

Summer 2002 Research Project

Jonathan Lee*

September 28, 2002

This report is divided mainly into three sections. The first introduces useful background material, the second elliptic curve theory, and the third an account of my experiences and a general overview.

Contents

I	Elliptic Curves	1
1	Preliminaries	1
1.1	Projective Space	1
1.2	Affine Algebraic Sets	2
1.3	Projective Algebraic Sets	2
1.4	Coordinate Rings	3
1.5	The Zariski Topology	3
1.6	Algebraic Sets and Rings	3
1.7	Tangent Spaces	3
1.8	Local Rings	4
2	Elliptic Curves	4
2.1	Weierstraß Equations	4
2.2	Singularities on Cubic Curves	5
2.3	Composition Law on Elliptic Curves	5

*This research was supervised by Salma Kuhlmann and Roland Auer (Mathematical Sciences Group, Department of Computer Science, University of Saskatchewan) and supported through an NSERC undergraduate research award.

2.4	Explicit Composition Formulae	6
2.5	Heights of Points over \mathbb{Q}	7
2.6	Height Estimates	8
2.7	Canonical Heights	10
2.8	Discrete Logarithms	11
3	Applications	11
3.1	Factorization	12
3.2	Primality Testing	13
3.3	Cryptosystems based on Elliptic Curves	14
A	Student Cryptography Seminar	15
B	As a Whole	15
C	Additional Materials	16
C.1	The Quadratic Sieve	16
C.2	Discrete Logarithm Problem	18
C.2.1	Preliminaries	18
C.2.2	Silver-Pohlig-Hellman method	18
C.2.3	Index Calculus Method	19
C.3	Overview of Elliptic Curves	20
C.3.1	Projective Planes	20
C.3.2	Weierstraß Equations	20
C.3.3	Bézout's Theorem	20
C.3.4	Group Structure on Curves	20
C.3.5	Group Law on Non-Singular Elliptic Curves	21
C.3.6	Group Law Formulae	21
C.3.7	Heights of Points	21
C.3.8	Canonical Heights	22
C.3.9	Discrete Logarithms in $E(\mathbb{Q})$	22

Part I

Elliptic Curves

1 Preliminaries

1.1 Projective Space

We first wish to develop some of the necessary geometry.

Let k be a field, and \bar{k} its algebraic closure. We define *affine n -space* over k to be the set of n -tuples over \bar{k} , that is, $\mathbb{A}^n(\bar{k}) = \{(x_1, \dots, x_n) : x_i \in \bar{k}\}$. Similarly, we consider the set of (k -)rational points to be

$$\mathbb{A}^n(k) = \{(x_1, \dots, x_n) : x_i \in k\} \subseteq \mathbb{A}^n(\bar{k}).$$

From an affine $n + 1$ -space, the *projective n -space* is constructed by introducing the equivalence relation \sim , where $(x_1, \dots, x_{n+1}) \sim (y_1, \dots, y_{n+1})$ iff for some $\lambda \in \bar{k}^*$, $x_i = \lambda y_i$. Then, $\mathbb{P}^n(k) = \frac{\mathbb{A}^{n+1}(k) \setminus 0}{\sim}$, and each equivalence class of \sim corresponds to a point of $\mathbb{P}^n(k)$ with homogeneous coordinates, written $[x_1, \dots, x_{n+1}]$.

Rational lines are those whose equations may be written with rational coordinates. Clearly, two rational points determine a rational line, and the intersection of distinct rational lines is a rational point.

Noting this, an intuitive way of characterizing projective space is to note the relation $\mathbb{P}^n(k) = \mathbb{A}^n(k) \cup \mathbb{P}^{n-1}(k)$, that is, projective n -space is obtained from the corresponding affine n -space through the adjunction of directions — ie., one direction for each set of parallel lines. (For an explicit identification, for some i , fix $x_i = 1$ for the “finite” points, and $x_i = 0$ for points at “infinity” — the directions.)

1.2 Affine Algebraic Sets

For some n , we wish to consider the Noetherian ring $k[x_1, \dots, x_n]$ (see Hilbert’s Basis Theorem). For any ideal I , we define

$$\mathcal{Z}(I) = \{P \in \mathbb{A}^n(k) : f(P) = 0 \quad \forall f \in I\}$$

to be the affine algebraic set corresponding to I ; that is, the set of points on which I vanishes.

Clearly, \mathcal{Z} is inclusion-reversing, or contravariant. Given ideals $I \subseteq J$, $\mathcal{Z}(I) \supseteq \mathcal{Z}(J)$. From this, we can make a few observations. Since any point (a_1, \dots, a_n) is itself an algebraic set (consider $I = (x_1 - a_1, \dots, x_n - a_n)$), each maximal ideal M corresponds to a single point.

We define a *variety* V to be an *irreducible* algebraic set, which is to say we may not express $V = V_1 \cup V_2$ for algebraic sets V_1, V_2 both different from V . As above, each prime ideal P corresponds to a variety.

1.3 Projective Algebraic Sets

Projective algebraic sets are defined analogously to affine algebraic sets, replacing ideals with homogeneous ideals. Thus, for an ideal $I \subset k[x_1, \dots, x_{n+1}]$, we obtain $\mathcal{Z}(I) = \{P \in \mathbb{P}^n(k) : f(P) = 0 \quad \forall \text{ homogeneous } f \in I\}$.

1.4 Coordinate Rings

Suppose for an algebraic set V that we wish to consider the restriction of $k[x_1, \dots, x_n] = k[\mathbb{A}^n]$ to V . Then, in defining the equivalence \sim , where $f_1 \sim f_2$ iff $f_1 - f_2 \in \mathcal{I}(V) := \{f \in k[x_1, \dots, x_n] : f(P) = 0 \quad \forall P \in V\}$, we obtain $\frac{k[\mathbb{A}^n]}{\sim} = \frac{k[x_1, \dots, x_n]}{\mathcal{I}(V)} =: k[V]$, which we label the *coordinate ring* of V .

1.5 The Zariski Topology

By taking the algebraic sets of $\mathbb{A}^n(k)$ as the closed sets, we impose a topology. The following usual axioms hold:

Suppose X, Y are algebraic sets with ideals I, J , respectively. Then, since $X \cup Y = \mathcal{Z}(I) \cup \mathcal{Z}(J) = \mathcal{Z}(IJ)$, closed sets are closed under finite union.

On the other hand, suppose X_j are algebraic sets with corresponding ideals I_j . Since $\bigcap_j X_j = \bigcap_j \mathcal{Z}(I_j) = \mathcal{Z}\left(\sum_j I_j\right)$, it follows closed sets are closed under arbitrary intersection.

Note that $\mathcal{Z}(0) = \mathbb{A}^n(k)$ and $\mathcal{Z}(1) = \emptyset$.

1.6 Algebraic Sets and Rings

We can relate rings and varieties even as follows.

Let a *morphism* be a polynomial map $\phi = (f_1, \dots, f_m) : V \rightarrow W$, where $V \subseteq \mathbb{A}^n$ and $W \subseteq \mathbb{A}^m$. This induces a k -algebra homomorphism $\tilde{\phi} : k[W] \rightarrow$

$k[V]$, $f \mapsto f \circ \phi$. In fact, there is a bijection between morphisms and k -algebra homomorphisms. For details, see [2, 15.1.6].

Note that when we deal with morphisms between $\mathbb{P}^n(k)$ and $\mathbb{P}^m(k)$, a morphism ϕ takes the form (f_0, \dots, f_m) , with $f_i : \mathbb{P}^n(k) \rightarrow k$. Assuming the f_i have no common roots except for $(0, \dots, 0)$, ϕ is well-defined.

1.7 Tangent Spaces

Let k be a field and V an algebraic set with ideal I . For the sake of simplicity, assume now that I is principal, that is, $I = (f)$ for some $f \in k[x_1, \dots, x_n]$. Through differentiation we obtain a tangent polynomial for any $v \in V$, which is $D_v(f) = \sum_{i=1}^n \frac{\partial f}{\partial x_i}(v)x_i$. From this, we define our *tangent space at v* to be $\mathcal{Z}(D_v(f))$.

In general, if $I = (f_1, \dots, f_n)$, then the tangent space is $\bigcap_j \mathcal{Z}(D_v(f_j))$.

1.8 Local Rings

Given k be algebraically closed and V a variety, we may define $k(V)$ to be the fraction field of the integral domain $k[V]$, ie. $k(V) \equiv \left\{ \frac{f}{g} : f, g \in k[V], g \neq 0 \right\}$.

We wish to treat f/g as a k -valued function. This makes no sense for $v \in V$, $g_1(v) = 0$, regardless if f vanishes at v as well. Thus, consider f/g to be defined, or regular, at v if there exists $f_1, g_1 \in k[V]$, $f \cdot g_1 = g \cdot f_1$, $g_1(v) \neq 0$. Then, simply set $\left(\frac{f}{g} \right)(v) = \left(\frac{f_1}{g_1} \right)(v)$.

Let $v \in V$. Localizing $k(V)$ at $\mathcal{I}(v)$ to obtain the subset of functions regular at v yields the local ring $\mathcal{O}_{v,V}$, with corresponding maximal ideal $\mathfrak{m}_{v,V} = \{f/g \in \mathcal{O}_{v,V} : (f/g)(v) = 0\}$. Since any $a \in k$ can be considered a constant function in $\mathcal{O}_{v,V}$, it follows that $\frac{\mathcal{O}_{v,V}}{\mathfrak{m}_{v,V}} \cong k$.

We define the *dimension* of a variety to be the transcendence degree of $k(V)$ over k .

2 Elliptic Curves

2.1 Weierstraß Equations

Let a *cubic curve* be the projective variety defined by a homogeneous cubic polynomial in $\mathbb{P}^3(k)$ of the form

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3,$$

a *long Weierstraß equation*. Desiring a restriction to the xy -plane, we set $Z = 1$ to obtain $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$. Assuming $\text{char}(k) \neq 2, 3$, through completing the square and subsequently the cube, this yields $(y + \frac{a_1x+a_3}{2})^2 = x^3 + a_2x^2 + a_4x + a_6 + \frac{(a_1x+a_3)^2}{4} = (x + \frac{4a_2+a_1^2}{12})^3 + \dots$. Thus, through such transformations we will henceforth assume the defining equation for each such curve takes the form

$$y^2 = x^3 + ax + b, \tag{1}$$

that of a *short Weierstraß equation*.

Assuming our curve is given by $\mathcal{Z}(y^2 - x^3 - ax - b)$, we make note of our projective point. In homogeneous coordinates, admitting $Z = 0$ in $Y^2Z = X^3 + aXZ^2 + bZ^3$ yields the point with (homogeneous) coordinates $[0, 1, 0]$, which we denote \mathcal{O} .

In the context of the xy -plane, this unique point is identified with the vertical direction, which will become more apparent with the group composition rules.

2.2 Singularities on Cubic Curves

Given a point $v \in V$, we say v is *singular* (that is, a *singular point*) if the dimension of its tangent space $\mathbb{T}_{v,V}$ does not match the dimension of the variety. For the present case, this is when $\dim \mathbb{T}_{v,V} \neq 1$.

Extending this to cubic curves, we call one *singular* if it has a singular point. Singularities correspond to points (x_0, y_0) where x_0 is a multiple root of $x^3 + ax + b$. Clearly, a curve can have at most one singularity — otherwise, a line connecting two such points would result in an intersection multiplicity greater than 3, contradicting Bézout's Theorem (see below).

A singularity corresponding to a double root is a *node*: corresponding short Weierstraß equations take the form $y^2 = (x - k)^2(x + 2k) = x^3 - (3k^2)x + 2k^3$; to a triple root, a *cusp*: $y^2 = x^3$.

We provide an easy test for the singularity of a cubic curve. For a polynomial $f(x)$ with not necessarily distinct roots α_i , we have the discriminant $\Delta(f) = \prod_{i < j} (\alpha_i - \alpha_j)^2$, so

$$\Delta(x^3 + ax + b) = -4a^3 - 27b^2$$

in the case of a cubic polynomial. For a cubic curve E given by the short Weierstraß equation (1), we define the discriminant

$$\Delta(E) = 16 \cdot \Delta(x^3 + ax + b).$$

As a multiple root results in zero discriminant, we see that a cubic curve is singular iff $\Delta(E) = 0$.

A non-singular cubic curve given by a short Weierstraß equation (1) together with its point at infinity \mathcal{O} is called an *elliptic curve*. Two elliptic curves are *isomorphic* if their equations are equivalent via the previously mentioned affine transformations. For an elliptic curve E defined over k , the set of k -rational points on E is denoted by $E(k)$.

2.3 Composition Law on Elliptic Curves

Given an elliptic curve, we may define a composition law. We need a special case of Bézout's Theorem; namely, that there are 3 intersections between a line and an elliptic curve, counting multiplicities and projective points. However, the proof for this special case is considerably easier than for the general situation (see [6, A.3]). For a given field k , we prove this for \bar{k} and use it to show that having at least 2 intersections in k implies exactly 3 intersections in k .

Suppose our line is vertical; that is, given by $x = c$ for some $c \in k$. We then have one intersection at \mathcal{O} ; the two others given by (x, y) where $y^2 = c^3 + ac + b$. Since $y \in k \iff (-y) \in k$, counting multiplicities, we have either 1 or 3 intersections in $E(k)$.

Otherwise, we may assume without loss of generality that our line is given by $y = 0$ by applying an affine transformation to our equations. Clearly, there are no projective solutions, and as \bar{k} is algebraically closed, there are 3 roots to the corresponding expression in x and thus intercepts. Suppose 2 of our roots are rational, say x_0 and x_1 . As the short Weierstraß equation has rational coefficients, this would imply the third root does as well.

Now, for any $\mathcal{O} \neq P \in E(k)$, set $-P$ to be the third point of intersection between $E(k)$ and the line connecting P with \mathcal{O} . As we assume a short Weierstraß equation, $P = (x, y) \iff -P = (x, -y)$. We let $\mathcal{O} = -\mathcal{O}$, and note for both cases that $-(-P) = P$. If $-P = P = (x_0, 0)$, then $P + P = \mathcal{O}$.

Similarly, for $\mathcal{O} \neq P, Q \in E(k)$, we define $-(P + Q)$ to be the third point of intersection between $E(k)$ and the line connecting P with Q (or tangent if $P = Q$), from which $P + Q$ arises naturally. We set $\mathcal{O} + P = P + \mathcal{O} = P$.

At this point it should be evident that $+$ is commutative with identity \mathcal{O} .

2.4 Explicit Composition Formulae

We now develop explicit formulae. We need only treat the remaining case where $\mathcal{O} \neq P, Q \in E(k)$, $P \neq Q$ with $P = (x_0, y_0), Q = (x_1, y_1)$. For notation, let us write $P + Q = (x_2, y_2)$.

Let us denote the slope of the secant line through P and Q by λ , which in the case $P \neq Q$ is $\frac{y_1 - y_0}{x_1 - x_0}$; otherwise, $\frac{3x_0^2 + a}{2y_0}$ which is obtained through implicit differentiation. From this we obtain the tangent line, $y = \lambda(x - x_0) + y_0 \Rightarrow y^2 = (\lambda(x - x_0) + y_0)^2$, from which it follows $\lambda^2 x^2 + 2(y_0 - \lambda x_0)x + (-\lambda x_0 + y_0)^2 = x^3 + ax + b$. Combining terms and noting that $x^3 - \lambda^2 x^2 + \dots = (x - x_0)(x - x_1)(x - x_2)$, we obtain $x_2 = \lambda^2 - x_0 - x_1$, and by substitution, $y_2 = \lambda(x_2 - x_0) + y_0$.

Note that with the preceding formulas, the associativity of $+$ is verifiable non-geometrically, so we have indeed a group structure on $E(k)$.

Keeping the above notation, we now wish to introduce $P - Q = (x_3, y_3)$, and determine $x_2 + x_3$ and $x_2 x_3$. Let λ_2 denote λ as above, and $\lambda_3 = -\frac{y_1 + y_0}{x_1 - x_0}$. We have $\lambda_2^2 + \lambda_3^2 = \frac{(y_1 - y_0)^2}{(x_1 - x_0)^2} + \frac{(y_1 + y_0)^2}{(x_1 - x_0)^2} = 2\frac{y_1^2 + y_0^2}{(x_1 - x_0)^2} = 2\frac{x_1^3 + x_0^3 + a(x_1 + x_0) + 2b}{(x_1 - x_0)^2}$, as well as $\lambda_2 \lambda_3 = \frac{-y_1^2 + y_0^2}{(x_1 - x_0)^2} = \frac{-(x_1^3 + ax_1 + b) + (x_0^3 + ax_0 + b)}{(x_1 - x_0)^2} = \frac{-x_1^3 + x_0^3 + a(-x_1 + x_0)}{(x_1 - x_0)^2} = -\frac{x_1^2 + x_0 x_1 + x_0^2 + a}{x_1 - x_0}$. Thus,

$$\begin{aligned} x_2 + x_3 &= (\lambda_2^2 - x_0 - x_1) + (\lambda_3^2 - x_0 - x_1) = (\lambda_2^2 + \lambda_3^2) - 2(x_0 + x_1) \\ &= \frac{2(x_1 + x_0)(a + x_1 x_0) + 4b}{(x_1 - x_0)^2} = \frac{2(x_1 + x_0)(a + x_1 x_0) + 4b}{(x_1 + x_0)^2 - 2x_1 x_0}. \end{aligned}$$

Similarly,

$$x_2 x_3 = \frac{(x_1 x_0 - a)^2 - 4b(x_1 + x_0)}{(x_1 - x_0)^2} = \frac{(x_1 x_0 - a)^2 - 4b(x_1 + x_0)}{(x_1 + x_0)^2 - 2x_1 x_0}.$$

2.5 Heights of Points over \mathbb{Q}

A *valuation* on a field k is a function $|\cdot| : K \rightarrow \mathbb{R}$, such that $|x| \geq 0 \quad \forall x \in K$, $|x| = 0 \iff x = 0$, $|xy| = |x||y|$ and $|x + y| \leq |x| + |y|$. We denote the set of non-trivial valuations on k by M_k , which will be useful later for defining heights. In addition, we define M_k^0 to be the set of *non-archimedean* valuations, which are those satisfying the additional property $|x + y| \leq \max\{|x|, |y|\}$. The others are called *archimedean*, or *infinite* valuations, denoted by M_k^∞ .

The case $k = \mathbb{Q}$ is of particular interest to us. In particular, $M_{\mathbb{Q}}^\infty$ has just one element $|\cdot|_\infty$, which is our standard absolute value on \mathbb{R} (and hence, \mathbb{Q}). On the other hand, $M_{\mathbb{Q}}^0$ consists of the p -adic absolute values $\{|\cdot|_p : p \text{ prime}\}$, where for $x \in \mathbb{Q}$, $|x|_p = p^{-n}$, $x = p^n \left(\frac{a}{b}\right)$, $(a, b) = 1$ (we set $|0|_p = 0$).

Now, for a projective point $P = (x_0, \dots, x_n) \in \mathbb{P}^n(k)$, we define its *height* by $H(P) = \prod_{v \in M_{\mathbb{Q}}} \max\{|x_0|_v, \dots, |x_n|_v\}$. We need to check that H is well-defined.

As an immediate consequence of unique factorization in \mathbb{Q} , we have the *Product Formula*: $\prod_{v \in M_{\mathbb{Q}}} |x|_v = 1$ for $x \in \mathbb{Q}^*$. From this it follows that

$$\prod_{v \in M_{\mathbb{Q}}} \max_i \{|x_i|_v\} = \prod_{v \in M_{\mathbb{Q}}} \max_i \{|\lambda|_v |x_i|_v\} = \prod_{v \in M_{\mathbb{Q}}} \max_i \{|\lambda x_i|_v\}$$

which implies $H(P) = H(\lambda P)$ for $\lambda \in \mathbb{Q}^*$, and H is well-defined. Moreover, we may even rewrite H for special homogeneous co-ordinates. Assume $P = (x_0, \dots, x_n)$, where $x_i \in \mathbb{Z}$ and $\gcd(x_0, \dots, x_n) = 1$. (If not, simply scale by an appropriate λ .) Then as $\prod_{v \in M_{\mathbb{Q}}^0} \max_i \{|x_i|_v\} = 1$, it follows that $H(P) = \prod_{v \in M_{\mathbb{Q}}^\infty} \max_i \{|x_i|_v\} = \max\{|x_0|, \dots, |x_n|\}$.

For notation, we will deal with the *logarithmic height*, defined by

$$h \equiv \log H.$$

Suppose $P = (x_0, y_0) \in E(\mathbb{Q})$. From the two heights given above, we also define *heights relative to x* in the case of $\mathbb{P}^2(\mathbb{Q})$, which are $H_x(P) = H([x_0, 1])$ and $h_x(P) = h([x_0, 1])$. If $x_0 = \frac{a}{b}$ with $\gcd(a, b) = 1$, then

$$H_x(P) = H([a, b]) = \max\{|a|, |b|\}.$$

2.6 Height Estimates

For $P, Q \in E(\mathbb{Q})$, we wish to relate $h(P + Q)$ to $h(P)$ and $h(Q)$. We require some basic facts about non-archimedean valuations, which we present.

In particular, let $|\cdot|_p \in M_{\mathbb{Q}}^0$. For $x, y \in \mathbb{Q}$, write $x = p^n \left(\frac{a}{b}\right)$, $y = p^m \left(\frac{c}{d}\right)$, $\gcd(p, abcd) = 1$. Now suppose $n = m$. Then $|x + y|_p = p^{-n} \left|\frac{ad+bc}{bd}\right|_p \leq |x|_p = |y|_p$ since $p \nmid bd$. On the other hand, if $n < m$, then $|x + y|_p = p^{-n} \left|\frac{a}{b} + p^{m-n} \left(\frac{c}{d}\right)\right|_p = p^{-n} = \max \left\{ |x|_p, |y|_p \right\}$.

For an arbitrary valuation v , set $\varepsilon(v)$ to be 2 if $v = |\cdot|_{\infty}$, 1 otherwise. Then, we may loosen the above to obtain $|x + y|_v \leq \varepsilon(v) \max \left\{ |x|_v, |y|_v \right\}$. (Clearly $|x + y|_{\infty} \leq |x|_{\infty} + |y|_{\infty} \leq 2 \cdot \max \left\{ |x|_{\infty}, |y|_{\infty} \right\}$.)

Now, let $P = (a, b) \in \mathbb{A}^2(\mathbb{Q})$. Write $T^2 + aT + b = T^2 + (\alpha + \beta)T + \alpha\beta = (T + \alpha)(T + \beta)$ and consider the extension of $M_{\mathbb{Q}}$ to $M_{\mathbb{Q}(\alpha, \beta)}$.

We first derive our upper bound. In particular, we wish to show

$$\max \left\{ |\alpha + \beta|_v, |\alpha\beta|_v, 1 \right\} \leq \varepsilon(v) \max \left\{ |\alpha|_v, 1 \right\} \cdot \max \left\{ |\beta|_v, 1 \right\}.$$

Let v be a valuation. Then by the above estimates,

$$|\alpha + \beta|_v \leq \varepsilon(v) \max \left\{ |\alpha|_v, |\beta|_v \right\} \leq \varepsilon(v) \max \left\{ |\alpha|_v, 1 \right\} \cdot \max \left\{ |\beta|_v, 1 \right\}.$$

Also,

$$|\alpha\beta|_v = |\alpha|_v |\beta|_v \leq \varepsilon(v) \max \left\{ |\alpha|_v, 1 \right\} \cdot \max \left\{ |\beta|_v, 1 \right\}.$$

Finally, $1 \leq \varepsilon(v) \max \left\{ |\alpha|_v, 1 \right\} \cdot \max \left\{ |\beta|_v, 1 \right\}$ trivially.

We proceed to our lower bound:

$$\max \left\{ |\alpha + \beta|_v, |\alpha\beta|_v, 1 \right\} \geq \frac{1}{\varepsilon(v)} \max \left\{ |\alpha|_v, 1 \right\} \cdot \max \left\{ |\beta|_v, 1 \right\}.$$

First we consider the case where $|\cdot|_v$ is archimedean. We may assume without loss of generality that $\max \left\{ |\alpha|_v, |\beta|_v \right\} > 1$, say $|\alpha|_v > 1$; otherwise $\max \left\{ |\alpha|_v, 1 \right\} \cdot \max \left\{ |\beta|_v, 1 \right\} \leq 1$. Now if in addition $|\beta|_v \geq 1$, clearly

$$|\alpha\beta|_v = |\alpha|_v |\beta|_v = \max \left\{ |\alpha|_v, 1 \right\} \cdot \max \left\{ |\beta|_v, 1 \right\};$$

else $|\beta|_v < 1$ and

$$|\alpha + \beta|_v = |\alpha|_v = \max \left\{ |\alpha|_v, 1 \right\} \cdot \max \left\{ |\beta|_v, 1 \right\}.$$

Consider the remaining case where $|\cdot|_v = |\cdot|_\infty$. If $\alpha, \beta \geq 1$ or $\alpha, \beta \leq 1$ then this is trivial; so we may assume $\alpha > 1, \beta < 1$. However, then $\frac{1}{\varepsilon(v)} \max\{|\alpha|_v, 1\} \cdot \max\{|\beta|_v, 1\} = \frac{|\alpha|}{2}$. We need only consider the case in which $\frac{|\alpha|}{2} > 1$, from which it follows

$$|\alpha + \beta| \geq |\alpha| - |\beta| \geq \frac{|\alpha|}{2},$$

and we are done.

Combining our bounds:

$$\begin{aligned} & \frac{1}{\varepsilon(v)} \max\{|\alpha|_v, 1\} \cdot \max\{|\beta|_v, 1\} \\ & \leq \max\{|\alpha + \beta|_v, |\alpha\beta|_v, 1\} \\ & \leq \varepsilon(v) \max\{|\alpha|_v, 1\} \cdot \max\{|\beta|_v, 1\}, \end{aligned}$$

multiplying through for all v and finally taking logarithms of each side, we obtain

$$\begin{aligned} |h([1, \alpha + \beta, \alpha\beta]) - (h([1, \alpha]) + h([1, \beta]))| &\leq \log 2 \\ |h(a, b) - (h([1, \alpha]) + h([1, \beta]))| &\leq \log 2 \end{aligned}$$

as desired.

For looser estimates but for $H(\alpha_1, \dots, \alpha_n)$ with arbitrary n , consult [Silverman, VIII.5.9].

We now outline a proof that $h(P+Q) + h(P-Q) = 2h(P) + 2h(Q) + O(1)$ from [5, VIII.6.2]. Using the formulas for the x -coordinates of $P+Q$ and $P-Q$ derived earlier as motivation, define the morphism $g : \mathbb{P}^2(k) \rightarrow \mathbb{P}^2(k)$, $[t, u, v] \mapsto [u^2 - 4tv, 2u(at+v) + 4bt^2, (v-at)^2 - 4btu]$, where a, b are the short Weierstraß equation coefficients. We define as well $\sigma : E(k) \times E(k) \rightarrow \mathbb{P}^2(k)$, $(P, Q) = ((x_0, y_0), (x_1, y_1)) \mapsto [1, x_0 + x_1, x_1x_2]$. Then if we set $G : E(k) \times E(k) \rightarrow E(k) \times E(k)$, $(P, Q) \mapsto (P+Q, P-Q)$, we have $\sigma \circ G = g \circ \sigma$.

For P, Q as above, note that $h(\sigma(P, Q)) = h([1, x_0 + x_1, x_0x_1])$. By the result proven above, we have

$$|h(\sigma(P, Q)) - (h_x(P) + h_x(Q))| = |h(\sigma(P, Q)) - (h([1, x_0]) + h([1, x_1]))| \leq \log 2.$$

Using the fact that if ϕ is a morphism then

$$|h(\phi(P)) - \deg(\phi) \cdot h(P)|$$

is bounded (Silverman, VIII.5.6), this yields

$$\begin{aligned} h_x(P+Q) + h_x(P-Q) &\approx h(\sigma(P+Q, P-Q)) = h(\sigma \circ G(P, Q)) \\ &= h(g \circ \sigma(P, Q)) \approx 2h(\sigma(P, Q)) \\ &\approx 2h_x(P) + 2h_x(Q), \end{aligned}$$

as desired.

2.7 Canonical Heights

From the height estimates derived above, it is possible to induce a refined height with the error terms given in the above results removed. We deal with the same cases as before; however, the following holds with any height (Silverman, VIII.9.3)

For $P \in E(\mathbb{Q})$, define

$$\hat{h}(P) = \lim_{n \rightarrow \infty} \frac{h_x(2^n P)}{4^n}.$$

We show \hat{h} exists. Take $n, m \in \mathbb{Z}$, $m \geq n \geq 0$. Then,

$$\left| \frac{h_x(2^m P)}{4^m} - \frac{h_x(2^n P)}{4^n} \right| \leq \frac{1}{4^n} \sum_{i=0}^{m-1} \left| \frac{h_x(2^{n+i+1} P)}{4^{i+1}} - \frac{h_x(2^{n+i} P)}{4^i} \right|$$

by applying the triangle inequality to the corresponding telescoping sum. At this point, we note the pseudo-parallelogram law from above. As $h_x(P+Q) + h_x(P-Q) = 2h_x(P) + 2h_x(Q) + O(1) \Rightarrow h_x(P+P) + h_x(P-P) = 2h_x(P) + 2h_x(Q) + O(1)$, we see $h_x(2P) = 4h_x(P) + O(1)$. From this it follows $\left| \frac{h_x(2^{n+i+1} P)}{4^{i+1}} - \frac{h_x(2^{n+i} P)}{4^i} \right| \leq \frac{O(1)}{4^i}$, and applying this to our earlier estimate, we have

$$\left| \frac{h_x(2^m P)}{4^m} - \frac{h_x(2^n P)}{4^n} \right| \leq \frac{1}{4^n} \sum_{i=0}^{m-1} \frac{1}{4^i} = \frac{1 - 4^{-m}}{3 \cdot 4^{n-1}} < 4^{1-n}.$$

Thus, $\left\{ \frac{h_x(2^n P)}{4^n} \right\}$ is Cauchy, so by the completeness of \mathbb{R} , \hat{h} , our *canonical height*, exists.

We now express $\hat{h}(mP)$ in terms of $\hat{h}(P)$. By induction and noting $h(mP) = m^2 h(P) + O(1) \Rightarrow \frac{h(2^n mP)}{4^n} = \frac{m^2 h(2^n P)}{4^n} + \frac{O(1)}{4^n}$, by taking limits we see $\hat{h}(mP) - m^2 \hat{h}(P) = \lim_{n \rightarrow \infty} \frac{O(1)}{4^n} = 0$, so

$$\hat{h}(mP) = m^2 \hat{h}(P).$$

2.8 Discrete Logarithms

With the existence of a canonical height, computing a discrete logarithm follows trivially. Supposing $Q = mP$, by $\hat{h}(mP) = m^2\hat{h}(P)$, we have

$$m^2 = \frac{\hat{h}(mP)}{\hat{h}(P)} \iff m = \pm \sqrt{\frac{\hat{h}(mP)}{\hat{h}(P)}}.$$

Note that we have non-trivial heights only in $E(k)$ for k global. For other fields, no such heights exist and the corresponding elliptic curve discrete logarithm algorithms perform comparable to those for general groups.

Consult the Appendix for an overview of the problem.

3 Applications

There exist many algorithms for general group structures which are enhanced with the utilisation of elliptic curves. We will attempt to illustrate a few such methods.

3.1 Factorization

Consider the problem of factoring a known composite n — in particular, extracting an (unknown) prime factor p , or in some cases, a composite proper one.

We first illustrate Pollard's $p-1$ algorithm. The algorithm involves first taking a number $a \in (1, n)$, for which it is assumed $\gcd(a, n) = 1$ (otherwise, no more work is needed). By Fermat's Little Theorem, $p|a^{p-1} - 1 \equiv a^k - 1 \pmod{p}$ for any multiple k of $p-1$. Combining this with the assumption that $p|n$, once we find a k such that $p-1|k$, it follows $\gcd(a^k, n) \neq 1$ (computed via the Euclidean algorithm).

Clearly, with a large enough k , n may be factored. Unfortunately, this method is favorable to primes p where $p-1$ factors into small primes (reducing the required size of k). The adaptation of Pollard's $p-1$ to elliptic curves is Lenstra's Elliptic Curve algorithm, for which we state a few results.

We show that if $P = (x, y) \in E(\mathbb{Q})$, then $x = \frac{n_x}{e^2}, y = \frac{n_y}{e^3}$ with $\gcd(n_x n_y, e) = 1$. Write $x = \frac{n_x}{m_x}$ and $y = \frac{n_y}{m_y}$ in reduced form. From $y^2 = x^3 + ax + b$, we obtain $n_y^2 m_x^3 = n_x^3 m_y^2 + a n_x m_x^2 m_y^2 + b m_x^3 m_y^2$. By the co-primality of

m_y and $n_y, m_y^2 | m_x^3$. Similarly, $m_x^2 | m_y^2$ from which we deduce $m_x^3 | m_y^2$. Thus, $m_x^3 = m_y^2$ and setting $e = \frac{m_y}{m_x}$, we have our desired result.

Noting this, suppose we have a point $P = (\frac{x}{e^2}, \frac{y}{e^3})$ with $\gcd(xy, e) = 1$. In normalized homogeneous coordinates, this is $[e^3, ex, y]$, which reduces to $\mathbb{A}^2(\mathbb{F}_p)$ iff $p \nmid e$. In other words, $P \mapsto \mathcal{O} \in E(\mathbb{F}_p)$ iff $p \nmid e$.

Thus, suppose as before that we have a prime $p|n$, but the group $E(\mathbb{F}_p)$ (reduced from $E(\mathbb{Q})$) instead of $(\mathbb{Z}/p\mathbb{Z})^*$. This grants considerable freedom, as the order of the group is no longer fixed in terms of p . By Hasse (Silverman V.1.1), $|E(\mathbb{F}_p)| \in [p+1-2\sqrt{p}, p+1+2\sqrt{p}]$, where $|E(\mathbb{F}_p)|$ is well-distributed around this range for different $E(\mathbb{F}_p)$. Then if $|E(\mathbb{F}_p)|$ divides k , then for any point $P \in E(\mathbb{Q})$, $kP = (\frac{x}{e^2}, \frac{y}{e^3}) \mapsto \mathcal{O} \in E(\mathbb{F}_p)$ under the reduction homomorphism and $p \mid \gcd(e, n)$, as desired.

We now proceed to the algorithm itself. We first check that $2, 3 \nmid n$ and that n is not a perfect power. Then, our curve is constructed by choosing random coordinates $x_0, y_0 \in \mathbb{Z}$ for $P = (x_0, y_0) \in E(\mathbb{Q})$ and some $a \in \mathbb{Z}$, implying the curve with short Weierstraß equation $y^2 = x^3 + ax + (y_0^2 - x_0^3 - ax_0)$. Following this, the discriminant Δ is checked: if $n|\Delta$, we have bad reduction for every prime $p < n$ and must select a new curve; if $\gcd(n, \Delta) \neq 1$, we are done; otherwise, the algorithm continues.

At this point, we choose some k as in Pollard's algorithm, and compute $kP = (\frac{x}{e^2}, \frac{y}{e^3})$. If our choice of k is sufficiently large for the chosen curve, $p \mid \gcd(e, n)$ and we are done. Otherwise, either $\gcd(e, n) = 1$ and k is increased (if not feasible, then a new curve is selected), or $\gcd(e, n) = n$, which implies k is too large.

To ease storage concerns, the intermediary computations are usually carried out in $\mathbb{Z}/n\mathbb{Z}$ instead of \mathbb{Q} . Computations proceed as in $E(\mathbb{Q})$, except occasionally the need to invert a non-unit arises when computing the composition law's slopes. But this means that we have hit a non-trivial factor of n .

3.2 Primality Testing

As attempts to factor composite numbers are generally more successful than for prime numbers, we describe primality tests which conclusively show primality. These tests are generally only applied to likely primes, that is, after tests designed to conclusively show compositeness have failed (for example, Miller-Rabin, [Koblitz, V.1]).

Assume we are testing $n \in \mathbb{Z}$ for primality. Suppose first we find a prime $q \mid n - 1$ with $q \geq \sqrt{n - 1}$, whose primality can be asserted with a recursive application of this test. If secondly we find an $a \in \mathbb{Z} \cap (1, n)$ such that $a^{n-1} \equiv 1 \pmod{n}$ and $a^{(n-1)/q} - 1$ is coprime to n , then n is prime. For if n were composite, taking a prime $p \leq n$, $p \mid n$ would imply

$$u, v \in \mathbb{Z} \quad uq + v(p - 1) = 1 \Rightarrow uq \equiv 1 \pmod{p - 1}$$

by the Euclidean algorithm and subsequently

$$p \mid a^{n-1} - 1 = a^{uq(n-1)/q} - 1 \equiv a^{(n-1)/q} - 1 \pmod{p},$$

contradicting coprimality. This is *Pocklington's primality test*.

The elliptic curve primality test works analogously. Let E be an elliptic curve given a Weierstraß equation with coefficients in \mathbb{Z} . Define $E(\mathbb{Z}/n\mathbb{Z})$ to be a set of points satisfying this Weierstraß equation with addition of points defined according to the previously-developed formulae where possible. (Note that if n is prime, this is indeed the group of points on an elliptic curve.)

Suppose that for some $m \in \mathbb{Z}$ we find a prime $q \mid m$, $q < (n^{\frac{1}{4}} + 1)^2$ (whose primality is again proved recursively). If further we locate a point $P \in E(\mathbb{Z}/n\mathbb{Z})$ such that $mP = \mathcal{O}$ and $\left(\frac{m}{q}\right)P \neq \mathcal{O}$, then n is prime. (Note that if mP or $\left(\frac{m}{q}\right)P$ are not defined, then n must be composite.) If otherwise and n is composite, take a prime $p \mid n$, $p \leq \sqrt{n}$ and reduce

$$E(\mathbb{Z}/n\mathbb{Z}) \rightarrow E(\mathbb{Z}/p\mathbb{Z}), \quad P \mapsto \tilde{P}.$$

However, proper by Hasse,

$$|E(\mathbb{Z}/p\mathbb{Z})| \leq p + 1 + 2\sqrt{p} = (\sqrt{p} + 1)^2 \leq (n^{\frac{1}{4}} + 1)^2 < q$$

so we take $u \in \mathbb{Z}$ with $uq \equiv 1 \pmod{|E(\mathbb{Z}/p\mathbb{Z})|}$. However, then

$$\left(\frac{m}{q}\right)P = uq \left(\frac{m}{q}\right)P = u(mP) = \mathcal{O},$$

contradicting the reduction $E(\mathbb{Z}/n\mathbb{Z}) \setminus \mathcal{O} \rightarrow E(\mathbb{Z}/p\mathbb{Z}) \setminus \mathcal{O}$.

3.3 Cryptosystems based on Elliptic Curves

We first introduce an example of a public-key cryptosystem, where two parties, without any prior knowledge from each other, wish to communicate some information securely — ie., inaccessible to third parties. In practise, public-key cryptosystems generally exist to support private-key cryptosystems via the initial determination of a private key due to lengthy computational run-times.

Let G be a publicly-known arbitrary group. Our goal between two parties is to establish a private key through public channels; that is, agree on some element $k \in G$ without publically divulging enough information for a third party to determine k .

The following scheme, called Diffie-Hellman Key Exchange, works as follows. A publically-known random $g \in G$ is first established through any means. The two parties in question each independently randomly pick an integer, say $a, b \in \mathbb{Z}$ and proceed to publically divulge g^a and g^b , respectively.

At this stage, we may consider g, g^a and g^b are open knowledge. With the additional knowledge of a or b , each of the original parties may easily compute $(g^b)^a = g^{ab} = (g^a)^b$, which is the desired key.

The basis of this cryptosystem rests on the secrecy of g^{ab} , and in particular, the Diffie-Hellman Assumption which claims the computational infeasibility of g^{ab} from only the publically-known g^a, g^b and g . This is no harder (but not necessarily easier) than the discrete logarithm problem; that is, determining n when g and g^n are given, which easily implies a solution to Diffie-Hellman.

References

- [1] Artin, Michael. *Algebra*. Prentice-Hall, 1991.
- [2] Dummit, David S.; Foote, Richard M. *Abstract Algebra*. Prentice-Hall, 1999.
- [3] Koblitz, Neal. *A course in number theory and cryptography*. Springer-Verlag, 1994.
- [4] Lidl, Rudolf; Niederreiter, Harald. *Introduction to finite fields and their applications*. Cambridge University Press, 1994.

- [5] Silverman, Joseph H. *The arithmetic of elliptic curves*. Springer-Verlag, 1986.
- [6] Silverman, Joseph H.; Tate, John. *Rational points on elliptic curves*. Springer-Verlag, 1992.

A Student Cryptography Seminar

This 11-week seminar was the first of a proposed student seminar series on cryptography and coding theory, primarily based on Johannes A. Buchmann's book *Introduction to Cryptography*, Springer-Verlag 2001.

To be honest, this was an interesting experience in many ways. Although I didn't gain much academically from the initial lectures, it was instructive to observe how various lecturers presented their material as well as how they interacted with the audience, especially with the occasional oft-heated debates.

I gave lectures on three of the last sessions. My presentations taught me a great deal of the art of conveying mathematics; in particular, I discovered many things not to do.

For further information, consult the web page located at:
<http://math.usask.ca/~marles/outline/references.html>

B As a Whole

This summer was the second I spent working doing mathematics at the University of Saskatchewan. However, as an experience this summer was considerably different, as it involved vastly more independence and self-direction on my part; previously I was assisting with an ongoing research project instead of undertaking one of my own. While this necessitated a great deal of focus from me, I would consider this a somewhat more rewarding experience, most notably towards the latter part of my term here.

I would venture claiming the latter half of my time spent was more immediately profitable than the former. As the summer progressed, I developed a better sense of direction and in fact, a better conception of research itself. Perhaps this was due to the increasing familiarity I gained with my research material, as I initially had no prior exposure to the general subject matter.

As I better acquainted myself with the field, I grasped a better sense of, simply put, what I was doing. During the early summer, although I was fortunate to have learned a massive amount of material, there was the discomforting feeling of being led around in the dark, in addition to the intimidating awe caused by the apparent vast infinitude of pre-established mathematics bearing down on me. Fortunately, as I established a better foothold and general awareness of my activities, this subsided, gradually replaced by an excited feeling of curiosity and discovery.

In any case, I enjoyed this experience and look forward to engaging in it again (albeit perhaps with something slightly more immediately accessible for the sake of time).

C Additional Materials

Following are the slide outlines of the 3 talks I presented, reproduced from <http://math.usask.ca/~leej/seminar/>.

C.1 The Quadratic Sieve

Many numerical methods (not necessarily just those for integers) involve a sieve, whereby undesirable numbers are systematically ruled out in order to leave a particular set of numbers satisfying a particular property.

Perhaps the most simple of these is the Sieve of Eratosthenes, where multiples of primes (except for the prime itself) are crossed off, leaving at the end of the algorithm a table of uncrossed numbers corresponding to the primes in the respective interval.

This sieve can be enhanced to yield the factorizations of all numbers in a given interval with a simple modification – instead of crossing out the multiples of a prime, we simply repeatedly divide by the prime as many times as possible.

For determining the factorizations of the numbers in $[1, n]$, this is actually fairly efficient, with approximately $n \cdot \left(\frac{1}{2} + \frac{1}{3} + \frac{1}{5} + \dots + \frac{1}{p_{\pi(n)}} \right)$, or $n \cdot \sum_{i=1}^{\pi(n)} \frac{1}{p_i}$ $\approx n \cdot \sum_{i=1}^{\pi(n)} \frac{1}{i \log i} \approx n \cdot \int_1^{\pi(n)} \frac{1}{x \log x} dx \approx n \cdot \log \log n = O(n \log \log n)$ steps. This is fairly efficient if we do desire all factorizations for $m \in [1, n]$, but for n itself, we need a better method.

As its name implies, the method of factoring integers via the quadratic

sieve involves quadratic terms, or those involving squares. We already know one such method, that is, the “difference of squares” identity, which states $a^2 - b^2 = (a + b) \cdot (a - b)$. Clearly, if we’re lucky enough to find $a, b \in \mathbb{Z}$, $a^2 - b^2 = n$, then factoring n is then trivialized.

Does such a factorization always exist? Suppose $n = ab, 2 \nmid a, b$. (Note that a and b need not be prime.) Then, $n = \left[\frac{1}{2}(a + b)\right]^2 - \left[\frac{1}{2}(a - b)\right]^2$, and such a difference of squares exists.

Since $n = a^2 - b^2 \iff a^2 - n = b^2$, we need only systematically try values for a until $a^2 - n$ is a square. (Using $n + b^2 = a^2$ instead would work equally well in theory; however, we will see that we wish to minimize our dependent variable.)

This is quite easy to check in \mathbb{Z} . Unfortunately, this method, due to Fermat, tends only to work well when b is small; ie., when n has two factors close to \sqrt{n} . (Note that there may be other “pairs of factors” as well.)

We can refine this method by relaxing the initial condition to $a^2 \equiv b^2 \pmod{n} \iff a^2 - b^2 = kn \quad k \in \mathbb{Z}$. Of course, this does not work well; for instance, if $a = b = 0$, we have nothing to work with. We thus impose the necessary and sufficient additional condition that $a \not\equiv \pm b \pmod{n}$.

Since $a^2 - b^2 \equiv 0 \pmod{n} \iff n \mid a^2 - b^2 = (a + b) \cdot (a - b)$, and that $a \not\equiv b \pmod{n} \iff n \nmid (a + b), (a - b)$, we obtain $d = \gcd(n, a - b) \neq 1$ to be a non-trivial factor of n and we are done. (Note that $a \equiv \pm b \pmod{n} \implies (a + b) \text{ or } (a - b) \equiv 0 \pmod{n} \implies n \mid (a + b)(a - b)$ trivially.)

It is important to note that, while trying different values of a , we have no way of determining *a priori* whether $a \equiv \pm b \pmod{n}$ for the resultant value of $b = \sqrt{a^2 - n} \in \mathbb{Z}$, if it even exists. This applies to the next refinement.

We now introduce the concept of factor bases. In determining whether a number is square, it is fairly useful to have a prime factorization, especially if we are to consider arbitrary products from a set of given numbers. For this purpose, we choose a $B < n$ and construct the prime factor base $F(B) = \{2, 3, 5, \dots, p_{\pi(B)}\} \cup \{-1\}$ consisting of the primes less than B in addition to -1 , which indicates sign.

With this factor base, we are able to define the concept of B -smooth numbers; that is, the integers factoring completely over $F(B)$. We may then represent each B -smooth integer $n = (-1)^{\lambda_0} \cdot \prod_{i=1}^{\pi(B)} p_i^{\lambda_i}$ by a vector $\{\lambda_0, \lambda_1, \dots, \lambda_{\pi(B)}\} \in \mathbb{Z}^{\pi(B)+1}$. By inspection, n is a square in \mathbb{Z} iff each of its corresponding λ_i are even. As exponent parity is all we care about, we therefore reduce n to an exponent vector in $\mathbb{F}_2^{\pi(B)+1}$. (This defines a

homomorphism $(\mathbb{Q}^*, \cdot) \rightarrow (\mathbb{F}_2^{\pi(B)+1}, +)$.

We now briefly modify notation. For some a_i , define $c_i = a_i^2 - n$. (Compare this to $b_i = \sqrt{a_i^2 - n}$, though we do not make use of it.) Above, we sought an a such that b^2 (existed and) was a square. Now, we seek some $\{a_i\}$ such that $\prod_i c_i$ forms a square. By linear algebra and considering the reductions of the c_i to $\mathbb{F}_2^{\pi(B)+1}$, we're assured a linearly dependent set $\{c_i\}$ and thus a square $\prod_i c_i$ after no more than $\pi(B) + 2$ candidates for c_i .

C.2 Discrete Logarithm Problem

C.2.1 Preliminaries

- definitions: suppose $G = \langle \gamma \rangle$
 - order of $\alpha \in G$: $\text{ord}(\alpha) := \min\{x \in \mathbb{Z}^+ : \alpha^x = 1\}$
 - γ -logarithm of $\alpha \in G$: $\log_\gamma(\alpha) := \min\{x \in \mathbb{Z}^+ : \gamma^x = \alpha\}$
 - exponent of G : $\text{exp}(G) := \min\{x \in \mathbb{Z}^+ : g^x = 1 \ \forall g \in G\} = \text{lcm}\{\text{ord}(\alpha) : g \in G\}$
- generalized discrete logarithm problem for infinite cyclic groups generally applies in non-cryptographic contexts (harder for curves)

C.2.2 Silver-Pohlig-Hellman method

- reduces problem to subproblems in group's prime decomposition ($(n, m) = 1 \iff C_{nm} = C_n \times C_m$)
 - subproblem: finding $\log_{\gamma_p} \alpha_p$, where $\gamma_p = \gamma^{n/p^{e_p}}$, $\alpha_p = \alpha^{n/p^{e_p}}$ (notice: $\log_\gamma \gamma_p = p^{e_p}$)
 - determine x , $x \equiv \log_{\gamma_p} \alpha_p \pmod{p^{e_p}}$ for all p (note that for all p : $1 = \gamma_p^{-x_p} \alpha_p = (\gamma^{-x_p} \alpha)^{n/p^{e_p}} = (\gamma^{-x_p + k \cdot p^{e_p}})^{n/p^{e_p}} = (\gamma^{-x} \alpha)^{n/p^{e_p}}$)
- further reduction from prime-power-order groups to prime-order groups
 - suppose $|G| = p^e$, and let $\sum_{i=0}^{e-1} x_i p^i$ be the base- p expansion of $\log_\gamma x$
 - defining $a_i = \alpha \cdot \gamma^{-\sum_{n=0}^i x_n p^n}$, we obtain $(\gamma^{p^{e-1}})^{x_i} = a_i^{p^{e-i-1}}$, $0 \leq i \leq e-1$

- actual algorithm - reduce to prime-power case (Chinese Remainder Theorem), reduce to prime case (Lagrange's Theorem / Fermat's Little Theorem), solve (Baby-Step, Giant Step / ρ -algorithm)
 - runtime: $O\left(\sum_{p||G|} (e_p (\log |G| + \sqrt{p}))\right)$
 - works best with small prime factors (Mersenne primes advantageous)

C.2.3 Index Calculus Method

- more suited to multiplicative groups of finite fields, ie. $\mathbb{F}_{p^n}^*$
- re-introduction of factor bases
 - note that if $\alpha = \prod_i \alpha_i$, then $\log_\gamma \alpha \equiv \sum_i \log_\gamma \alpha_i \pmod{|G|}$
 - compute $\log_\gamma v$ for v in factor base
 - * take exponent vectors for $\{\alpha^t\}$, note that $t \equiv \sum_i \log_\gamma \alpha_i^{e_i} \pmod{|\langle \gamma \rangle|}$
 - * acquire independent set of $|\{v\}|$ relations, solve to obtain $\log_\gamma v$
- determine $\log_\gamma \alpha$
 - find t so that $\alpha\gamma^t$ is smooth
 - factor and obtain $\log_\gamma \alpha \equiv \sum_i \log_\gamma (\alpha\gamma)_i \cdot e_i - t \pmod{|\langle \gamma \rangle|}$

C.3 Overview of Elliptic Curves

C.3.1 Projective Planes

- given k a field, the affine n -space \mathbb{A}^n is constructed
- by identifying "projective" points (can be considered at "infinity") with directions in \mathbb{A}^n , the projective n -space \mathbb{P}^n is constructed
- this gives the relation $\mathbb{P}^n = \mathbb{A}^n \cup \mathbb{P}^{n-1}$

C.3.2 Weierstraß Equations

- Weierstraß equation: in simplest form, takes the form: $y^2 = x^3 + ax + b$ (assuming $\text{char}(k) \neq 2, 3$)
- defines a curve over \mathbb{A}^2 , which can be extended to via homogenization ($Y^2Z = X^3 + aXZ^2 + bZ^3$) and then to \mathbb{P}^2 by imposing $Z = 0$
- results in elliptic curve over \mathbb{P}^2 with one point at infinity, allowing for Bézout to hold

C.3.3 Bézout's Theorem

- let C_1 and C_2 be projective curves with no common components
- then, $\sum_{P \in C_1 \cap C_2} I(C_1 \cap C_2, P) = (\deg C_1)(\deg C_2)$, where I denotes intersection multiplicity

C.3.4 Group Structure on Curves

- two classes of curves: singular (cusp or node) and non-singular (smooth)
- singular curves permit easy parameterizations (and thus groups with trivial structures)
- non-singular curves admit obscure group structures

C.3.5 Group Law on Non-Singular Elliptic Curves

- define an additive abelian group with \mathcal{O} as the point at infinity
- given two points, $P, Q \in E(k)$:
 - take the line connecting P and Q and find its other intersection with $E(k)$, call it $-(P + Q)$
 - take the line connecting $-(P+Q)$ and \mathcal{O} ; the resulting intersection is $(P + Q)$
- easy to verify identity, inverses and commutativity

C.3.6 Group Law Formulae

- easily derivable through some algebra
- given $P = (x_1, y_1)$ $Q = (x_2, y_2)$, take λ to be the slope of the line joining P, Q
- this results in $P + Q = (x_3, y_3)$, where $x_3 = (\lambda^2 - a - x_1 - x_2)$, $y_3 = -\lambda x_3 - (y_1 - \lambda x_1)$

C.3.7 Heights of Points

- given $x = (m, n) \in E(\mathbb{Q})$ with $\gcd(m, n) = 1$, we define the (naïve) height of x to be $H(x) = \max(|m|, |n|)$, and the corresponding logarithmic height to be $h(x) = \log H(x)$
- this induces a height on curves $E(\mathbb{Q})$, for if $E(\mathbb{Q}) \ni P = (x, y)$, then $h(P) = h(x)$ (we ignore y)
- this is almost a bi-linear form — in particular:
 - for each $Q \in E(\mathbb{Q})$ we have $\kappa_0, h(P+Q) \leq 2 \cdot h(P) + \kappa_0 \forall P \in E(\mathbb{Q})$
 - there is κ , so that $h(2P) \geq 4 \cdot h(P) - \kappa$

C.3.8 Canonical Heights

- any naïve height induces the same canonical height
- define $\hat{h} = \lim_{n \rightarrow \infty} \frac{h(2^n P)}{4^n}$ — by Néron-Tate, we have:
 - $\hat{h}(P + Q) + \hat{h}(P - Q) = 2 \cdot \hat{h}(P) + 2 \cdot \hat{h}(Q)$
 - $\hat{h}(mP) = m^2 \cdot \hat{h}(P)$
 - $\langle P, Q \rangle := \hat{h}(P + Q) - \hat{h}(P) - \hat{h}(Q)$ is a bilinear form
 - $\hat{h}(P) = 0 \iff P \in E(\mathbb{Q})_{\text{tor}}$

C.3.9 Discrete Logarithms in $E(\mathbb{Q})$

- assuming $P = mQ$ for $P, Q \in E(\mathbb{Q})$ and some $m \in \mathbb{Z}$, m is easily found via the canonical height

- $m = \sqrt{\frac{\hat{h}(P)}{\hat{h}(Q)}}$