(f) < n\} = p^n$.

Probability of splitting in reduced factor base is $\frac{\sim 1}{n!}$.

Need $O(n!p)$ tries to find p relations, $O(p^2)$ for sparse matrix.
For n fixed, p growing the running time $O(n!p + p^2)$ translates to $O(p^2)$
Very fast – beware of constants!

Tiny factorbase

Take
$F \subseteq \{f \in \mathbf{F}_p[x] | \deg(f) = 1\}$
with $\#F = p^r$ for some $r \in (0, 1)$.
Gives $\tilde{O}(p^{2-\frac{2}{n+1}})$.

Use large prime variation, i.e. have a further set F' of elements for which relations are accepted. Then for each of them linear algebra is used to cancel them out (slightly more entries per row).
Use double large prime variation, . . .

Relevance for ECC?

End up in finite fields after pairings.

Weil descent maps to curve of larger genus, where index calculus attacks are applicable.

Pairings

Let $(G_1, +), (G_1', +)$ and $(G, \cdot)$ be groups of prime order ℓ and let
$e : G_1 \times G_1' \to G$
be a map satisfying
$e(P + Q, R') = e(P, R')e(Q, R')$,
$e(P, R' + S') = e(P, R')e(P, S')$.

Request further that e is non-degenerate in the first argument, i.e., if for some P
$e(P, R') = 1$ for all $R' \in G_1'$,
then P is the identity in G_1

Such an e is called a *bilinear map* or *pairing*.

Consequences of pairings

Assume that $G_1 = G_1'$,
in particular $e(P, P) \neq 1$.

Then for all triples
$(P_1, P_2, P_3) \in \langle P \rangle^3$
one can decide in time polynomial
in $\log \ell$ whether
$\log_P(P_3) = \log_P(P_1) \log_P(P_2)$
by comparing
$e(P_1, P_2)$ and $e(P, P_3)$.
This means that the decisional
Diffie-Hellman problem is easy.

The DL system G_1 is at most as secure as the system G.

Even if $G_1 \neq G_1'$ one can transfer the DLP in G_1 to a DLP in G, provided one can find an element $P' \in G_1'$ such that the map $P \to e(P, P')$ is injective.

Pairings are interesting attack tool if DLP in G is easier to solve; e.g. if G has index calculus attacks.

We want to define pairings
$G_1 \times G_1' \to G$
preserving the group structure.

The pairings we will use
map to the multiplicative group of
a finite extension field $\mathbf{F}_{q^k}$.

To embed the points of order ℓ
into $\mathbf{F}_{q^k}$ there need to be ℓ-th
roots of unity are in $\mathbf{F}^*_{q^k}$.

The *embedding degree* k satisfies
k is minimal with $\ell \mid q^k - 1$.

E is supersingular if
$E[p^s](\overline{\mathbf{F}}_q) = \{P_\infty\}$.
$t \equiv 0 \bmod p$.
End_E is order in quaternion algebra.

Otherwise it is ordinary and one has $E[p^s](\overline{\mathbf{F}}_q) = \mathbf{Z}/p^s\mathbf{Z}$.
These statements hold for all s if they hold for one.

Example:
$y^2 + y = x^3 + a_4 x + a_6$ over $\mathbf{F}_{2^r}$ is supersingular, as a point of order 2 would satisfy $y_P = y_P + 1$ which is impossible.

Embedding degrees

Let E be supersingular and $p \geq 5$, i.e $p > 2\sqrt{p}$.

Hasse's Theorem states $|t| \leq 2\sqrt{q}$.
E supersingular implies $t \equiv 0 \bmod p$, so $t = 0$ and $|E(\mathbf{F}_p)| = p + 1$.

Obviously
$(p+1) \mid p^2 - 1 = (p+1)(p-1)$
so $k \leq 2$ for supersingular curves over prime fields.

Distortion maps

For supersingular curves there exist maps
$\phi : E(\mathbf{F}_q) \to E(\mathbf{F}_{q^k})$
i.e. maps $G_1 \to G_1'$, giving
$\tilde{e}(P, P) \neq 1$ for $\tilde{e}(P, P) = e(P, \phi(P))$.
Such a map is called a *distortion map*.

These maps are important since the only pairings we know how to compute are variants of *Weil pairing* and *Tate pairing* which have $e(P, P) = 1$.

Examples:
$y^2 = x^3 + a_4 x$,
for $p \equiv 3 \pmod 4$.
Distortion map
$(x, y) \mapsto (-x, \sqrt{-1}y)$.

$y^2 = x^3 + a_6$, for $p \equiv 2 \pmod 3$.
Distortion map $(x, y) \mapsto (jx, y)$
with $j^3 = 1, j \neq 1$.

In both cases, $\#E(\mathbf{F}_p) = p + 1$,
so $k = 2$.

Example from Tuesday:

$p = 1000003 \equiv 3 \bmod 4$ and $y^2 = x^3 - x$ over $\mathbf{F}_p$.

Has $1000004 = p + 1$ points.

$P = (101384, 614510)$ is a point of order 500002.

$nP = (670366, 740819)$.

Construct $\mathbf{F}_{p^2}$ as $\mathbf{F}_p(i)$.

$\phi(P) = (898619, 614510i)$.

Invoke the magma and compute

$e(P, \phi(P)) = 387265 + 276048i$;

$e(Q, \phi(P)) = 609466 + 807033i$.

Solve with index calculus to get $n = 78654$.

(Btw. this is the clock).

Summary of pairings

Menezes, Okamoto, and Vanstone for E supersingular:
For $p = 2$ have $k \leq 4$.
For $p = 3$ we $k \leq 6$
Over $\mathbf{F}_p$, $p \geq 5$ have $k \leq 2$.
These bounds are attained.

Not only supersingular curves:
MNT curves are non-supersingular curves with small k.
Other examples constructed for pairing-based cryptography –
but small k unlikely to occur for random curve.

Summary of other attacks

Definition of embedding degree does not cover all attacks.
For $\mathbf{F}_{p^n}$ watch out that pairing can map to $\mathbf{F}_{p^{km}}$ with $m < n$.
Watch out for this when selecting curves over $\mathbf{F}_{p^n}$!

Anomalous curves:
If $E/\mathbf{F}_p$ has $\#E(\mathbf{F}_p) = p$ then transfer $E(\mathbf{F}_p)$ to $(\mathbf{F}_p, +)$.
Very easy DLP.
Not a problem for Koblitz curves, attack applies to order-p subgroup.

Weil descent:
Maps DLP in E over $\mathbf{F}_{p^{mn}}$
to DLP on variety J over $\mathbf{F}_{p^n}$.
J has larger dimension; elements represented as polynomials of low degree. $\Rightarrow$ index calculus.

This is efficient if dimension of J is not too big.

Particularly nice to compute with J if it is the Jacobian of a hyperelliptic curve C.
For genus g get complexity $\tilde{O}(p^{2-\frac{2}{g+1}})$ with the factor base described before, since polynomials have degree $<= g$.