Cryptanalysis

Lecture 8: Lattices and Elliptic Curves

John Manferdelli
jmanfer@microsoft.com
JohnManferdelli@hotmail.com

This material is provided without warranty of any kind including, without limitation, warranty of non-infringement or suitability for any purpose. This material is not guaranteed to be error free and is intended for instructional use only.

Lattices

- Definition: Let $<v_1, \ldots, v_k>$ be linearly independent vectors in K^n. K is often the real numbers or complex numbers. The lattice, L is $L= \{ v: v= a_1 v_1+\ldots+ a_k v_k\}$, where a_i □ Z.

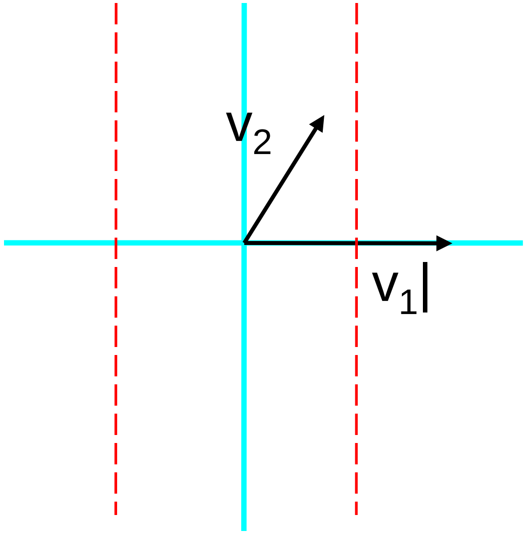
- Area parallel-piped formed by $<v_1, \ldots, v_n>$ is

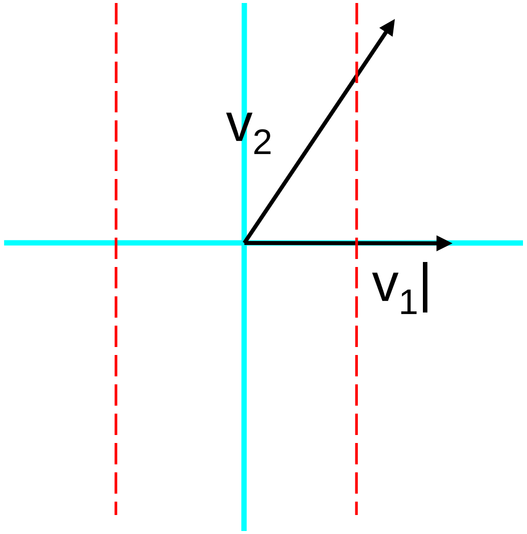
  $|\det(v_1, \ldots, v_n)|$.

- Shortest vector problem: Given the lattice L, find the shortest v, ||v||=□, v □ L.

Reduced Basis

- $<v_1 , v_2>$ is reduced if
  - $||v_2|| \le ||v_1||$; and,
  - $-1/2 \, ||v_1||^2 \le (v_1 , v_2) \le 1/2 \, ||v_1||^2$.





Reduced

Not

Gauss again

- Let $\langle v_1 , v_2 \rangle$ be a basis for a two dimensional lattice L in R^2. The following algorithm produces a reduced basis.

```
for(;;) {
    if($||v_1||$ □ $||v_2||$)
        swap $v_1$ and $v_2$;
    t= $[(v_1, v_2)/(v_1, v_1)]$;   // [] is the “closest integer” function
    if(t==0)
        return;
    $v_2 = v_2 - t\, v_1$;
    }
```

- $\langle v_1 , v_2 \rangle$ is now a reduced basis and v_1 is a shortest vector in the lattice.

LLL

- Definition: $B = \{b_1, \ldots, b_n\}$, L in R^n. $\square_{i,j} = (b_i, b_j^*)/(b_j^*, b_j^*)$. $b_i^* = b_i - \square_{j=1}^{i-1} \square_{i,j} b_j^*$. B is *reduced* if

  1. $| \square_{i,j} | \leq 1/2$; $1 \leq j < i \leq n$
  2. $||b_i^*||^2 \geq (3/4 - \square_{i,i-1}^2)\, ||b_{i-1}^*||^2$.

- Note $b_1^* = b_1$.

LLL algorithm

```
$b_1$*= $b_1$; k= 2;
for(i=2; i≤n; i++) {
    $b_i$*= $b_i$;
    for(j=1; j<i; j++)
    {   $μ_{i,j}$= ($b_i$ , $b_j$*)/$B_j$;
        $b_i$*= $b_i$- $μ_{i,j}b_j$*;$B_i$= ($b_i$*, $b_i$*);}
}
for(;;) {
    RED(k, k-1);
    if($B_k$<(3/4 – $μ_{k,k-1}^2$)$B_{k-1}$) {
        μ= $μ_{k,k-1}$; B= $B_k$+ μμ$B_{k-1}$;$μ_{k,k-1}$= μ$B_{k-1}$/B;
        $B_k$= $B_{k-1}B_k$/B; $B_{k-1}$= B; swap($b_k$, $b_{k-1}$);
        if(k>2) swap($b_k$, $b_{k-1}$);
        for(i=k+1; i≤n;i++)
        {  t= $μ_{i,k}$;; $μ_{i,k}$;= $μ_{i,k-1}$- μt;
           $μ_{i,k-1}$=t+ $μ_{k,k-1}$ $μ_{i,k}$; }
        k= max(2, k-1);
        if(k>n)  return($b_1$, …, $b_n$);
}
```

```
RED(k, k-1)

if(|$μ_{k,l}$|)> 1/2) {
    r= ⌊1/2+$μ_{k,l}$⌋;
    $b_k$= $b_k$ -r $b_l$;
    for(j=1; j<l;j++) {
        $μ_{k,j}$= $μ_{k,j}$-r$μ_{l,j}$;
        $μ_{k,l}$ = $μ_{k,l}$-r;
    }
}
```

LLL Theorem

- Let L be the n-dimensional lattice generated by $<v_1, \ldots, v_n>$ and □□the length of the shortest vector in L. The LLL algorithm produces a reduced basis $<b_1, \ldots, b_n>$ of L.

  1. $||b_1|| \leq 2^{(n-1)/4} D^{1/n}$.
  2. $||b_1|| \leq 2^{(n-1)/2}$ □.
  3. $||b_1|| \, ||b_2|| \ldots ||b_n|| \leq 2^{n(n-1)/4} D$.

- If $||b_i||^2 \leq C$ algorithm takes $O(n^4 \lg(C))$.

Attack on RSA using LLL

- Attack applies to messages of the form "M xxx" where only "xxx" varies (e.g.- "The key is xxx") and xxx is small.
- From now on, assume M(x)=B+x where B is fixed
  - $|x|<Y$.
  - Not that $E(M(x))=c= (B+x)^3$ (mod n)
  - $f(x)= (B+x)^3-c= x^3 + a_2 x^2 + a_1 x + a_0$ (mod n).
- We want to find x: f(x)=0 (mod n), a solution to this, m, will be the corresponding plaintext.

Attack on RSA using LLL

- To apply LLL, let:
  - v_1= (n, 0, 0, 0),
  - v_2= (0, Yn, 0, 0),
  - v_3= (0, 0, Y^2n, 0),
  - v_4= (a_0 , a_1 Y, a_2Y^2, a_3 Y^3)
- When we apply LLL, we get a vector, b_1:
  - $||b_1|| \leq 2^{(3/4)} |\det(v_1, v_2, v_3, v_4)| = 2^{(3/4)} n^{(3/4)} Y^{(3/2)}$ …. Equation 1.

- Let $b_1 = c_1 v_1 + \ldots + c_4 v_4 = (e_0 , Y e_1 , Y^2 e_2, Y^3 e_3)$. Then:
  - $e_0 = c_1 n + c_4 a_0$
  - $e_1 = c_2 n + c_4 a_1$
  - $e_2 = c_3 n + c_4 a_2$
  - $e_3 = c_4$

Attack on RSA using LLL

- Now set $g(x)= e_3 x^3 + e_2 x^2 + e_1 x + e_0$.
- From the definition of the e_i, $c_4 f(x)= g(x) \pmod n$, so if m is a solution of $f(x) \pmod n$, $g(m)= c_4 f(m)= 0 \pmod n$.
- The trick is to regard g as being defined over the real numbers, then the solution can be calculated using an iterative solver.
- If $Y < 2^{(7/6)} n^{(1/6)}$, $|g(x)| \leq 2 ||b_1||$.
- So, using the Cauchy-Schwartz inequality, $||b_1|| \leq 2^{-1}n$.
- Thus $|g(x)| < n$ and $g(x)=0$ yielding 3 candidates for x.

- Coppersmith extended this to small solutions of polynomials of degree d using a d+1 dimensional lattice by examining the monic polynomial $f(T)= 0 \pmod n$ of degree d when $|x| <= n^{1/d}$.

Example attack on RSA using LLL

- $p= 757285757575769$, $q= 2545724696579693$.
- $n= 1927841055428697487157594258917$.
- $B= 2008050001141923051800009190000$.
- $c= (B+m)^3$, $0 \leq m<100$.
- $f(x)= (B+x)^3-c= x^3 + a_2 x^2 + a_1 x + a_0 \pmod{n}$.
  - $a_2= 6024150003425769155400027570000$
  - $a_1= 1123549124004247469362171467964$
  - $a_0= 5873241144456798769544457927616$
  - $v_1= (n,0,0,0)$
  - $v_2= (0,100n,0,0)$
  - $v_3= (0,0,10^4n,0)$
  - $v_4= (a_0, a_1 100, a_2 10^4,10^6)$

Example attack on RSA using LLL

- Apply LLL, b_1=
  - 308331465484476402v_1 + 589837092377839611v_2 +
  - 316253828707108264v_3 + (-1012071602751202635)v_4 =
  - (246073430665887186108474, -577816087453534232385300, 405848565585194400880000, -1012071602751202635000000)
- g(x)= (-1012071602751202635) t^3 + 40584856558519440088 t^2 + (-57781608745353442323853) t + 246073430665887186108474.

- Roots of g(x) are 42.0000000, (-.9496 +/- 76.0796i)
- The answer is 42.

Elliptic Curves

- Motivation:
  - Full employment act for mathematicians
  - Elliptic curves over finite fields have an arithmetic operation
  - Pohlig-Hellman and index calculus don’t work on elliptic curves.
  - Even for large elliptic curves, field size is relatively modest.
- Use this operation to define a discrete log problem.
- To do this we need to:
  - Define point addition and multiplication on an elliptic curve
  - Find elliptic curve whose arithmetic gives rise to large finite groups with elements of high order
  - Figure out how to embed a message in a point multiplication.
  - Figure out how to pick “good” curves.

Rational Points

- Bezout
- Linear equations
- $x^2+5y^2=1$
- $y^2=x^3-ax-b$
  - Disconnected: $y^2= 4x^3-4x +1$
  - Connected: $a= 7$, $b=-10$
  - Troublesome: $a=3$, $b=-2$
- Arithmetic
- $D= 4a^3-27b^2$
- Genus, rational point for $g>1$
- Mordell
- $Z_{n1} \times Z_{n2}$, $n2|n1$, $n2|(p-1)$

Equation solving in the rational numbers

- Linear case: Solve ax+by=c or, find the rational points on the curve C: f(x,y)= ax+by-c=0.
  - Clearing the fractions in x and y, this is equivalent to solving the equation in the integers. Suppose (a,b)=d, there are x, $y \in Z$: ax+by=d. If d|c, say c=d'd, a(d'x)+b(d'y)=d'd=c and we have a solution. If d does not divide c, there isn't any. We can homogenize the equation to get ax+by=cz and extend this procedure, here, because of z, there is always a solution.
- Quadratic (conic) case: solve $x^2+5y^2=1$ or find the rational points on the curve C: $g(x,y)= x^2+5y^2-1=0$.
  - $(-1,0) \in C$. Let (x,y) be another rational point and join the two by a line: y= m(x+1). Note m is rational. Then $x^2+5(m(x+1))^2=1$ and $(5m^2+1) x^2 + 2 (5m^2)x + (5m^2-1)= 0 \rightarrow x^2 + 2 [(5m^2)/(5m^2+1)] x + [(5m^2-1)/ (5m^2+1)]= 0$. Completing the square and simplifying we get $(x+(5m^2)/(5m^2+1))^2= [25m^4 –(25m^4 -1)]/(5m^2+1)^2= 1/(5m^2+1)^2$. So $x= \pm(1-5m^2)/(5m^2+1)$ and substituting in the linear equation, $y= \pm(2m)/(5m^2+1)$. These are all the solutions.
- Cubic case is more interesting!

Bezout's Theorem

- Let deg(f(x,y,z))=m and deg(g(x,y,z))=n be homogeneous polynomials over **C**, the complex numbers and C_1 and C_2 be the curves in $\mathbf{CP}^2$, the projective plane, defined by:
  - $C_1 = \{(x,y,z): f(x,y,z)=0\}$; and,
  - $C_2 = \{(x,y,z): g(x,y,z)=0\}$.
- If f and g have no common components and $D=C_1 \cap C_2$, then $\square_{x \in D}\ I(C_1 \cap C_2, x)=mn$.

- I is the intersection multiplicity. This is a fancy way of saying that (multiple points aside), there are mn points of intersection between C_1 and C_2. There is a nice proof in Silverman and Tate, Rational Points on Elliptic Curves, pp 242-251. The entire book is a must read.
- A consequence of this theorem is that two cubic curves intersect in nine points.

Elliptic Curve Preliminaries -1

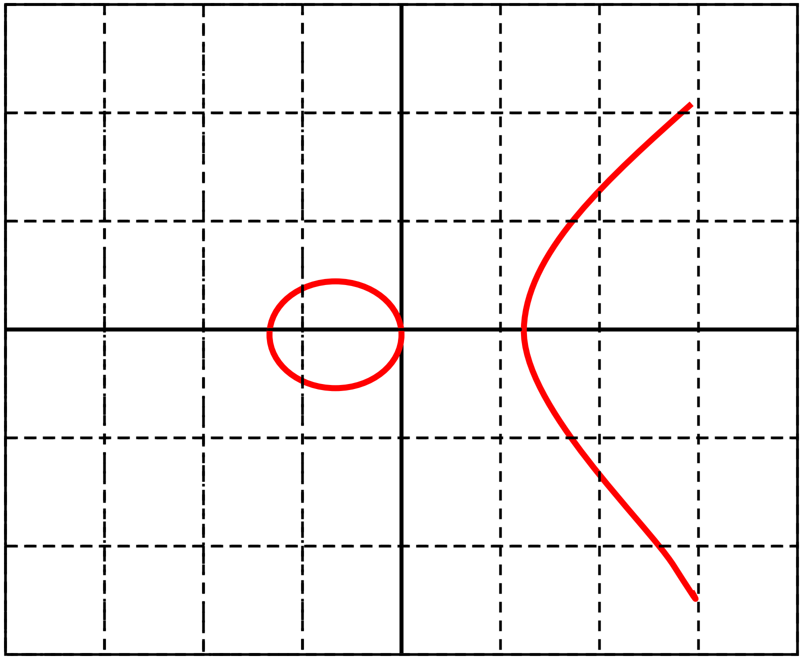
- Let K be a field. char(K) is the characteristic of K which is either 0 or p^n for some prime p, n>0.
- $F(x,y)= y^2+axy+by+cx^3+dx^2+ex+f$ is a general cubic.
- F(x,y) is non-singular if $F_x(x,y)$ or $F_y(x,y) \neq 0$.
- If char(K) $\neq$ 2,3, F(x,y)=0 is equivalent to $y^2= x^3+ax+b$ which is denoted by $E_K(a, b)$ and is called the Weierstrass equation.
- Note that the intersection of a line (y=mx+d) and a cubic, $E_K(a,b)$ is 1, 2 or 3 points.
- Idea is: given 2 points, P,Q on a cubic, the line between P and Q generally identifies a third point on the cubic, R.
- Two identical points on a cubic generally identify another point which is the intersection of the tangent line to the cubic at the given point with the cubic.
- The last observation is the motivation for defining a binary operation on points of a cubic (like addition).

Elliptic Curve Preliminaries - 2

- We are most interested in cubics with a finite number of points.
- Cubics over finite fields have a finite number of points.
- $E_K(a,b)$ is an elliptic equation over an “affine plane.”
- It is often easier to work with elliptic equations over the “projective plane”. The projective plane consists of the points (a,b,c) (not all 0) and (a,b,c) and (ad,bd,cd) represent the same point.
- The map $(x,y,1) \rightarrow (xz,yz,z)$ sets up a 1-1 correspondence between the affine plane and the projective plane.
- E(a,b) is $zy^2= x^3+axz^2+bz^3$.
- The points (x,y,0) are called the line at infinity.
- The point at infinity, (0,1,0) is the natural “identity element” that is rather artificial in the case of the affine equations.

Elliptic Curves

- A non-singular Elliptic Curve is a curve, having no multiple roots, satisfying the equation: $y^2=x^3+ax+b$.
  - The points of interest on the curve are those with rational coordinates which can be combined using the "addition" operation. These are called "rational points."



Graphic by Richard Spillman

Multiple roots

- Here is the condition that the elliptic curve, $E_R(a, b)$: $y^2=x^3+ax+b$, does not have multiple roots:

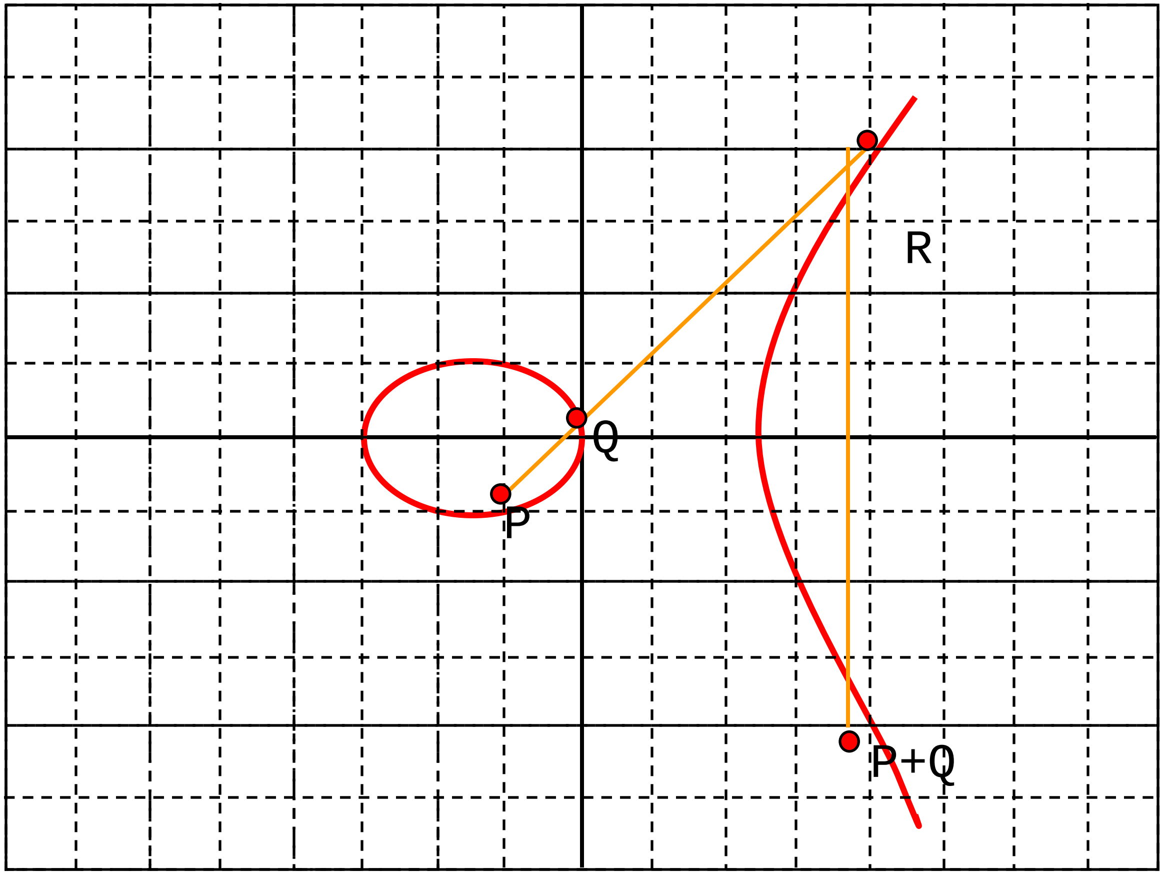
- Let $f(x,y)= y^2-x^3-ax-b=0$. At a double point, $f_x(x,y)=f_y(x,y)=0$, $f_x(x,y)= -(3x^2+a)$, $f_y(x,y)=2y$. So $y=0=x^3+ax+b$ and $0=(3x^2+a)$ have a common zero.

- Substituting $a= -3x^2$, we get $0=x^3-3x^3+b$, $b= 2x^3$, $b^2=4x^6$. Cubing $a= -3x^2$, we get $a^3= -27x^6$. So $b^2/4=a^3/(-27)$ or $27b^2+4a^3=0$. Thus, if $27b^2+4a^3\neq0$, then $E_R(a, b)$ does not have multiple roots.

Elliptic curve addition

- The addition operator on a non-singular elliptic curve maps two points, P and Q, into a third "P+Q". Here's how we construct "P+Q" when P ≠Q .
- Construct straight line through P and Q which hits E at R.

- P+Q is the point which is the reflection of R across the x-axis.



Graphic by Richard Spillman

Addition for points P, Q in $E_R(a, b)$ - 1

- Suppose we want to add two distinct points P and Q lying on the curve $E_R(a, b)$: $y^2=x^3+ax+b$, where $P=(x_1, y_1)$ and $Q=(x_2, y_2)$ with $P\neq Q$, then $P+Q=R=(x_3, y_3)$. Also, suppose $x_1\neq x_2$, here is the computation:

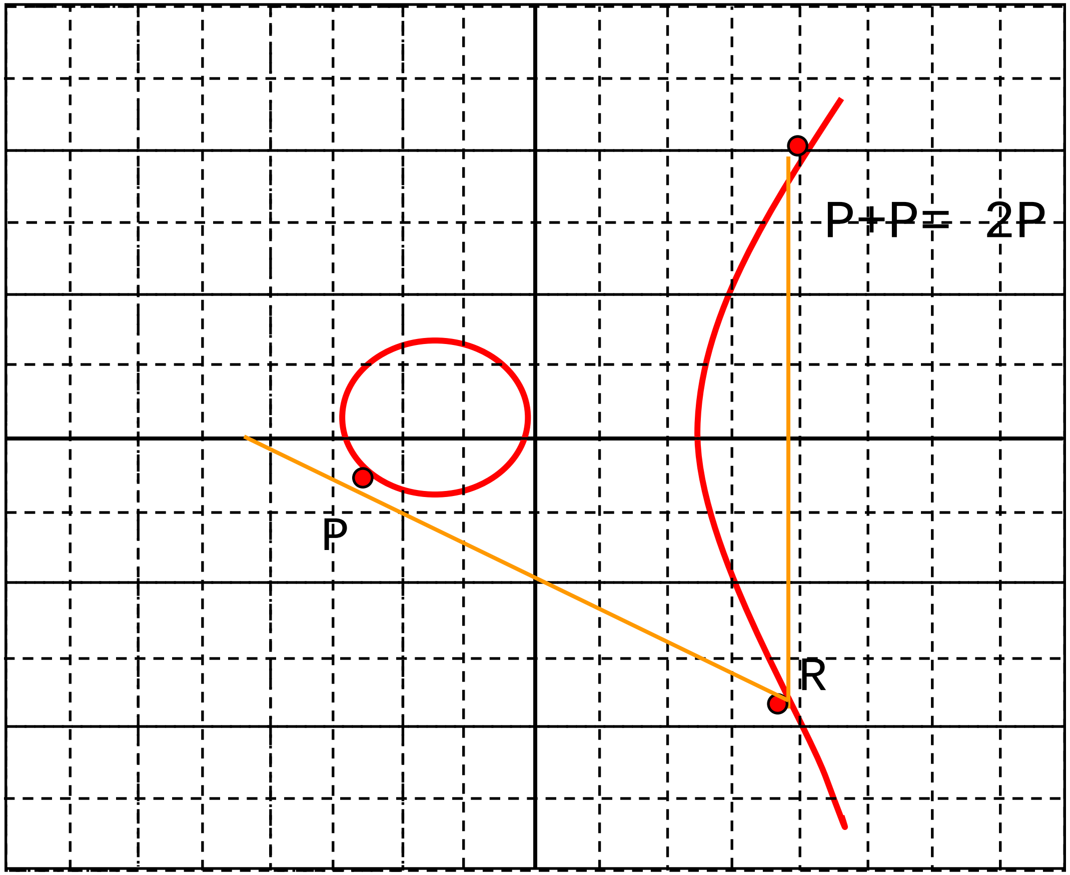
- Join P and Q by the line $y=mx+u$. $m=(y_2-y_1)/(x_2-x_1)$. $u= (mx_1-y_1)= (mx_2-y_2)$. Substituting for $y(=mx+u)$ into $E_R(a, b)$, we get $(mx+u)^2= y^2=x^3+ax+b$; so $0= x^3-m^2x+(a-2mu)x+b-u^2$. x_1, x_2, x_3 are the roots of this equations so $m^2= x_1+x_2+x_3$. and $x_3= m^2-x_1-x_2$. $P*Q= (x_3, -y_3)$ and substituting back into the linear equation, we get: , $-y_3= m(x_3)+u$. So $y_3= -mx_3 – u= -m(x_3) -(mx_1 -y_1)= m(x_1 – x_3) – y_1$.

- To summarize, if $P\neq Q$ (and $x_1\neq x_2$):
  - $x_3 =m^2 – x_1 – x_2$
  - $y_3 =m(x_1 – x_3) – y_1$
  - $m=(y_2-y_1)/(x_2-x_1)$

Multiples in Elliptic Curves 1

- P+P (or 2P) is defined in terms of the tangent to the cubic at P.
- Construct tangent to P and reflect the point at which it intercepts the curve (R) to obtain 2P.
- P can be added to itself

k times resulting in a point Q = kP.



Graphic by Richard Spillman

Addition for points P, Q in E_R(a, b) - 2

- Suppose we want to add two distinct points P and Q lying on the curve E_R(a, b): $y^2=x^3+ax+b$, where $P=(x_1, y_1)$ and $Q=(x_2, y_2)$ and $x_1=x_2$.

- Case 1, $y_1 \neq y_2$: In this case, $y_1=-y_2$ and the line between P and Q “meet at infinity,” this is the point we called O and we get P+Q=O. Note Q=-P so –(x,y)=(x,-y).

- Case 2, $y_1=y_2$ so P=Q: The slope of the tangent line to E_R(a, b) at (x_1, y_1) is m. Differentiating $y^2=x^3+ax+b$, we get 2y y’= $3x_2+a$, so $m=(3x_1^2+a)/(2y_1)$. The addition formulas on the previous page still hold.

Addition in $E_R(a, b)$ - summary

- Given two points P and Q lying on the curve $E_R(a, b)$: $y^2=x^3+ax+b$, where $P=(x_1, y_1)$ and $Q=(x_2, y_2)$ with $P\neq Q$, then $P+Q=R=(x_3, y_3)$ where:

- If $x_1\neq x_2$, $m=(y_2-y_1)/(x_2-x_1)$, and
  - $x_3 = m^2 – x_1 – x_2$
  - $y_3 = m(x_1 – x_3) – y_1$
- If $x_1=x_2$ and $y_1\neq y_2$, then $y_1=-y_2$ and $P+Q=O$, $Q= -P$
- If $x_1=x_2$ and $y_1=y_2$, then $P=Q$, $R=2P$, $m=(3x_1^2+a)/(2y_1)$, and
  - $x_3 = m^2 – x_1 – x_2$
  - $y_3 = m(x_1 – x_3) – y_1$

Point multiplication in $E_R(a, b)$

- By using the doubling operation just defined, we can easily calculate P, 2P, 4P, 8P ,…, 2^eP and by adding appropriate multiples calculate nP for any n.

- If nP=O, and n is the smallest positive integer with this property, we say P has order n.
- Example:
  - The order of P=(2,3) on $E_R(0,1)$ is 6.
  - 2P=(0,1), 4P= (0,-1), 6P=O.

Example of Addition and Element Order

- $E(-36,0)$: $y^2=x^3-36x$. $P=(-3, 9)$, $Q=(-2,8)$.
- $P + Q = (\lambda^2 - x_1 - x_2, \lambda(x_1 - x_3) - y_1)$
  - $\lambda = (y_2 - y_1)/(x_2 - x_1)$, if $P \neq Q$.
  - $= (3 x_1^2 + a)/2y_1$, if $P = Q$.
- $P+Q= (x_3,y_3)=(6,0)$
- $2P=(25/4,-35/8)$
- Note growth of denominators

Proof of group laws

- From the formulas and definitions it is easy to see the operation “+” is commutative, O acts like an identity and if P=(x,y), -P = (x,-y) with P + (-P)= O.

- Associativity is the only law that’s hard to verify. We could use the formulas to prove it but that’s pretty ugly.

  - There is a shorter poof that uses the following result: Let C, C_1, C_2 be three cubic curves. Suppose C goes through eight of the nine intersection points of $C_1 \cap C_2$, then C also goes through the ninth intersection point.

Associativity

- If P and Q are points on an elliptic curve, E, let P*Q denote the third point of intersection of the line PQ and E.

- Now let P, Q, R be points on an elliptic curve E. We want to prove (P+Q)+R=P+(Q+R). To get (P+Q), form P*Q and find the intersection point, between P*Q and E and the vertical line through P*Q; this latter operation is the same as finding the intersection of P*Q, O (the point at infinity) and E. To get (P+Q)+R, find (P+Q)*R and the vertical line, the other intersection point with E is (P+Q)+R. A similar calculation applies to P+(Q+R) and it suffices to show (P+Q)*R=P*(Q+R). O,P,Q,R, P*Q, P+Q, Q*R, Q+R and the intersection of the line between (P+Q), R and E lie on the two cubics:
  - C_1: Product of the lines [(P,Q), (R,P+Q), (Q+R, O)]
  - C_2: Product of the lines [(P,Q+R), (P+Q,O), (R,Q)]
- The original curve E goes through eight of these points, so it must go through the ninth [(P+Q)*R]. Thus the intersection of the two lines lies on E and (P+Q)*R= P*(Q+R).

- This proof will seem more natural if you’ve taken projective geometry. You could just slog out the algebra though.

Mordell and Mazur

- Mordell: Let E be the elliptic curve given by the equation E: $y^2=x^3 + ax^2 + bx +c$ and suppose that $\Delta(E)=-4a^3c+a^2b^2-4b^3-27c^2+18abc\neq 0$. There exist r points $P_1, P_2, \ldots, P_r$ such that all rational points on E are of the form $a_1P_1 + \ldots + a_rP_r$ where $a_i \in Z$.

- Mazur: Let C be a non-singular rational cubic curve and C(Q) contain a point of order m, then $1\leq m\leq 10$ or m=12. In fact, the order of the group of finite order points is either cyclic or a product of a group of order 2 with a cyclic group of order less than or equal to 4.

Fermat's Last Theorem

- $x^n + y^n = z^n$ has no non-trivial solutions in Z for $n>2$.
- It is sufficient to prove this for $n=p$, where p is an odd prime.

- Proof (full version will be on HW):
  1. Suppose $A^p+B^p=C^p$, $(A,B,C)=1$.
  2. E_{AB}: $y^2 = x(x+A^p)(x+B^p)$
  3. Wiles: E_{AB} is modular.
  4. Ribet: E_{AB} is too weird to be modular.
  5. Fermat was right.

Why may elliptic curves might be valuable in crypto

- Consider E: $y^2 = x^3+17$. Let $P_n=(A_n/B_n, C_n/D_n)$ be a rational point on E. Define $\text{ht}(P_n)= \max(|A_n|, |B_n|)$.

- Define $P_1= (2,3)$, $P_2= (-1,4)$ and $P_{n+1}= P_n + P_1$.

n	ht(P_n)
1	2
2	1
3	4
4	2
5	4
6	106
7	2228

n	ht(P_n)
8	76271
9	9776276
10	3497742218
20	8309471981636130322638066614339972215969861310

- In fact, ht(P_n)≈ (1.574□^{ns}, ns=n^2.

Points on elliptic curves over F_q

- The number of points N on $E_q(a,b)$ is the number of solutions of $y^2=x^3+ax+b$.
- For each of q x's there are up to 2 square roots plus O, giving a maximum of 2q+1. However, not every number in F_q has a square root. In fact, $N= q + 1 + \sum_x\chi(x^3 + ax + b)$, where χ is the quadratic character of F_q.
- Hasses' Theorem:
  - $| N – (q+1)|\leq 2\sqrt{q}$ where N is the number of points
- $E_q(a,b)$ is supersingular if N = (q+1)-t, t= 0,q, 2q, 3q or 4q.
- The abelian group over F_q does not need to be cyclic, but it can be decomposed into cyclic groups. Let G be the Elliptic group for $E_q(a,b)$. Theorem: $G=\square_{p} Z/Zp^{\square}$ x $Z/Zp^{\square}$.

- Example: $E_{71}(-1,0)$. N= 72, G is of type (2,4,9).

Addition for points P, Q in $E_p(a, b)$

1. P+O=P
2. If P=(x, y), then P+(x, -y)=O. The point (x, -y) is the negative of P, denoted as –P.
3. If $P=(x_1, y_1)$ and $Q=(x_2, y_2)$ with P≠Q, then $P+Q=(x_3, y_3)$ is determined by the following rules:
   - $x_3 = \lambda^2 - x_1 - x_2$ (mod p)
   - $y_3 = \lambda(x_1 - x_3) - y_1$ (mod p)
   - $\lambda=(y_2-y_1)/(x_2-x_1)$ (mod p) if P≠Q
   - $\lambda=(3(x_1)^2+a)/(2y_1)$ (mod p) if P=Q
4. The order of P is the number n: nP=O

End