Elliptic curves mod p

~ or: $GF(p^k)$

EG $E: y^2 = x^3 - x + 9 \mod 7$, $9 \equiv 2$

x	± 1	± 2	± 3
x^2	1	-3	2

List all points.

$(0, \pm 3)$ — $x=0$: $y^2 = 0^3 - 0 + 9 \equiv 2 \rightsquigarrow y \equiv \pm 3$

$(1, \pm 3)$ — $x=1$: $y^2 = 1^3 - 1 + 9 \equiv 2 \rightsquigarrow y \equiv \pm 3$

$(2, \pm 1)$ — $x=2$: $y^2 = 2^3 - 2 + 9 = 15 \equiv 1 \rightsquigarrow y \equiv \pm 1$

$x=3$: $y^2 = 3^3 - 3 + 9 \equiv -2 \rightsquigarrow$ no sol.

$x=-3$: $y^2 = (-3)^3 - (-3) + 9 \equiv -1 \rightsquigarrow$ no sol.

$x=-2$: $y^2 = (-2)^3 - (-2) + 9 \equiv 3 \rightsquigarrow$ no sol.

$(-1, \pm 3)$ — $x=-1$: $y^2 = (-1)^3 - (-1) + 9 \equiv 2 \rightsquigarrow y \equiv \pm 3$

$\mathcal{O}$ point at "∞"

in total: 9 points

Hasse-Weil: EC mod p always has about p points

last time $(0,3) \boxplus (1,-3) = (35, 207)$

now $\equiv (0,-3) \mod 7$

ECDH key exchange

- A + B select elliptic curve E mod p and point A on E
- A selects random y, reveals yA
  B x xA

$\Rightarrow$ A+B now share secret: xyA

[A: knows y, $xA \rightsquigarrow xyA = y(xA)$]

DH mod p ~ 2048 bit
ECDH mod p ~ 256 bit

DH: P, g; g^y; g^x; g^{xy}