ELLIPTIC CURVES: MOTIVATION

A fundamental question is whether an equation with integer coefficients

$$F(x_1, \ldots, x_n) = 0 \tag{1}$$

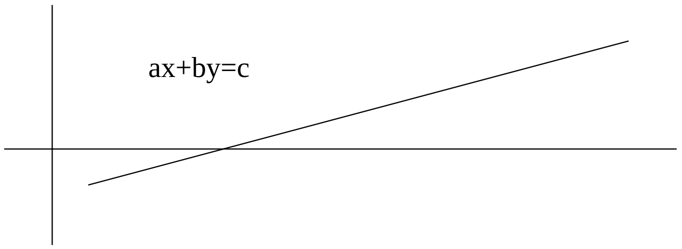
has integer solutions; F is a polynomial in variables $x_1, \ldots, x_n$ with integer coefficients.

1. Does (1) have solutions in the integers?
2. Does (1) have solutions in the rationals?
3. Does (1) have infinitely many solutions in the integers?
4. Does (1) have infinitely many solutions in the rationals?

A two variable equation $F(x, y) = 0$ forms a curve in the plane. So we are seeking geometric-arithmetic methods to find solutions.

LINEAR EQUATIONS

$$ax + by = c, \quad a, b, c \in Z$$



- In the integers it has a solution if and only if gcd$(a, b)|c$, in which case it has infinitely many solutions.

- In the rationals it has infinitely many solutions.

EXAMPLES

- $2x+3y=13$ has a solution in the integers. Namely, $x=2, y=3$. It also has solutions in the rationals. For each rational value of x the corresponding value of y is $\frac{13-2x}{3}$.

- $4x-6y=13$ has no solution in the integers, because $\gcd(4,6)=2 \not| 13$. But it has solutions in the rationals.

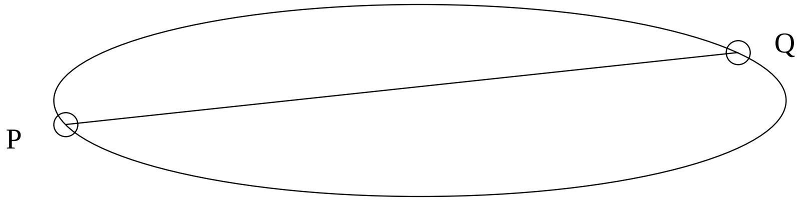
- Pythagorean triples (X,Y,Z) are triples of integers satisfying $X^2+Y^2=Z^2$. E.g., $(3,4,5)$. This is equivalent to solving $x^2+y^2=1$ in the rationals. The solutions are $x=\frac{1-t^2}{1+t^2}, y=\frac{2t}{1+t^2}$.

- For $n \geq 3$, $X^n+Y^n=Z^n$ has no solution in the integers (Fermat's conjecture). This is equivalent to saying that $x^n+y^n=1$ has no solution in the rationals, for $n \geq 3$.

CONIC (QUADRATIC) EQUATIONS

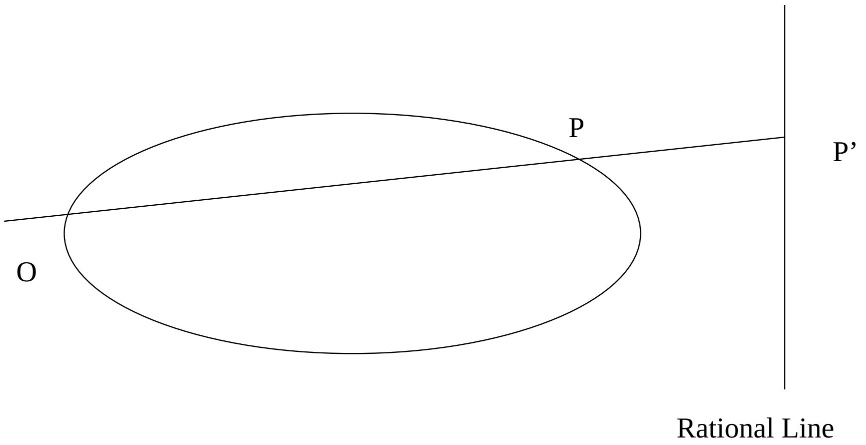
$ax^2 + by^2 + cxy + dx + ey + f = 0, a, \ldots, f \in Q$

Variable-transformation (rotation) transforms this to the familiar equation of ellipse or hyperbola ($c = d = e = 0$). Take the intersection of the conic with a rational line. Are the points of intersection rationals?



If you solve the system of a conic equation and an equation of a line you come up with a quadratic that has two solutions. Moreover, if one solution is rational so is the other (this is easy to see because the discriminant of the quadratic is a rational).

If we know a rational point, say O, here is how we get all of them. For any point P draw the straight line OP and find its intersection P' with L. Then P is rational $\Leftrightarrow P'$ is rational

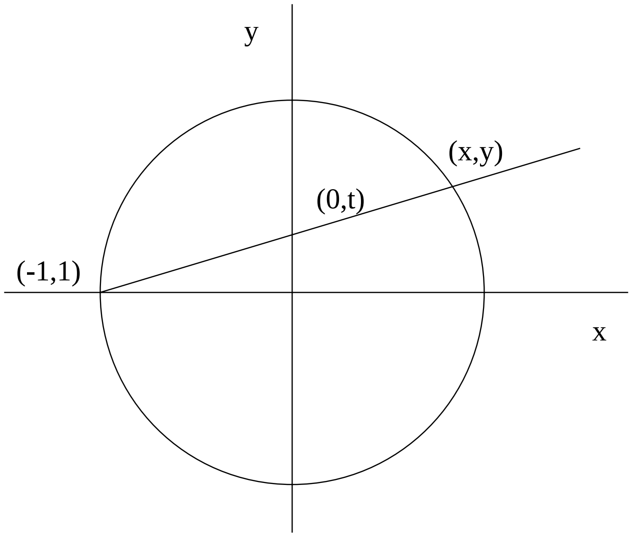


Question: How do we test for a rational point? Convert it into a "homogeneous" equation. Using the projective transformation $x = \frac{X}{Z}, y = \frac{Y}{Z}$ it becomes equivalent to

$$aX^2 + bY^2 = cZ^2 \tag{2}$$

Theorem (Legendre): There is an integer m depending on a, b, c such that equation (2) has a nontrivial solution in the integers if and only if $aX^2 + bY^2 \equiv cZ^2 \bmod m$ has a solution in Z_m^*.

Example: We can reproduce this method on a circle $C : x^2 + y^2 = 1$. Consider a point (x, y) moving on a circle. Take the line L connecting $(0, 0)$ to (x, y). Say it intersects y-axis at $(0, t)$.



The equation of the line is $L : y = t(1 + x)$. Since the point lies in L and in C we have $1 - x^2 = y^2 = t^2(1 + x^2)$, which gives the familiar parametric equations

$$x = \frac{1 - t^2}{1 + t^2}, \quad y = \frac{2t}{1 + t^2},$$

Moreover, t is rational $\Leftrightarrow$ both x, y are rationals, which of course gives you all the rational points.

CUBIC EQUATIONS

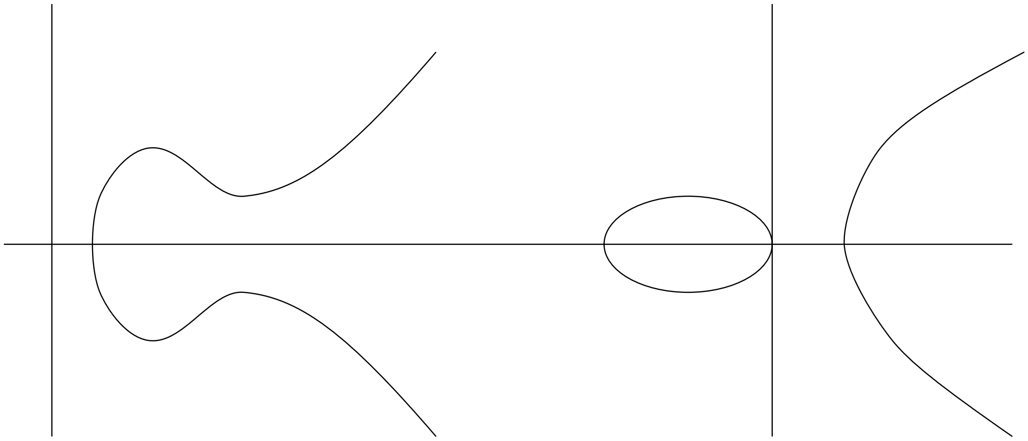
This is an equation of the form

$ay^3 + bx^3 + cx^2y + dxy^2 + exy + fx + gy + h = 0$

with rational coefficients. Weirstrass has shown that using appropriate (e.g., projective) transformations (possibly changing the coefficients) it becomes equivalent to a **Weirstrass Normal Form:**

$$y^2 = x^3 + ax^2 + bx + c$$

Assuming its roots are all distinct it is called an **Elliptic Curve**. The polynomial $f(x) = x^3 + ax^2 + bx + c$ has either one real (and hence two complex) or three real roots.



One Real Root

Three Real Roots

WHY THE NAME ELLIPTIC CURVE?

Consider the ellipse $\frac{x^2}{a^2}+\frac{y^2}{b^2}=1$. Then $y^2 = b^2 - \frac{b^2x^2}{a^2}$. Differentiate $\frac{dy}{dx}$ to obtain $yy' = -\frac{b^2x}{a^2}$. Hence, $(y')^2 = \frac{b^4x^2}{a^4y^4} = \frac{b^4}{a^4}\cdot\frac{x^2}{b^2-b^2x^2/a^2}$. Choose the constant k appropriately and the length of the ellipse is given by the formula

$$\begin{aligned}\textstyle\int \sqrt{1+(y')^2}dx &= \textstyle\int \sqrt{\frac{1-k^2x^2}{1-x^2}}dx \\ &= \textstyle\int \frac{1-k^2x^2}{\sqrt{(1-x^2)(1-k^2x^2)}}dx\end{aligned} \tag{3}$$

Call $g(x) = (1-x^2)(1-k^2x^2)$. Consider the curve $u^2 = g(x)$; use the transformations

$$\bar{x} = \frac{1}{x-1}, \quad \bar{y} = x^2u = \frac{u}{(x-1)^2}$$

and $u^2 = g(x)$ becomes $u^2 = f(\bar{x})$, where $f(\bar{x}) = g'(1)\bar{x}^3 + \frac{1}{2}g''(1) + \bar{x}^2 + \frac{1}{6}g'''(1)\bar{x} + \frac{1}{24}g''''(1)$. Hence equation (3) becomes

$$\int \sqrt{1+(y')^2}dx = \int \frac{1-k^2x^2}{u}dx$$

SINGULARITIES

For an elliptic curve $y^2 = x^3 + ax^2 + bx + c$ define $F(x, y) = y^2 - f(x)$. A singularity of the elliptic curve is a point (x_0, y_0) such that

$$\frac{\partial F}{\partial x}(x_0, y_0) = \frac{\partial F}{\partial y}(x_0, y_0) = 0$$

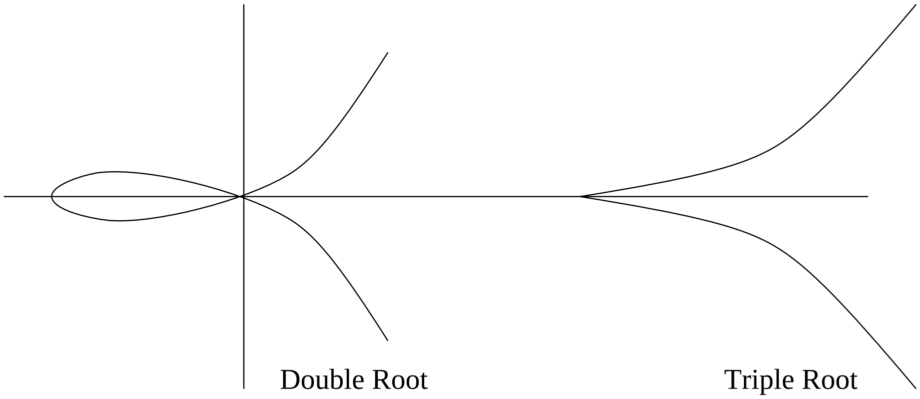
However, $\frac{\partial F}{\partial x} = -f'(x)$ and $\frac{\partial F}{\partial y} = 2y$.

Setting both equal to 0 we see that singularities occur when $2y = -f'(x) = 0$. But $y = 0$ if and only if $f(x) = 0$. Hence, singularities occur at x_0 when $f(x_0) = f'(x_0) = 0$, i.e., x_0 is a common root of f, f', which also means f has a double root (at x_0).

It follows that

$y^2 = f(x)$ has singularity $\Leftrightarrow$ f has double root

This gives two possible pictures for the singularities: $y^2 = x^2(x+1)$ and $y^2 = x^3$.



Singular cubics are easy to analyze because they behave like conics.

"Draw the axis of symmetry and project rational points".

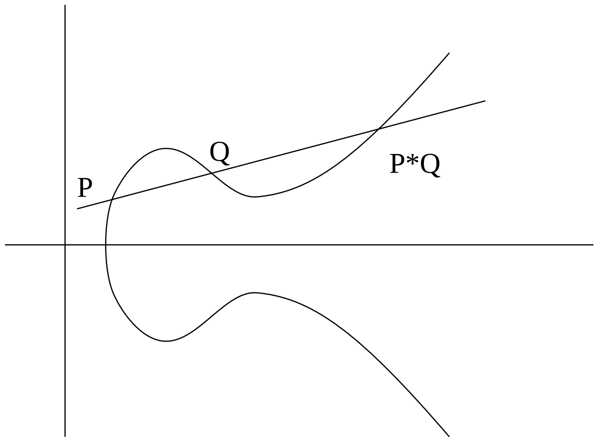
It is usual to assume the elliptic curve has no singularities.

If an elliptic curve is $y^2 = f(x)$, with $f(x) = x^3 + ax^2 + bx + c$ then $f(x)$ has the form

$$f(x) = (x - \alpha)(x^2 + \beta x + \gamma)$$

It follows that

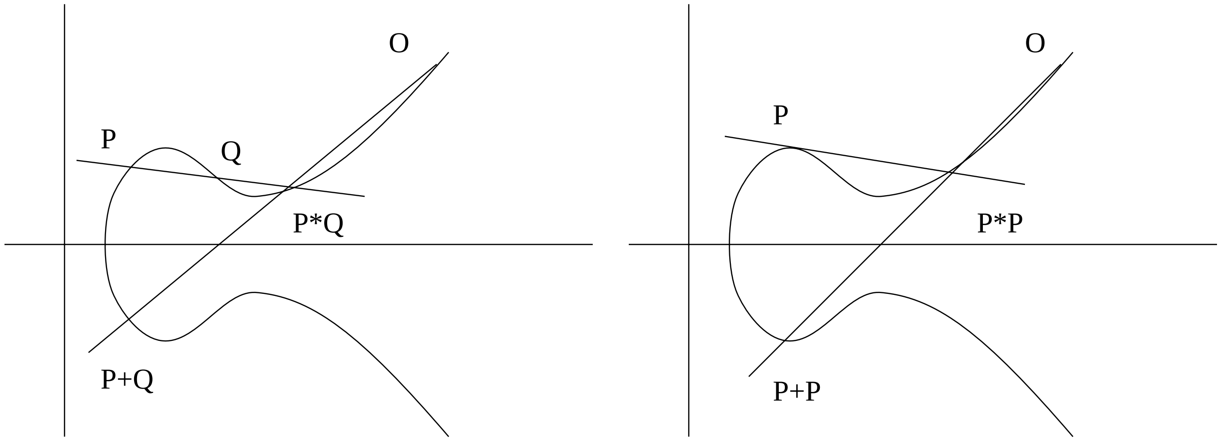
Claim: If two roots of an elliptic curve are rational so is the third.



More generally, if P, Q are rational points on the elliptic curve so is the point $P * Q$ depicted in the picture. This operation is not yet a group (because it is not associative!) but can be made into one by adding an extra point O.

FORMING A GROUP

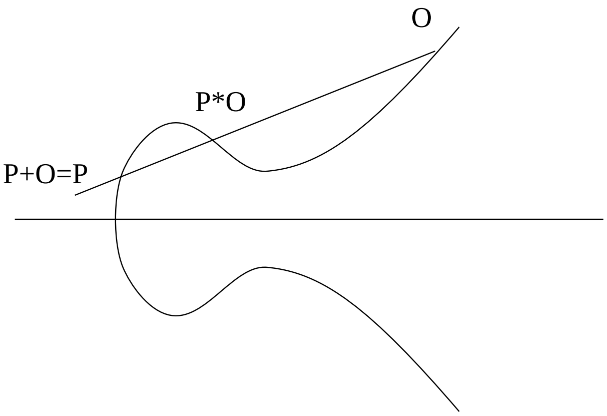
By adding a rational point O at infinity we can make this operation form a group.



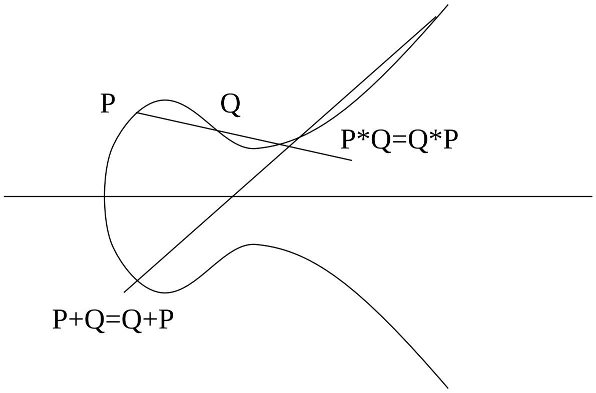
Notice that when $P = Q$ then we draw the line tangent to the elliptic curve at P and form the point $P + P$ exactly as before.

The proof that it is a group is explained in the next picture (except for associativity which is more complicated).

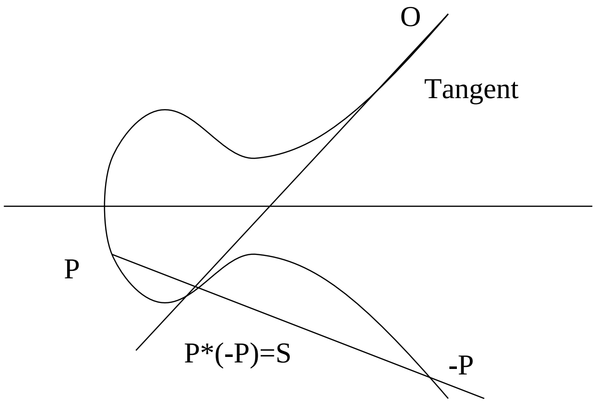
GROUP PROPERTIES



P+O=P



P+Q=Q+P

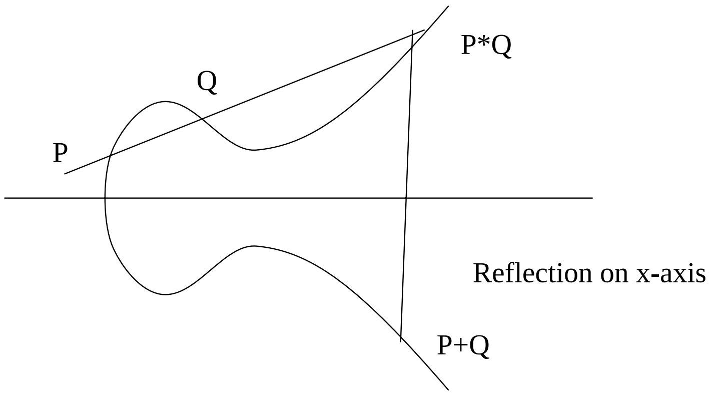


-P

This turns out to be an abelian group and the operation $+$ is independent of the point O we choose.

Now we can also answer our original question!

Theorem (Mordel): The group of rational points of a nonsingular elliptic curve is finitely generated.



In practice we determine the point O using a bit of projective Geometry. We assume O is a point at infinity which is a rational point of the cubic. Thus we can even derive explicit formulas for the group operation.

EXPLICIT FORMULAS

We can derive an explicit formula for the point P_1+P_2 in terms of the points $P_1=(x_1,y_1)$ and $P_2=(x_2,y_2)$. Consider the elliptic curve $y^2=x^3+ax^2+bx+c$ and put $P_1*P_2=(x_3,y_3), P_1+P_2=(x_3,-y_3)$.

Assume $(x_1,y_1)\neq(x_2,y_2)$. Equation of line through P_1,P_2 is $y=\lambda x+v$, where $\lambda=\frac{y_2-y_1}{x_2-x_1}$ and $v=y_1-\lambda x_1=y_2-\lambda x_2$. Substituting we get $y^2=(\lambda x+v)^2=x^3+ax^2+bx+c$, i.e., $x^3+(a-\lambda^2)x^2+(b-2\lambda v)x+(c-v^2)=0=(x-x_1)(x-x_2)(x-x_3)$, since all three points $(x_1,y_1),(x_2,y_2),(x_3,y_3)$ satisfy this equation.

If we multiply out and equate terms we can prove trivially $x_3=\lambda^2-a-x_1-x_2, y_3=\lambda x_3+v$. Hence, we have the formulas

$$(x_1,y_1)*(x_2,y_2)=(\lambda^2-a-x_1-x_2,\lambda(x_3-x_1)+y_1)$$

$$(x_1,y_1)+(x_2,y_2)=(\lambda^2-a-x_1-x_2,\lambda(x_1-x_3)-y_1)$$

Different formula needed when $P_1 = P_2$. We find the tangent to the elliptic curve at P_1 (which is also the slope λ of the tangent at P_1) by implicit differentiation of $y^2 = f(x)$: $\lambda = y' = \frac{f'(x)}{2y}$.

Open Problem: No algorithm is known for determining whether or not a cubic has a rational point.

Example Consider the elliptic curve $y^2 = x^3 + 17$.

It has the two points $P_1 = (-1, 4)$ and $P_2 = (2, 5)$.

$P_1 * P_2 = \left(-\frac{8}{9}, \frac{109}{27}\right)$ and $P_1 + P_2 = \left(-\frac{8}{9}, -\frac{109}{27}\right)$.

The tangent at $P_1 = (-1, 4)$ has slope $\lambda = 3/8$. Using the previous formula we get $2P_1 = \left(\frac{137}{64}, -\frac{2651}{512}\right)$.

AVOIDING SINGULARITIES

Let $E(a,b)$ be the abelian group of rational points of the elliptic curve

$$y^2 = f(x) = x^3 + ax + b.$$

We saw before that the curve has no singular points iff $f(x)$ has no double roots.

Having double roots is equivalent to $f(x) = f'(x) = 0$, i.e.

$$x^3 + ax + b = 3x^2 + a = 0 \qquad (4)$$

It follows that $x^2 = -a/3$. But also $x^4 + ax^2 + bx = 0$. This implies

$$\frac{a^2}{9} + a\left(-\frac{a}{3}\right) + bx = 0, \text{ and hence, } x = \frac{2a^2}{9b}$$

Substituting in (4) we obtain

$$3\left(\frac{2a^2}{9b}\right)^2 + a = 0, \text{ and hence } 4a^3 + 27b^2 = 0.$$

Theorem: $y^2 = x^3 + ax + b$ is non-singular iff $4a^3 + 27b^2 \neq 0$.

ELLIPTIC CURVES OVER Z_p

Almost everything said before works over finite fields.

Given a prime p, an elliptic curve over Z_p is a congruence $y^2 \equiv x^3 + ax + b \bmod p$ together with a special point O at infinity such that the "non-singularity" condition $4a^3+27b^2 \not\equiv 0 \bmod p$ is satisfied.

Given points $P{=}(x_1, y_1), P_2 = (x_2, y_2)$ on the elliptic curve we define

$$P_1 + P_2 = (\lambda^2 - x_1 - x_2, \lambda(x_1 - x_3) - y_1),$$

where

$$\lambda = \begin{cases} \frac{y_2-y_1}{x_2-x_1} & \text{if } P_1 \neq P_2 \\ \frac{3x_1^2+a}{2y_1} & \text{if } P_1 = P_2 \end{cases}$$

We also define $(x_1, y_1) + (x_1, -y_1) = O$ and $P_1 + O = O + P_1 = P_1$. This is an abelian group, denoted $E_p(a, b)$.

This same idea works over $GF(p^n)$ as well.

PROPERTIES

Let p be a prime > 3

- **Hasse:** $p+1-2\sqrt{p} < |E_p(a,b)| < p+1+2\sqrt{p}$

- **Schoof:** There is an efficient $O(\log^8 p)$ algorithm for computing $|E_p(a,b)|$.

- **Waterhouse:** For any integer such that
$$p + 1 - 2\sqrt{p} < n < p + 1 + 2\sqrt{p}$$
there exist $a, b < p$ such that $|E_p(a,b)| = n$. Moreover, the orders of the groups of elliptic curves are uniformly distributed in this interval.

- **Theorem:** $E_p(a,b) \cong Z_{n_1} \times Z_{n_2}$, for some n_1, n_2 such that $n_2|n_1$ and $n_2|p-1$.

Example

Consider the elliptic curve $y^2 = x^3 + x + 6$ over Z_{11}^*. To determine the points on E we look at each possible point of Z_{11} computing x^3+x+6 and then trying to solve equation $y^2 \equiv x^3+x+6 \bmod 11$.

This involves computing square roots modulo 11. There is an explicit formula to do this because $11 \equiv 3 \bmod 4$. In fact the square roots of a quadratic residue r are $\pm r^{(11+1)/4} \equiv r^3 \bmod 11$. To compute we tabulate:

x	$x^3 + x + 6$	$\in QR_{11}$?	y
0	6	*no*	
1	8	*no*	
2	5	*yes*	4, 7
3	3	*yes*	5, 6
4	8	*no*	
5	4	*yes*	2, 9
6	8	*no*	
7	4	*yes*	2, 9
8	9	*yes*	3, 8
9	7	*no*	
10	4	*yes*	2, 9

Example (Continued)

The elliptic curve has 13 points (x, y) on it (including the point at infinity). Being of prime order 13 it must be a cyclic group itself. E.g., take the generator $\alpha = (2, 7)$.

Powers of α, e.g. $(2, 7) + (2, 7)$ can be computed as follows. First compute λ:

$$\begin{aligned}\lambda &= (3 \cdot 2^2 + 1)(2 \cdot 7)^{-1} \bmod 11 \\ &= (2 \cdot 3)^{-1} \bmod 11 \\ &= 2 \cdot 4 \bmod 11 \\ &= 8\end{aligned}$$

Hence $x_3 = 8^2 - 2 - 2 = 5 \bmod 11$, and $y_3 = 8(2-5)-7 = 2 \bmod 11$. It follows that $(2, 7) + (2, 7) = (5, 2)$.

Next $(2, 7) + (2, 7) + (2, 7) = 2(2, 7) + (2, 7) = (5, 2) + (2, 7)$.

ELLIPTIC CURVE SYSTEMS

ElGamal is applicable to the cyclic subgroup Z_{n_1} of $E_p(a,b)$, but its expansion factor is 4 (versus 2 over Z_p). Moreover, the plaintext space consists of the points in $E_p(a,b)$ and no convenient method is known for generating deterministically points in $E_p(a,b)$.

Take an Elliptic Curve E_p which contains a cyclic subgroup $H = Z_{n_1}$ with intractable discrete logarithm. Plaintext space is $Z_p^* \times Z_p^*$ and Ciphertext space is $E_p \times Z_p^* \times Z_p^*$.

$$\begin{array}{ll}
 & \textbf{Menezes – Vanstone System}: \\
\textbf{Public}: & \alpha, \beta \in E_p \\
\textbf{Private}: & a \text{ such that } \beta = a\alpha \\
\textbf{Encryption}: & \text{Choose Random } k \in Z_{n_1} \\
 & (x,k) \rightarrow E(x,k) = (y_0, y_1, y_2): \\
 & y_0 = k\alpha, (c_1, c_2) = k\beta \\
 & x = (x_1, x_2), y_1 \equiv c_1 x_1 \bmod p, \\
 & \text{and } y_2 \equiv c_2 x_2 \bmod p \\
\textbf{Decryption}: & (y_0, y_1, y_2) \rightarrow D(y_0, y_1, y_2) = \\
 & (y_1 c_1^{-1} \bmod p, y_2 c_2^{-1} \bmod p), \\
 & \text{where } a y_0 = (c_1, c_2)
\end{array}$$

FACTORING, PRIMALITY, GROUPS

We are given an integer n to be tested for primality and a group $G \subseteq (Z_n)^k$, for some k. For $x \in G$ define $|x|_G =$ order of x in G.

Assumption: There is a set S_G of integers such that

$$\exists x \in G(|x|_G \in S_G) \Leftrightarrow n \text{ is prime}$$

Primality Testing: $\exists x \in G(|x|_G \in S_G)$?

We can test $|x|_G = m$ as follows:

$$|x|_G = m \Leftrightarrow x^m = e \ \& \ \forall(\text{prime } p|m)(x^{\frac{m}{p}} \neq e).$$

Thus testing primality for n reduces to factorization of $m \in S_G$. Usually we know prime factors of each $m \in S_G$.

Groups $E_n(a, b)$ of elliptic curves are used for primality testing and factoring n.