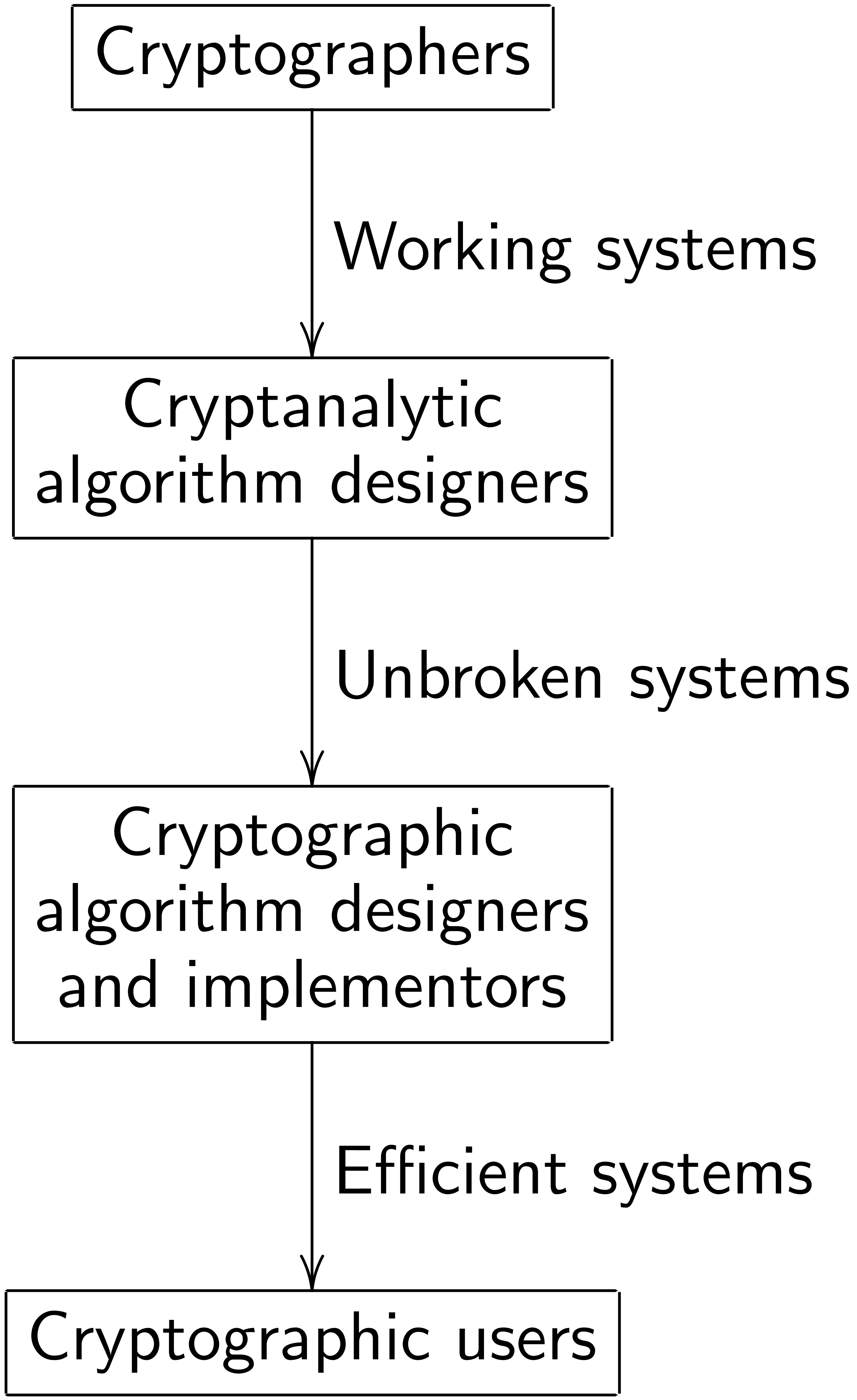
High-speed cryptography, part 3: more cryptosystems

Daniel J. Bernstein
University of Illinois at Chicago &
Technische Universiteit Eindhoven



Cryptographers

Working systems

Cryptanalytic algorithm designers

Unbroken systems

Cryptographic algorithm designers and implementors

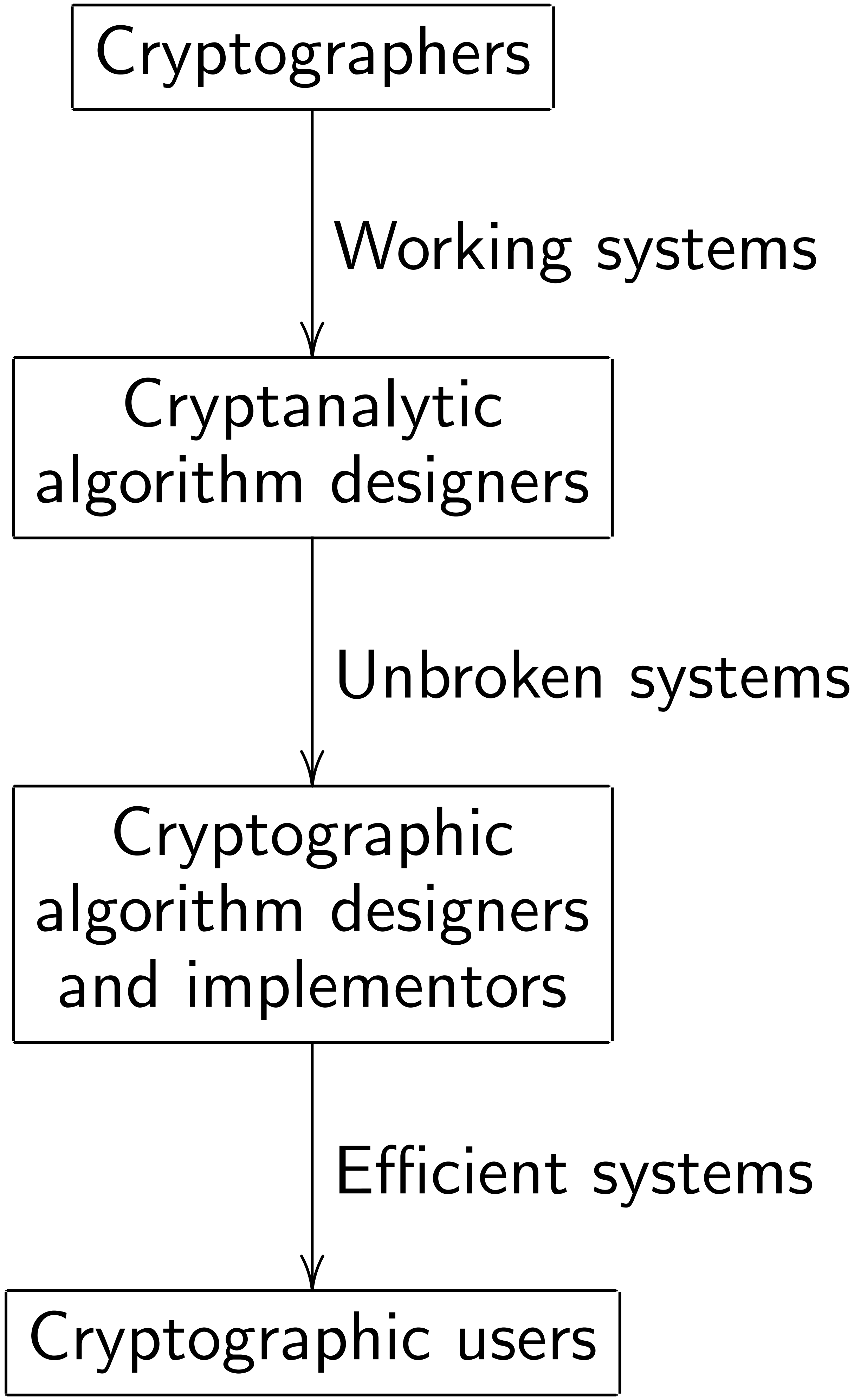
Efficient systems

Cryptographic users

eed cryptography,

yptosystems

. Bernstein
ty of Illinois at Chicago &
che Universiteit Eindhoven



Cryptographers

Working systems

Cryptanalytic algorithm designers

Unbroken systems

Cryptographic algorithm designers and implementors

Efficient systems

Cryptographic users

1. Work

Fundam
cryptogr
How car
sign, ver

Many ar
DES, Tr
RSA, M
Merkle h
Merkle–
encrypti
class-grc
ECDSA,

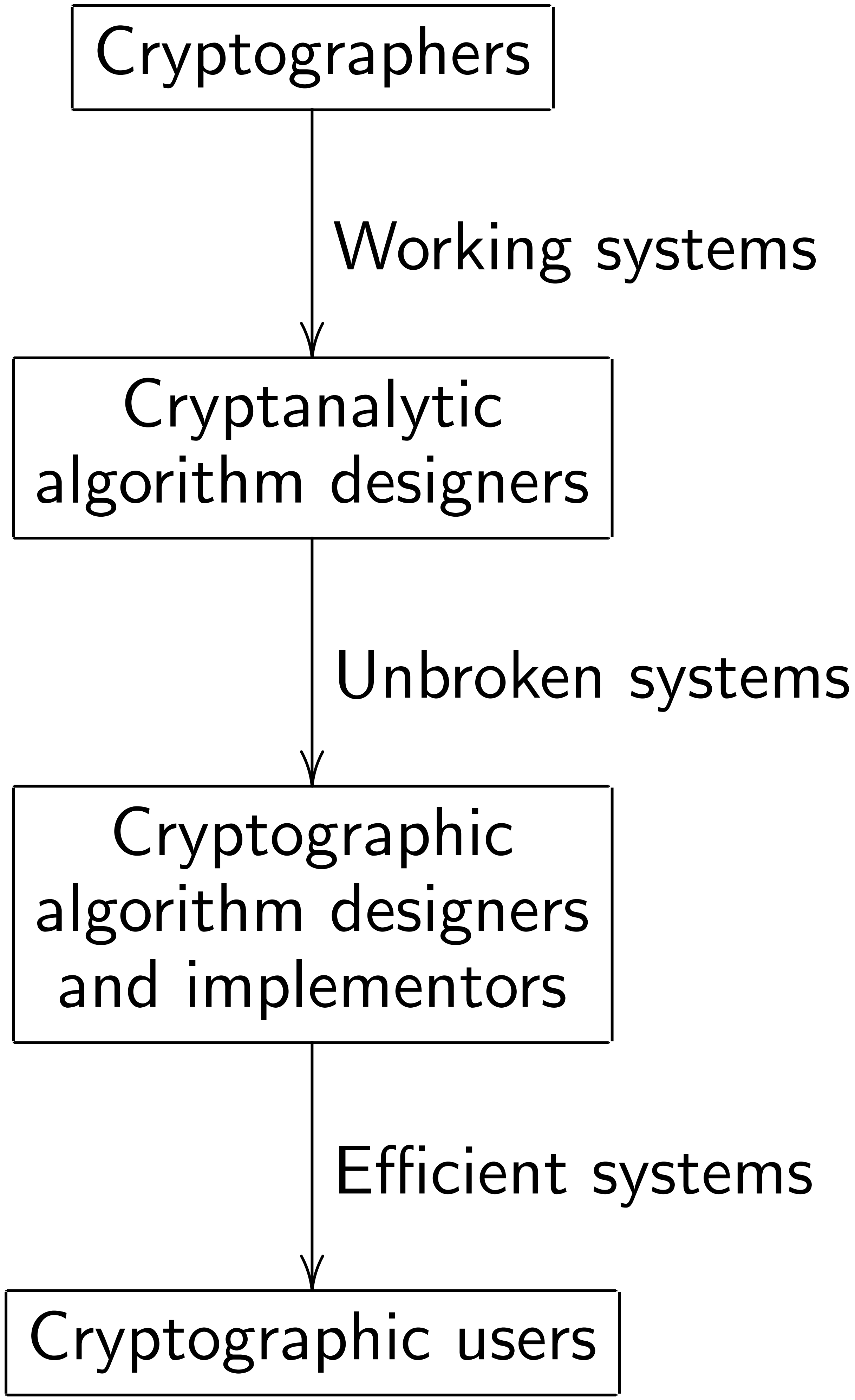
graphy,

ns

n

is at Chicago &

siteit Eindhoven



Cryptographers

Working systems

Cryptanalytic algorithm designers

Unbroken systems

Cryptographic algorithm designers and implementors

Efficient systems

Cryptographic users

---

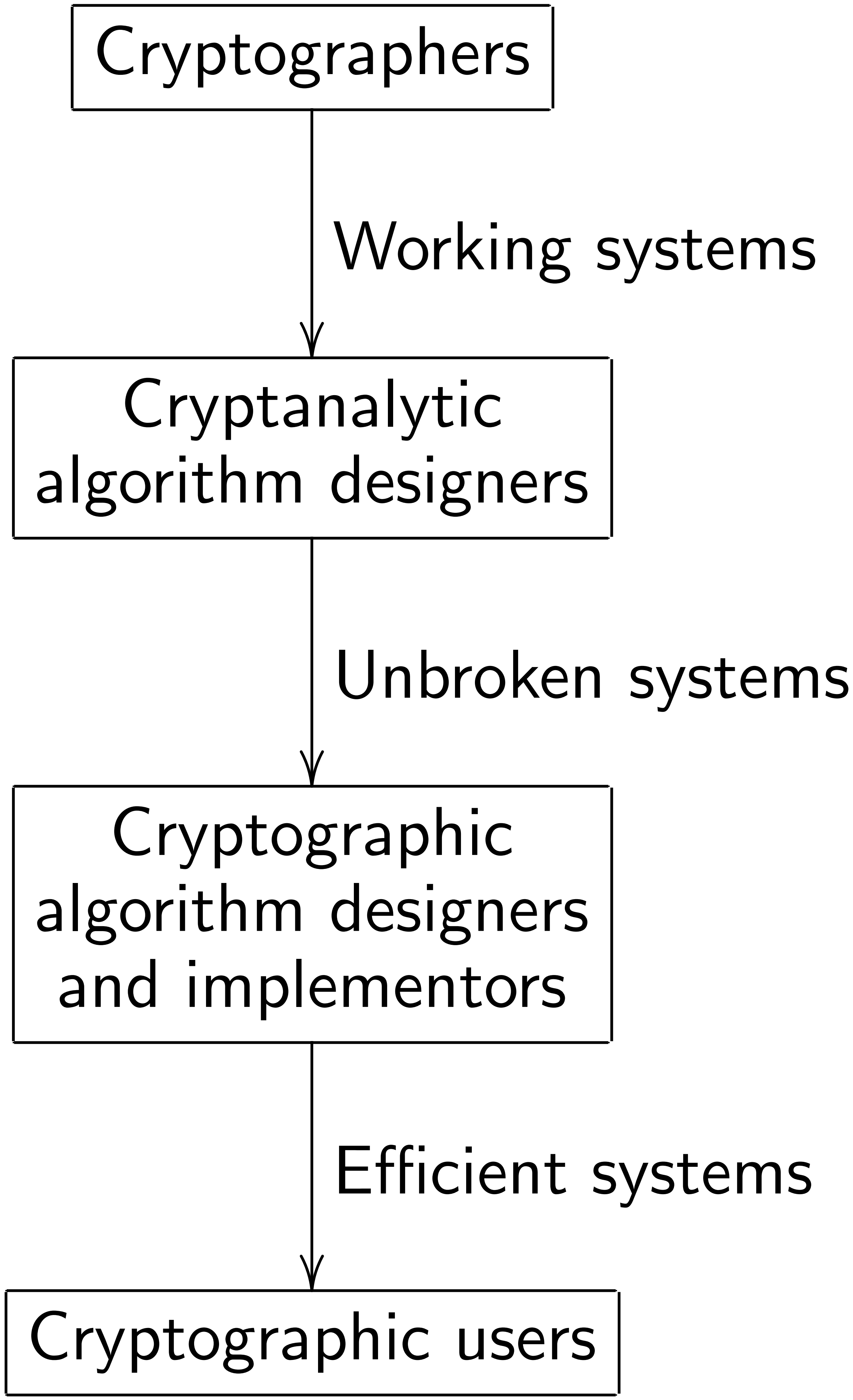
1. Working system

Fundamental ques
cryptographers:
How can we encry
sign, verify, etc.?

Many answers:
DES, Triple DES,
RSA, McEliece en
Merkle hash-tree s
Merkle–Hellman k
encryption, Buchm
class-group encryp
ECDSA, HFE^{v-}, N

ago &

hoven



Cryptographers

Working systems

Cryptanalytic algorithm designers

Unbroken systems

Cryptographic algorithm designers and implementors

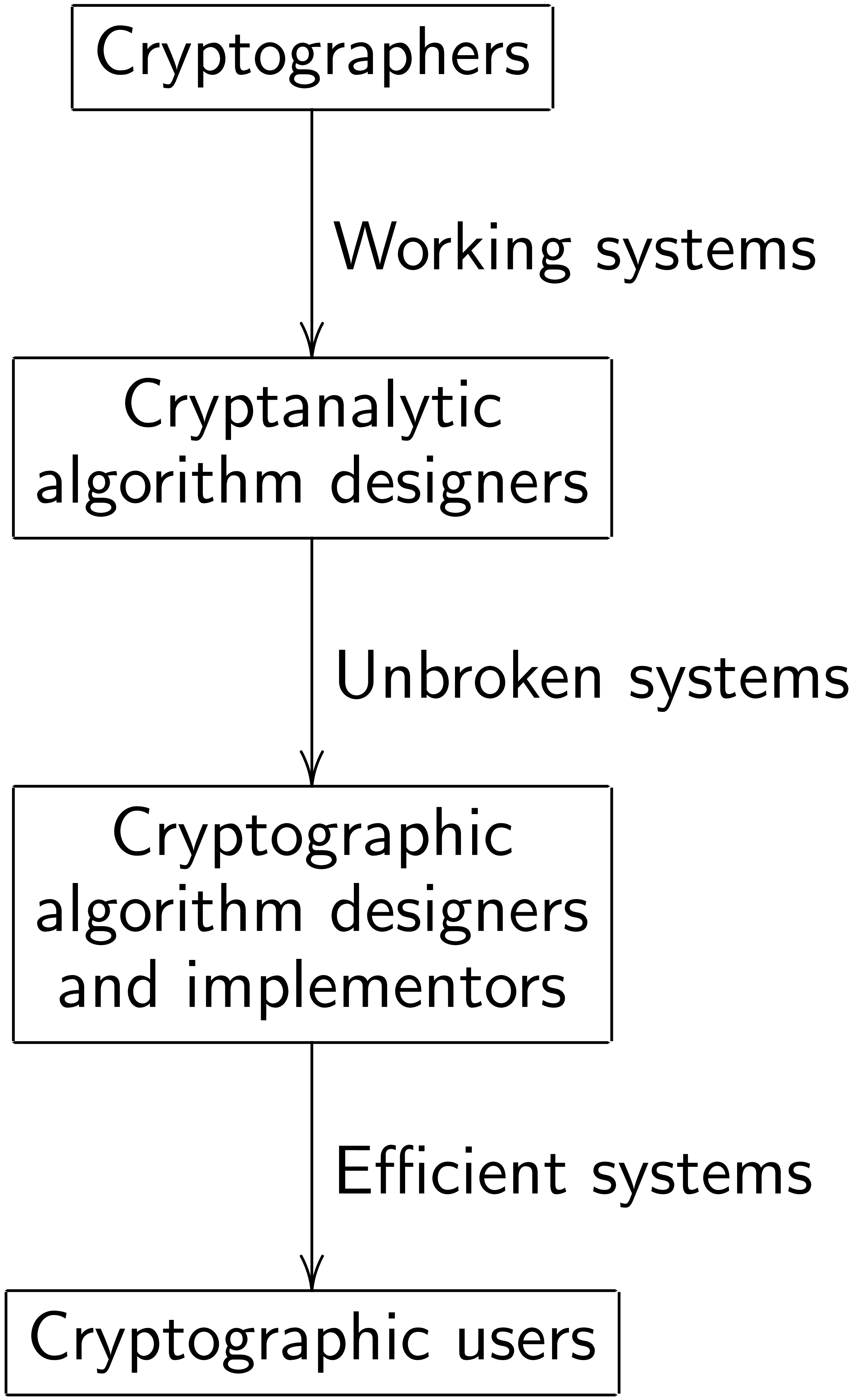
Efficient systems

Cryptographic users

1. Working systems

Fundamental question for cryptographers:
How can we encrypt, decryp
sign, verify, etc.?

Many answers:
DES, Triple DES, FEAL-4, A
RSA, McEliece encryption,
Merkle hash-tree signatures,
Merkle–Hellman knapsack
encryption, Buchmann–Willi
class-group encryption,
ECDSA, HFE^{v-}, NTRU, et



Cryptographers

Working systems

Cryptanalytic algorithm designers

Unbroken systems

Cryptographic algorithm designers and implementors

Efficient systems

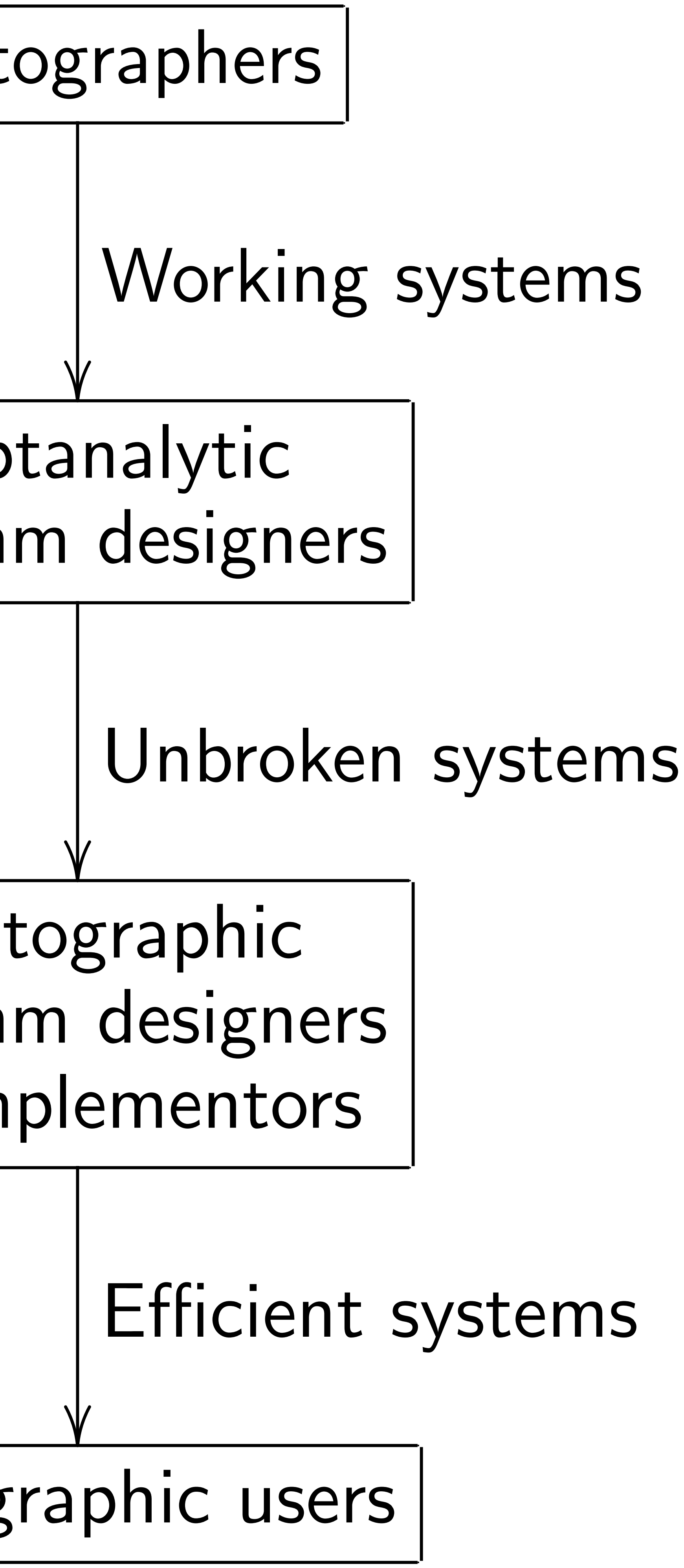
Cryptographic users

---

1. Working systems

Fundamental question for cryptographers:
How can we encrypt, decrypt, sign, verify, etc.?

Many answers:
DES, Triple DES, FEAL-4, AES, RSA, McEliece encryption, Merkle hash-tree signatures, Merkle–Hellman knapsack encryption, Buchmann–Williams class-group encryption, ECDSA, HFE^{v-}, NTRU, et al.



tographers

Working systems

ptanalytic
m designers

Unbroken systems

tographic
m designers
plementors

Efficient systems

graphic users

1. Working systems

Fundamental question for cryptographers:
How can we encrypt, decrypt, sign, verify, etc.?

Many answers:
DES, Triple DES, FEAL-4, AES, RSA, McEliece encryption, Merkle hash-tree signatures, Merkle–Hellman knapsack encryption, Buchmann–Williams class-group encryption, ECDSA, HFE^{v-}, NTRU, et al.

2. Unbro

Fundame
pre-quan
What ca
using <2
on a *cla*

Fundame
post-qua
What ca
using <2
on a *qua*

Goal: id
not brea

g systems

ers

ken systems

ers
rs

nt systems

ers

1. Working systems

Fundamental question for cryptographers:
How can we encrypt, decrypt, sign, verify, etc.?

Many answers:
DES, Triple DES, FEAL-4, AES, RSA, McEliece encryption, Merkle hash-tree signatures, Merkle–Hellman knapsack encryption, Buchmann–Williams class-group encryption, ECDSA, HFE^{v-}, NTRU, et al.

2. Unbroken syste

Fundamental ques
pre-quantum crypt
What can an attac
using $<2^b$ operatio
on a *classical* com

Fundamental ques
post-quantum cryp
What can an attac
using $<2^b$ operatio
on a *quantum* con

Goal: identify syst
not breakable in <

ns

1. Working systems

Fundamental question for
cryptographers:
How can we encrypt, decrypt,
sign, verify, etc.?

Many answers:
DES, Triple DES, FEAL-4, AES,
RSA, McEliece encryption,
Merkle hash-tree signatures,
Merkle–Hellman knapsack
encryption, Buchmann–Williams
class-group encryption,
ECDSA, HFE^{v-}, NTRU, et al.

2. Unbroken systems

Fundamental question for
pre-quantum cryptanalysts:
What can an attacker do
using $<2^b$ operations
on a *classical* computer?

Fundamental question for
post-quantum cryptanalysts
What can an attacker do
using $<2^b$ operations
on a *quantum* computer?

Goal: identify systems that
not breakable in $<2^b$ operat

1. Working systems

Fundamental question for cryptographers:
How can we encrypt, decrypt, sign, verify, etc.?

Many answers:
DES, Triple DES, FEAL-4, AES, RSA, McEliece encryption, Merkle hash-tree signatures, Merkle–Hellman knapsack encryption, Buchmann–Williams class-group encryption, ECDSA, $\text{HFE}^{\text{v}-}$, NTRU, et al.

2. Unbroken systems

Fundamental question for *pre-quantum* cryptanalysts:
What can an attacker do using $<2^b$ operations on a *classical* computer?

Fundamental question for *post-quantum* cryptanalysts:
What can an attacker do using $<2^b$ operations on a *quantum* computer?

Goal: identify systems that are *not* breakable in $<2^b$ operations.

king systems

ental question for
raphers:
n we encrypt, decrypt,
rify, etc.?

nswers:
iple DES, FEAL-4, AES,
cEliece encryption,
hash-tree signatures,
Hellman knapsack
on, Buchmann–Williams
oup encryption,
HFE^{v-}, NTRU, et al.

---

2. Unbroken systems

Fundamental question for *pre-quantum* cryptanalysts: What can an attacker do using $<2^b$ operations on a *classical* computer?

Fundamental question for *post-quantum* cryptanalysts: What can an attacker do using $<2^b$ operations on a *quantum* computer?

Goal: identify systems that are *not* breakable in $<2^b$ operations.

Example

Schroep
mention
factors
$(2+o(1$
simple o

To push
must ch
$(0.5+o$

Note 1:

Note 2:
about, e
Today:

ns

tion for

pt, decrypt,

FEAL-4, AES,
cryption,
signatures,
napsack
nann–Williams
otion,
NTRU, et al.

2. Unbroken systems

Fundamental question for
pre-quantum cryptanalysts:
What can an attacker do
using $<2^b$ operations
on a *classical* computer?

Fundamental question for
post-quantum cryptanalysts:
What can an attacker do
using $<2^b$ operations
on a *quantum* computer?

Goal: identify systems that are
not breakable in $<2^b$ operations.

Examples of RSA

Schroeppel's “line
mentioned in 1978
factors pq into p,
$(2 + o(1))^{(\lg pq)^{1/2}}$
simple operations

To push this beyon
must choose pq to
$(0.5 + o(1))b^2/\lg b$

Note 1: $\lg = \log_2$.

Note 2: $o(1)$ says
about, e.g., $b = 12$
Today: focus on a

t,

AES,

ams

al.

2. Unbroken systems

Fundamental question for *pre-quantum* cryptanalysts: What can an attacker do using $<2^b$ operations on a *classical* computer?

Fundamental question for *post-quantum* cryptanalysts: What can an attacker do using $<2^b$ operations on a *quantum* computer?

Goal: identify systems that are *not* breakable in $<2^b$ operations.

Examples of RSA cryptanaly

Schroeppel's "linear sieve",
mentioned in 1978 RSA pap
factors pq into p, q using
$(2+o(1))^{(\lg pq)^{1/2}(\lg \lg pq)^{1/2}}$
simple operations (conjectur

To push this beyond 2^b,
must choose pq to have at l
$(0.5+o(1))b^2/\lg b$ bits.

Note 1: $\lg = \log_2$.

Note 2: $o(1)$ says *nothing*
about, e.g., $b = 128$.
Today: focus on asymptotic

2. Unbroken systems

Fundamental question for *pre-quantum* cryptanalysts: What can an attacker do using $<2^b$ operations on a *classical* computer?

Fundamental question for *post-quantum* cryptanalysts: What can an attacker do using $<2^b$ operations on a *quantum* computer?

Goal: identify systems that are *not* breakable in $<2^b$ operations.

Examples of RSA cryptanalysis:

Schroeppel's "linear sieve", mentioned in 1978 RSA paper, factors pq into p, q using $(2 + o(1))^{(\lg pq)^{1/2}(\lg \lg pq)^{1/2}}$ simple operations (conjecturally).

To push this beyond 2^b, must choose pq to have at least $(0.5 + o(1))b^2/\lg b$ bits.

Note 1: $\lg = \log_2$.

Note 2: $o(1)$ says *nothing* about, e.g., $b = 128$.
Today: focus on asymptotics.

oken systems

ental question for
ntum cryptanalysts:
n an attacker do
2^b operations
ssical computer?

ental question for
antum cryptanalysts:
n an attacker do
2^b operations
antum computer?

entify systems that are
kable in $<2^b$ operations.

Examples of RSA cryptanalysis:

Schroeppel's "linear sieve", mentioned in 1978 RSA paper, factors pq into p, q using $(2+o(1))^{(\lg pq)^{1/2}(\lg \lg pq)^{1/2}}$ simple operations (conjecturally).

To push this beyond 2^b, must choose pq to have at least $(0.5+o(1))b^2/\lg b$ bits.

Note 1: $\lg = \log_2$.

Note 2: $o(1)$ says *nothing* about, e.g., $b = 128$.
Today: focus on asymptotics.

1993 Bu
generaliz
"numbe
factors p
$(3.79\ldots$
simple o

To push
must ch
$(0.015\ldots$

Subsequ
$3.73\ldots$;
But can
that $2^{(\lg}$
—for cla

ms

tion for
tanalysts:
cker do
ons
puter?

tion for
ptanalysts:
cker do
ons
nputer?

tems that are
$<2^b$ operations.

Examples of RSA cryptanalysis:

Schroeppel's “linear sieve”,
mentioned in 1978 RSA paper,
factors pq into p, q using
$(2 + o(1))^{(\lg pq)^{1/2}(\lg\lg pq)^{1/2}}$
simple operations (conjecturally).

To push this beyond 2^b,
must choose pq to have at least
$(0.5 + o(1))b^2/\lg b$ bits.

Note 1: $\lg = \log_2$.

Note 2: $o(1)$ says *nothing*
about, e.g., $b = 128$.
Today: focus on asymptotics.

1993 Buhler–Lenst
generalizing 1988
“number-field siev
factors pq into p,
$(3.79\ldots + o(1))^{(\lg}$
simple operations

To push this beyon
must choose pq to
$(0.015\ldots + o(1))$

Subsequent impro
$3.73\ldots$; details of
But can reasonabl
that $2^{(\lg pq)^{1/3+o(1)}}$
—for classical com

:

are

ions.

Examples of RSA cryptanalysis:

Schroeppel's "linear sieve", mentioned in 1978 RSA paper, factors pq into p, q using $(2+o(1))^{(\lg pq)^{1/2}(\lg\lg pq)^{1/2}}$ simple operations (conjecturally).

To push this beyond 2^b, must choose pq to have at least $(0.5+o(1))b^2/\lg b$ bits.

Note 1: $\lg = \log_2$.

Note 2: $o(1)$ says *nothing* about, e.g., $b = 128$.
Today: focus on asymptotics.

1993 Buhler–Lenstra–Pomer
generalizing 1988 Pollard
"number-field sieve",
factors pq into p, q using
$(3.79\ldots+o(1))^{(\lg pq)^{1/3}(\lg \lg}$
simple operations (conjectur

To push this beyond 2^b,
must choose pq to have at l
$(0.015\ldots+o(1))b^3/(\lg b)^2$

Subsequent improvements:
$3.73\ldots$; details of $o(1)$.
But can reasonably conjectu
that $2^{(\lg pq)^{1/3+o(1)}}$ is optima
—for classical computers.

Examples of RSA cryptanalysis:

Schroeppel's "linear sieve", mentioned in 1978 RSA paper, factors pq into p, q using $(2 + o(1))^{(\lg pq)^{1/2}(\lg\lg pq)^{1/2}}$ simple operations (conjecturally).

To push this beyond 2^b, must choose pq to have at least $(0.5 + o(1))b^2/\lg b$ bits.

Note 1: $\lg = \log_2$.

Note 2: $o(1)$ says *nothing* about, e.g., $b = 128$.
Today: focus on asymptotics.

1993 Buhler–Lenstra–Pomerance, generalizing 1988 Pollard "number-field sieve", factors pq into p, q using $(3.79\ldots + o(1))^{(\lg pq)^{1/3}(\lg\lg pq)^{2/3}}$ simple operations (conjecturally).

To push this beyond 2^b, must choose pq to have at least $(0.015\ldots + o(1))b^3/(\lg b)^2$ bits.

Subsequent improvements: $3.73\ldots$; details of $o(1)$.
But can reasonably conjecture that $2^{(\lg pq)^{1/3+o(1)}}$ is optimal —for classical computers.

es of RSA cryptanalysis:

pel's “linear sieve”,
ed in 1978 RSA paper,
pq into p, q using
$))^{(\lg pq)^{1/2}(\lg\lg pq)^{1/2}}$
perations (conjecturally).

this beyond 2^b,
oose pq to have at least
$(1))b^2/\lg b$ bits.

$\lg = \log_2$.

$o(1)$ says *nothing*
.g., $b = 128$.
focus on asymptotics.

1993 Buhler–Lenstra–Pomerance,
generalizing 1988 Pollard
“number-field sieve”,
factors pq into p, q using
$(3.79\ldots + o(1))^{(\lg pq)^{1/3}(\lg\lg pq)^{2/3}}$
simple operations (conjecturally).

To push this beyond 2^b,
must choose pq to have at least
$(0.015\ldots + o(1))b^3/(\lg b)^2$ bits.

Subsequent improvements:
$3.73\ldots$; details of $o(1)$.
But can reasonably conjecture
that $2^{(\lg pq)^{1/3+o(1)}}$ is optimal
—for classical computers.

Cryptogr
pre-quar

Triple D
AES-256
RSA wit
McEliec
$b^{1+o(1)}$,
with “st
BW wit
bit discr
“strong”
HFE^{v-} v
NTRU w

cryptanalysis:

ar sieve”,
RSA paper,
q using
$(\lg\lg pq)^{1/2}$

(conjecturally).

nd 2^b,
have at least
bits.

.

nothing
28.
symptotics.

1993 Buhler–Lenstra–Pomerance, generalizing 1988 Pollard “number-field sieve”, factors pq into p, q using $(3.79\ldots + o(1))^{(\lg pq)^{1/3}(\lg\lg pq)^{2/3}}$ simple operations (conjecturally).

To push this beyond 2^b, must choose pq to have at least $(0.015\ldots + o(1))b^3/(\lg b)^2$ bits.

Subsequent improvements: 3.73…; details of $o(1)$.
But can reasonably conjecture that $2^{(\lg pq)^{1/3+o(1)}}$ is optimal —for classical computers.

Cryptographic syst
pre-quantum crypt

Triple DES (for b
AES-256 (for $b \le$
RSA with $b^{3+o(1)}$-
McEliece with cod
$b^{1+o(1)}$, Merkle sig
with “strong” b^{1+}
BW with “strong”
bit discriminant, E
“strong” $b^{1+o(1)}$-b
HFE^{v-} with $b^{1+o(}$
NTRU with $b^{1+o(1}$

ysis:

er,

rally).

east

s.

1993 Buhler–Lenstra–Pomerance, generalizing 1988 Pollard "number-field sieve", factors pq into p, q using $(3.79\ldots + o(1))^{(\lg pq)^{1/3}(\lg\lg pq)^{2/3}}$ simple operations (conjecturally).

To push this beyond 2^b, must choose pq to have at least $(0.015\ldots + o(1))b^3/(\lg b)^2$ bits.

Subsequent improvements: $3.73\ldots$; details of $o(1)$.
But can reasonably conjecture that $2^{(\lg pq)^{1/3+o(1)}}$ is optimal —for classical computers.

Cryptographic systems survi
pre-quantum cryptanalysis:

Triple DES (for $b \le 112$),
AES-256 (for $b \le 256$),
RSA with $b^{3+o(1)}$-bit modul
McEliece with code length
$b^{1+o(1)}$, Merkle signatures
with "strong" $b^{1+o(1)}$-bit ha
BW with "strong" $b^{2+o(1)}$-
bit discriminant, ECDSA wi
"strong" $b^{1+o(1)}$-bit curve,
HFE$^{\mathrm{v}-}$ with $b^{1+o(1)}$ polyno
NTRU with $b^{1+o(1)}$ bits, et

1993 Buhler–Lenstra–Pomerance, generalizing 1988 Pollard "number-field sieve", factors pq into p, q using $(3.79\ldots + o(1))^{(\lg pq)^{1/3}(\lg\lg pq)^{2/3}}$ simple operations (conjecturally).

To push this beyond 2^b, must choose pq to have at least $(0.015\ldots + o(1))b^3/(\lg b)^2$ bits.

Subsequent improvements: $3.73\ldots$; details of $o(1)$. But can reasonably conjecture that $2^{(\lg pq)^{1/3+o(1)}}$ is optimal —for classical computers.

Cryptographic systems surviving *pre-quantum* cryptanalysis:

Triple DES (for $b \le 112$), AES-256 (for $b \le 256$), RSA with $b^{3+o(1)}$-bit modulus, McEliece with code length $b^{1+o(1)}$, Merkle signatures with "strong" $b^{1+o(1)}$-bit hash, BW with "strong" $b^{2+o(1)}$-bit discriminant, ECDSA with "strong" $b^{1+o(1)}$-bit curve, HFE$^{\text{v}-}$ with $b^{1+o(1)}$ polynomials, NTRU with $b^{1+o(1)}$ bits, et al.

uhler–Lenstra–Pomerance,
zing 1988 Pollard
r-field sieve”,
pq into p, q using
$+ o(1))^{(\lg pq)^{1/3}(\lg \lg pq)^{2/3}}$
perations (conjecturally).

this beyond 2^b,
oose pq to have at least
$. . + o(1))b^3/(\lg b)^2$ bits.

ent improvements:
details of $o(1)$.
reasonably conjecture
$pq)^{1/3+o(1)}$ is optimal
assical computers.

Cryptographic systems surviving *pre-quantum* cryptanalysis:

Triple DES (for $b \le 112$),
AES-256 (for $b \le 256$),
RSA with $b^{3+o(1)}$-bit modulus,
McEliece with code length $b^{1+o(1)}$, Merkle signatures with “strong” $b^{1+o(1)}$-bit hash,
BW with “strong” $b^{2+o(1)}$-bit discriminant, ECDSA with “strong” $b^{1+o(1)}$-bit curve,
HFE$^{\mathrm{v}-}$ with $b^{1+o(1)}$ polynomials,
NTRU with $b^{1+o(1)}$ bits, et al.

Typical a
pre-quar
NFS, ρ,

Post-qua
have all
plus qua

Spectacu
1994 Sh
using (lg
simple q
To push
must ch
$2^{(0.5+o(1}$

tra–Pomerance,
Pollard
e",
q using
$g\,pq)^{1/3}(\lg\lg pq)^{2/3}$
(conjecturally).

nd 2^b,
o have at least
$b^3/(\lg b)^2$ bits.

vements:
$o(1)$.
y conjecture
is optimal
nputers.

Cryptographic systems surviving *pre-quantum* cryptanalysis:

Triple DES (for $b \le 112$),
AES-256 (for $b \le 256$),
RSA with $b^{3+o(1)}$-bit modulus,
McEliece with code length $b^{1+o(1)}$, Merkle signatures with "strong" $b^{1+o(1)}$-bit hash,
BW with "strong" $b^{2+o(1)}$-bit discriminant, ECDSA with "strong" $b^{1+o(1)}$-bit curve,
HFE$^{\mathrm{v}-}$ with $b^{1+o(1)}$ polynomials,
NTRU with $b^{1+o(1)}$ bits, et al.

Typical algorithmi
pre-quantum crypt
NFS, ρ, ISD, LLL,

Post-quantum cry
have all the same
plus quantum algo

Spectacular examp
1994 Shor factors
using $(\lg pq)^{2+o(1)}$
simple quantum o
To push this beyo
must choose pq to
$2^{(0.5+o(1))b}$ bits. Y

rance,

$pq)^{2/3}$
rally).

east
bits.

re
l

Cryptographic systems surviving *pre-quantum* cryptanalysis:

Triple DES (for $b \le 112$),
AES-256 (for $b \le 256$),
RSA with $b^{3+o(1)}$-bit modulus,
McEliece with code length $b^{1+o(1)}$, Merkle signatures with "strong" $b^{1+o(1)}$-bit hash,
BW with "strong" $b^{2+o(1)}$-bit discriminant, ECDSA with "strong" $b^{1+o(1)}$-bit curve,
HFE$^{\mathrm{v}-}$ with $b^{1+o(1)}$ polynomials,
NTRU with $b^{1+o(1)}$ bits, et al.

Typical algorithmic tools for
pre-quantum cryptanalysts:
NFS, ρ, ISD, LLL, F4, XL, e

Post-quantum cryptanalysts
have all the same tools
plus quantum algorithms.

Spectacular example:
1994 Shor factors pq into p,
using $(\lg pq)^{2+o(1)}$
simple quantum operations.
To push this beyond 2^b,
must choose pq to have at l
$2^{(0.5+o(1))b}$ bits. Yikes.

Cryptographic systems surviving *pre-quantum* cryptanalysis:

Triple DES (for $b \le 112$),
AES-256 (for $b \le 256$),
RSA with $b^{3+o(1)}$-bit modulus,
McEliece with code length $b^{1+o(1)}$, Merkle signatures with "strong" $b^{1+o(1)}$-bit hash,
BW with "strong" $b^{2+o(1)}$-bit discriminant, ECDSA with "strong" $b^{1+o(1)}$-bit curve,
HFE$^{\mathrm{v}-}$ with $b^{1+o(1)}$ polynomials,
NTRU with $b^{1+o(1)}$ bits, et al.

Typical algorithmic tools for *pre-quantum* cryptanalysts:
NFS, ρ, ISD, LLL, F4, XL, et al.

Post-quantum cryptanalysts have all the same tools *plus* quantum algorithms.

Spectacular example:
1994 Shor factors pq into p, q using $(\lg pq)^{2+o(1)}$ simple quantum operations.
To push this beyond 2^b, must choose pq to have at least $2^{(0.5+o(1))b}$ bits. Yikes.

raphic systems surviving
ntum cryptanalysis:

ES (for $b \leq 112$),
6 (for $b \leq 256$),
th $b^{3+o(1)}$-bit modulus,
e with code length
Merkle signatures
rong" $b^{1+o(1)}$-bit hash,
n "strong" $b^{2+o(1)}$-
iminant, ECDSA with
$b^{1+o(1)}$-bit curve,
with $b^{1+o(1)}$ polynomials,
vith $b^{1+o(1)}$ bits, et al.

Typical algorithmic tools for *pre-quantum* cryptanalysts: NFS, ρ, ISD, LLL, F4, XL, et al.

Post-quantum cryptanalysts have all the same tools *plus* quantum algorithms.

Spectacular example:
1994 Shor factors pq into p, q using $(\lg pq)^{2+o(1)}$ simple quantum operations.
To push this beyond 2^b, must choose pq to have at least $2^{(0.5+o(1))b}$ bits. Yikes.

Cryptog
post-qua

AES-256
McEliece
with coc
Merkle h
with "st
$\text{HFE}^{\text{v}-}$ I
$b^{1+o(1)}$ p
NTRU la
with b^{1+}
et al.

tems surviving
tanalysis:

≤ 112),
256),
bit modulus,
le length
gnatures
$^{o(1)}$-bit hash,
$b^{2+o(1)}$-
ECDSA with
it curve,
$^{1)}$ polynomials,
$^{)}$ bits, et al.

Typical algorithmic tools for *pre-quantum* cryptanalysts: NFS, ρ, ISD, LLL, F4, XL, et al.

Post-quantum cryptanalysts have all the same tools *plus* quantum algorithms.

Spectacular example:
1994 Shor factors pq into p, q using $(\lg pq)^{2+o(1)}$ simple quantum operations.
To push this beyond 2^b, must choose pq to have at least $2^{(0.5+o(1))b}$ bits. Yikes.

Cryptographic syst
post-quantum cry

AES-256 (for $b \leq$
McEliece code-bas
with code length b
Merkle hash-based
with “strong” b^{1+}
HFE^{v-} MQ signat
$b^{1+o(1)}$ polynomia
NTRU lattice-base
with $b^{1+o(1)}$ bits,
et al.

ving

us,

sh,

th

mials,

al.

Typical algorithmic tools for
pre-quantum cryptanalysts:
NFS, ρ, ISD, LLL, F4, XL, et al.

Post-quantum cryptanalysts
have all the same tools
plus quantum algorithms.

Spectacular example:
1994 Shor factors pq into p, q
using $(\lg pq)^{2+o(1)}$
simple quantum operations.
To push this beyond 2^b,
must choose pq to have at least
$2^{(0.5+o(1))b}$ bits. Yikes.

Cryptographic systems survi
post-quantum cryptanalysis:

AES-256 (for $b \le 128$),
McEliece code-based encryp
with code length $b^{1+o(1)}$,
Merkle hash-based signature
with “strong” $b^{1+o(1)}$-bit ha
HFE$^{\text{v}-}$ MQ signatures with
$b^{1+o(1)}$ polynomials,
NTRU lattice-based encrypt
with $b^{1+o(1)}$ bits,
et al.

Typical algorithmic tools for *pre-quantum* cryptanalysts:
NFS, ρ, ISD, LLL, F4, XL, et al.

Post-quantum cryptanalysts have all the same tools *plus* quantum algorithms.

Spectacular example:
1994 Shor factors pq into p, q using $(\lg pq)^{2+o(1)}$ simple quantum operations.
To push this beyond 2^b, must choose pq to have at least $2^{(0.5+o(1))b}$ bits. Yikes.

Cryptographic systems surviving *post-quantum* cryptanalysis:

AES-256 (for $b \le 128$),
McEliece code-based encryption with code length $b^{1+o(1)}$,
Merkle hash-based signatures with "strong" $b^{1+o(1)}$-bit hash,
HFE$^{\text{v}-}$ MQ signatures with $b^{1+o(1)}$ polynomials,
NTRU lattice-based encryption with $b^{1+o(1)}$ bits,
et al.

algorithmic tools for
ntum cryptanalysts:
ISD, LLL, F4, XL, et al.

antum cryptanalysts
the same tools
ntum algorithms.

ular example:
or factors pq into p, q
$g\,pq)^{2+o(1)}$
uantum operations.
this beyond 2^b,
oose pq to have at least
$))^b$ bits. Yikes.

Cryptographic systems surviving
post-quantum cryptanalysis:

AES-256 (for $b \le 128$),
McEliece code-based encryption
with code length $b^{1+o(1)}$,
Merkle hash-based signatures
with "strong" $b^{1+o(1)}$-bit hash,
HFE^{v-} MQ signatures with
$b^{1+o(1)}$ polynomials,
NTRU lattice-based encryption
with $b^{1+o(1)}$ bits,
et al.

3. Effici

Fundam
designer
of crypt
Exactly
unbroke

Many go
time, siz

Pre-qua
RSA enc
in $b^{3+o(1}$
Signatur

c tools for
tanalysts:
F4, XL, et al.

ptanalysts
tools
orithms.

ple:
pq into p, q

perations.
nd 2^b,
have at least
Yikes.

Cryptographic systems surviving *post-quantum* cryptanalysis:

AES-256 (for $b \le 128$),
McEliece code-based encryption with code length $b^{1+o(1)}$,
Merkle hash-based signatures with "strong" $b^{1+o(1)}$-bit hash,
HFE^{v-} MQ signatures with $b^{1+o(1)}$ polynomials,
NTRU lattice-based encryption with $b^{1+o(1)}$ bits,
et al.

3. Efficient system

Fundamental ques
designers and impl
of cryptographic a
Exactly how efficie
unbroken cryptosy

Many goals: minin
time, size, decrypt

Pre-quantum exan
RSA encrypts and
in $b^{3+o(1)}$ simple o
Signature occupies

et al.

q

east

Cryptographic systems surviving *post-quantum* cryptanalysis:

AES-256 (for $b \le 128$),
McEliece code-based encryption with code length $b^{1+o(1)}$,
Merkle hash-based signatures with "strong" $b^{1+o(1)}$-bit hash,
HFE$^{\text{v}-}$ MQ signatures with $b^{1+o(1)}$ polynomials,
NTRU lattice-based encryption with $b^{1+o(1)}$ bits,
et al.

3. Efficient systems

Fundamental question for
designers and implementors
of cryptographic algorithms:
Exactly how efficient are the
unbroken cryptosystems?

Many goals: minimize encry
time, size, decryption time,

Pre-quantum example:
RSA encrypts and verifies
in $b^{3+o(1)}$ simple operations.
Signature occupies $b^{3+o(1)}$ b

Cryptographic systems surviving *post-quantum* cryptanalysis:

AES-256 (for $b \le 128$),
McEliece code-based encryption with code length $b^{1+o(1)}$,
Merkle hash-based signatures with "strong" $b^{1+o(1)}$-bit hash,
$\mathrm{HFE}^{\mathrm{v}-}$ MQ signatures with $b^{1+o(1)}$ polynomials,
NTRU lattice-based encryption with $b^{1+o(1)}$ bits,
et al.

3. Efficient systems

Fundamental question for designers and implementors of cryptographic algorithms: Exactly how efficient are the unbroken cryptosystems?

Many goals: minimize encryption time, size, decryption time, etc.

Pre-quantum example:
RSA encrypts and verifies in $b^{3+o(1)}$ simple operations.
Signature occupies $b^{3+o(1)}$ bits.

raphic systems surviving
antum cryptanalysis:

5 (for $b \le 128$),
e code-based encryption
de length $b^{1+o(1)}$,
hash-based signatures
rong" $b^{1+o(1)}$-bit hash,
MQ signatures with
polynomials,
attice-based encryption
$o(1)$ bits,

3. Efficient systems

Fundamental question for
designers and implementors
of cryptographic algorithms:
Exactly how efficient are the
unbroken cryptosystems?

Many goals: minimize encryption
time, size, decryption time, etc.

Pre-quantum example:
RSA encrypts and verifies
in $b^{3+o(1)}$ simple operations.
Signature occupies $b^{3+o(1)}$ bits.

ECC (wi
reasonab

ECDL co
by Pollar
Conjectu
optimal

Can take

Encrypti
costs (lg

Summar
Asympto
Bonus:

tems surviving
ptanalysis:

128),
sed encryption
$^{1+o(1)}$,
l signatures
$^{o(1)}$-bit hash,
tures with
ls,
ed encryption

---

3. Efficient systems

Fundamental question for designers and implementors of cryptographic algorithms: Exactly how efficient are the unbroken cryptosystems?

Many goals: minimize encryption time, size, decryption time, etc.

Pre-quantum example:
RSA encrypts and verifies in $b^{3+o(1)}$ simple operations.
Signature occupies $b^{3+o(1)}$ bits.

ECC (with strong
reasonable paddin

ECDL costs $2^{(1/2+}$
by Pollard's rho m
Conjecture: this is
optimal attack ag

Can take $\lg q \in$ (2

Encryption: Fast s
costs $(\lg q)^{2+o(1)}$ =

Summary: ECC co
Asymptotically fas
Bonus: also $b^{2+o(}$

ving

tion

es
sh,

ion

3. Efficient systems

Fundamental question for designers and implementors of cryptographic algorithms: Exactly how efficient are the unbroken cryptosystems?

Many goals: minimize encryption time, size, decryption time, etc.

Pre-quantum example:
RSA encrypts and verifies in $b^{3+o(1)}$ simple operations.
Signature occupies $b^{3+o(1)}$ bits.

ECC (with strong curve/$\mathbf{F}_q$,
reasonable padding, etc.):

ECDL costs $2^{(1/2+o(1))\lg q}$
by Pollard's rho method.
Conjecture: this is the
optimal attack against ECC

Can take $\lg q \in (2 + o(1))b$.

Encryption: Fast scalar mul
costs $(\lg q)^{2+o(1)} = b^{2+o(1)}$.

Summary: ECC costs $b^{2+o(1}$
Asymptotically faster than R
Bonus: also $b^{2+o(1)}$ *decrypt*

3. Efficient systems

Fundamental question for designers and implementors of cryptographic algorithms: Exactly how efficient are the unbroken cryptosystems?

Many goals: minimize encryption time, size, decryption time, etc.

Pre-quantum example:
RSA encrypts and verifies in $b^{3+o(1)}$ simple operations.
Signature occupies $b^{3+o(1)}$ bits.

ECC (with strong curve/$\mathbf{F}_q$, reasonable padding, etc.):

ECDL costs $2^{(1/2+o(1))\lg q}$ by Pollard's rho method.
Conjecture: this is the optimal attack against ECC.

Can take $\lg q \in (2+o(1))b$.

Encryption: Fast scalar mult costs $(\lg q)^{2+o(1)} = b^{2+o(1)}$.

Summary: ECC costs $b^{2+o(1)}$.
Asymptotically faster than RSA.
Bonus: also $b^{2+o(1)}$ *decryption*.

ent systems

ental question for
s and implementors
ographic algorithms:
how efficient are the
n cryptosystems?

oals: minimize encryption
ze, decryption time, etc.

ntum example:
crypts and verifies
$^{1)}$ simple operations.
re occupies $b^{3+o(1)}$ bits.

ECC (with strong curve/$\mathbf{F}_q$, reasonable padding, etc.):

ECDL costs $2^{(1/2+o(1))\lg q}$ by Pollard's rho method. Conjecture: this is the optimal attack against ECC.

Can take $\lg q \in (2+o(1))b$.

Encryption: Fast scalar mult costs $(\lg q)^{2+o(1)} = b^{2+o(1)}$.

Summary: ECC costs $b^{2+o(1)}$. Asymptotically faster than RSA. Bonus: also $b^{2+o(1)}$ *decryption*.

Efficienc
users ha

Cryptog
impleme
focus on
citing th

But Sho

ns

tion for
lementors
lgorithms:
ent are the
stems?

mize encryption
tion time, etc.

mple:
verifies
operations.
s $b^{3+o(1)}$ bits.

ECC (with strong curve/$\mathbf{F}_q$, reasonable padding, etc.):

ECDL costs $2^{(1/2+o(1))\lg q}$ by Pollard's rho method. Conjecture: this is the optimal attack against ECC.

Can take $\lg q \in (2+o(1))b$.

Encryption: Fast scalar mult costs $(\lg q)^{2+o(1)} = b^{2+o(1)}$.

Summary: ECC costs $b^{2+o(1)}$. Asymptotically faster than RSA. Bonus: also $b^{2+o(1)}$ *decryption*.

Efficiency is impor
users have cost co

Cryptographers, cr
implementors, etc.
focus on RSA and
citing these cost c

But Shor breaks R

e

ption
etc.

r
bits.

ECC (with strong curve/$\mathbf{F}_q$, reasonable padding, etc.):

ECDL costs $2^{(1/2+o(1))\lg q}$ by Pollard's rho method. Conjecture: this is the optimal attack against ECC.

Can take $\lg q \in (2 + o(1))b$.

Encryption: Fast scalar mult costs $(\lg q)^{2+o(1)} = b^{2+o(1)}$.

Summary: ECC costs $b^{2+o(1)}$. Asymptotically faster than RSA. Bonus: also $b^{2+o(1)}$ *decryption*.

Efficiency is important: users have cost constraints.

Cryptographers, cryptanalys
implementors, etc. tend to
focus on RSA and ECC,
citing these cost constraints

But Shor breaks RSA and E

ECC (with strong curve/$\mathbf{F}_q$, reasonable padding, etc.):

ECDL costs $2^{(1/2+o(1))\lg q}$ by Pollard's rho method. Conjecture: this is the optimal attack against ECC.

Can take $\lg q \in (2+o(1))b$.

Encryption: Fast scalar mult costs $(\lg q)^{2+o(1)} = b^{2+o(1)}$.

Summary: ECC costs $b^{2+o(1)}$. Asymptotically faster than RSA. Bonus: also $b^{2+o(1)}$ *decryption*.

Efficiency is important: users have cost constraints.

Cryptographers, cryptanalysts, implementors, etc. tend to focus on RSA and ECC, citing these cost constraints.

But Shor breaks RSA and ECC!

ECC (with strong curve/$\mathbf{F}_q$, reasonable padding, etc.):

ECDL costs $2^{(1/2+o(1))\lg q}$ by Pollard's rho method. Conjecture: this is the optimal attack against ECC.

Can take $\lg q \in (2+o(1))b$.

Encryption: Fast scalar mult costs $(\lg q)^{2+o(1)} = b^{2+o(1)}$.

Summary: ECC costs $b^{2+o(1)}$. Asymptotically faster than RSA. Bonus: also $b^{2+o(1)}$ *decryption*.

Efficiency is important: users have cost constraints.

Cryptographers, cryptanalysts, implementors, etc. tend to focus on RSA and ECC, citing these cost constraints.

But Shor breaks RSA and ECC!

We think that
the most efficient unbroken *post-quantum* systems will be
hash-based signatures,
code-based encryption,
lattice-based encryption,
multivariate-quadratic sigs.

ith strong curve/$\mathbf{F}_q$,
ble padding, etc.):

osts $2^{(1/2+o(1))\lg q}$
rd's rho method.
ure: this is the
attack against ECC.

e $\lg q \in (2+o(1))b$.

on: Fast scalar mult
$q)^{2+o(1)} = b^{2+o(1)}$.

y: ECC costs $b^{2+o(1)}$.
otically faster than RSA.
also $b^{2+o(1)}$ *decryption*.

Efficiency is important:
users have cost constraints.

Cryptographers, cryptanalysts,
implementors, etc. tend to
focus on RSA and ECC,
citing these cost constraints.

But Shor breaks RSA and ECC!

We think that
the most efficient unbroken
post-quantum systems will be
hash-based signatures,
code-based encryption,
lattice-based encryption,
multivariate-quadratic sigs.

1978 Mc
length-n
reasonab

Conjectu
cost $2^{(\beta}$
Quantu

Can take

Encrypti
costs n^2

Summar

Hmmm:
Need mo

curve/$\mathbf{F}_q$,
g, etc.):
$+o(1))\lg q$

ethod.
s the
ainst ECC.

$+ o(1))b$.

scalar mult
$= b^{2+o(1)}$.

osts $b^{2+o(1)}$.
ster than RSA.
$1)$ *decryption*.

Efficiency is important:
users have cost constraints.

Cryptographers, cryptanalysts, implementors, etc. tend to focus on RSA and ECC, citing these cost constraints.

But Shor breaks RSA and ECC!

We think that
the most efficient unbroken *post-quantum* systems will be
hash-based signatures,
code-based encryption,
lattice-based encryption,
multivariate-quadratic sigs.

1978 McEliece sys
length-n classical
reasonable paddin

Conjecture: Faste
cost $2^{(\beta+o(1))n/\lg}$
Quantum attacks:

Can take $n \in (1/$

Encryption: Matri
costs $n^{2+o(1)} = b^2$

Summary: McElie

Hmmm: is this *fas*
Need more detaile

.

t

).

RSA.

ion.

Efficiency is important:
users have cost constraints.

Cryptographers, cryptanalysts,
implementors, etc. tend to
focus on RSA and ECC,
citing these cost constraints.

But Shor breaks RSA and ECC!

We think that
the most efficient unbroken
post-quantum systems will be
hash-based signatures,
code-based encryption,
lattice-based encryption,
multivariate-quadratic sigs.

1978 McEliece system (with
length-n classical Goppa co
reasonable padding, etc.):

Conjecture: Fastest attacks
cost $2^{(\beta+o(1))n/\lg n}$.
Quantum attacks: smaller β

Can take $n \in (1/\beta + o(1))b$

Encryption: Matrix mult
costs $n^{2+o(1)} = b^{2+o(1)}$.

Summary: McEliece costs b^2

Hmmm: is this *faster* than
Need more detailed analysis.

Efficiency is important:
users have cost constraints.

Cryptographers, cryptanalysts, implementors, etc. tend to focus on RSA and ECC, citing these cost constraints.

But Shor breaks RSA and ECC!

We think that
the most efficient unbroken *post-quantum* systems will be
hash-based signatures,
code-based encryption,
lattice-based encryption,
multivariate-quadratic sigs.

1978 McEliece system (with length-n classical Goppa codes, reasonable padding, etc.):

Conjecture: Fastest attacks cost $2^{(\beta+o(1))n/\lg n}$.
Quantum attacks: smaller β.

Can take $n \in (1/\beta + o(1))b \lg b$.

Encryption: Matrix mult costs $n^{2+o(1)} = b^{2+o(1)}$.

Summary: McEliece costs $b^{2+o(1)}$.

Hmmm: is this *faster* than ECC?
Need more detailed analysis.

ty is important:
ve cost constraints.

raphers, cryptanalysts,
ntors, etc. tend to
RSA and ECC,
ese cost constraints.

r breaks RSA and ECC!

k that
t efficient unbroken
antum systems will be
sed signatures,
sed encryption,
ased encryption,
iate-quadratic sigs.

1978 McEliece system (with length-n classical Goppa codes, reasonable padding, etc.):

Conjecture: Fastest attacks cost $2^{(\beta+o(1))n/\lg n}$.
Quantum attacks: smaller β.

Can take $n \in (1/\beta + o(1)) b \lg b$.

Encryption: Matrix mult costs $n^{2+o(1)} = b^{2+o(1)}$.

Summary: McEliece costs $b^{2+o(1)}$.

Hmmm: is this *faster* than ECC?
Need more detailed analysis.

ECC enc
$\Theta(\lg q)$
Each op
$\Theta(\lg q \lg$
Total Θ

rtant:

nstraints.

ryptanalysts,

, tend to

ECC,

onstraints.

RSA and ECC!

unbroken

tems will be

ures,

otion,

yption,

ratic sigs.

1978 McEliece system (with length-n classical Goppa codes, reasonable padding, etc.):

Conjecture: Fastest attacks cost $2^{(\beta+o(1))n/\lg n}$.

Quantum attacks: smaller β.

Can take $n \in (1/\beta + o(1))b \lg b$.

Encryption: Matrix mult costs $n^{2+o(1)} = b^{2+o(1)}$.

Summary: McEliece costs $b^{2+o(1)}$.

Hmmm: is this *faster* than ECC? Need more detailed analysis.

ECC encryption:

$\Theta(\lg q)$ operations

Each operation in

$\Theta(\lg q \lg \lg q \lg \lg \lg$

Total $\Theta(b^2 \lg b \lg \lg$

ts,

.

CC!

be

1978 McEliece system (with length-n classical Goppa codes, reasonable padding, etc.):

Conjecture: Fastest attacks cost $2^{(\beta+o(1))n/\lg n}$.
Quantum attacks: smaller β.

Can take $n \in (1/\beta + o(1))b \lg b$.

Encryption: Matrix mult costs $n^{2+o(1)} = b^{2+o(1)}$.

Summary: McEliece costs $b^{2+o(1)}$.

Hmmm: is this *faster* than ECC?
Need more detailed analysis.

ECC encryption:
$\Theta(\lg q)$ operations in $\mathbf{F}_q$.
Each operation in $\mathbf{F}_q$ costs $\Theta(\lg q \lg\lg q \lg\lg\lg q)$.
Total $\Theta(b^2 \lg b \lg\lg b)$.

1978 McEliece system (with length-n classical Goppa codes, reasonable padding, etc.):

Conjecture: Fastest attacks cost $2^{(\beta+o(1))n/\lg n}$.
Quantum attacks: smaller β.

Can take $n \in (1/\beta + o(1)) b \lg b$.

Encryption: Matrix mult costs $n^{2+o(1)} = b^{2+o(1)}$.

Summary: McEliece costs $b^{2+o(1)}$.

Hmmm: is this *faster* than ECC?
Need more detailed analysis.

ECC encryption:
$\Theta(\lg q)$ operations in $\mathbf{F}_q$.
Each operation in $\mathbf{F}_q$ costs $\Theta(\lg q \lg\lg q \lg\lg\lg q)$.
Total $\Theta(b^2 \lg b \lg\lg b)$.

1978 McEliece system (with length-n classical Goppa codes, reasonable padding, etc.):

Conjecture: Fastest attacks cost $2^{(\beta+o(1))n/\lg n}$.
Quantum attacks: smaller β.

Can take $n \in (1/\beta + o(1))b \lg b$.

Encryption: Matrix mult costs $n^{2+o(1)} = b^{2+o(1)}$.

Summary: McEliece costs $b^{2+o(1)}$.

Hmmm: is this *faster* than ECC? Need more detailed analysis.

ECC encryption:
$\Theta(\lg q)$ operations in $\mathbf{F}_q$.
Each operation in $\mathbf{F}_q$ costs $\Theta(\lg q \lg\lg q \lg\lg\lg q)$.
Total $\Theta(b^2 \lg b \lg\lg b)$.

McEliece encryption, with 1986 Niederreiter speedup:
$\Theta(n/\lg n)$ additions in $\mathbf{F}_2^n$, each costing $\Theta(n)$.
Total $\Theta(b^2 \lg b)$.

1978 McEliece system (with length-n classical Goppa codes, reasonable padding, etc.):

Conjecture: Fastest attacks cost $2^{(\beta+o(1))n/\lg n}$.
Quantum attacks: smaller β.

Can take $n \in (1/\beta + o(1))b \lg b$.

Encryption: Matrix mult costs $n^{2+o(1)} = b^{2+o(1)}$.

Summary: McEliece costs $b^{2+o(1)}$.

Hmmm: is this *faster* than ECC?
Need more detailed analysis.

ECC encryption:
$\Theta(\lg q)$ operations in $\mathbf{F}_q$.
Each operation in $\mathbf{F}_q$ costs $\Theta(\lg q \lg\lg q \lg\lg\lg q)$.
Total $\Theta(b^2 \lg b \lg\lg b)$.

McEliece encryption,
with 1986 Niederreiter speedup:
$\Theta(n/\lg n)$ additions in $\mathbf{F}_2^n$,
each costing $\Theta(n)$.
Total $\Theta(b^2 \lg b)$.

McEliece is asymptotically faster.
Bonus: Even faster decryption.
Another bonus: Post-quantum.

cEliece system (with
, classical Goppa codes,
ble padding, etc.):

ure: Fastest attacks
$+o(1))n/\lg n$.

m attacks: smaller β.

e $n \in (1/\beta + o(1))b \lg b$.

on: Matrix mult
$+o(1) = b^{2+o(1)}$.

y: McEliece costs $b^{2+o(1)}$.

is this *faster* than ECC?
ore detailed analysis.

ECC encryption:
$\Theta(\lg q)$ operations in $\mathbf{F}_q$.
Each operation in $\mathbf{F}_q$ costs
$\Theta(\lg q \lg \lg q \lg \lg \lg q)$.
Total $\Theta(b^2 \lg b \lg \lg b)$.

McEliece encryption,
with 1986 Niederreiter speedup:
$\Theta(n/\lg n)$ additions in $\mathbf{F}_2^n$,
each costing $\Theta(n)$.
Total $\Theta(b^2 \lg b)$.

McEliece is asymptotically faster.
Bonus: Even faster decryption.
Another bonus: Post-quantum.

Algorith
the com

1. Spee
$\lg \lg b$ us
someday

stem (with
Goppa codes,
g, etc.):

st attacks
^{n}.

smaller β.

$\beta + o(1))b \lg b$.

x mult
$^{2+o(1)}$.

ce costs $b^{2+o(1)}$.

ster than ECC?
d analysis.

ECC encryption:
$\Theta(\lg q)$ operations in $\mathbf{F}_q$.
Each operation in $\mathbf{F}_q$ costs
$\Theta(\lg q \lg \lg q \lg \lg \lg q)$.
Total $\Theta(b^2 \lg b \lg \lg b)$.

McEliece encryption,
with 1986 Niederreiter speedup:
$\Theta(n/\lg n)$ additions in $\mathbf{F}_2^n$,
each costing $\Theta(n)$.
Total $\Theta(b^2 \lg b)$.

McEliece is asymptotically faster.
Bonus: Even faster decryption.
Another bonus: Post-quantum.

Algorithmic advan
the competition.

1. Speed up ECC:
$\lg \lg b$ using 2007
someday eliminate

des,

3.

$\lg b$.

$^{2+o(1)}$.

ECC?

.

ECC encryption:
$\Theta(\lg q)$ operations in $\mathbf{F}_q$.
Each operation in $\mathbf{F}_q$ costs
$\Theta(\lg q \lg \lg q \lg \lg \lg q)$.
Total $\Theta(b^2 \lg b \lg \lg b)$.

McEliece encryption,
with 1986 Niederreiter speedup:
$\Theta(n/\lg n)$ additions in $\mathbf{F}_2^n$,
each costing $\Theta(n)$.
Total $\Theta(b^2 \lg b)$.

McEliece is asymptotically faster.
Bonus: Even faster decryption.
Another bonus: Post-quantum.

Algorithmic advances can ch
the competition. Examples:

1. Speed up ECC: can reduc
$\lg \lg b$ using 2007 Fürer; may
someday eliminate $\lg \lg b$?

ECC encryption:
$\Theta(\lg q)$ operations in $\mathbf{F}_q$.
Each operation in $\mathbf{F}_q$ costs
$\Theta(\lg q \lg\lg q \lg\lg\lg q)$.
Total $\Theta(b^2 \lg b \lg\lg b)$.

McEliece encryption,
with 1986 Niederreiter speedup:
$\Theta(n/\lg n)$ additions in $\mathbf{F}_2^n$,
each costing $\Theta(n)$.
Total $\Theta(b^2 \lg b)$.

McEliece is asymptotically faster.
Bonus: Even faster decryption.
Another bonus: Post-quantum.

Algorithmic advances can change the competition. Examples:

1. Speed up ECC: can reduce $\lg\lg b$ using 2007 Fürer; maybe someday eliminate $\lg\lg b$?

ECC encryption:
$\Theta(\lg q)$ operations in $\mathbf{F}_q$.
Each operation in $\mathbf{F}_q$ costs
$\Theta(\lg q \lg\lg q \lg\lg\lg q)$.
Total $\Theta(b^2 \lg b \lg\lg b)$.

McEliece encryption,
with 1986 Niederreiter speedup:
$\Theta(n/\lg n)$ additions in $\mathbf{F}_2^n$,
each costing $\Theta(n)$.
Total $\Theta(b^2 \lg b)$.

McEliece is asymptotically faster.
Bonus: Even faster decryption.
Another bonus: Post-quantum.

Algorithmic advances can change the competition. Examples:

1. Speed up ECC: can reduce $\lg\lg b$ using 2007 Fürer; maybe someday eliminate $\lg\lg b$?

2. Faster attacks on McEliece:
2010 Bernstein–Lange–Peters,
2011 May–Meurer–Thomae,
2012 Becker–Joux–May–Meurer.
. . . but still $\Theta(b^2 \lg b)$.

ECC encryption:
$\Theta(\lg q)$ operations in $\mathbf{F}_q$.
Each operation in $\mathbf{F}_q$ costs
$\Theta(\lg q \lg\lg q \lg\lg\lg q)$.
Total $\Theta(b^2 \lg b \lg\lg b)$.

McEliece encryption,
with 1986 Niederreiter speedup:
$\Theta(n/\lg n)$ additions in $\mathbf{F}_2^n$,
each costing $\Theta(n)$.
Total $\Theta(b^2 \lg b)$.

McEliece is asymptotically faster.
Bonus: Even faster decryption.
Another bonus: Post-quantum.

Algorithmic advances can change the competition. Examples:

1. Speed up ECC: can reduce $\lg\lg b$ using 2007 Fürer; maybe someday eliminate $\lg\lg b$?

2. Faster attacks on McEliece:
2010 Bernstein–Lange–Peters,
2011 May–Meurer–Thomae,
2012 Becker–Joux–May–Meurer.
. . . but still $\Theta(b^2 \lg b)$.

3. We're optimizing "subfield AG" variant of McEliece.
Conjecture: Fastest attacks cost $2^{(\alpha+o(1))n}$; encryption $\Theta(b^2)$.

cryption:

operations in $\mathbf{F}_q$.

eration in $\mathbf{F}_q$ costs

lg q lg lg lg q).

$(b^2 \lg b \lg\lg b)$.

e encryption,

86 Niederreiter speedup:

n) additions in $\mathbf{F}_2^n$,

sting $\Theta(n)$.

$(b^2 \lg b)$.

e is asymptotically faster.

Even faster decryption.

bonus: Post-quantum.

Algorithmic advances can change the competition. Examples:

1. Speed up ECC: can reduce $\lg\lg b$ using 2007 Fürer; maybe someday eliminate $\lg\lg b$?

2. Faster attacks on McEliece:
2010 Bernstein–Lange–Peters,
2011 May–Meurer–Thomae,
2012 Becker–Joux–May–Meurer.
… but still $\Theta(b^2 \lg b)$.

3. We're optimizing "subfield AG" variant of McEliece.
Conjecture: Fastest attacks cost $2^{(\alpha+o(1))n}$; encryption $\Theta(b^2)$.

Code-ba

Modern

Receiver

$t \lg n \times$

Specifies

Typically

e.g., $n =$

Message

$\{m \in \mathbf{F}$

Encrypti

Use hash

GCM ke

in $\mathbf{F}_q$.
$\mathbf{F}_q$ costs
g q).
g b).

on,
eiter speedup:
ns in $\mathbf{F}_2^n$,
).

totically faster.
r decryption.
ost-quantum.

Algorithmic advances can change the competition. Examples:

1. Speed up ECC: can reduce $\lg\lg b$ using 2007 Fürer; maybe someday eliminate $\lg\lg b$?

2. Faster attacks on McEliece: 2010 Bernstein–Lange–Peters, 2011 May–Meurer–Thomae, 2012 Becker–Joux–May–Meurer. … but still $\Theta(b^2 \lg b)$.

3. We're optimizing "subfield AG" variant of McEliece. Conjecture: Fastest attacks cost $2^{(\alpha+o(1))n}$; encryption $\Theta(b^2)$.

Code-based encryp

Modern version of

Receiver's public k
$t \lg n \times n$ matrix
Specifies linear $\mathbf{F}_2^n$

Typically $t \lg n \approx$
e.g., $n = 2048$, t =

Messages suitable
$\{m \in \mathbf{F}_2^n : \#\{i :$

Encryption of m i

Use hash of m as
GCM key to encry

dup:

aster.

on.

um.

Algorithmic advances can change the competition. Examples:

1. Speed up ECC: can reduce $\lg \lg b$ using 2007 Fürer; maybe someday eliminate $\lg \lg b$?

2. Faster attacks on McEliece:
2010 Bernstein–Lange–Peters,
2011 May–Meurer–Thomae,
2012 Becker–Joux–May–Meurer.
… but still $\Theta(b^2 \lg b)$.

3. We're optimizing "subfield AG" variant of McEliece.
Conjecture: Fastest attacks cost $2^{(\alpha+o(1))n}$; encryption $\Theta(b^2)$.

Code-based encryption

Modern version of McEliece

Receiver's public key is "ran
$t \lg n \times n$ matrix K over $\mathbf{F}_2$
Specifies linear $\mathbf{F}_2^n \to \mathbf{F}_2^{t \lg n}$

Typically $t \lg n \approx 0.2n$;
e.g., $n = 2048$, $t = 40$.

Messages suitable for encryp
$\{m \in \mathbf{F}_2^n : \#\{i : m_i = 1\} =$

Encryption of m is $Km \in \mathbf{F}$

Use hash of m as secret AE
GCM key to encrypt more d

Algorithmic advances can change the competition. Examples:

1. Speed up ECC: can reduce $\lg \lg b$ using 2007 Fürer; maybe someday eliminate $\lg \lg b$?

2. Faster attacks on McEliece: 2010 Bernstein–Lange–Peters, 2011 May–Meurer–Thomae, 2012 Becker–Joux–May–Meurer. . . . but still $\Theta(b^2 \lg b)$.

3. We're optimizing "subfield AG" variant of McEliece. Conjecture: Fastest attacks cost $2^{(\alpha+o(1))n}$; encryption $\Theta(b^2)$.

Code-based encryption

Modern version of McEliece:

Receiver's public key is "random" $t \lg n \times n$ matrix K over $\mathbf{F}_2$. Specifies linear $\mathbf{F}_2^n \to \mathbf{F}_2^{t \lg n}$.

Typically $t \lg n \approx 0.2n$; e.g., $n = 2048$, $t = 40$.

Messages suitable for encryption: $\{m \in \mathbf{F}_2^n : \#\{i : m_i = 1\} = t\}$.

Encryption of m is $Km \in \mathbf{F}_2^{t \lg n}$.

Use hash of m as secret AES-GCM key to encrypt more data.

mic advances can change
petition. Examples:

d up ECC: can reduce
sing 2007 Fürer; maybe
eliminate $\lg\lg b$?

er attacks on McEliece:
rnstein–Lange–Peters,
ay–Meurer–Thomae,
cker–Joux–May–Meurer.
still $\Theta(b^2 \lg b)$.

e optimizing “subfield
iant of McEliece.
ure: Fastest attacks cost
$)^{n}$; encryption $\Theta(b^2)$.

Code-based encryption

Modern version of McEliece:

Receiver’s public key is “random” $t \lg n \times n$ matrix K over $\mathbf{F}_2$. Specifies linear $\mathbf{F}_2^n \to \mathbf{F}_2^{t \lg n}$.

Typically $t \lg n \approx 0.2n$; e.g., $n = 2048$, $t = 40$.

Messages suitable for encryption: $\{m \in \mathbf{F}_2^n : \#\{i : m_i = 1\} = t\}$.

Encryption of m is $Km \in \mathbf{F}_2^{t \lg n}$.

Use hash of m as secret AES-GCM key to encrypt more data.

Attacker
easily wo
from K
such tha

i.e. Atta
element
Note tha

Attacker
to find e
at dista
Presuma
But deco

Receiver
Goppa s

ces can change
Examples:

can reduce
Fürer; maybe
e lg lg b?

on McEliece:
ange–Peters,
–Thomae,
–May–Meurer.
g b).

ng “subfield
cEliece.
st attacks cost
tion $\Theta(b^2)$.

Code-based encryption

Modern version of McEliece:

Receiver’s public key is “random” $t \lg n \times n$ matrix K over $\mathbf{F}_2$. Specifies linear $\mathbf{F}_2^n \to \mathbf{F}_2^{t \lg n}$.

Typically $t \lg n \approx 0.2n$; e.g., $n = 2048$, $t = 40$.

Messages suitable for encryption: $\{m \in \mathbf{F}_2^n : \#\{i : m_i = 1\} = t\}$.

Encryption of m is $Km \in \mathbf{F}_2^{t \lg n}$.

Use hash of m as secret AES-GCM key to encrypt more data.

Attacker, by linear
easily works backw
from Km to *some*
such that $Kv = K$

i.e. Attacker finds
element $v \in m +$
Note that #Ker$K$

Attacker wants to
to find element of
at distance only t
Presumably unique
But decoding isn’t

Receiver builds K
Goppa structure fo

hange

ce
ybe

ce:
rs,

urer.

ld

cost
).

Code-based encryption

Modern version of McEliece:

Receiver's public key is "random" $t \lg n \times n$ matrix K over $\mathbf{F}_2$. Specifies linear $\mathbf{F}_2^n \to \mathbf{F}_2^{t \lg n}$.

Typically $t \lg n \approx 0.2n$; e.g., $n = 2048$, $t = 40$.

Messages suitable for encryption: $\left\{m \in \mathbf{F}_2^n : \#\{i : m_i = 1\} = t\right\}$.

Encryption of m is $Km \in \mathbf{F}_2^{t \lg n}$.

Use hash of m as secret AES-GCM key to encrypt more data.

Attacker, by linear algebra, easily works backwards from Km to *some* $v \in \mathbf{F}_2^n$ such that $Kv = Km$.

i.e. Attacker finds *some* element $v \in m + \mathrm{Ker} K$. Note that $\#\mathrm{Ker} K \geq 2^{n-t \lg}$

Attacker wants to decode v: to find element of $\mathrm{Ker} K$ at distance only t from v. Presumably unique, revealin But decoding isn't easy!

Receiver builds K with *secre* Goppa structure for fast dec

Code-based encryption

Modern version of McEliece:

Receiver's public key is "random" $t \lg n \times n$ matrix K over $\mathbf{F}_2$.
Specifies linear $\mathbf{F}_2^n \to \mathbf{F}_2^{t \lg n}$.

Typically $t \lg n \approx 0.2n$;
e.g., $n = 2048$, $t = 40$.

Messages suitable for encryption:
$\{m \in \mathbf{F}_2^n : \#\{i : m_i = 1\} = t\}$.

Encryption of m is $Km \in \mathbf{F}_2^{t \lg n}$.

Use hash of m as secret AES-GCM key to encrypt more data.

Attacker, by linear algebra, easily works backwards from Km to *some* $v \in \mathbf{F}_2^n$ such that $Kv = Km$.

i.e. Attacker finds *some* element $v \in m + \text{Ker}K$.
Note that $\#\text{Ker}K \geq 2^{n - t \lg n}$.

Attacker wants to decode v: to find element of $\text{Ker}K$ at distance only t from v.
Presumably unique, revealing m.
But decoding isn't easy!

Receiver builds K with *secret* Goppa structure for fast decoding.

sed encryption

version of McEliece:

’s public key is “random”
n matrix K over $\mathbf{F}_2$.
s linear $\mathbf{F}_2^n \to \mathbf{F}_2^{t \lg n}$.

y $t \lg n \approx 0.2n$;
$= 2048$, $t = 40$.

es suitable for encryption:
$_2^n : \#\{i : m_i = 1\} = t\}$.

on of m is $Km \in \mathbf{F}_2^{t \lg n}$.

n of m as secret AES-
y to encrypt more data.

Attacker, by linear algebra, easily works backwards from Km to *some* $v \in \mathbf{F}_2^n$ such that $Kv = Km$.

i.e. Attacker finds *some* element $v \in m + \mathrm{Ker} K$. Note that $\#\mathrm{Ker} K \ge 2^{n - t \lg n}$.

Attacker wants to decode v: to find element of $\mathrm{Ker} K$ at distance only t from v. Presumably unique, revealing m. But decoding isn’t easy!

Receiver builds K with *secret* Goppa structure for fast decoding.

Goppa c

Fix $q \in$
$t \in \{2, 3$
$n \in \{t \lg$
e.g. $q =$
or $q = 4$

Receiver
as the p
for the c
irreducib
binary G
a monic
polynom
distinct

ption

McEliece:

key is “random”
K over $\mathbf{F}_2$.
$\to \mathbf{F}_2^{t \lg n}$.

$0.2n$;
$= 40$.

for encryption:
$m_i = 1\} = t\}$.

s $Km \in \mathbf{F}_2^{t \lg n}$.

secret AES-
pt more data.

Attacker, by linear algebra, easily works backwards from Km to *some* $v \in \mathbf{F}_2^n$ such that $Kv = Km$.

i.e. Attacker finds *some* element $v \in m + \mathrm{Ker} K$. Note that $\#\mathrm{Ker} K \geq 2^{n - t \lg n}$.

Attacker wants to decode v: to find element of $\mathrm{Ker} K$ at distance only t from v. Presumably unique, revealing m. But decoding isn't easy!

Receiver builds K with *secret* Goppa structure for fast decoding.

Goppa codes

Fix $q \in \{8, 16, 32,$
$t \in \{2, 3, \ldots, \lfloor(q$
$n \in \{t \lg q + 1, t \lg$
e.g. $q = 1024$, $t =$
or $q = 4096$, $t = 1$

Receiver builds a
as the parity-chec
for the classical (g
irreducible length-
binary Goppa code
a monic degree-t i
polynomial $g \in \mathbf{F}_q$
distinct $a_1, a_2, \ldots$

:

dom”

.

ption:

$= t\}$.

$t \lg n$

2 .

S-

ata.

Attacker, by linear algebra,
easily works backwards
from Km to *some* $v \in \mathbf{F}_2^n$
such that $Kv = Km$.

i.e. Attacker finds *some*
element $v \in m + \mathrm{Ker}K$.
Note that $\#\mathrm{Ker}K \ge 2^{n-t\lg n}$.

Attacker wants to decode v:
to find element of $\mathrm{Ker}K$
at distance only t from v.
Presumably unique, revealing m.
But decoding isn't easy!

Receiver builds K with *secret*
Goppa structure for fast decoding.

Goppa codes

Fix $q \in \{8, 16, 32, \ldots\}$;
$t \in \{2, 3, \ldots, \lfloor (q-1)/\lg q \rfloor$
$n \in \{t \lg q + 1, t \lg q + 2, \ldots$
e.g. $q = 1024$, $t = 50$, $n =$
or $q = 4096$, $t = 150$, $n = 3$

Receiver builds a matrix H
as the parity-check matrix
for the classical (genus-0)
irreducible length-n degree-t
binary Goppa code defined b
a monic degree-t irreducible
polynomial $g \in \mathbf{F}_q[x]$ and
distinct $a_1, a_2, \ldots, a_n \in \mathbf{F}_q$.

Attacker, by linear algebra, easily works backwards from Km to *some* $v \in \mathbf{F}_2^n$ such that $Kv = Km$.

i.e. Attacker finds *some* element $v \in m + \mathrm{Ker}K$. Note that $\#\mathrm{Ker}K \geq 2^{n - t \lg n}$.

Attacker wants to decode v: to find element of Ker$K$ at distance only t from v. Presumably unique, revealing m. But decoding isn't easy!

Receiver builds K with *secret* Goppa structure for fast decoding.

Goppa codes

Fix $q \in \{8, 16, 32, \ldots\}$;
$t \in \{2, 3, \ldots, \lfloor (q-1)/\lg q \rfloor\}$;
$n \in \{t \lg q + 1, t \lg q + 2, \ldots, q\}$.
e.g. $q = 1024$, $t = 50$, $n = 1024$.
or $q = 4096$, $t = 150$, $n = 3600$.

Receiver builds a matrix H as the parity-check matrix for the classical (genus-0) irreducible length-n degree-t binary Goppa code defined by a monic degree-t irreducible polynomial $g \in \mathbf{F}_q[x]$ and distinct $a_1, a_2, \ldots, a_n \in \mathbf{F}_q$.

r, by linear algebra,
orks backwards
m to *some* $v \in \mathbf{F}_2^n$
nt $Kv = Km$.

acker finds *some*
$v \in m + \mathrm{Ker}K$.
at $\#\mathrm{Ker}K \geq 2^{n-t\lg n}$.

r wants to decode v:
element of Ker$K$
nce only t from v.
ably unique, revealing m.
oding isn't easy!

r builds K with *secret*
tructure for fast decoding.

Goppa codes

Fix $q \in \{8, 16, 32, \ldots\}$;
$t \in \{2, 3, \ldots, \lfloor (q-1)/\lg q \rfloor\}$;
$n \in \{t \lg q + 1, t \lg q + 2, \ldots, q\}$.
e.g. $q = 1024$, $t = 50$, $n = 1024$.
or $q = 4096$, $t = 150$, $n = 3600$.

Receiver builds a matrix H
as the parity-check matrix
for the classical (genus-0)
irreducible length-n degree-t
binary Goppa code defined by
a monic degree-t irreducible
polynomial $g \in \mathbf{F}_q[x]$ and
distinct $a_1, a_2, \ldots, a_n \in \mathbf{F}_q$.

. . . which

View eac
as a colu
Then H

algebra,
vards
e $v \in \mathbf{F}_2^n$
m.

some
Ker$K$.
$\geq 2^{n-t\lg n}$.

decode v:
Ker$K$
from v.
e, revealing m.
easy!

with *secret*
or fast decoding.

Goppa codes

Fix $q \in \{8, 16, 32, \ldots\}$;
$t \in \{2, 3, \ldots, \lfloor (q-1)/\lg q \rfloor\}$;
$n \in \{t \lg q + 1, t \lg q + 2, \ldots, q\}$.
e.g. $q = 1024$, $t = 50$, $n = 1024$.
or $q = 4096$, $t = 150$, $n = 3600$.

Receiver builds a matrix H as the parity-check matrix for the classical (genus-0) irreducible length-n degree-t binary Goppa code defined by a monic degree-t irreducible polynomial $g \in \mathbf{F}_q[x]$ and distinct $a_1, a_2, \ldots, a_n \in \mathbf{F}_q$.

. . . which means:

$$\left(\begin{array}{ll} \dfrac{1}{g(a_1)} & \cdots \\ \dfrac{a_1}{g(a_1)} & \cdots \\ \vdots & \ddots \\ \dfrac{a_1^{t-1}}{g(a_1)} & \cdots \end{array} \right.$$

View each element
as a column in $\mathbf{F}_2^{\lg}$
Then $H : \mathbf{F}_2^n \to \mathbf{F}$

n.

:

g m.

et

oding.

Goppa codes

Fix $q \in \{8, 16, 32, \ldots\}$;
$t \in \{2, 3, \ldots, \lfloor (q-1)/\lg q \rfloor\}$;
$n \in \{t \lg q + 1, t \lg q + 2, \ldots, q\}$.
e.g. $q = 1024$, $t = 50$, $n = 1024$.
or $q = 4096$, $t = 150$, $n = 3600$.

Receiver builds a matrix H as the parity-check matrix for the classical (genus-0) irreducible length-n degree-t binary Goppa code defined by a monic degree-t irreducible polynomial $g \in \mathbf{F}_q[x]$ and distinct $a_1, a_2, \ldots, a_n \in \mathbf{F}_q$.

…which means: $H =$

$$\begin{pmatrix} \dfrac{1}{g(a_1)} & \cdots & \dfrac{1}{g(a_n)} \\ \dfrac{a_1}{g(a_1)} & \cdots & \dfrac{a_n}{g(a_n)} \\ \vdots & \ddots & \vdots \\ \dfrac{a_1^{t-1}}{g(a_1)} & \cdots & \dfrac{a_n^{t-1}}{g(a_n)} \end{pmatrix}$$

View each element of $\mathbf{F}_q$ he
as a column in $\mathbf{F}_2^{\lg q}$.
Then $H : \mathbf{F}_2^n \to \mathbf{F}_2^{t \lg q}$.

Goppa codes

Fix $q \in \{8, 16, 32, \ldots\}$;
$t \in \{2, 3, \ldots, \lfloor (q-1)/\lg q \rfloor\}$;
$n \in \{t \lg q + 1, t \lg q + 2, \ldots, q\}$.
e.g. $q = 1024$, $t = 50$, $n = 1024$.
or $q = 4096$, $t = 150$, $n = 3600$.

Receiver builds a matrix H as the parity-check matrix for the classical (genus-0) irreducible length-n degree-t binary Goppa code defined by a monic degree-t irreducible polynomial $g \in \mathbf{F}_q[x]$ and distinct $a_1, a_2, \ldots, a_n \in \mathbf{F}_q$.

…which means: $H =$

$$\begin{pmatrix} \frac{1}{g(a_1)} & \cdots & \frac{1}{g(a_n)} \\ \frac{a_1}{g(a_1)} & \cdots & \frac{a_n}{g(a_n)} \\ \vdots & \ddots & \vdots \\ \frac{a_1^{t-1}}{g(a_1)} & \cdots & \frac{a_n^{t-1}}{g(a_n)} \end{pmatrix}.$$

View each element of $\mathbf{F}_q$ here as a column in $\mathbf{F}_2^{\lg q}$.
Then $H : \mathbf{F}_2^n \to \mathbf{F}_2^{t \lg q}$.

odes

$\{8, 16, 32, \ldots\}$;

$3, \ldots, \lfloor (q-1)/\lg q \rfloor\}$;

$g\, q + 1, t \lg q + 2, \ldots, q\}$.

$= 1024$, $t = 50$, $n = 1024$.

096, $t = 150$, $n = 3600$.

builds a matrix H

arity-check matrix

classical (genus-0)

ble length-n degree-t

Goppa code defined by

degree-t irreducible

nial $g \in \mathbf{F}_q[x]$ and

$a_1, a_2, \ldots, a_n \in \mathbf{F}_q$.

…which means: $H =$

$$\begin{pmatrix} \dfrac{1}{g(a_1)} & \cdots & \dfrac{1}{g(a_n)} \\ \dfrac{a_1}{g(a_1)} & \cdots & \dfrac{a_n}{g(a_n)} \\ \vdots & \ddots & \vdots \\ \dfrac{a_1^{t-1}}{g(a_1)} & \cdots & \dfrac{a_n^{t-1}}{g(a_n)} \end{pmatrix}.$$

View each element of $\mathbf{F}_q$ here as a column in $\mathbf{F}_2^{\lg q}$.

Then $H : \mathbf{F}_2^n \to \mathbf{F}_2^{t \lg q}$.

More us

the map

from $\mathbf{F}_2^n$

H is the

where $\mathbf{F}$

and $\mathbf{F}_q[x$

$\lfloor g/x \rfloor$, $\lfloor$

One-line

$$\frac{g - g(a_i}{x - a_i}$$

Receiver

as row r

revealing

$\ldots\}$;

$-1)/\lg q\rfloor\}$;

$g\, q+2,\ldots,q\}$.

$= 50$, $n = 1024$.

150, $n = 3600$.

matrix H

k matrix

genus-0)

n degree-t

e defined by

rreducible

$[x]$ and

$, a_n \in \mathbf{F}_q$.

…which means: $H =$

$$\begin{pmatrix} \dfrac{1}{g(a_1)} & \cdots & \dfrac{1}{g(a_n)} \\ \dfrac{a_1}{g(a_1)} & \cdots & \dfrac{a_n}{g(a_n)} \\ \vdots & \ddots & \vdots \\ \dfrac{a_1^{t-1}}{g(a_1)} & \cdots & \dfrac{a_n^{t-1}}{g(a_n)} \end{pmatrix}.$$

View each element of $\mathbf{F}_q$ here as a column in $\mathbf{F}_2^{\lg q}$.
Then $H : \mathbf{F}_2^n \to \mathbf{F}_2^{t \lg q}$.

More useful view:

the map $m \mapsto \sum_i$

from $\mathbf{F}_2^n$ to $\mathbf{F}_q[x]/$

H is the matrix fo

where $\mathbf{F}_2^n$ has stan

and $\mathbf{F}_q[x]/g$ has b

$\lfloor g/x \rfloor$, $\lfloor g/x^2 \rfloor$, $\ldots$

One-line proof: In

$$\frac{g - g(a_i)}{x - a_i} = \sum_{j \ge 0} a$$

Receiver generates

as row reduction o

revealing only Ker

$\}$;

$, q\}$.

1024.

600.

t

by

…which means: $H =$

$$\begin{pmatrix} \dfrac{1}{g(a_1)} & \cdots & \dfrac{1}{g(a_n)} \\ \dfrac{a_1}{g(a_1)} & \cdots & \dfrac{a_n}{g(a_n)} \\ \vdots & \ddots & \vdots \\ \dfrac{a_1^{t-1}}{g(a_1)} & \cdots & \dfrac{a_n^{t-1}}{g(a_n)} \end{pmatrix}.$$

View each element of $\mathbf{F}_q$ here as a column in $\mathbf{F}_2^{\lg q}$.
Then $H : \mathbf{F}_2^n \to \mathbf{F}_2^{t \lg q}$.

More useful view: Consider the map $m \mapsto \sum_i m_i/(x -$
from $\mathbf{F}_2^n$ to $\mathbf{F}_q[x]/g$.

H is the matrix for this map where $\mathbf{F}_2^n$ has standard basi
and $\mathbf{F}_q[x]/g$ has basis
$\lfloor g/x \rfloor$, $\lfloor g/x^2 \rfloor$, …, $\lfloor g/x^t \rfloor$.

One-line proof: In $\mathbf{F}_q[x]$ hav

$$\frac{g - g(a_i)}{x - a_i} = \sum_{j \ge 0} a_i^j \left\lfloor g/x^{j+1}\right.$$

Receiver generates key K
as row reduction of H,
revealing only Ker$H$.

. . . which means: $H =$

$$\begin{pmatrix} \dfrac{1}{g(a_1)} & \cdots & \dfrac{1}{g(a_n)} \\ \dfrac{a_1}{g(a_1)} & \cdots & \dfrac{a_n}{g(a_n)} \\ \vdots & \ddots & \vdots \\ \dfrac{a_1^{t-1}}{g(a_1)} & \cdots & \dfrac{a_n^{t-1}}{g(a_n)} \end{pmatrix}.$$

View each element of $\mathbf{F}_q$ here as a column in $\mathbf{F}_2^{\lg q}$.
Then $H : \mathbf{F}_2^n \to \mathbf{F}_2^{t \lg q}$.

More useful view: Consider the map $m \mapsto \sum_i m_i/(x - a_i)$ from $\mathbf{F}_2^n$ to $\mathbf{F}_q[x]/g$.

H is the matrix for this map where $\mathbf{F}_2^n$ has standard basis and $\mathbf{F}_q[x]/g$ has basis $\lfloor g/x \rfloor$, $\lfloor g/x^2 \rfloor$, . . . , $\lfloor g/x^t \rfloor$.

One-line proof: In $\mathbf{F}_q[x]$ have

$$\frac{g - g(a_i)}{x - a_i} = \sum_{j \ge 0} a_i^j \left\lfloor g/x^{j+1} \right\rfloor.$$

Receiver generates key K as row reduction of H, revealing only Ker$H$.

n means: $H =$

$$\begin{matrix} \frac{1}{g(a_1)} & \cdots & \frac{1}{g(a_n)} \\ \frac{a_1}{g(a_1)} & \cdots & \frac{a_n}{g(a_n)} \\ \vdots & \ddots & \vdots \\ \frac{a_1^{t-1}}{g(a_1)} & \cdots & \frac{a_n^{t-1}}{g(a_n)} \end{matrix}\right) .$$

ch element of $\mathbf{F}_q$ here
umn in $\mathbf{F}_2^{\lg q}$.
$: \mathbf{F}_2^n \to \mathbf{F}_2^{t \lg q}$.

More useful view: Consider the map $m \mapsto \sum_i m_i/(x - a_i)$ from $\mathbf{F}_2^n$ to $\mathbf{F}_q[x]/g$.

H is the matrix for this map where $\mathbf{F}_2^n$ has standard basis and $\mathbf{F}_q[x]/g$ has basis $\lfloor g/x \rfloor$, $\lfloor g/x^2 \rfloor$, $\ldots$, $\lfloor g/x^t \rfloor$.

One-line proof: In $\mathbf{F}_q[x]$ have

$$\frac{g - g(a_i)}{x - a_i} = \sum_{j \ge 0} a_i^j \left\lfloor g/x^{j+1} \right\rfloor .$$

Receiver generates key K as row reduction of H, revealing only Ker$H$.

Lattice-b

1998 Ho
NTRU (
without

Receiver
$h \in ((\mathbf{Z}$

Cipherte
$m, r \in ($
all coeffi
$\#\{i : r_i$

p: prime
q: powe
with ord
t: rough

$H =$

$$\left. \begin{matrix} \dfrac{1}{g(a_n)} \\ \dfrac{a_n}{g(a_n)} \\ \vdots \\ \dfrac{a_n^{t-1}}{g(a_n)} \end{matrix} \right) .$$

t of $\mathbf{F}_q$ here

q

.

$t \lg q$

2

.

More useful view: Consider the map $m \mapsto \sum_i m_i/(x - a_i)$ from $\mathbf{F}_2^n$ to $\mathbf{F}_q[x]/g$.

H is the matrix for this map where $\mathbf{F}_2^n$ has standard basis and $\mathbf{F}_q[x]/g$ has basis $\lfloor g/x \rfloor$, $\lfloor g/x^2 \rfloor$, …, $\lfloor g/x^t \rfloor$.

One-line proof: In $\mathbf{F}_q[x]$ have

$$\frac{g - g(a_i)}{x - a_i} = \sum_{j \geq 0} a_i^j \left\lfloor g/x^{j+1} \right\rfloor .$$

Receiver generates key K as row reduction of H, revealing only Ker$H$.

Lattice-based encr

1998 Hoffstein–Pi

NTRU (textbook

without required p

Receiver's public k

$h \in ((\mathbf{Z}/q)[x]/(x^p$

Ciphertext: $m + r$

$m, r \in (\mathbf{Z}/q)[x]/($

all coefficients in $\{$

$\#\{i : r_i{=}{-1}\} = \#$

p: prime; e.g., $p =$

q: power of 2 arou

with order $\geq (p -$

t: roughly $0.1p$.

.

re

More useful view: Consider the map $m \mapsto \sum_i m_i/(x-a_i)$ from $\mathbf{F}_2^n$ to $\mathbf{F}_q[x]/g$.

H is the matrix for this map where $\mathbf{F}_2^n$ has standard basis and $\mathbf{F}_q[x]/g$ has basis $\lfloor g/x \rfloor$, $\lfloor g/x^2 \rfloor$, …, $\lfloor g/x^t \rfloor$.

One-line proof: In $\mathbf{F}_q[x]$ have

$$\frac{g-g(a_i)}{x-a_i} = \sum_{j \ge 0} a_i^j \left\lfloor g/x^{j+1} \right\rfloor.$$

Receiver generates key K as row reduction of H, revealing only Ker$H$.

Lattice-based encryption

1998 Hoffstein–Pipher–Silve NTRU (textbook version, without required padding):

Receiver's public key is "ran $h \in ((\mathbf{Z}/q)[x]/(x^p-1))^*$.

Ciphertext: $m + rh$ given $m, r \in (\mathbf{Z}/q)[x]/(x^p-1)$; all coefficients in $\{-1, 0, 1\}$; $\#\{i : r_i{=}{-1}\} = \#\{i : r_i{=}1$

p: prime; e.g., $p = 613$.

q: power of 2 around $8p$, with order $\ge (p-1)/2$ in ($\mathbf{Z}$

t: roughly $0.1p$.

More useful view: Consider the map $m \mapsto \sum_i m_i/(x - a_i)$ from $\mathbf{F}_2^n$ to $\mathbf{F}_q[x]/g$.

H is the matrix for this map where $\mathbf{F}_2^n$ has standard basis and $\mathbf{F}_q[x]/g$ has basis $\lfloor g/x \rfloor$, $\lfloor g/x^2 \rfloor$, . . . , $\lfloor g/x^t \rfloor$.

One-line proof: In $\mathbf{F}_q[x]$ have

$$\frac{g - g(a_i)}{x - a_i} = \sum_{j \ge 0} a_i^j \left\lfloor g/x^{j+1} \right\rfloor.$$

Receiver generates key K as row reduction of H, revealing only Ker$H$.

Lattice-based encryption

1998 Hoffstein–Pipher–Silverman NTRU (textbook version, without required padding):

Receiver's public key is "random" $h \in ((\mathbf{Z}/q)[x]/(x^p - 1))^*$.

Ciphertext: $m + rh$ given $m, r \in (\mathbf{Z}/q)[x]/(x^p - 1)$; all coefficients in $\{-1, 0, 1\}$; $\#\{i : r_i{=}{-1}\} = \#\{i : r_i{=}1\} = t$.

p: prime; e.g., $p = 613$.
q: power of 2 around $8p$, with order $\ge (p-1)/2$ in $(\mathbf{Z}/p)^*$.
t: roughly $0.1p$.

eful view: Consider

$m \mapsto \sum_i m_i/(x-a_i)$

to $\mathbf{F}_q[x]/g$.

matrix for this map

${}^n_2$ has standard basis

$x]/g$ has basis

$g/x^2\rfloor$, …, $\lfloor g/x^t\rfloor$.

proof: In $\mathbf{F}_q[x]$ have

$$\frac{i)}{} = \sum_{j\ge 0} a_i^j \left\lfloor g/x^{j+1}\right\rfloor.$$

generates key K

eduction of H,

g only Ker$H$.

Lattice-based encryption

1998 Hoffstein–Pipher–Silverman NTRU (textbook version, without required padding):

Receiver's public key is "random" $h \in ((\mathbf{Z}/q)[x]/(x^p-1))^*$.

Ciphertext: $m + rh$ given $m, r \in (\mathbf{Z}/q)[x]/(x^p-1)$; all coefficients in $\{-1,0,1\}$; $\#\{i : r_i{=}-1\} = \#\{i : r_i{=}1\} = t$.

p: prime; e.g., $p = 613$.

q: power of 2 around $8p$, with order $\ge(p-1)/2$ in $(\mathbf{Z}/p)^*$.

t: roughly $0.1p$.

Receiver

where f,

all coeffs

$\#\{i : f_i$

$\#\{i : g_i$

both $1+$

Given ci

receiver

$(1+3f)$

in $(\mathbf{Z}/q)$

lifts to $\mathbf{Z}$

coeffs in

reduces

to obtai

Consider

$m_i/(x-a_i)$

$/g$.

r this map

ndard basis

asis

. ., $\lfloor g/x^t \rfloor$.

$\mathbf{F}_q[x]$ have

${}^j_i \left\lfloor g/x^{j+1} \right\rfloor$.

s key K

of H,

H.

Lattice-based encryption

1998 Hoffstein–Pipher–Silverman NTRU (textbook version, without required padding):

Receiver's public key is "random" $h \in ((\mathbf{Z}/q)[x]/(x^p-1))^*$.

Ciphertext: $m + rh$ given
$m, r \in (\mathbf{Z}/q)[x]/(x^p-1)$;
all coefficients in $\{-1, 0, 1\}$;
$\#\{i : r_i{=}{-1}\} = \#\{i : r_i{=}1\} = t$.

p: prime; e.g., $p = 613$.
q: power of 2 around $8p$,
with order $\geq (p-1)/2$ in $(\mathbf{Z}/p)^*$.
t: roughly $0.1p$.

Receiver built $h =$
where $f, g \in (\mathbf{Z}/q$
all coeffs in $\{-1, 0$
$\#\{i : f_i{=}{-1}\} =$
$\#\{i : g_i{=}{-1}\} \approx \#$
both $1+3f$ and g

Given ciphertext c
receiver computes
$(1+3f)c = (1+$
in $(\mathbf{Z}/q)[x]/(x^p -$
lifts to $\mathbf{Z}[x]/(x^p -$
coeffs in $\{-q/2, \ldots$
reduces modulo 3
to obtain m.

$a_i)$

o

s

ve

].

Lattice-based encryption

1998 Hoffstein–Pipher–Silverman
NTRU (textbook version,
without required padding):

Receiver's public key is "random"
$h \in ((\mathbf{Z}/q)[x]/(x^p - 1))^*$.

Ciphertext: $m + rh$ given
$m, r \in (\mathbf{Z}/q)[x]/(x^p - 1)$;
all coefficients in $\{-1, 0, 1\}$;
$\#\{i : r_i{=}{-1}\} = \#\{i : r_i{=}1\} = t$.

p: prime; e.g., $p = 613$.
q: power of 2 around $8p$,
with order $\geq (p - 1)/2$ in $(\mathbf{Z}/p)^*$.
t: roughly $0.1p$.

Receiver built $h = 3g/(1 + 3$
where $f, g \in (\mathbf{Z}/q)[x]/(x^p -$
all coeffs in $\{-1, 0, 1\}$,
$\#\{i : f_i{=}{-1}\} = \#\{i : f_i{=}1$
$\#\{i : g_i{=}{-1}\} \approx \#\{i : g_i{=}1$
both $1 + 3f$ and g invertibl

Given ciphertext $c = m + r$
receiver computes
$(1 + 3f)c = (1 + 3f)m + 3$
in $(\mathbf{Z}/q)[x]/(x^p - 1)$,
lifts to $\mathbf{Z}[x]/(x^p - 1)$ with
coeffs in $\{-q/2, \ldots, q/2 -$
reduces modulo 3
to obtain m.

Lattice-based encryption

1998 Hoffstein–Pipher–Silverman NTRU (textbook version, without required padding):

Receiver's public key is "random" $h \in ((\mathbf{Z}/q)[x]/(x^p - 1))^*$.

Ciphertext: $m + rh$ given
$m, r \in (\mathbf{Z}/q)[x]/(x^p - 1)$;
all coefficients in $\{-1, 0, 1\}$;
$\#\{i : r_i{=}{-1}\} = \#\{i : r_i{=}1\} = t$.

p: prime; e.g., $p = 613$.
q: power of 2 around $8p$,
with order $\geq (p-1)/2$ in $(\mathbf{Z}/p)^*$.
t: roughly $0.1p$.

Receiver built $h = 3g/(1 + 3f)$
where $f, g \in (\mathbf{Z}/q)[x]/(x^p - 1)$,
all coeffs in $\{-1, 0, 1\}$,
$\#\{i : f_i{=}{-1}\} = \#\{i : f_i{=}1\} = t$,
$\#\{i : g_i{=}{-1}\} \approx \#\{i : g_i{=}1\} \approx \frac{p}{3}$,
both $1 + 3f$ and g invertible.

Given ciphertext $c = m + rh$,
receiver computes
$(1 + 3f)c = (1 + 3f)m + 3rg$
in $(\mathbf{Z}/q)[x]/(x^p - 1)$,
lifts to $\mathbf{Z}[x]/(x^p - 1)$ with
coeffs in $\{-q/2, \ldots, q/2 - 1\}$,
reduces modulo 3
to obtain m.

based encryption

offstein–Pipher–Silverman
textbook version,
required padding):

's public key is "random"
$/q)[x]/(x^p - 1))^*$.

ext: $m + rh$ given
$\mathbf{Z}/q)[x]/(x^p - 1)$;
icients in $\{-1, 0, 1\}$;
$=-1\} = \#\{i : r_i=1\} = t$.

e; e.g., $p = 613$.
r of 2 around $8p$,
er $\ge (p - 1)/2$ in $(\mathbf{Z}/p)^*$.
ly $0.1p$.

Receiver built $h = 3g/(1 + 3f)$
where $f, g \in (\mathbf{Z}/q)[x]/(x^p - 1)$,
all coeffs in $\{-1, 0, 1\}$,
$\#\{i : f_i{=}-1\} = \#\{i : f_i{=}1\} = t$,
$\#\{i : g_i{=}-1\} \approx \#\{i : g_i{=}1\} \approx \frac{p}{3}$,
both $1 + 3f$ and g invertible.

Given ciphertext $c = m + rh$,
receiver computes
$(1 + 3f)c = (1 + 3f)m + 3rg$
in $(\mathbf{Z}/q)[x]/(x^p - 1)$,
lifts to $\mathbf{Z}[x]/(x^p - 1)$ with
coeffs in $\{-q/2, \ldots, q/2 - 1\}$,
reduces modulo 3
to obtain m.

Basic at
Lift pair
to obtai

Attackin
$(1 + 3f,$
in this la

Attackin
$(0, c)$ is
lattice v

Standar
(SVP, C
Nothing
even pos

ryption

pher–Silverman
version,
padding):

key is “random”
$^p - 1))^*$.

rh given
$x^p - 1)$;
$\{-1, 0, 1\}$;
$\#\{i : r_i{=}1\} = t$.

$= 613$.
und $8p$,
$1)/2$ in $(\mathbf{Z}/p)^*$.

Receiver built $h = 3g/(1 + 3f)$
where $f, g \in (\mathbf{Z}/q)[x]/(x^p - 1)$,
all coeffs in $\{-1, 0, 1\}$,
$\#\{i : f_i{=}-1\} = \#\{i : f_i{=}1\} = t$,
$\#\{i : g_i{=}-1\} \approx \#\{i : g_i{=}1\} \approx \frac{p}{3}$,
both $1 + 3f$ and g invertible.

Given ciphertext $c = m + rh$,
receiver computes
$(1 + 3f)c = (1 + 3f)m + 3rg$
in $(\mathbf{Z}/q)[x]/(x^p - 1)$,
lifts to $\mathbf{Z}[x]/(x^p - 1)$ with
coeffs in $\{-q/2, \ldots, q/2 - 1\}$,
reduces modulo 3
to obtain m.

Basic attack tool:
Lift pairs (u, uh)
to obtain a lattice

Attacking key h:
$(1 + 3f, 3g)$ is a s
in this lattice.

Attacking ciphert
$(0, c)$ is close to
lattice vector $(r, r$

Standard lattice al
(SVP, CVP) cost
Nothing subexpon
even post-quantur

rman

dom”

$\} = t$.

$/p)^*$.

Receiver built $h = 3g/(1+3f)$
where $f, g \in (\mathbf{Z}/q)[x]/(x^p - 1)$,
all coeffs in $\{-1, 0, 1\}$,
$\#\{i : f_i{=}{-1}\} = \#\{i : f_i{=}1\} = t$,
$\#\{i : g_i{=}{-1}\} \approx \#\{i : g_i{=}1\} \approx \frac{p}{3}$,
both $1+3f$ and g invertible.

Given ciphertext $c = m + rh$,
receiver computes
$(1+3f)c = (1+3f)m + 3rg$
in $(\mathbf{Z}/q)[x]/(x^p - 1)$,
lifts to $\mathbf{Z}[x]/(x^p - 1)$ with
coeffs in $\{-q/2, \ldots, q/2 - 1\}$,
reduces modulo 3
to obtain m.

Basic attack tool:
Lift pairs (u, uh) to $\mathbf{Z}^{2p}$
to obtain a lattice.

Attacking key h:
$(1+3f, 3g)$ is a short vecto
in this lattice.

Attacking ciphertext c:
$(0, c)$ is close to
lattice vector (r, rh).

Standard lattice algorithms
(SVP, CVP) cost $2^{\Theta(p)}$.
Nothing subexponential kno
even post-quantum.

Receiver built $h = 3g/(1+3f)$
where $f, g \in (\mathbf{Z}/q)[x]/(x^p - 1)$,
all coeffs in $\{-1, 0, 1\}$,
$\#\{i : f_i{=}{-1}\} = \#\{i : f_i{=}1\} = t$,
$\#\{i : g_i{=}{-1}\} \approx \#\{i : g_i{=}1\} \approx \frac{p}{3}$,
both $1+3f$ and g invertible.

Given ciphertext $c = m + rh$,
receiver computes
$(1+3f)c = (1+3f)m + 3rg$
in $(\mathbf{Z}/q)[x]/(x^p - 1)$,
lifts to $\mathbf{Z}[x]/(x^p - 1)$ with
coeffs in $\{-q/2, \ldots, q/2 - 1\}$,
reduces modulo 3
to obtain m.

Basic attack tool:
Lift pairs (u, uh) to $\mathbf{Z}^{2p}$
to obtain a lattice.

Attacking key h:
$(1+3f, 3g)$ is a short vector
in this lattice.

Attacking ciphertext c:
$(0, c)$ is close to
lattice vector (r, rh).

Standard lattice algorithms
(SVP, CVP) cost $2^{\Theta(p)}$.
Nothing subexponential known,
even post-quantum.

built $h = 3g/(1+3f)$
$, g \in (\mathbf{Z}/q)[x]/(x^p - 1)$,
s in $\{-1, 0, 1\}$,
$=-1\} = \#\{i : f_i{=}1\} = t$,
$=-1\} \approx \#\{i : g_i{=}1\} \approx \frac{p}{3}$,
$3f$ and g invertible.

phertext $c = m + rh$,
computes
$c = (1+3f)m + 3rg$
$[x]/(x^p - 1)$,
$\mathbf{Z}[x]/(x^p - 1)$ with
$\{-q/2, \ldots, q/2 - 1\}$,
modulo 3
n m.

Basic attack tool:
Lift pairs (u, uh) to $\mathbf{Z}^{2p}$
to obtain a lattice.

Attacking key h:
$(1+3f, 3g)$ is a short vector
in this lattice.

Attacking ciphertext c:
$(0, c)$ is close to
lattice vector (r, rh).

Standard lattice algorithms
(SVP, CVP) cost $2^{\Theta(p)}$.
Nothing subexponential known,
even post-quantum.

Take p
against a

$\Theta(b \lg b)$

Time $b($
to multi
$(\mathbf{Z}/q)[x]$

Time $b($
for encry

Excellen

$3g/(1+3f)$
$)[x]/(x^p-1)$,
$0, 1\}$,
$\#\{i : f_i{=}1\} = t$,
$\{i : g_i{=}1\} \approx \frac{p}{3}$,
invertible.

$= m + rh$,

$3f)m + 3rg$
$1)$,
$1)$ with
$\ldots, q/2 - 1\}$,

Basic attack tool:
Lift pairs (u, uh) to $\mathbf{Z}^{2p}$
to obtain a lattice.

Attacking key h:
$(1 + 3f, 3g)$ is a short vector
in this lattice.

Attacking ciphertext c:
$(0, c)$ is close to
lattice vector (r, rh).

Standard lattice algorithms
(SVP, CVP) cost $2^{\Theta(p)}$.
Nothing subexponential known,
even post-quantum.

Take $p \in \Theta(b)$ for
against all known

$\Theta(b \lg b)$ bits in ke

Time $b(\lg b)^{2+o(1)}$
to multiply in
$(\mathbf{Z}/q)[x]/(x^p - 1)$

Time $b(\lg b)^{2+o(1)}$
for encryption, dec

Excellent overall p

$3f)$

$1)$,

$1\} = t$,

$\} \approx \frac{p}{3}$,

e.

h,

rg

$1\}$,

Basic attack tool:
Lift pairs (u, uh) to $\mathbf{Z}^{2p}$
to obtain a lattice.

Attacking key h:
$(1 + 3f, 3g)$ is a short vector
in this lattice.

Attacking ciphertext c:
$(0, c)$ is close to
lattice vector (r, rh).

Standard lattice algorithms
(SVP, CVP) cost $2^{\Theta(p)}$.
Nothing subexponential known,
even post-quantum.

Take $p \in \Theta(b)$ for security 2
against all known attacks.

$\Theta(b \lg b)$ bits in key.

Time $b(\lg b)^{2+o(1)}$
to multiply in
$(\mathbf{Z}/q)[x]/(x^p - 1)$.

Time $b(\lg b)^{2+o(1)}$
for encryption, decryption.

Excellent overall performanc

Basic attack tool:
Lift pairs (u, uh) to $\mathbf{Z}^{2p}$
to obtain a lattice.

Attacking key h:
$(1 + 3f, 3g)$ is a short vector
in this lattice.

Attacking ciphertext c:
$(0, c)$ is close to
lattice vector (r, rh).

Standard lattice algorithms
(SVP, CVP) cost $2^{\Theta(p)}$.
Nothing subexponential known,
even post-quantum.

Take $p \in \Theta(b)$ for security 2^b
against all known attacks.

$\Theta(b \lg b)$ bits in key.

Time $b(\lg b)^{2+o(1)}$
to multiply in
$(\mathbf{Z}/q)[x]/(x^p - 1)$.

Time $b(\lg b)^{2+o(1)}$
for encryption, decryption.

Excellent overall performance.

Basic attack tool:
Lift pairs (u, uh) to $\mathbf{Z}^{2p}$
to obtain a lattice.

Attacking key h:
$(1 + 3f, 3g)$ is a short vector
in this lattice.

Attacking ciphertext c:
$(0, c)$ is close to
lattice vector (r, rh).

Standard lattice algorithms
(SVP, CVP) cost $2^{\Theta(p)}$.
Nothing subexponential known,
even post-quantum.

Take $p \in \Theta(b)$ for security 2^b
against all known attacks.

$\Theta(b \lg b)$ bits in key.

Time $b(\lg b)^{2+o(1)}$
to multiply in
$(\mathbf{Z}/q)[x]/(x^p - 1)$.

Time $b(\lg b)^{2+o(1)}$
for encryption, decryption.

Excellent overall performance.

The McEliece cryptosystem
inspires more confidence
but has much larger keys.

tack tool:
s (u, uh) to $\mathbf{Z}^{2p}$
n a lattice.

g key h:
$3g)$ is a short vector
attice.

g ciphertext c:
close to
ector (r, rh).

d lattice algorithms
VP) cost $2^{\Theta(p)}$.
subexponential known,
st-quantum.

Take $p \in \Theta(b)$ for security 2^b
against all known attacks.

$\Theta(b \lg b)$ bits in key.

Time $b(\lg b)^{2+o(1)}$
to multiply in
$(\mathbf{Z}/q)[x]/(x^p - 1)$.

Time $b(\lg b)^{2+o(1)}$
for encryption, decryption.

Excellent overall performance.

The McEliece cryptosystem
inspires more confidence
but has much larger keys.

Somethi

1985 H.
$A(\overline{k})$ has
of additi
Symmet

"The pr
To deter
complete
requires
already i
of an ell
in Weier

to $\mathbf{Z}^{2p}$

.

hort vector

ext c:

h).

lgorithms

$2^{\Theta(p)}$.

ential known,

n.

Take $p \in \Theta(b)$ for security 2^b against all known attacks.

$\Theta(b \lg b)$ bits in key.

Time $b(\lg b)^{2+o(1)}$ to multiply in $(\mathbf{Z}/q)[x]/(x^p - 1)$.

Time $b(\lg b)^{2+o(1)}$ for encryption, decryption.

Excellent overall performance.

The McEliece cryptosystem inspires more confidence but has much larger keys.

Something comple

1985 H. Lange–Ru

$A(\bar{k})$ has a comple

of addition laws, d

Symmetry ⇒ degr

“The proof is non

To determine expl

complete system o

requires tedious co

already in the easi

of an elliptic curve

in Weierstrass nor

r

wn,

Take $p \in \Theta(b)$ for security 2^b against all known attacks.

$\Theta(b \lg b)$ bits in key.

Time $b(\lg b)^{2+o(1)}$ to multiply in $(\mathbf{Z}/q)[x]/(x^p - 1)$.

Time $b(\lg b)^{2+o(1)}$ for encryption, decryption.

Excellent overall performance.

The McEliece cryptosystem inspires more confidence but has much larger keys.

Something completely differe

1985 H. Lange–Ruppert:
$A(\bar{k})$ has a complete system
of addition laws, degree $\leq$ (
Symmetry $\Rightarrow$ degree $\leq (2, 2$

"The proof is nonconstructi
To determine explicitly a
complete system of addition
requires tedious computatio
already in the easiest case
of an elliptic curve
in Weierstrass normal form."

Take $p \in \Theta(b)$ for security 2^b against all known attacks.

$\Theta(b \lg b)$ bits in key.

Time $b(\lg b)^{2+o(1)}$ to multiply in $(\mathbf{Z}/q)[x]/(x^p - 1)$.

Time $b(\lg b)^{2+o(1)}$ for encryption, decryption.

Excellent overall performance.

The McEliece cryptosystem inspires more confidence but has much larger keys.

Something completely different

1985 H. Lange–Ruppert:
$A(\bar{k})$ has a complete system of addition laws, degree $\leq (3,3)$.
Symmetry $\Rightarrow$ degree $\leq (2,2)$.

“The proof is nonconstructive. . . To determine explicitly a complete system of addition laws requires tedious computations already in the easiest case of an elliptic curve in Weierstrass normal form.”

$\in \Theta(b)$ for security 2^b
all known attacks.

bits in key.

lg $b)^{2+o(1)}$
ply in
$]/(x^p - 1)$.

lg $b)^{2+o(1)}$
yption, decryption.

t overall performance.

Eliece cryptosystem
more confidence
much larger keys.

Something completely different

1985 H. Lange–Ruppert:
$A(\bar{k})$ has a complete system
of addition laws, degree $\le (3,3)$.
Symmetry $\Rightarrow$ degree $\le (2,2)$.

“The proof is nonconstructive. . .
To determine explicitly a
complete system of addition laws
requires tedious computations
already in the easiest case
of an elliptic curve
in Weierstrass normal form.”

1985 La
Explicit
of 3 add
for short

Reduce
by introd
$x_i y_j + x$

1987 La
Explicit
of 3 add
for long

security 2^b
attacks.

ey.

.

cryption.

erformance.

otosystem
idence
er keys.

Something completely different

1985 H. Lange–Ruppert:
$A(\bar{k})$ has a complete system
of addition laws, degree $\leq (3,3)$.
Symmetry $\Rightarrow$ degree $\leq (2,2)$.

“The proof is nonconstructive. . .
To determine explicitly a
complete system of addition laws
requires tedious computations
already in the easiest case
of an elliptic curve
in Weierstrass normal form.”

1985 Lange–Rupp
Explicit complete s
of 3 addition laws
for short Weierstra

Reduce formulas t
by introducing ext
$x_i y_j + x_j y_i$, $x_i y_j$

1987 Lange–Rupp
Explicit complete s
of 3 addition laws
for long Weierstras

^{b}

e.

Something completely different

1985 H. Lange–Ruppert:
$A(\bar{k})$ has a complete system
of addition laws, degree $\le (3,3)$.
Symmetry $\Rightarrow$ degree $\le (2,2)$.

"The proof is nonconstructive. . .
To determine explicitly a
complete system of addition laws
requires tedious computations
already in the easiest case
of an elliptic curve
in Weierstrass normal form."

1985 Lange–Ruppert:
Explicit complete system
of 3 addition laws
for short Weierstrass curves.

Reduce formulas to 53 mono
by introducing extra variable
$\boldsymbol{x_i y_j + x_j y_i}$, $\boldsymbol{x_i y_j - x_j y_i}$.

1987 Lange–Ruppert:
Explicit complete system
of 3 addition laws
for long Weierstrass curves.

Something completely different

1985 H. Lange–Ruppert:
$A(\bar{k})$ has a complete system
of addition laws, degree $\le (3,3)$.
Symmetry $\Rightarrow$ degree $\le (2,2)$.

"The proof is nonconstructive…
To determine explicitly a
complete system of addition laws
requires tedious computations
already in the easiest case
of an elliptic curve
in Weierstrass normal form."

1985 Lange–Ruppert:
Explicit complete system
of 3 addition laws
for short Weierstrass curves.

Reduce formulas to 53 monomials
by introducing extra variables
$x_iy_j + x_jy_i$, $x_iy_j - x_jy_i$.

1987 Lange–Ruppert:
Explicit complete system
of 3 addition laws
for long Weierstrass curves.

ng completely different

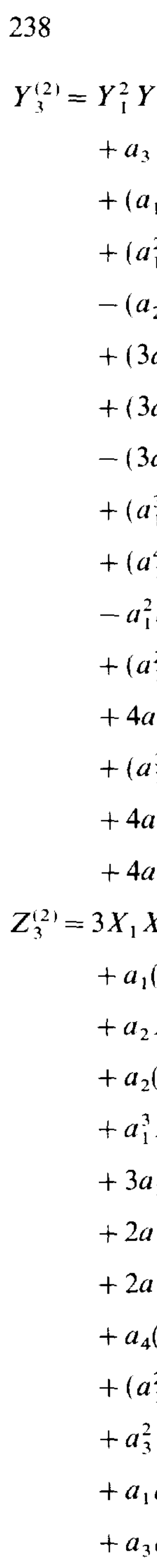
Lange–Ruppert:
s a complete system
on laws, degree $\leq (3, 3)$.
ry $\Rightarrow$ degree $\leq (2, 2)$.

oof is nonconstructive. . .
rmine explicitly a
e system of addition laws
tedious computations
in the easiest case
iptic curve
rstrass normal form.”

1985 Lange–Ruppert:
Explicit complete system
of 3 addition laws
for short Weierstrass curves.

Reduce formulas to 53 monomials
by introducing extra variables
$x_i y_j + x_j y_i$, $x_i y_j - x_j y_i$.

1987 Lange–Ruppert:
Explicit complete system
of 3 addition laws
for long Weierstrass curves.



<u>etely different</u>

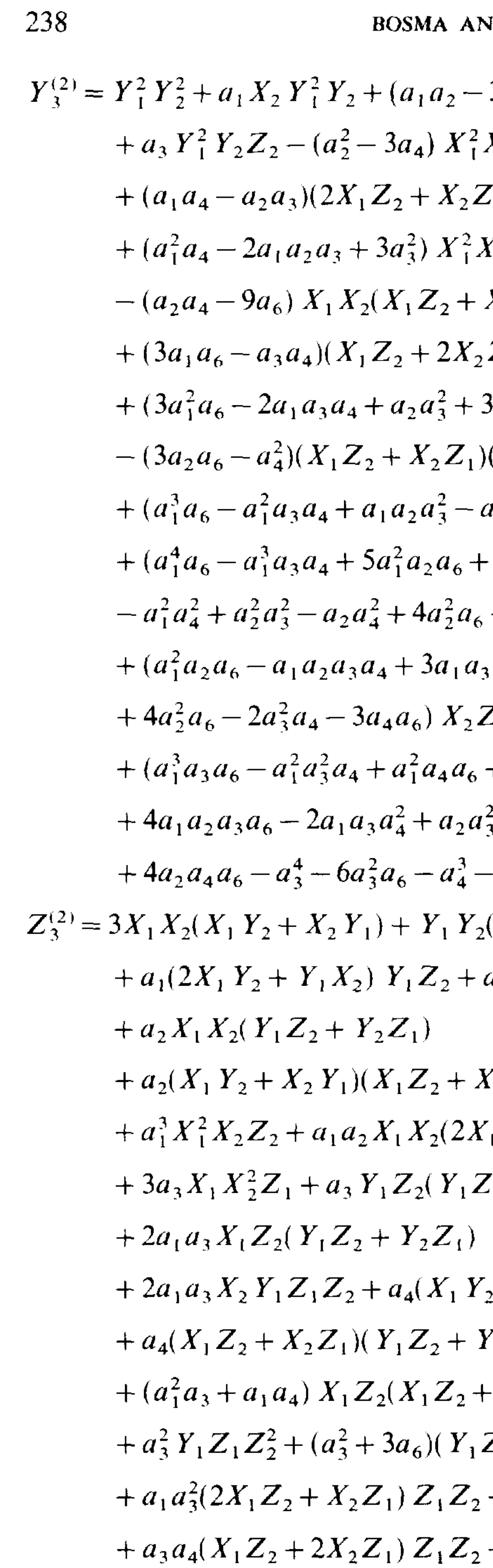
uppert:
ete system
legree $\leq (3,3)$.
ree $\leq (2,2)$.

constructive. . .
icitly a
of addition laws
omputations
est case
e
mal form.”

1985 Lange–Ruppert:
Explicit complete system
of 3 addition laws
for short Weierstrass curves.

Reduce formulas to 53 monomials
by introducing extra variables
$x_iy_j + x_jy_i$, $x_iy_j - x_jy_i$.

1987 Lange–Ruppert:
Explicit complete system
of 3 addition laws
for long Weierstrass curves.



238 BOSMA AN

$$
\begin{aligned}
Y_3^{(2)} = {} & Y_1^2 Y_2^2 + a_1 X_2 Y_1^2 Y_2 + (a_1 a_2 - \\
& + a_3 Y_1^2 Y_2 Z_2 - (a_2^2 - 3a_4)\, X_1^2 \\
& + (a_1 a_4 - a_2 a_3)(2X_1 Z_2 + X_2 Z \\
& + (a_1^2 a_4 - 2a_1 a_2 a_3 + 3a_3^2)\, X_1^2 \\
& - (a_2 a_4 - 9a_6)\, X_1 X_2 (X_1 Z_2 + \\
& + (3a_1 a_6 - a_3 a_4)(X_1 Z_2 + 2X_2 \\
& + (3a_1^2 a_6 - 2a_1 a_3 a_4 + a_2 a_3^2 + 3 \\
& - (3a_2 a_6 - a_4^2)(X_1 Z_2 + X_2 Z_1)(\\
& + (a_1^3 a_6 - a_1^2 a_3 a_4 + a_1 a_2 a_3^2 - \\
& + (a_1^4 a_6 - a_1^3 a_3 a_4 + 5a_1^2 a_2 a_6 + \\
& - a_1^2 a_4^2 + a_2^2 a_3^2 - a_2 a_4^2 + 4a_2^2 a_6 \\
& + (a_1^2 a_2 a_6 - a_1 a_2 a_3 a_4 + 3a_1 a_3 \\
& + 4a_2^2 a_6 - 2a_3^2 a_4 - 3a_4 a_6)\, X_2 Z \\
& + (a_1^3 a_3 a_6 - a_1^2 a_3^2 a_4 + a_1^2 a_4 a_6 \\
& + 4a_1 a_2 a_3 a_6 - 2a_1 a_3 a_4^2 + a_2 a_3^2 \\
& + 4a_2 a_4 a_6 - a_3^4 - 6a_3^2 a_6 - a_4^3 - \\
Z_3^{(2)} = {} & 3X_1 X_2 (X_1 Y_2 + X_2 Y_1) + Y_1 Y_2 (\\
& + a_1 (2X_1 Y_2 + Y_1 X_2)\, Y_1 Z_2 + \\
& + a_2 X_1 X_2 (Y_1 Z_2 + Y_2 Z_1) \\
& + a_2 (X_1 Y_2 + X_2 Y_1)(X_1 Z_2 + X \\
& + a_1^3 X_1^2 X_2 Z_2 + a_1 a_2 X_1 X_2 (2X \\
& + 3a_3 X_1 X_2^2 Z_1 + a_3 Y_1 Z_2 (Y_1 Z \\
& + 2a_1 a_3 X_1 Z_2 (Y_1 Z_2 + Y_2 Z_1) \\
& + 2a_1 a_3 X_2 Y_1 Z_1 Z_2 + a_4 (X_1 Y \\
& + a_4 (X_1 Z_2 + X_2 Z_1)(Y_1 Z_2 + Y \\
& + (a_1^2 a_3 + a_1 a_4)\, X_1 Z_2 (X_1 Z_2 + \\
& + a_3^2 Y_1 Z_1 Z_2^2 + (a_3^2 + 3a_6)(Y_1 Z \\
& + a_1 a_3^2 (2X_1 Z_2 + X_2 Z_1)\, Z_1 Z_2 \\
& + a_3 a_4 (X_1 Z_2 + 2X_2 Z_1)\, Z_1 Z_2
\end{aligned}
$$

<u>ent</u>

3, 3).

).

ve. . .

laws

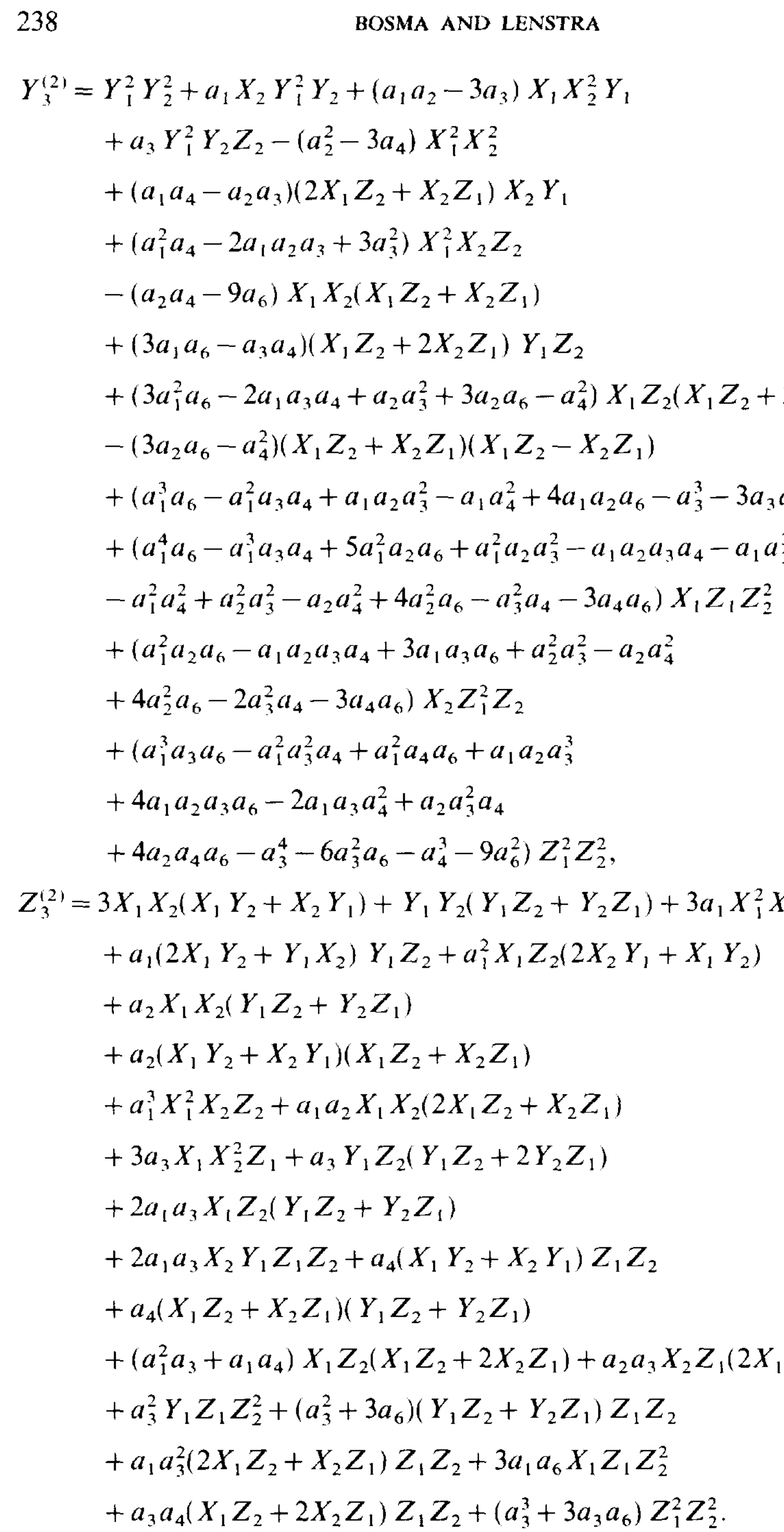
ns

,

1985 Lange–Ruppert:
Explicit complete system
of 3 addition laws
for short Weierstrass curves.

Reduce formulas to 53 monomials
by introducing extra variables
$x_iy_j + x_jy_i$, $x_iy_j - x_jy_i$.

1987 Lange–Ruppert:
Explicit complete system
of 3 addition laws
for long Weierstrass curves.



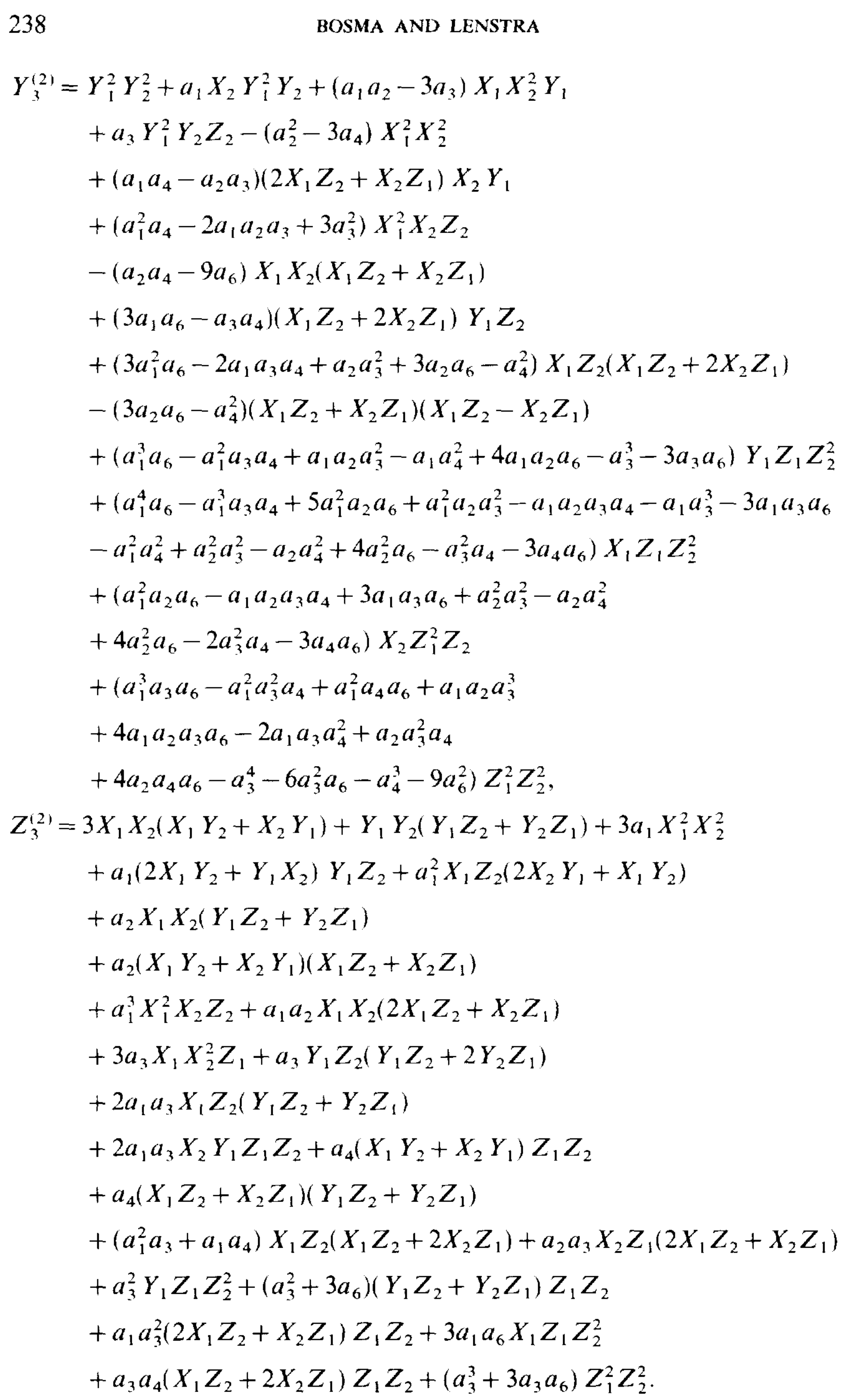
238 BOSMA AND LENSTRA

$$
\begin{aligned}
Y_3^{(2)} = {} & Y_1^2Y_2^2 + a_1X_2Y_1^2Y_2 + (a_1a_2 - 3a_3)\,X_1X_2^2Y_1 \\
& + a_3Y_1^2Y_2Z_2 - (a_2^2 - 3a_4)\,X_1^2X_2^2 \\
& + (a_1a_4 - a_2a_3)(2X_1Z_2 + X_2Z_1)\,X_2Y_1 \\
& + (a_1^2a_4 - 2a_1a_2a_3 + 3a_3^2)\,X_1^2X_2Z_2 \\
& - (a_2a_4 - 9a_6)\,X_1X_2(X_1Z_2 + X_2Z_1) \\
& + (3a_1a_6 - a_3a_4)(X_1Z_2 + 2X_2Z_1)\,Y_1Z_2 \\
& + (3a_1^2a_6 - 2a_1a_3a_4 + a_2a_3^2 + 3a_2a_6 - a_4^2)\,X_1Z_2(X_1Z_2 + \\
& - (3a_2a_6 - a_4^2)(X_1Z_2 + X_2Z_1)(X_1Z_2 - X_2Z_1) \\
& + (a_1^3a_6 - a_1^2a_3a_4 + a_1a_2a_3^2 - a_1a_4^2 + 4a_1a_2a_6 - a_3^3 - 3a_3 \\
& + (a_1^4a_6 - a_1^3a_3a_4 + 5a_1^2a_2a_6 + a_1^2a_2a_3^2 - a_1a_2a_3a_4 - a_1a \\
& - a_1^2a_4^2 + a_2^2a_3^2 - a_2a_4^2 + 4a_2^2a_6 - a_3^2a_4 - 3a_4a_6)\,X_1Z_1Z_2^2 \\
& + (a_1^2a_2a_6 - a_1a_2a_3a_4 + 3a_1a_3a_6 + a_2^2a_3^2 - a_2a_4^2 \\
& + 4a_2^2a_6 - 2a_3^2a_4 - 3a_4a_6)\,X_2Z_1^2Z_2 \\
& + (a_1^3a_3a_6 - a_1^2a_3^2a_4 + a_1^2a_4a_6 + a_1a_2a_3^3 \\
& + 4a_1a_2a_3a_6 - 2a_1a_3a_4^2 + a_2a_3^2a_4 \\
& + 4a_2a_4a_6 - a_3^4 - 6a_3^2a_6 - a_4^3 - 9a_6^2)\,Z_1^2Z_2^2, \\
Z_3^{(2)} = {} & 3X_1X_2(X_1Y_2 + X_2Y_1) + Y_1Y_2(Y_1Z_2 + Y_2Z_1) + 3a_1X_1^2X \\
& + a_1(2X_1Y_2 + Y_1X_2)\,Y_1Z_2 + a_1^2X_1Z_2(2X_2Y_1 + X_1Y_2) \\
& + a_2X_1X_2(Y_1Z_2 + Y_2Z_1) \\
& + a_2(X_1Y_2 + X_2Y_1)(X_1Z_2 + X_2Z_1) \\
& + a_1^3X_1^2X_2Z_2 + a_1a_2X_1X_2(2X_1Z_2 + X_2Z_1) \\
& + 3a_3X_1X_2^2Z_1 + a_3Y_1Z_2(Y_1Z_2 + 2Y_2Z_1) \\
& + 2a_1a_3X_1Z_2(Y_1Z_2 + Y_2Z_1) \\
& + 2a_1a_3X_2Y_1Z_1Z_2 + a_4(X_1Y_2 + X_2Y_1)\,Z_1Z_2 \\
& + a_4(X_1Z_2 + X_2Z_1)(Y_1Z_2 + Y_2Z_1) \\
& + (a_1^2a_3 + a_1a_4)\,X_1Z_2(X_1Z_2 + 2X_2Z_1) + a_2a_3X_2Z_1(2X_1 \\
& + a_3^2Y_1Z_1Z_2^2 + (a_3^2 + 3a_6)(Y_1Z_2 + Y_2Z_1)\,Z_1Z_2 \\
& + a_1a_3^2(2X_1Z_2 + X_2Z_1)\,Z_1Z_2 + 3a_1a_6X_1Z_1Z_2^2 \\
& + a_3a_4(X_1Z_2 + 2X_2Z_1)\,Z_1Z_2 + (a_3^3 + 3a_3a_6)\,Z_1^2Z_2^2.
\end{aligned}
$$

1985 Lange–Ruppert:
Explicit complete system
of 3 addition laws
for short Weierstrass curves.

Reduce formulas to 53 monomials
by introducing extra variables
$x_i y_j + x_j y_i$, $x_i y_j - x_j y_i$.

1987 Lange–Ruppert:
Explicit complete system
of 3 addition laws
for long Weierstrass curves.



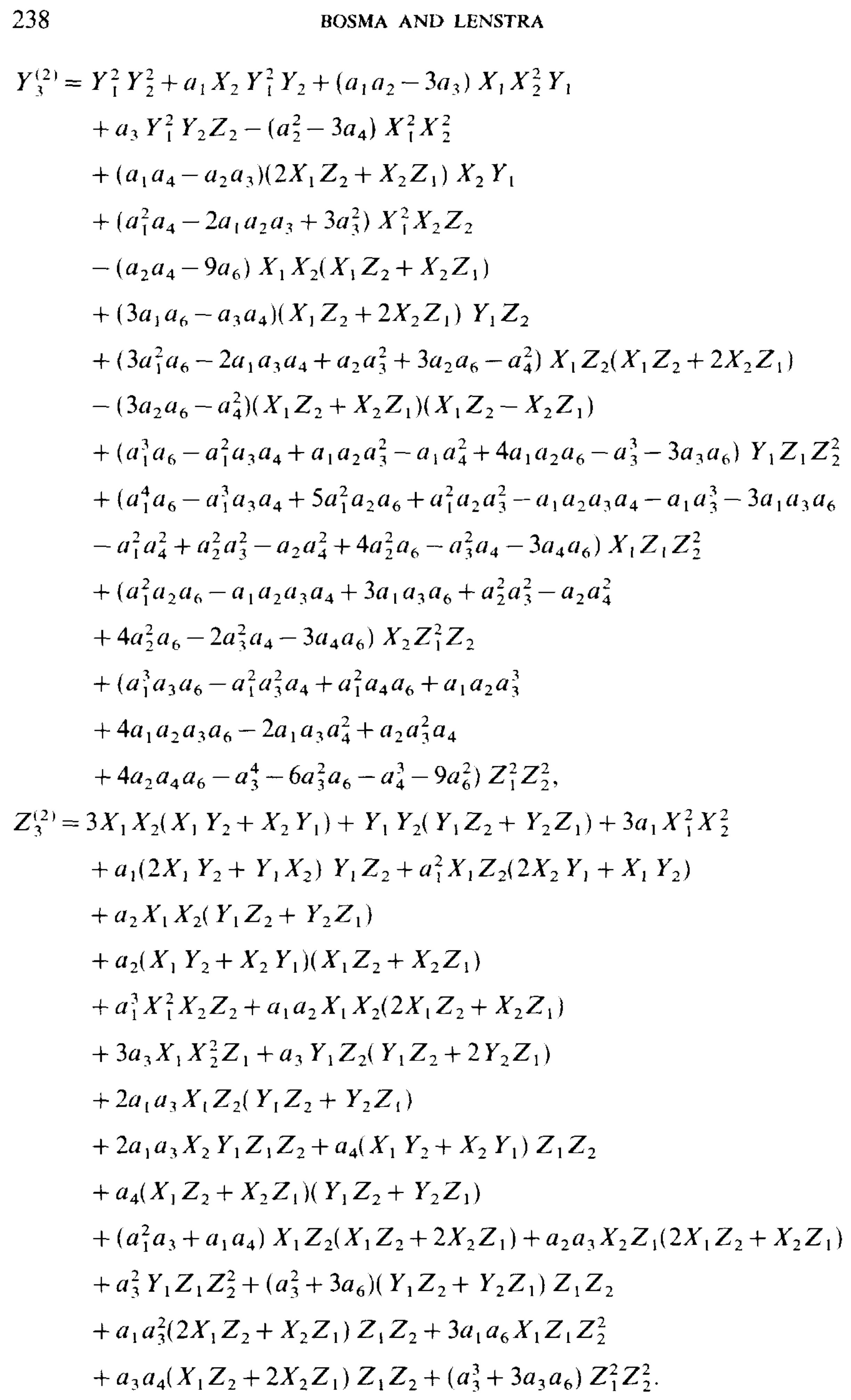
238 BOSMA AND LENSTRA

$$
\begin{aligned}
Y_3^{(2)} = {} & Y_1^2 Y_2^2 + a_1 X_2 Y_1^2 Y_2 + (a_1 a_2 - 3a_3)\, X_1 X_2^2 Y_1 \\
& + a_3 Y_1^2 Y_2 Z_2 - (a_2^2 - 3a_4)\, X_1^2 X_2^2 \\
& + (a_1 a_4 - a_2 a_3)(2X_1 Z_2 + X_2 Z_1)\, X_2 Y_1 \\
& + (a_1^2 a_4 - 2a_1 a_2 a_3 + 3a_3^2)\, X_1^2 X_2 Z_2 \\
& - (a_2 a_4 - 9a_6)\, X_1 X_2 (X_1 Z_2 + X_2 Z_1) \\
& + (3a_1 a_6 - a_3 a_4)(X_1 Z_2 + 2X_2 Z_1)\, Y_1 Z_2 \\
& + (3a_1^2 a_6 - 2a_1 a_3 a_4 + a_2 a_3^2 + 3a_2 a_6 - a_4^2)\, X_1 Z_2 (X_1 Z_2 + 2X_2 Z_1) \\
& - (3a_2 a_6 - a_4^2)(X_1 Z_2 + X_2 Z_1)(X_1 Z_2 - X_2 Z_1) \\
& + (a_1^3 a_6 - a_1^2 a_3 a_4 + a_1 a_2 a_3^2 - a_1 a_4^2 + 4a_1 a_2 a_6 - a_3^3 - 3a_3 a_6)\, Y_1 Z_1 Z_2^2 \\
& + (a_1^4 a_6 - a_1^3 a_3 a_4 + 5a_1^2 a_2 a_6 + a_1^2 a_2 a_3^2 - a_1 a_2 a_3 a_4 - a_1 a_3^3 - 3a_1 a_3 a_6 \\
& - a_1^2 a_4^2 + a_2^2 a_3^2 - a_2 a_4^2 + 4a_2^2 a_6 - a_3^2 a_4 - 3a_4 a_6)\, X_1 Z_1 Z_2^2 \\
& + (a_1^2 a_2 a_6 - a_1 a_2 a_3 a_4 + 3a_1 a_3 a_6 + a_2^2 a_3^2 - a_2 a_4^2 \\
& + 4a_2^2 a_6 - 2a_3^2 a_4 - 3a_4 a_6)\, X_2 Z_1^2 Z_2 \\
& + (a_1^3 a_3 a_6 - a_1^2 a_3^2 a_4 + a_1^2 a_4 a_6 + a_1 a_2 a_3^3 \\
& + 4a_1 a_2 a_3 a_6 - 2a_1 a_3 a_4^2 + a_2 a_3^2 a_4 \\
& + 4a_2 a_4 a_6 - a_3^4 - 6a_3^2 a_6 - a_4^3 - 9a_6^2)\, Z_1^2 Z_2^2, \\
Z_3^{(2)} = {} & 3X_1 X_2 (X_1 Y_2 + X_2 Y_1) + Y_1 Y_2 (Y_1 Z_2 + Y_2 Z_1) + 3a_1 X_1^2 X_2^2 \\
& + a_1 (2X_1 Y_2 + Y_1 X_2)\, Y_1 Z_2 + a_1^2 X_1 Z_2 (2X_2 Y_1 + X_1 Y_2) \\
& + a_2 X_1 X_2 (Y_1 Z_2 + Y_2 Z_1) \\
& + a_2 (X_1 Y_2 + X_2 Y_1)(X_1 Z_2 + X_2 Z_1) \\
& + a_1^3 X_1^2 X_2 Z_2 + a_1 a_2 X_1 X_2 (2X_1 Z_2 + X_2 Z_1) \\
& + 3a_3 X_1 X_2^2 Z_1 + a_3 Y_1 Z_2 (Y_1 Z_2 + 2Y_2 Z_1) \\
& + 2a_1 a_3 X_1 Z_2 (Y_1 Z_2 + Y_2 Z_1) \\
& + 2a_1 a_3 X_2 Y_1 Z_1 Z_2 + a_4 (X_1 Y_2 + X_2 Y_1)\, Z_1 Z_2 \\
& + a_4 (X_1 Z_2 + X_2 Z_1)(Y_1 Z_2 + Y_2 Z_1) \\
& + (a_1^2 a_3 + a_1 a_4)\, X_1 Z_2 (X_1 Z_2 + 2X_2 Z_1) + a_2 a_3 X_2 Z_1 (2X_1 Z_2 + X_2 Z_1) \\
& + a_3^2 Y_1 Z_1 Z_2^2 + (a_3^2 + 3a_6)(Y_1 Z_2 + Y_2 Z_1)\, Z_1 Z_2 \\
& + a_1 a_3^2 (2X_1 Z_2 + X_2 Z_1)\, Z_1 Z_2 + 3a_1 a_6 X_1 Z_1 Z_2^2 \\
& + a_3 a_4 (X_1 Z_2 + 2X_2 Z_1)\, Z_1 Z_2 + (a_3^3 + 3a_3 a_6)\, Z_1^2 Z_2^2.
\end{aligned}
$$

nge–Ruppert:
complete system
ition laws
: Weierstrass curves.

formulas to 53 monomials
ducing extra variables
$_jy_i$, $x_iy_j - x_jy_i$.

nge–Ruppert:
complete system
ition laws
Weierstrass curves.



238 BOSMA AND LENSTRA

$$
\begin{aligned}
Y_3^{(2)} = {} & Y_1^2Y_2^2 + a_1X_2Y_1^2Y_2 + (a_1a_2 - 3a_3)\,X_1X_2^2Y_1 \\
& + a_3Y_1^2Y_2Z_2 - (a_2^2 - 3a_4)\,X_1^2X_2^2 \\
& + (a_1a_4 - a_2a_3)(2X_1Z_2 + X_2Z_1)\,X_2Y_1 \\
& + (a_1^2a_4 - 2a_1a_2a_3 + 3a_3^2)\,X_1^2X_2Z_2 \\
& - (a_2a_4 - 9a_6)\,X_1X_2(X_1Z_2 + X_2Z_1) \\
& + (3a_1a_6 - a_3a_4)(X_1Z_2 + 2X_2Z_1)\,Y_1Z_2 \\
& + (3a_1^2a_6 - 2a_1a_3a_4 + a_2a_3^2 + 3a_2a_6 - a_4^2)\,X_1Z_2(X_1Z_2 + 2X_2Z_1) \\
& - (3a_2a_6 - a_4^2)(X_1Z_2 + X_2Z_1)(X_1Z_2 - X_2Z_1) \\
& + (a_1^3a_6 - a_1^2a_3a_4 + a_1a_2a_3^2 - a_1a_4^2 + 4a_1a_2a_6 - a_3^3 - 3a_3a_6)\,Y_1Z_1Z_2^2 \\
& + (a_1^4a_6 - a_1^3a_3a_4 + 5a_1^2a_2a_6 + a_1^2a_2a_3^2 - a_1a_2a_3a_4 - a_1a_3^3 - 3a_1a_3a_6 \\
& - a_1^2a_4^2 + a_2^2a_3^2 - a_2a_4^2 + 4a_2^2a_6 - a_3^2a_4 - 3a_4a_6)\,X_1Z_1Z_2^2 \\
& + (a_1^2a_2a_6 - a_1a_2a_3a_4 + 3a_1a_3a_6 + a_2^2a_3^2 - a_2a_4^2 \\
& + 4a_2^2a_6 - 2a_3^2a_4 - 3a_4a_6)\,X_2Z_1^2Z_2 \\
& + (a_1^3a_3a_6 - a_1^2a_3^2a_4 + a_1^2a_4a_6 + a_1a_2a_3^3 \\
& + 4a_1a_2a_3a_6 - 2a_1a_3a_4^2 + a_2a_3^2a_4 \\
& + 4a_2a_4a_6 - a_3^4 - 6a_3^2a_6 - a_4^3 - 9a_6^2)\,Z_1^2Z_2^2, \\
Z_3^{(2)} = {} & 3X_1X_2(X_1Y_2 + X_2Y_1) + Y_1Y_2(Y_1Z_2 + Y_2Z_1) + 3a_1X_1^2X_2^2 \\
& + a_1(2X_1Y_2 + Y_1X_2)\,Y_1Z_2 + a_1^2X_1Z_2(2X_2Y_1 + X_1Y_2) \\
& + a_2X_1X_2(Y_1Z_2 + Y_2Z_1) \\
& + a_2(X_1Y_2 + X_2Y_1)(X_1Z_2 + X_2Z_1) \\
& + a_1^3X_1^2X_2Z_2 + a_1a_2X_1X_2(2X_1Z_2 + X_2Z_1) \\
& + 3a_3X_1X_2^2Z_1 + a_3Y_1Z_2(Y_1Z_2 + 2Y_2Z_1) \\
& + 2a_1a_3X_1Z_2(Y_1Z_2 + Y_2Z_1) \\
& + 2a_1a_3X_2Y_1Z_1Z_2 + a_4(X_1Y_2 + X_2Y_1)\,Z_1Z_2 \\
& + a_4(X_1Z_2 + X_2Z_1)(Y_1Z_2 + Y_2Z_1) \\
& + (a_1^2a_3 + a_1a_4)\,X_1Z_2(X_1Z_2 + 2X_2Z_1) + a_2a_3X_2Z_1(2X_1Z_2 + X_2Z_1) \\
& + a_3^2Y_1Z_1Z_2^2 + (a_3^2 + 3a_6)(Y_1Z_2 + Y_2Z_1)\,Z_1Z_2 \\
& + a_1a_3^2(2X_1Z_2 + X_2Z_1)\,Z_1Z_2 + 3a_1a_6X_1Z_1Z_2^2 \\
& + a_3a_4(X_1Z_2 + 2X_2Z_1)\,Z_1Z_2 + (a_3^3 + 3a_3a_6)\,Z_1^2Z_2^2.
\end{aligned}
$$

1995 Bo
Explicit
of 2 add
for long
X_3, Y_3, Z
$\in \mathbf{Z}[a_1,$
$X_1,$

ert:

system

ass curves.

o 53 monomials

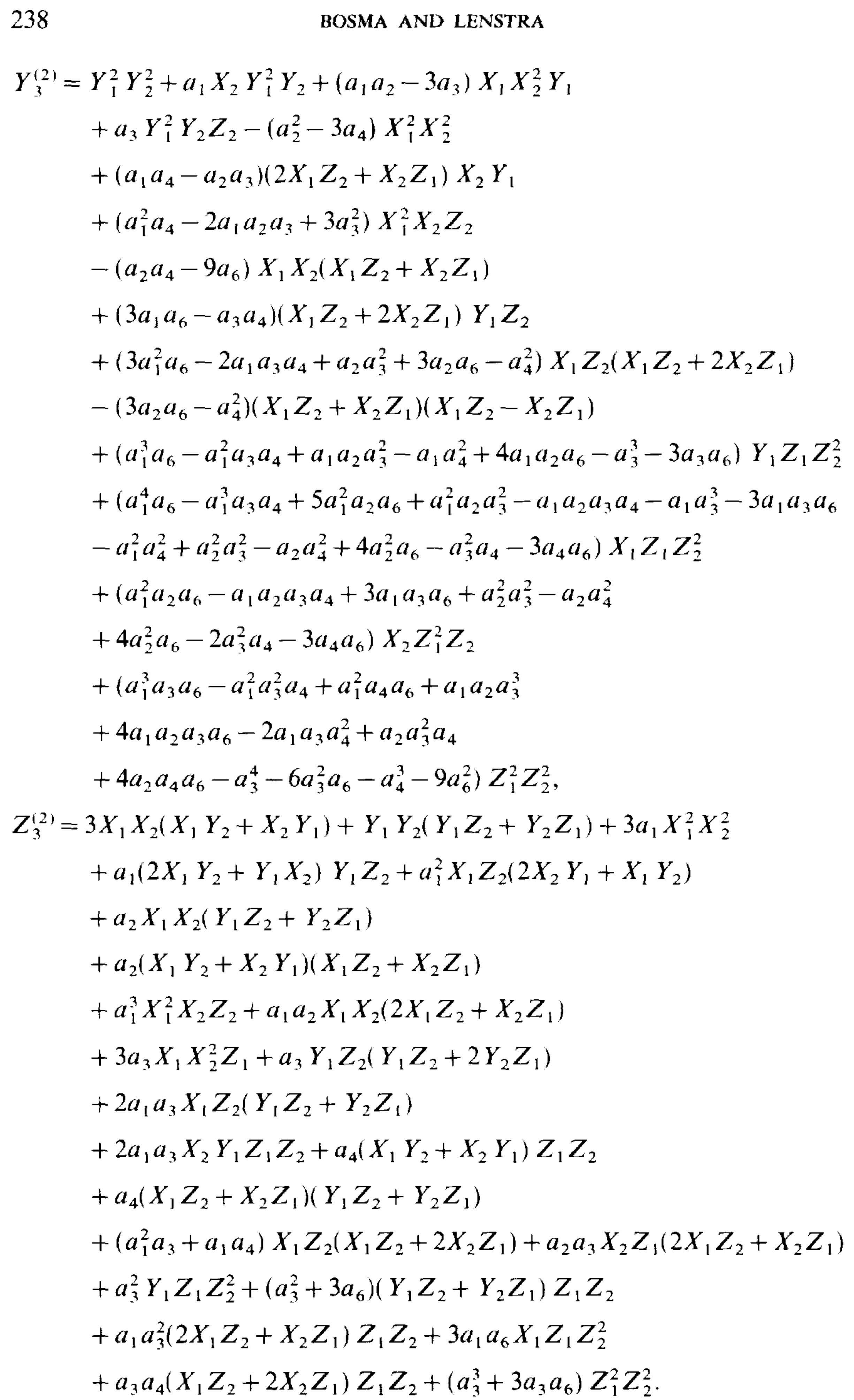
ra variables

$- x_j y_i$.

ert:

system

ss curves.



238 BOSMA AND LENSTRA

$$\begin{aligned}
Y_3^{(2)} = {} & Y_1^2 Y_2^2 + a_1 X_2 Y_1^2 Y_2 + (a_1 a_2 - 3a_3) X_1 X_2^2 Y_1 \\
& + a_3 Y_1^2 Y_2 Z_2 - (a_2^2 - 3a_4) X_1^2 X_2^2 \\
& + (a_1 a_4 - a_2 a_3)(2X_1 Z_2 + X_2 Z_1) X_2 Y_1 \\
& + (a_1^2 a_4 - 2a_1 a_2 a_3 + 3a_3^2) X_1^2 X_2 Z_2 \\
& - (a_2 a_4 - 9a_6) X_1 X_2 (X_1 Z_2 + X_2 Z_1) \\
& + (3a_1 a_6 - a_3 a_4)(X_1 Z_2 + 2X_2 Z_1) Y_1 Z_2 \\
& + (3a_1^2 a_6 - 2a_1 a_3 a_4 + a_2 a_3^2 + 3a_2 a_6 - a_4^2) X_1 Z_2 (X_1 Z_2 + 2X_2 Z_1) \\
& - (3a_2 a_6 - a_4^2)(X_1 Z_2 + X_2 Z_1)(X_1 Z_2 - X_2 Z_1) \\
& + (a_1^3 a_6 - a_1^2 a_3 a_4 + a_1 a_2 a_3^2 - a_1 a_4^2 + 4a_1 a_2 a_6 - a_3^3 - 3a_3 a_6) Y_1 Z_1 Z_2^2 \\
& + (a_1^4 a_6 - a_1^3 a_3 a_4 + 5a_1^2 a_2 a_6 + a_1^2 a_2 a_3^2 - a_1 a_2 a_3 a_4 - a_1 a_3^3 - 3a_1 a_3 a_6 \\
& - a_1^2 a_4^2 + a_2^2 a_3^2 - a_2 a_4^2 + 4a_2^2 a_6 - a_3^2 a_4 - 3a_4 a_6) X_1 Z_1 Z_2^2 \\
& + (a_1^2 a_2 a_6 - a_1 a_2 a_3 a_4 + 3a_1 a_3 a_6 + a_2^2 a_3^2 - a_2 a_4^2 \\
& + 4a_2^2 a_6 - 2a_3^2 a_4 - 3a_4 a_6) X_2 Z_1^2 Z_2 \\
& + (a_1^3 a_3 a_6 - a_1^2 a_3^2 a_4 + a_1^2 a_4 a_6 + a_1 a_2 a_3^3 \\
& + 4a_1 a_2 a_3 a_6 - 2a_1 a_3 a_4^2 + a_2 a_3^2 a_4 \\
& + 4a_2 a_4 a_6 - a_3^4 - 6a_3^2 a_6 - a_4^3 - 9a_6^2) Z_1^2 Z_2^2, \\
Z_3^{(2)} = {} & 3X_1 X_2 (X_1 Y_2 + X_2 Y_1) + Y_1 Y_2 (Y_1 Z_2 + Y_2 Z_1) + 3a_1 X_1^2 X_2^2 \\
& + a_1 (2X_1 Y_2 + Y_1 X_2) Y_1 Z_2 + a_1^2 X_1 Z_2 (2X_2 Y_1 + X_1 Y_2) \\
& + a_2 X_1 X_2 (Y_1 Z_2 + Y_2 Z_1) \\
& + a_2 (X_1 Y_2 + X_2 Y_1)(X_1 Z_2 + X_2 Z_1) \\
& + a_1^3 X_1^2 X_2 Z_2 + a_1 a_2 X_1 X_2 (2X_1 Z_2 + X_2 Z_1) \\
& + 3a_3 X_1 X_2^2 Z_1 + a_3 Y_1 Z_2 (Y_1 Z_2 + 2Y_2 Z_1) \\
& + 2a_1 a_3 X_1 Z_2 (Y_1 Z_2 + Y_2 Z_1) \\
& + 2a_1 a_3 X_2 Y_1 Z_1 Z_2 + a_4 (X_1 Y_2 + X_2 Y_1) Z_1 Z_2 \\
& + a_4 (X_1 Z_2 + X_2 Z_1)(Y_1 Z_2 + Y_2 Z_1) \\
& + (a_1^2 a_3 + a_1 a_4) X_1 Z_2 (X_1 Z_2 + 2X_2 Z_1) + a_2 a_3 X_2 Z_1 (2X_1 Z_2 + X_2 Z_1) \\
& + a_3^2 Y_1 Z_1 Z_2^2 + (a_3^2 + 3a_6)(Y_1 Z_2 + Y_2 Z_1) Z_1 Z_2 \\
& + a_1 a_3^2 (2X_1 Z_2 + X_2 Z_1) Z_1 Z_2 + 3a_1 a_6 X_1 Z_1 Z_2^2 \\
& + a_3 a_4 (X_1 Z_2 + 2X_2 Z_1) Z_1 Z_2 + (a_3^3 + 3a_3 a_6) Z_1^2 Z_2^2.
\end{aligned}$$

1995 Bosma–Lens

Explicit complete s

of 2 addition laws

for long Weierstra

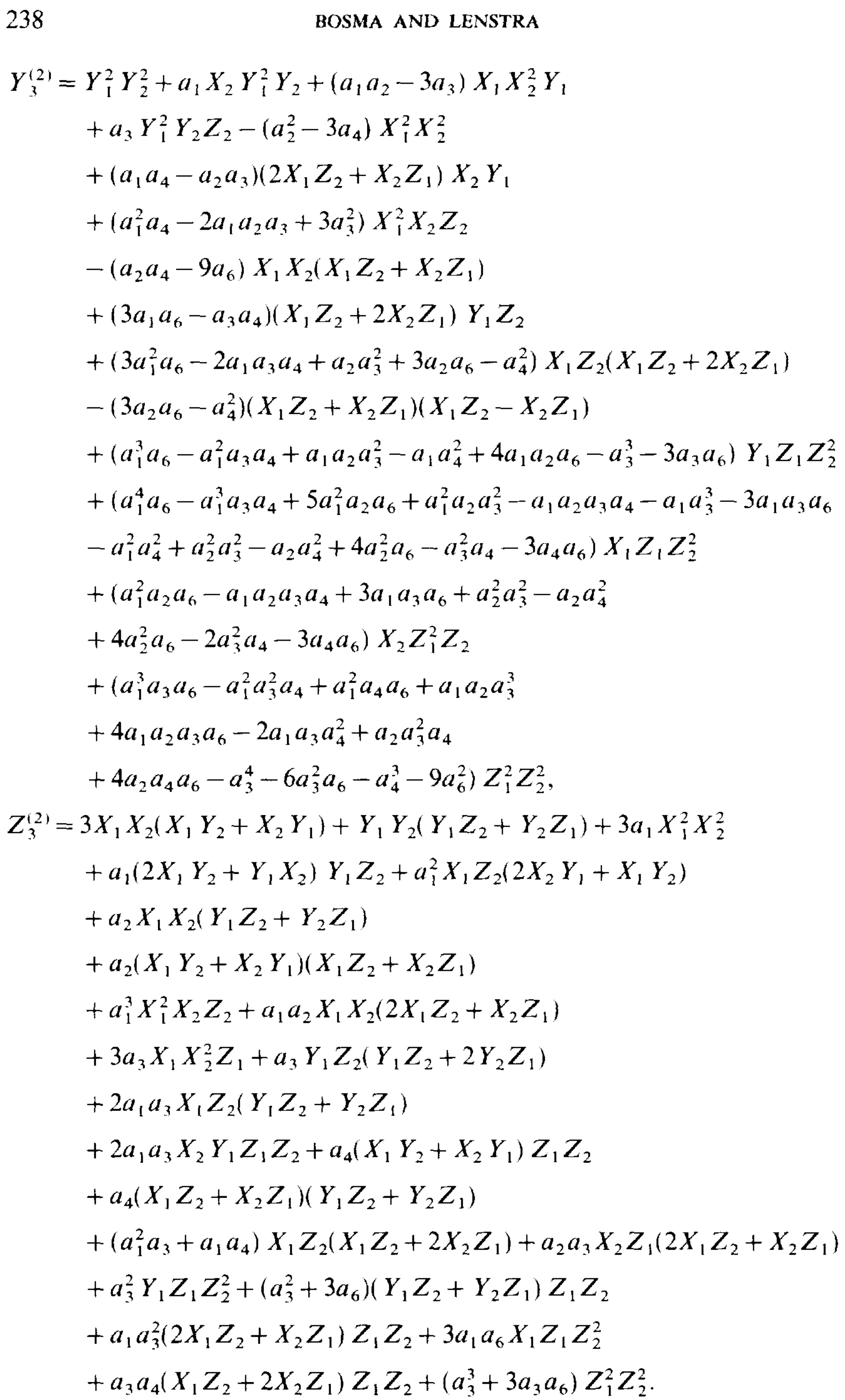
$X_3, Y_3, Z_3, X'_3, Y'_3,$

$\in \mathbf{Z}[a_1, a_2, a_3, a_4,$

X_1, Y_1, Z_1, X_2

omials

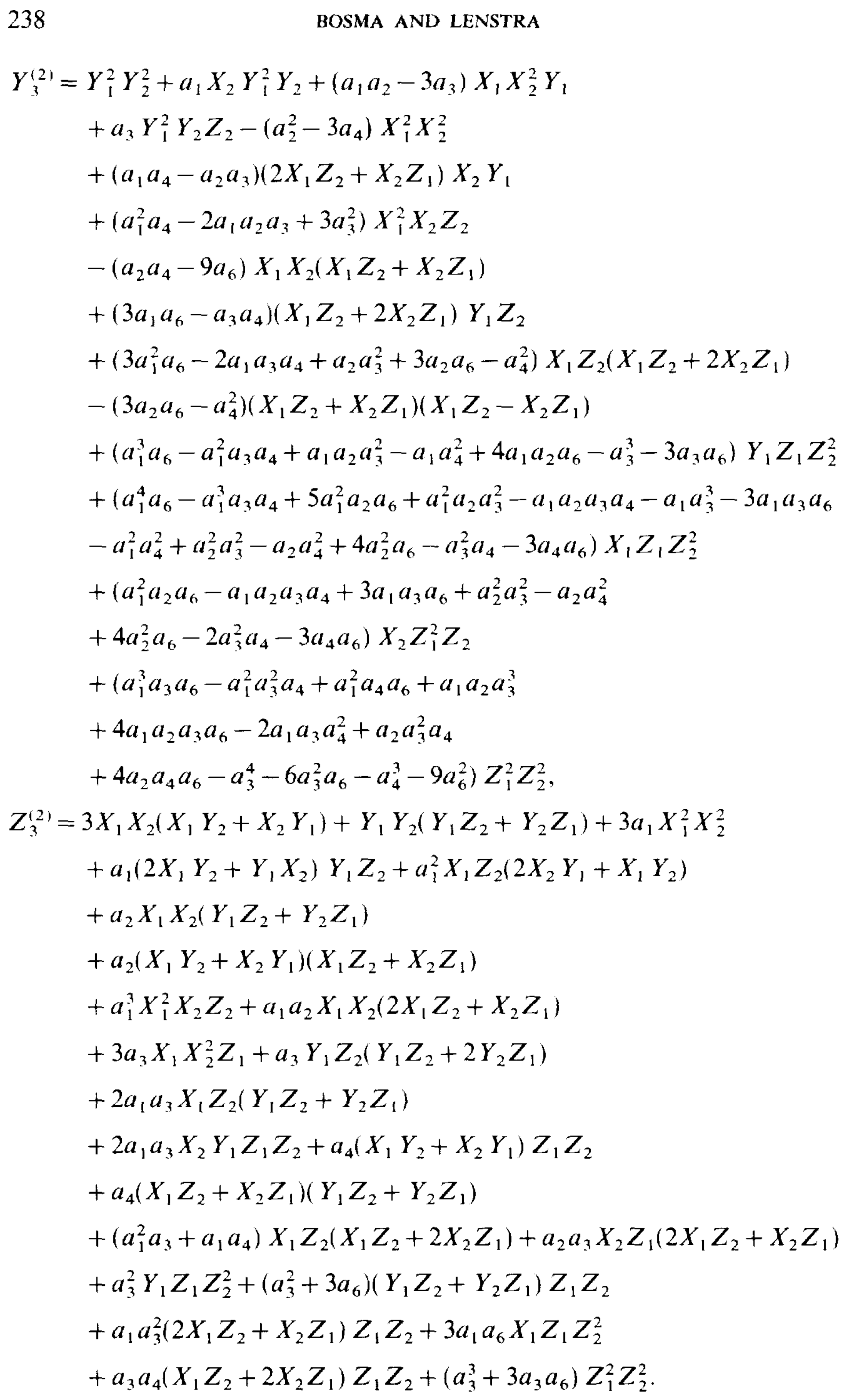
es



238 BOSMA AND LENSTRA

$$\begin{aligned}
Y_3^{(2)} = {} & Y_1^2 Y_2^2 + a_1 X_2 Y_1^2 Y_2 + (a_1 a_2 - 3a_3)\, X_1 X_2^2 Y_1 \\
& + a_3 Y_1^2 Y_2 Z_2 - (a_2^2 - 3a_4)\, X_1^2 X_2^2 \\
& + (a_1 a_4 - a_2 a_3)(2X_1 Z_2 + X_2 Z_1)\, X_2 Y_1 \\
& + (a_1^2 a_4 - 2a_1 a_2 a_3 + 3a_3^2)\, X_1^2 X_2 Z_2 \\
& - (a_2 a_4 - 9a_6)\, X_1 X_2 (X_1 Z_2 + X_2 Z_1) \\
& + (3a_1 a_6 - a_3 a_4)(X_1 Z_2 + 2X_2 Z_1)\, Y_1 Z_2 \\
& + (3a_1^2 a_6 - 2a_1 a_3 a_4 + a_2 a_3^2 + 3a_2 a_6 - a_4^2)\, X_1 Z_2 (X_1 Z_2 + 2X_2 Z_1) \\
& - (3a_2 a_6 - a_4^2)(X_1 Z_2 + X_2 Z_1)(X_1 Z_2 - X_2 Z_1) \\
& + (a_1^3 a_6 - a_1^2 a_3 a_4 + a_1 a_2 a_3^2 - a_1 a_4^2 + 4a_1 a_2 a_6 - a_3^3 - 3a_3 a_6)\, Y_1 Z_1 Z_2^2 \\
& + (a_1^4 a_6 - a_1^3 a_3 a_4 + 5a_1^2 a_2 a_6 + a_1^2 a_2 a_3^2 - a_1 a_2 a_3 a_4 - a_1 a_3^3 - 3a_1 a_3 a_6 \\
& - a_1^2 a_4^2 + a_2^2 a_3^2 - a_2 a_4^2 + 4a_2^2 a_6 - a_3^2 a_4 - 3a_4 a_6)\, X_1 Z_1 Z_2^2 \\
& + (a_1^2 a_2 a_6 - a_1 a_2 a_3 a_4 + 3a_1 a_3 a_6 + a_2^2 a_3^2 - a_2 a_4^2 \\
& + 4a_2^2 a_6 - 2a_3^2 a_4 - 3a_4 a_6)\, X_2 Z_1^2 Z_2 \\
& + (a_1^3 a_3 a_6 - a_1^2 a_3^2 a_4 + a_1^2 a_4 a_6 + a_1 a_2 a_3^3 \\
& + 4a_1 a_2 a_3 a_6 - 2a_1 a_3 a_4^2 + a_2 a_3^2 a_4 \\
& + 4a_2 a_4 a_6 - a_3^4 - 6a_3^2 a_6 - a_4^3 - 9a_6^2)\, Z_1^2 Z_2^2, \\
Z_3^{(2)} = {} & 3X_1 X_2 (X_1 Y_2 + X_2 Y_1) + Y_1 Y_2 (Y_1 Z_2 + Y_2 Z_1) + 3a_1 X_1^2 X_2^2 \\
& + a_1 (2X_1 Y_2 + Y_1 X_2)\, Y_1 Z_2 + a_1^2 X_1 Z_2 (2X_2 Y_1 + X_1 Y_2) \\
& + a_2 X_1 X_2 (Y_1 Z_2 + Y_2 Z_1) \\
& + a_2 (X_1 Y_2 + X_2 Y_1)(X_1 Z_2 + X_2 Z_1) \\
& + a_1^3 X_1^2 X_2 Z_2 + a_1 a_2 X_1 X_2 (2X_1 Z_2 + X_2 Z_1) \\
& + 3a_3 X_1 X_2^2 Z_1 + a_3 Y_1 Z_2 (Y_1 Z_2 + 2Y_2 Z_1) \\
& + 2a_1 a_3 X_1 Z_2 (Y_1 Z_2 + Y_2 Z_1) \\
& + 2a_1 a_3 X_2 Y_1 Z_1 Z_2 + a_4 (X_1 Y_2 + X_2 Y_1)\, Z_1 Z_2 \\
& + a_4 (X_1 Z_2 + X_2 Z_1)(Y_1 Z_2 + Y_2 Z_1) \\
& + (a_1^2 a_3 + a_1 a_4)\, X_1 Z_2 (X_1 Z_2 + 2X_2 Z_1) + a_2 a_3 X_2 Z_1 (2X_1 Z_2 + X_2 Z_1) \\
& + a_3^2 Y_1 Z_1 Z_2^2 + (a_3^2 + 3a_6)(Y_1 Z_2 + Y_2 Z_1)\, Z_1 Z_2 \\
& + a_1 a_3^2 (2X_1 Z_2 + X_2 Z_1)\, Z_1 Z_2 + 3a_1 a_6 X_1 Z_1 Z_2^2 \\
& + a_3 a_4 (X_1 Z_2 + 2X_2 Z_1)\, Z_1 Z_2 + (a_3^3 + 3a_3 a_6)\, Z_1^2 Z_2^2.
\end{aligned}$$

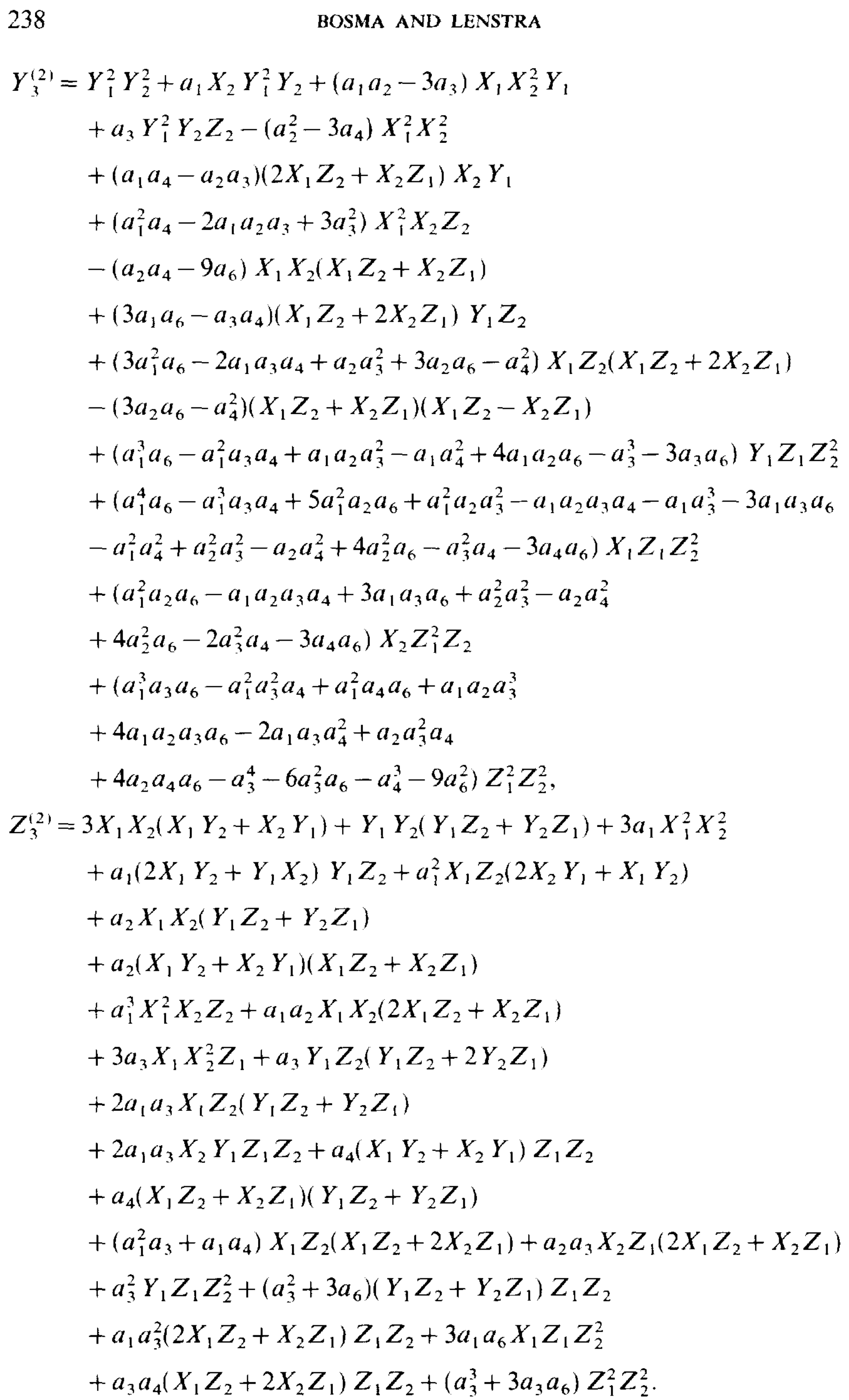
1995 Bosma–Lenstra:
Explicit complete system
of 2 addition laws
for long Weierstrass curves:
$X_3, Y_3, Z_3, X'_3, Y'_3, Z'_3$
$\in \mathbf{Z}[a_1, a_2, a_3, a_4, a_6,$
$X_1, Y_1, Z_1, X_2, Y_2, Z_2]$.



238 BOSMA AND LENSTRA

$$\begin{aligned}
Y_3^{(2)} = {} & Y_1^2 Y_2^2 + a_1 X_2 Y_1^2 Y_2 + (a_1 a_2 - 3a_3)\, X_1 X_2^2 Y_1 \\
& + a_3 Y_1^2 Y_2 Z_2 - (a_2^2 - 3a_4)\, X_1^2 X_2^2 \\
& + (a_1 a_4 - a_2 a_3)(2X_1 Z_2 + X_2 Z_1)\, X_2 Y_1 \\
& + (a_1^2 a_4 - 2a_1 a_2 a_3 + 3a_3^2)\, X_1^2 X_2 Z_2 \\
& - (a_2 a_4 - 9a_6)\, X_1 X_2 (X_1 Z_2 + X_2 Z_1) \\
& + (3a_1 a_6 - a_3 a_4)(X_1 Z_2 + 2X_2 Z_1)\, Y_1 Z_2 \\
& + (3a_1^2 a_6 - 2a_1 a_3 a_4 + a_2 a_3^2 + 3a_2 a_6 - a_4^2)\, X_1 Z_2 (X_1 Z_2 + 2X_2 Z_1) \\
& - (3a_2 a_6 - a_4^2)(X_1 Z_2 + X_2 Z_1)(X_1 Z_2 - X_2 Z_1) \\
& + (a_1^3 a_6 - a_1^2 a_3 a_4 + a_1 a_2 a_3^2 - a_1 a_4^2 + 4a_1 a_2 a_6 - a_3^3 - 3a_3 a_6)\, Y_1 Z_1 Z_2^2 \\
& + (a_1^4 a_6 - a_1^3 a_3 a_4 + 5a_1^2 a_2 a_6 + a_1^2 a_2 a_3^2 - a_1 a_2 a_3 a_4 - a_1 a_3^3 - 3a_1 a_3 a_6 \\
& - a_1^2 a_4^2 + a_2^2 a_3^2 - a_2 a_4^2 + 4a_2^2 a_6 - a_3^2 a_4 - 3a_4 a_6)\, X_1 Z_1 Z_2^2 \\
& + (a_1^2 a_2 a_6 - a_1 a_2 a_3 a_4 + 3a_1 a_3 a_6 + a_2^2 a_3^2 - a_2 a_4^2 \\
& + 4a_2^2 a_6 - 2a_3^2 a_4 - 3a_4 a_6)\, X_2 Z_1^2 Z_2 \\
& + (a_1^3 a_3 a_6 - a_1^2 a_3^2 a_4 + a_1^2 a_4 a_6 + a_1 a_2 a_3^3 \\
& + 4a_1 a_2 a_3 a_6 - 2a_1 a_3 a_4^2 + a_2 a_3^2 a_4 \\
& + 4a_2 a_4 a_6 - a_3^4 - 6a_3^2 a_6 - a_4^3 - 9a_6^2)\, Z_1^2 Z_2^2, \\
Z_3^{(2)} = {} & 3X_1 X_2 (X_1 Y_2 + X_2 Y_1) + Y_1 Y_2 (Y_1 Z_2 + Y_2 Z_1) + 3a_1 X_1^2 X_2^2 \\
& + a_1 (2X_1 Y_2 + Y_1 X_2)\, Y_1 Z_2 + a_1^2 X_1 Z_2 (2X_2 Y_1 + X_1 Y_2) \\
& + a_2 X_1 X_2 (Y_1 Z_2 + Y_2 Z_1) \\
& + a_2 (X_1 Y_2 + X_2 Y_1)(X_1 Z_2 + X_2 Z_1) \\
& + a_1^3 X_1^2 X_2 Z_2 + a_1 a_2 X_1 X_2 (2X_1 Z_2 + X_2 Z_1) \\
& + 3a_3 X_1 X_2^2 Z_1 + a_3 Y_1 Z_2 (Y_1 Z_2 + 2Y_2 Z_1) \\
& + 2a_1 a_3 X_1 Z_2 (Y_1 Z_2 + Y_2 Z_1) \\
& + 2a_1 a_3 X_2 Y_1 Z_1 Z_2 + a_4 (X_1 Y_2 + X_2 Y_1)\, Z_1 Z_2 \\
& + a_4 (X_1 Z_2 + X_2 Z_1)(Y_1 Z_2 + Y_2 Z_1) \\
& + (a_1^2 a_3 + a_1 a_4)\, X_1 Z_2 (X_1 Z_2 + 2X_2 Z_1) + a_2 a_3 X_2 Z_1 (2X_1 Z_2 + X_2 Z_1) \\
& + a_3^2 Y_1 Z_1 Z_2^2 + (a_3^2 + 3a_6)(Y_1 Z_2 + Y_2 Z_1)\, Z_1 Z_2 \\
& + a_1 a_3^2 (2X_1 Z_2 + X_2 Z_1)\, Z_1 Z_2 + 3a_1 a_6 X_1 Z_1 Z_2^2 \\
& + a_3 a_4 (X_1 Z_2 + 2X_2 Z_1)\, Z_1 Z_2 + (a_3^3 + 3a_3 a_6)\, Z_1^2 Z_2^2.
\end{aligned}$$

1995 Bosma–Lenstra:
Explicit complete system
of 2 addition laws
for long Weierstrass curves:
$X_3, Y_3, Z_3, X_3', Y_3', Z_3'$
$\in \mathbf{Z}[a_1, a_2, a_3, a_4, a_6,$
$X_1, Y_1, Z_1, X_2, Y_2, Z_2].$

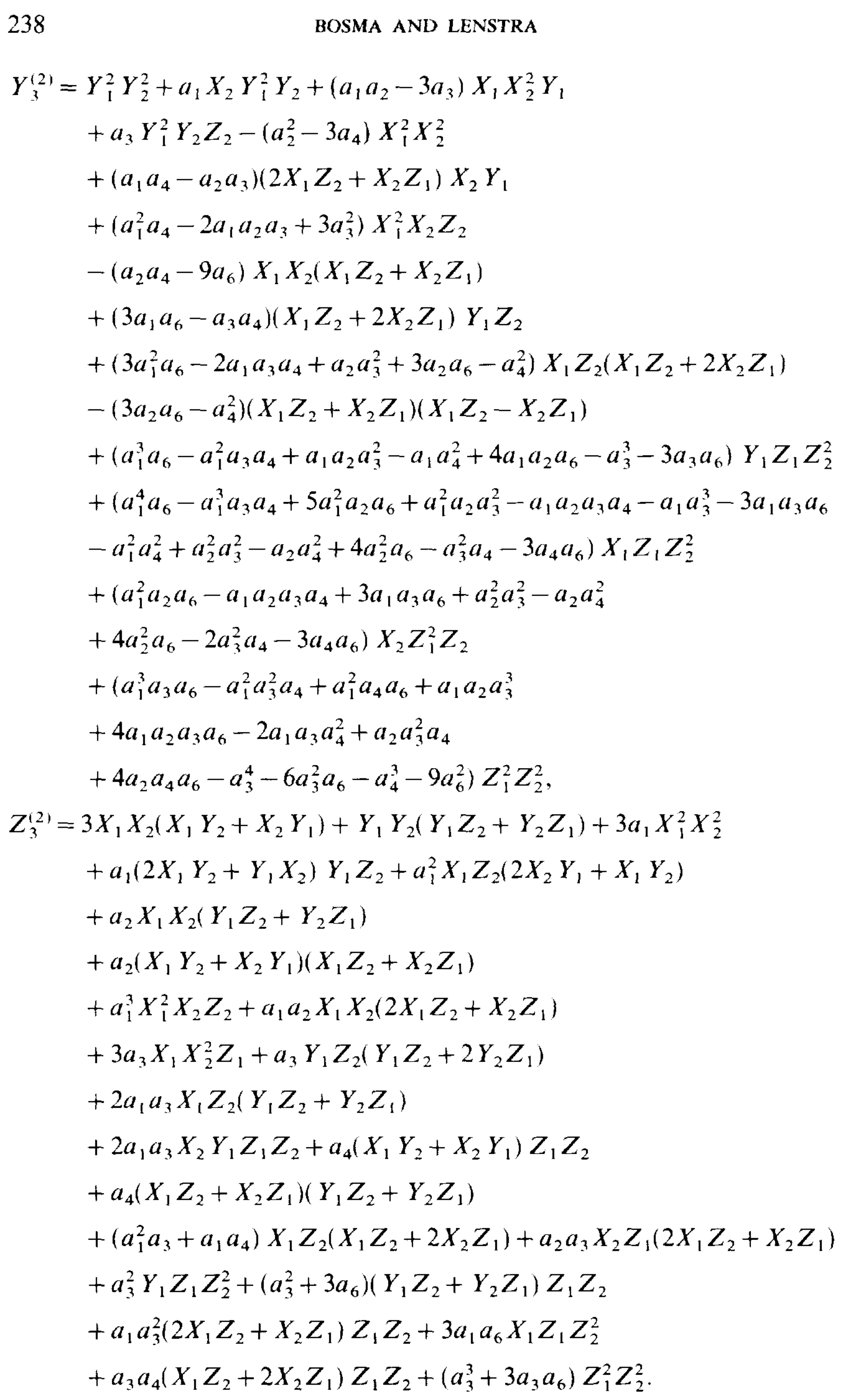


238 BOSMA AND LENSTRA

$$
\begin{aligned}
Y_3^{(2)} = {} & Y_1^2 Y_2^2 + a_1 X_2 Y_1^2 Y_2 + (a_1 a_2 - 3a_3)\, X_1 X_2^2 Y_1 \\
& + a_3 Y_1^2 Y_2 Z_2 - (a_2^2 - 3a_4)\, X_1^2 X_2^2 \\
& + (a_1 a_4 - a_2 a_3)(2X_1 Z_2 + X_2 Z_1)\, X_2 Y_1 \\
& + (a_1^2 a_4 - 2a_1 a_2 a_3 + 3a_3^2)\, X_1^2 X_2 Z_2 \\
& - (a_2 a_4 - 9a_6)\, X_1 X_2 (X_1 Z_2 + X_2 Z_1) \\
& + (3a_1 a_6 - a_3 a_4)(X_1 Z_2 + 2X_2 Z_1)\, Y_1 Z_2 \\
& + (3a_1^2 a_6 - 2a_1 a_3 a_4 + a_2 a_3^2 + 3a_2 a_6 - a_4^2)\, X_1 Z_2 (X_1 Z_2 + 2X_2 Z_1) \\
& - (3a_2 a_6 - a_4^2)(X_1 Z_2 + X_2 Z_1)(X_1 Z_2 - X_2 Z_1) \\
& + (a_1^3 a_6 - a_1^2 a_3 a_4 + a_1 a_2 a_3^2 - a_1 a_4^2 + 4a_1 a_2 a_6 - a_3^3 - 3a_3 a_6)\, Y_1 Z_1 Z_2^2 \\
& + (a_1^4 a_6 - a_1^3 a_3 a_4 + 5a_1^2 a_2 a_6 + a_1^2 a_2 a_3^2 - a_1 a_2 a_3 a_4 - a_1 a_3^3 - 3a_1 a_3 a_6 \\
& - a_1^2 a_4^2 + a_2^2 a_3^2 - a_2 a_4^2 + 4a_2^2 a_6 - a_3^2 a_4 - 3a_4 a_6)\, X_1 Z_1 Z_2^2 \\
& + (a_1^2 a_2 a_6 - a_1 a_2 a_3 a_4 + 3a_1 a_3 a_6 + a_2^2 a_3^2 - a_2 a_4^2 \\
& + 4a_2^2 a_6 - 2a_3^2 a_4 - 3a_4 a_6)\, X_2 Z_1^2 Z_2 \\
& + (a_1^3 a_3 a_6 - a_1^2 a_3^2 a_4 + a_1^2 a_4 a_6 + a_1 a_2 a_3^3 \\
& + 4a_1 a_2 a_3 a_6 - 2a_1 a_3 a_4^2 + a_2 a_3^2 a_4 \\
& + 4a_2 a_4 a_6 - a_3^4 - 6a_3^2 a_6 - a_4^3 - 9a_6^2)\, Z_1^2 Z_2^2, \\
Z_3^{(2)} = {} & 3X_1 X_2 (X_1 Y_2 + X_2 Y_1) + Y_1 Y_2 (Y_1 Z_2 + Y_2 Z_1) + 3a_1 X_1^2 X_2^2 \\
& + a_1 (2X_1 Y_2 + Y_1 X_2)\, Y_1 Z_2 + a_1^2 X_1 Z_2 (2X_2 Y_1 + X_1 Y_2) \\
& + a_2 X_1 X_2 (Y_1 Z_2 + Y_2 Z_1) \\
& + a_2 (X_1 Y_2 + X_2 Y_1)(X_1 Z_2 + X_2 Z_1) \\
& + a_1^3 X_1^2 X_2 Z_2 + a_1 a_2 X_1 X_2 (2X_1 Z_2 + X_2 Z_1) \\
& + 3a_3 X_1 X_2^2 Z_1 + a_3 Y_1 Z_2 (Y_1 Z_2 + 2Y_2 Z_1) \\
& + 2a_1 a_3 X_1 Z_2 (Y_1 Z_2 + Y_2 Z_1) \\
& + 2a_1 a_3 X_2 Y_1 Z_1 Z_2 + a_4 (X_1 Y_2 + X_2 Y_1)\, Z_1 Z_2 \\
& + a_4 (X_1 Z_2 + X_2 Z_1)(Y_1 Z_2 + Y_2 Z_1) \\
& + (a_1^2 a_3 + a_1 a_4)\, X_1 Z_2 (X_1 Z_2 + 2X_2 Z_1) + a_2 a_3 X_2 Z_1 (2X_1 Z_2 + X_2 Z_1) \\
& + a_3^2 Y_1 Z_1 Z_2^2 + (a_3^2 + 3a_6)(Y_1 Z_2 + Y_2 Z_1)\, Z_1 Z_2 \\
& + a_1 a_3^2 (2X_1 Z_2 + X_2 Z_1)\, Z_1 Z_2 + 3a_1 a_6 X_1 Z_1 Z_2^2 \\
& + a_3 a_4 (X_1 Z_2 + 2X_2 Z_1)\, Z_1 Z_2 + (a_3^3 + 3a_3 a_6)\, Z_1^2 Z_2^2.
\end{aligned}
$$

1995 Bosma–Lenstra:
Explicit complete system
of 2 addition laws
for long Weierstrass curves:
$X_3, Y_3, Z_3, X'_3, Y'_3, Z'_3$
$\in \mathbf{Z}[a_1, a_2, a_3, a_4, a_6,$
$X_1, Y_1, Z_1, X_2, Y_2, Z_2]$.

My previous slide in this talk:
Bosma–Lenstra Y'_3, Z'_3.

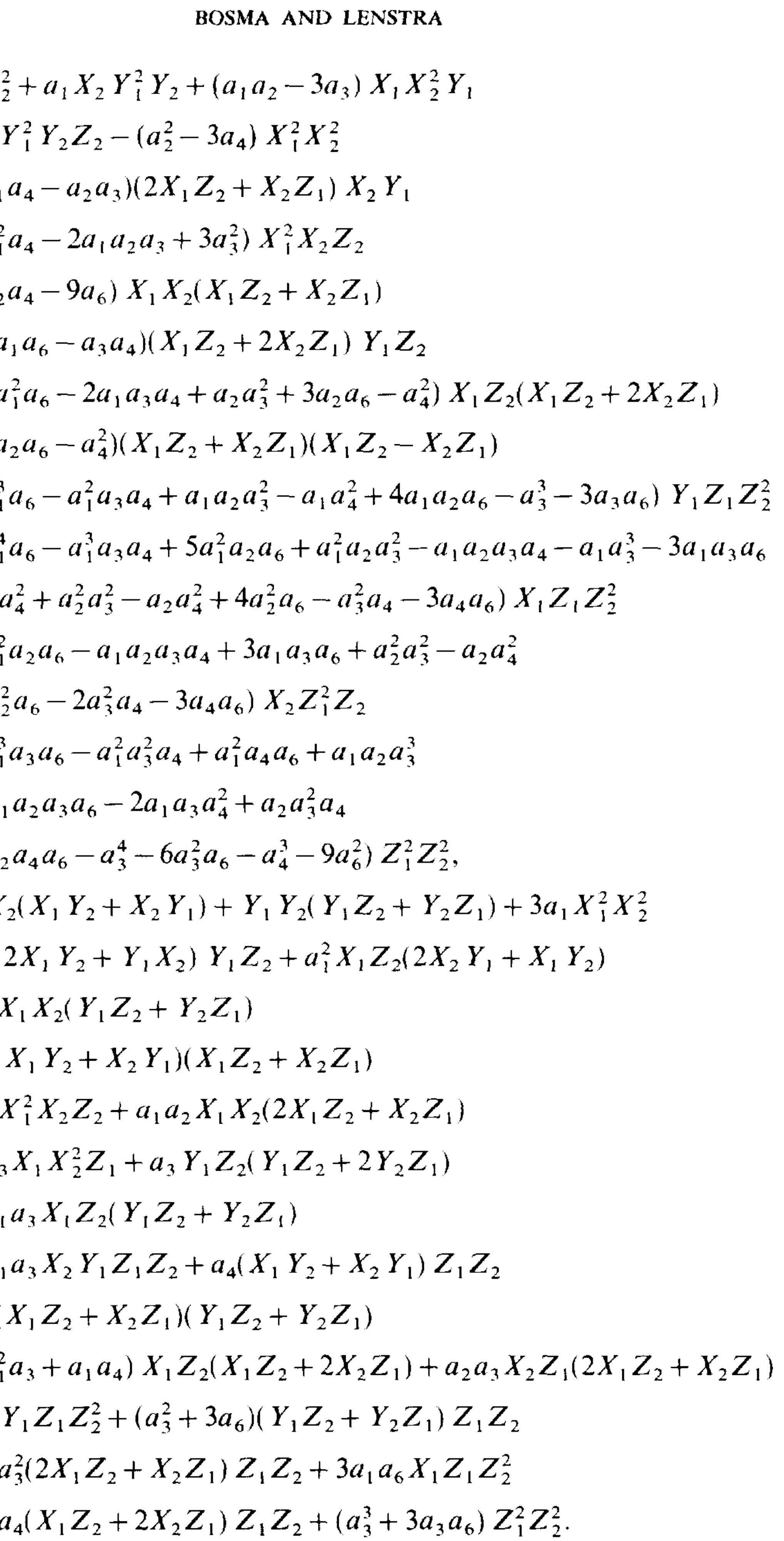


238 BOSMA AND LENSTRA

$$
\begin{aligned}
Y_3^{(2)} = {} & Y_1^2 Y_2^2 + a_1 X_2 Y_1^2 Y_2 + (a_1 a_2 - 3a_3)\, X_1 X_2^2 Y_1 \\
& + a_3 Y_1^2 Y_2 Z_2 - (a_2^2 - 3a_4)\, X_1^2 X_2^2 \\
& + (a_1 a_4 - a_2 a_3)(2X_1 Z_2 + X_2 Z_1)\, X_2 Y_1 \\
& + (a_1^2 a_4 - 2a_1 a_2 a_3 + 3a_3^2)\, X_1^2 X_2 Z_2 \\
& - (a_2 a_4 - 9a_6)\, X_1 X_2 (X_1 Z_2 + X_2 Z_1) \\
& + (3a_1 a_6 - a_3 a_4)(X_1 Z_2 + 2X_2 Z_1)\, Y_1 Z_2 \\
& + (3a_1^2 a_6 - 2a_1 a_3 a_4 + a_2 a_3^2 + 3a_2 a_6 - a_4^2)\, X_1 Z_2 (X_1 Z_2 + 2X_2 Z_1) \\
& - (3a_2 a_6 - a_4^2)(X_1 Z_2 + X_2 Z_1)(X_1 Z_2 - X_2 Z_1) \\
& + (a_1^3 a_6 - a_1^2 a_3 a_4 + a_1 a_2 a_3^2 - a_1 a_4^2 + 4a_1 a_2 a_6 - a_3^3 - 3a_3 a_6)\, Y_1 Z_1 Z_2^2 \\
& + (a_1^4 a_6 - a_1^3 a_3 a_4 + 5a_1^2 a_2 a_6 + a_1^2 a_2 a_3^2 - a_1 a_2 a_3 a_4 - a_1 a_3^3 - 3a_1 a_3 a_6 \\
& - a_1^2 a_4^2 + a_2^2 a_3^2 - a_2 a_4^2 + 4a_2^2 a_6 - a_3^2 a_4 - 3a_4 a_6)\, X_1 Z_1 Z_2^2 \\
& + (a_1^2 a_2 a_6 - a_1 a_2 a_3 a_4 + 3a_1 a_3 a_6 + a_2^2 a_3^2 - a_2 a_4^2 \\
& + 4a_2^2 a_6 - 2a_3^2 a_4 - 3a_4 a_6)\, X_2 Z_1^2 Z_2 \\
& + (a_1^3 a_3 a_6 - a_1^2 a_3^2 a_4 + a_1^2 a_4 a_6 + a_1 a_2 a_3^3 \\
& + 4a_1 a_2 a_3 a_6 - 2a_1 a_3 a_4^2 + a_2 a_3^2 a_4 \\
& + 4a_2 a_4 a_6 - a_3^4 - 6a_3^2 a_6 - a_4^3 - 9a_6^2)\, Z_1^2 Z_2^2, \\
Z_3^{(2)} = {} & 3X_1 X_2 (X_1 Y_2 + X_2 Y_1) + Y_1 Y_2 (Y_1 Z_2 + Y_2 Z_1) + 3a_1 X_1^2 X_2^2 \\
& + a_1 (2X_1 Y_2 + Y_1 X_2)\, Y_1 Z_2 + a_1^2 X_1 Z_2 (2X_2 Y_1 + X_1 Y_2) \\
& + a_2 X_1 X_2 (Y_1 Z_2 + Y_2 Z_1) \\
& + a_2 (X_1 Y_2 + X_2 Y_1)(X_1 Z_2 + X_2 Z_1) \\
& + a_1^3 X_1^2 X_2 Z_2 + a_1 a_2 X_1 X_2 (2X_1 Z_2 + X_2 Z_1) \\
& + 3a_3 X_1 X_2^2 Z_1 + a_3 Y_1 Z_2 (Y_1 Z_2 + 2Y_2 Z_1) \\
& + 2a_1 a_3 X_1 Z_2 (Y_1 Z_2 + Y_2 Z_1) \\
& + 2a_1 a_3 X_2 Y_1 Z_1 Z_2 + a_4 (X_1 Y_2 + X_2 Y_1)\, Z_1 Z_2 \\
& + a_4 (X_1 Z_2 + X_2 Z_1)(Y_1 Z_2 + Y_2 Z_1) \\
& + (a_1^2 a_3 + a_1 a_4)\, X_1 Z_2 (X_1 Z_2 + 2X_2 Z_1) + a_2 a_3 X_2 Z_1 (2X_1 Z_2 + X_2 Z_1) \\
& + a_3^2 Y_1 Z_1 Z_2^2 + (a_3^2 + 3a_6)(Y_1 Z_2 + Y_2 Z_1)\, Z_1 Z_2 \\
& + a_1 a_3^2 (2X_1 Z_2 + X_2 Z_1)\, Z_1 Z_2 + 3a_1 a_6 X_1 Z_1 Z_2^2 \\
& + a_3 a_4 (X_1 Z_2 + 2X_2 Z_1)\, Z_1 Z_2 + (a_3^3 + 3a_3 a_6)\, Z_1^2 Z_2^2.
\end{aligned}
$$

1995 Bosma–Lenstra:
Explicit complete system
of 2 addition laws
for long Weierstrass curves:
$X_3, Y_3, Z_3, X_3', Y_3', Z_3'$
$\in \mathbf{Z}[a_1, a_2, a_3, a_4, a_6,$
$X_1, Y_1, Z_1, X_2, Y_2, Z_2].$

My previous slide in this talk:
Bosma–Lenstra Y_3', Z_3'.
Actually, slide shows
$\text{Publish}(Y_3'), \text{Publish}(Z_3')$,
where Publish introduces typos.



BOSMA AND LENSTRA

${}^2_2 + a_1 X_2 Y_1^2 Y_2 + (a_1 a_2 - 3a_3) X_1 X_2^2 Y_1$

$Y_1^2 Y_2 Z_2 - (a_2^2 - 3a_4) X_1^2 X_2^2$

${}_1 a_4 - a_2 a_3)(2X_1 Z_2 + X_2 Z_1) X_2 Y_1$

${}^2_1 a_4 - 2a_1 a_2 a_3 + 3a_3^2) X_1^2 X_2 Z_2$

${}_2 a_4 - 9a_6) X_1 X_2(X_1 Z_2 + X_2 Z_1)$

$a_1 a_6 - a_3 a_4)(X_1 Z_2 + 2X_2 Z_1) Y_1 Z_2$

$a_1^2 a_6 - 2a_1 a_3 a_4 + a_2 a_3^2 + 3a_2 a_6 - a_4^2) X_1 Z_2(X_1 Z_2 + 2X_2 Z_1)$

$a_2 a_6 - a_4^2)(X_1 Z_2 + X_2 Z_1)(X_1 Z_2 - X_2 Z_1)$

${}^3_1 a_6 - a_1^2 a_3 a_4 + a_1 a_2 a_3^2 - a_1 a_4^2 + 4a_1 a_2 a_6 - a_3^3 - 3a_3 a_6) Y_1 Z_1 Z_2^2$

${}^4_1 a_6 - a_1^3 a_3 a_4 + 5a_1^2 a_2 a_6 + a_1^2 a_2 a_3^2 - a_1 a_2 a_3 a_4 - a_1 a_3^3 - 3a_1 a_3 a_6$

$a_4^2 + a_2^2 a_3^2 - a_2 a_4^2 + 4a_2^2 a_6 - a_3^2 a_4 - 3a_4 a_6) X_1 Z_1 Z_2^2$

${}^2_1 a_2 a_6 - a_1 a_2 a_3 a_4 + 3a_1 a_3 a_6 + a_2^2 a_3^2 - a_2 a_4^2$

${}^2_2 a_6 - 2a_3^2 a_4 - 3a_4 a_6) X_2 Z_1^2 Z_2$

${}^3_1 a_3 a_6 - a_1^2 a_3^2 a_4 + a_1^2 a_4 a_6 + a_1 a_2 a_3^3$

${}_1 a_2 a_3 a_6 - 2a_1 a_3 a_4^2 + a_2 a_3^2 a_4$

${}_2 a_4 a_6 - a_3^4 - 6a_3^2 a_6 - a_4^3 - 9a_6^2) Z_1^2 Z_2^2,$

${}_2(X_1 Y_2 + X_2 Y_1) + Y_1 Y_2(Y_1 Z_2 + Y_2 Z_1) + 3a_1 X_1^2 X_2^2$

$2X_1 Y_2 + Y_1 X_2) Y_1 Z_2 + a_1^2 X_1 Z_2(2X_2 Y_1 + X_1 Y_2)$

$X_1 X_2(Y_1 Z_2 + Y_2 Z_1)$

$X_1 Y_2 + X_2 Y_1)(X_1 Z_2 + X_2 Z_1)$

$X_1^2 X_2 Z_2 + a_1 a_2 X_1 X_2(2X_1 Z_2 + X_2 Z_1)$

${}_3 X_1 X_2^2 Z_1 + a_3 Y_1 Z_2(Y_1 Z_2 + 2Y_2 Z_1)$

${}_1 a_3 X_1 Z_2(Y_1 Z_2 + Y_2 Z_1)$

${}_1 a_3 X_2 Y_1 Z_1 Z_2 + a_4(X_1 Y_2 + X_2 Y_1) Z_1 Z_2$

$(X_1 Z_2 + X_2 Z_1)(Y_1 Z_2 + Y_2 Z_1)$

${}^2_1 a_3 + a_1 a_4) X_1 Z_2(X_1 Z_2 + 2X_2 Z_1) + a_2 a_3 X_2 Z_1(2X_1 Z_2 + X_2 Z_1)$

$Y_1 Z_1 Z_2^2 + (a_3^2 + 3a_6)(Y_1 Z_2 + Y_2 Z_1) Z_1 Z_2$

$a_3^2(2X_1 Z_2 + X_2 Z_1) Z_1 Z_2 + 3a_1 a_6 X_1 Z_1 Z_2^2$

$a_4(X_1 Z_2 + 2X_2 Z_1) Z_1 Z_2 + (a_3^3 + 3a_3 a_6) Z_1^2 Z_2^2.$

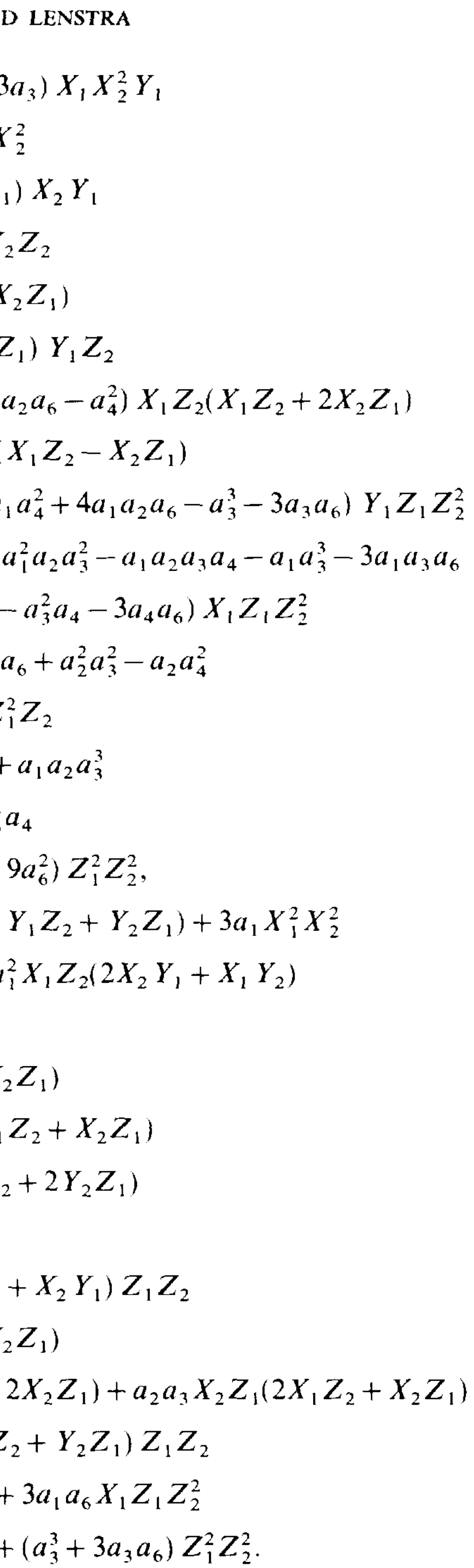
1995 Bosma–Lenstra:
Explicit complete system
of 2 addition laws
for long Weierstrass curves:
$X_3, Y_3, Z_3, X_3', Y_3', Z_3'$
$\in \mathbf{Z}[a_1, a_2, a_3, a_4, a_6,$
$X_1, Y_1, Z_1, X_2, Y_2, Z_2].$

My previous slide in this talk:
Bosma–Lenstra Y_3', Z_3'.
Actually, slide shows
$\text{Publish}(Y_3'), \text{Publish}(Z_3')$,
where Publish introduces typos.

What th

For all fi
all $\mathbf{P}^2$ W
$E/k : Y$
$X^3 + a_2$
all $P_1 =$
all $P_2 =$

$(X_3 : Y_3$
is $P_1 +$
$(X_3' : Y_3'$
is $P_1 +$
at most



D LENSTRA

$3a_3)\,X_1X_2^2Y_1$

X_2^2

$_1)\,X_2Y_1$

$_2Z_2$

$X_2Z_1)$

$Z_1)\,Y_1Z_2$

$a_2a_6-a_4^2)\,X_1Z_2(X_1Z_2+2X_2Z_1)$

$(X_1Z_2-X_2Z_1)$

$_1a_4^2+4a_1a_2a_6-a_3^3-3a_3a_6)\,Y_1Z_1Z_2^2$

$a_1^2a_2a_3^2-a_1a_2a_3a_4-a_1a_3^3-3a_1a_3a_6$

$-a_3^2a_4-3a_4a_6)\,X_1Z_1Z_2^2$

$a_6+a_2^2a_3^2-a_2a_4^2$

$Z_1^2Z_2$

$+a_1a_2a_3^3$

a_4

$9a_6^2)\,Z_1^2Z_2^2,$

$Y_1Z_2+Y_2Z_1)+3a_1X_1^2X_2^2$

$X_1Z_2(2X_2Y_1+X_1Y_2)$

$_2Z_1)$

$Z_2+X_2Z_1)$

$_2+2Y_2Z_1)$

$+X_2Y_1)\,Z_1Z_2$

$_2Z_1)$

$2X_2Z_1)+a_2a_3X_2Z_1(2X_1Z_2+X_2Z_1)$

$Z_2+Y_2Z_1)\,Z_1Z_2$

$+3a_1a_6X_1Z_1Z_2^2$

$+(a_3^3+3a_3a_6)\,Z_1^2Z_2^2.$

1995 Bosma–Lenstra:
Explicit complete system
of 2 addition laws
for long Weierstrass curves:
$X_3, Y_3, Z_3, X_3', Y_3', Z_3'$
$\in \mathbf{Z}[a_1, a_2, a_3, a_4, a_6,$
$X_1, Y_1, Z_1, X_2, Y_2, Z_2].$

My previous slide in this talk:
Bosma–Lenstra Y_3', Z_3'.
Actually, slide shows
$\text{Publish}(Y_3'), \text{Publish}(Z_3')$,
where Publish introduces typos.

What this means:

For all fields k,
all $\mathbf{P}^2$ Weierstrass
$E/k : Y^2Z + a_1X$
$X^3 + a_2X^2Z + a_4$
all $P_1 = (X_1 : Y_1 :$
all $P_2 = (X_2 : Y_2 :$

$(X_3 : Y_3 : Z_3)$
is $P_1 + P_2$ or $(0 :$
$(X_3' : Y_3' : Z_3')$
is $P_1 + P_2$ or $(0 :$
at most one of the

$2X_2Z_1)$

$a_6)\ Y_1Z_1Z_2^2$

${}_3^3 - 3a_1a_3a_6$

${}_2^2$

$Z_2 + X_2Z_1)$

1995 Bosma–Lenstra:
Explicit complete system
of 2 addition laws
for long Weierstrass curves:

$$X_3, Y_3, Z_3, X_3', Y_3', Z_3' \in \mathbf{Z}[a_1, a_2, a_3, a_4, a_6, X_1, Y_1, Z_1, X_2, Y_2, Z_2].$$

My previous slide in this talk:
Bosma–Lenstra Y_3', Z_3'.
Actually, slide shows
$\text{Publish}(Y_3'), \text{Publish}(Z_3')$,
where Publish introduces typos.

What this means:

For all fields k,
all $\mathbf{P}^2$ Weierstrass curves
$E/k : Y^2Z + a_1XYZ + a_3Y$
$X^3 + a_2X^2Z + a_4XZ^2 + a$
all $P_1 = (X_1 : Y_1 : Z_1) \in E($
all $P_2 = (X_2 : Y_2 : Z_2) \in E($

$(X_3 : Y_3 : Z_3)$
is $P_1 + P_2$ or $(0 : 0 : 0)$;
$(X_3' : Y_3' : Z_3')$
is $P_1 + P_2$ or $(0 : 0 : 0)$;
at most one of these is $(0 :$

1995 Bosma–Lenstra:
Explicit complete system
of 2 addition laws
for long Weierstrass curves:
$X_3, Y_3, Z_3, X_3', Y_3', Z_3'$
$\in \mathbf{Z}[a_1, a_2, a_3, a_4, a_6,$
$X_1, Y_1, Z_1, X_2, Y_2, Z_2]$.

My previous slide in this talk:
Bosma–Lenstra Y_3', Z_3'.
Actually, slide shows
$\text{Publish}(Y_3'), \text{Publish}(Z_3')$,
where Publish introduces typos.

What this means:

For all fields k,
all $\mathbf{P}^2$ Weierstrass curves
$E/k : Y^2Z + a_1XYZ + a_3YZ^2 =$
$X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3$,
all $P_1 = (X_1 : Y_1 : Z_1) \in E(k)$,
all $P_2 = (X_2 : Y_2 : Z_2) \in E(k)$:

$(X_3 : Y_3 : Z_3)$
is $P_1 + P_2$ or $(0 : 0 : 0)$;
$(X_3' : Y_3' : Z_3')$
is $P_1 + P_2$ or $(0 : 0 : 0)$;
at most one of these is $(0 : 0 : 0)$.

osma–Lenstra:

complete system
ition laws
Weierstrass curves:
Z_3, X'_3, Y'_3, Z'_3
$a_2, a_3, a_4, a_6,$
$Y_1, Z_1, X_2, Y_2, Z_2]$.

ious slide in this talk:
Lenstra Y'_3, Z'_3.
, slide shows
$Y'_3), \mathrm{Publish}(Z'_3),$
ublish introduces typos.

What this means:

For all fields k,
all $\mathbf{P}^2$ Weierstrass curves
$E/k : Y^2Z + a_1XYZ + a_3YZ^2 =$
$X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3,$
all $P_1 = (X_1 : Y_1 : Z_1) \in E(k)$,
all $P_2 = (X_2 : Y_2 : Z_2) \in E(k)$:

$(X_3 : Y_3 : Z_3)$
is $P_1 + P_2$ or $(0 : 0 : 0)$;
$(X'_3 : Y'_3 : Z'_3)$
is $P_1 + P_2$ or $(0 : 0 : 0)$;
at most one of these is $(0 : 0 : 0)$.

2009 Be

For all fi
all $\mathbf{P}^1 \times$
$X^2T^2 +$
all P_1, P
$P_1 = (($
$P_2 = (($

$(X_3 : Z_3$
$(X'_3 : Z'_3$
$(Y_3 : T_3)$
$(Y'_3 : T'_3)$
at most

tra:

system

ss curves:

Z_3'

a_6,

$_2, Y_2, Z_2]$.

in this talk:

$', Z_3'$.

ws

sh(Z_3'),

oduces typos.

What this means:

For all fields k,

all $\mathbf{P}^2$ Weierstrass curves

$E/k : Y^2Z + a_1XYZ + a_3YZ^2 =$

$X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3$,

all $P_1 = (X_1 : Y_1 : Z_1) \in E(k)$,

all $P_2 = (X_2 : Y_2 : Z_2) \in E(k)$:

$(X_3 : Y_3 : Z_3)$

is $P_1 + P_2$ or $(0 : 0 : 0)$;

$(X_3' : Y_3' : Z_3')$

is $P_1 + P_2$ or $(0 : 0 : 0)$;

at most one of these is $(0 : 0 : 0)$.

2009 Bernstein–T.

For all fields k wit

all $\mathbf{P}^1 \times \mathbf{P}^1$ Edwar

$X^2T^2 + Y^2Z^2 =$

all $P_1, P_2 \in E(k)$,

$P_1 = ((X_1 : Z_1), ($

$P_2 = ((X_2 : Z_2), ($

$(X_3 : Z_3)$ is $x(P_1$

$(X_3' : Z_3')$ is $x(P_1$

$(Y_3 : T_3)$ is $y(P_1 +$

$(Y_3' : T_3')$ is $y(P_1 +$

at most one of the

k:

pos.

What this means:

For all fields k,
all $\mathbf{P}^2$ Weierstrass curves
$E/k : Y^2Z + a_1XYZ + a_3YZ^2 =$
$X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3$,
all $P_1 = (X_1 : Y_1 : Z_1) \in E(k)$,
all $P_2 = (X_2 : Y_2 : Z_2) \in E(k)$:

$(X_3 : Y_3 : Z_3)$
is $P_1 + P_2$ or $(0 : 0 : 0)$;
$(X'_3 : Y'_3 : Z'_3)$
is $P_1 + P_2$ or $(0 : 0 : 0)$;
at most one of these is $(0 : 0 : 0)$.

2009 Bernstein–T. Lange:

For all fields k with $2 \neq 0$,
all $\mathbf{P}^1 \times \mathbf{P}^1$ Edwards curves
$X^2T^2 + Y^2Z^2 = Z^2T^2 + d$
all $P_1, P_2 \in E(k)$,
$P_1 = ((X_1 : Z_1), (Y_1 : T_1))$,
$P_2 = ((X_2 : Z_2), (Y_2 : T_2))$:

$(X_3 : Z_3)$ is $x(P_1 + P_2)$ or (
$(X'_3 : Z'_3)$ is $x(P_1 + P_2)$ or (
$(Y_3 : T_3)$ is $y(P_1 + P_2)$ or (0
$(Y'_3 : T'_3)$ is $y(P_1 + P_2)$ or (0
at most one of these is (0 :

What this means:

For all fields k,
all $\mathbf{P}^2$ Weierstrass curves
$E/k : Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3$,
all $P_1 = (X_1 : Y_1 : Z_1) \in E(k)$,
all $P_2 = (X_2 : Y_2 : Z_2) \in E(k)$:

$(X_3 : Y_3 : Z_3)$
is $P_1 + P_2$ or $(0 : 0 : 0)$;
$(X'_3 : Y'_3 : Z'_3)$
is $P_1 + P_2$ or $(0 : 0 : 0)$;
at most one of these is $(0 : 0 : 0)$.

2009 Bernstein–T. Lange:

For all fields k with $2 \neq 0$,
all $\mathbf{P}^1 \times \mathbf{P}^1$ Edwards curves E/k :
$X^2T^2 + Y^2Z^2 = Z^2T^2 + dX^2Y^2$,
all $P_1, P_2 \in E(k)$,
$P_1 = ((X_1 : Z_1), (Y_1 : T_1))$,
$P_2 = ((X_2 : Z_2), (Y_2 : T_2))$:

$(X_3 : Z_3)$ is $x(P_1 + P_2)$ or $(0 : 0)$;
$(X'_3 : Z'_3)$ is $x(P_1 + P_2)$ or $(0 : 0)$;
$(Y_3 : T_3)$ is $y(P_1 + P_2)$ or $(0 : 0)$;
$(Y'_3 : T'_3)$ is $y(P_1 + P_2)$ or $(0 : 0)$;
at most one of these is $(0 : 0)$.

is means:

ields k,
eierstrass curves
$^2Z + a_1XYZ + a_3YZ^2 =$
$X^2Z + a_4XZ^2 + a_6Z^3$,
$(X_1 : Y_1 : Z_1) \in E(k)$,
$(X_2 : Y_2 : Z_2) \in E(k)$:

$: Z_3)$
P_2 or $(0 : 0 : 0)$;
$: Z'_3)$
P_2 or $(0 : 0 : 0)$;
one of these is $(0 : 0 : 0)$.

2009 Bernstein–T. Lange:

For all fields k with $2 \neq 0$,
all $\mathbf{P}^1 \times \mathbf{P}^1$ Edwards curves E/k :
$X^2T^2 + Y^2Z^2 = Z^2T^2 + dX^2Y^2$,
all $P_1, P_2 \in E(k)$,
$P_1 = ((X_1 : Z_1), (Y_1 : T_1))$,
$P_2 = ((X_2 : Z_2), (Y_2 : T_2))$:

$(X_3 : Z_3)$ is $x(P_1 + P_2)$ or $(0 : 0)$;
$(X'_3 : Z'_3)$ is $x(P_1 + P_2)$ or $(0 : 0)$;
$(Y_3 : T_3)$ is $y(P_1 + P_2)$ or $(0 : 0)$;
$(Y'_3 : T'_3)$ is $y(P_1 + P_2)$ or $(0 : 0)$;
at most one of these is $(0 : 0)$.

$X_3 = X$
$Z_3 = Z_1$
$Y_3 = Y_1$
$T_3 = Z_1$

$X'_3 = X$
$Z'_3 = X_1$
$Y'_3 = X_1$
$T'_3 = X_1$

Much, m

Lange–R

Also mu

curves

$YZ + a_3YZ^2 =$

$_4XZ^2 + a_6Z^3$,

$Z_1) \in E(k)$,

$Z_2) \in E(k)$:

$0 : 0)$;

$0 : 0)$;

ese is $(0 : 0 : 0)$.

2009 Bernstein–T. Lange:

For all fields k with $2 \neq 0$,
all $\mathbf{P}^1 \times \mathbf{P}^1$ Edwards curves E/k:
$X^2T^2 + Y^2Z^2 = Z^2T^2 + dX^2Y^2$,
all $P_1, P_2 \in E(k)$,
$P_1 = ((X_1 : Z_1), (Y_1 : T_1))$,
$P_2 = ((X_2 : Z_2), (Y_2 : T_2))$:

$(X_3 : Z_3)$ is $x(P_1 + P_2)$ or $(0 : 0)$;
$(X_3' : Z_3')$ is $x(P_1 + P_2)$ or $(0 : 0)$;
$(Y_3 : T_3)$ is $y(P_1 + P_2)$ or $(0 : 0)$;
$(Y_3' : T_3')$ is $y(P_1 + P_2)$ or $(0 : 0)$;
at most one of these is $(0 : 0)$.

$X_3 = X_1Y_2Z_2T_1 +$
$Z_3 = Z_1Z_2T_1T_2 +$
$Y_3 = Y_1Y_2Z_1Z_2 -$
$T_3 = Z_1Z_2T_1T_2 -$

$X_3' = X_1Y_1Z_2T_2 +$
$Z_3' = X_1X_2T_1T_2 +$
$Y_3' = X_1Y_1Z_2T_2 -$
$T_3' = X_1Y_2Z_2T_1 -$

Much, much, muc

Lange–Ruppert, B

Also much easier t

$Z^2 =$

${}_6Z^3$,

$k)$,

$k)$:

$0 : 0)$.

2009 Bernstein–T. Lange:

For all fields k with $2 \neq 0$,
all $\mathbf{P}^1 \times \mathbf{P}^1$ Edwards curves E/k :
$X^2T^2 + Y^2Z^2 = Z^2T^2 + dX^2Y^2$,
all $P_1, P_2 \in E(k)$,
$P_1 = ((X_1 : Z_1), (Y_1 : T_1))$,
$P_2 = ((X_2 : Z_2), (Y_2 : T_2))$:

$(X_3 : Z_3)$ is $x(P_1 + P_2)$ or $(0 : 0)$;
$(X_3' : Z_3')$ is $x(P_1 + P_2)$ or $(0 : 0)$;
$(Y_3 : T_3)$ is $y(P_1 + P_2)$ or $(0 : 0)$;
$(Y_3' : T_3')$ is $y(P_1 + P_2)$ or $(0 : 0)$;
at most one of these is $(0 : 0)$.

$X_3 = X_1Y_2Z_2T_1 + X_2Y_1Z_1T$
$Z_3 = Z_1Z_2T_1T_2 + dX_1X_2Y_1$
$Y_3 = Y_1Y_2Z_1Z_2 - X_1X_2T_1T$
$T_3 = Z_1Z_2T_1T_2 - dX_1X_2Y_1$

$X_3' = X_1Y_1Z_2T_2 + X_2Y_2Z_1T$
$Z_3' = X_1X_2T_1T_2 + Y_1Y_2Z_1Z$
$Y_3' = X_1Y_1Z_2T_2 - X_2Y_2Z_1T$
$T_3' = X_1Y_2Z_2T_1 - X_2Y_1Z_1T$

Much, much, much simpler
Lange–Ruppert, Bosma–Len
Also much easier to prove.

2009 Bernstein–T. Lange:

For all fields k with $2 \neq 0$,
all $\mathbf{P}^1 \times \mathbf{P}^1$ Edwards curves E/k :
$X^2T^2 + Y^2Z^2 = Z^2T^2 + dX^2Y^2$,
all $P_1, P_2 \in E(k)$,
$P_1 = ((X_1 : Z_1), (Y_1 : T_1))$,
$P_2 = ((X_2 : Z_2), (Y_2 : T_2))$:

$(X_3 : Z_3)$ is $x(P_1 + P_2)$ or $(0 : 0)$;
$(X_3' : Z_3')$ is $x(P_1 + P_2)$ or $(0 : 0)$;
$(Y_3 : T_3)$ is $y(P_1 + P_2)$ or $(0 : 0)$;
$(Y_3' : T_3')$ is $y(P_1 + P_2)$ or $(0 : 0)$;
at most one of these is $(0 : 0)$.

$$X_3 = X_1Y_2Z_2T_1 + X_2Y_1Z_1T_2,$$
$$Z_3 = Z_1Z_2T_1T_2 + dX_1X_2Y_1Y_2,$$
$$Y_3 = Y_1Y_2Z_1Z_2 - X_1X_2T_1T_2,$$
$$T_3 = Z_1Z_2T_1T_2 - dX_1X_2Y_1Y_2,$$

$$X_3' = X_1Y_1Z_2T_2 + X_2Y_2Z_1T_1,$$
$$Z_3' = X_1X_2T_1T_2 + Y_1Y_2Z_1Z_2,$$
$$Y_3' = X_1Y_1Z_2T_2 - X_2Y_2Z_1T_1,$$
$$T_3' = X_1Y_2Z_2T_1 - X_2Y_1Z_1T_2.$$

Much, much, much simpler than
Lange–Ruppert, Bosma–Lenstra.
Also much easier to prove.

rnstein–T. Lange:

ields k with $2 \neq 0$,

$\mathbf{P}^1$ Edwards curves E/k :

$Y^2Z^2 = Z^2T^2 + dX^2Y^2$,

$_2 \in E(k)$,

$X_1 : Z_1), (Y_1 : T_1))$,

$X_2 : Z_2), (Y_2 : T_2))$:

) is $x(P_1 + P_2)$ or $(0 : 0)$;

) is $x(P_1 + P_2)$ or $(0 : 0)$;

) is $y(P_1 + P_2)$ or $(0 : 0)$;

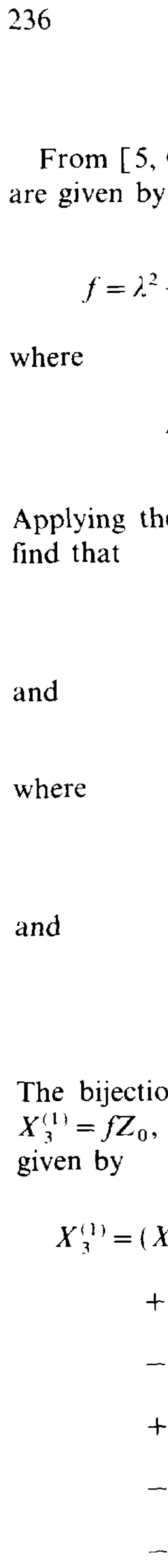
) is $y(P_1 + P_2)$ or $(0 : 0)$;

one of these is $(0 : 0)$.

$$
\begin{aligned}
X_3 &= X_1Y_2Z_2T_1 + X_2Y_1Z_1T_2,\\
Z_3 &= Z_1Z_2T_1T_2 + dX_1X_2Y_1Y_2,\\
Y_3 &= Y_1Y_2Z_1Z_2 - X_1X_2T_1T_2,\\
T_3 &= Z_1Z_2T_1T_2 - dX_1X_2Y_1Y_2,
\end{aligned}
$$

$$
\begin{aligned}
X_3' &= X_1Y_1Z_2T_2 + X_2Y_2Z_1T_1,\\
Z_3' &= X_1X_2T_1T_2 + Y_1Y_2Z_1Z_2,\\
Y_3' &= X_1Y_1Z_2T_2 - X_2Y_2Z_1T_1,\\
T_3' &= X_1Y_2Z_2T_1 - X_2Y_1Z_1T_2.
\end{aligned}
$$

Much, much, much simpler than Lange–Ruppert, Bosma–Lenstra. Also much easier to prove.



236

From [5,

are given by

$f = \lambda^2$

where

Applying th

find that

and

where

and

The bijectio

$X_3^{(1)} = fZ_0,$

given by

$X_3^{(1)} = (X$

. Lange:

h $2 \neq 0$,

rds curves E/k :

$Z^2T^2 + dX^2Y^2$,

$Y_1 : T_1))$,

$Y_2 : T_2))$:

$+ P_2)$ or $(0 : 0)$;

$+ P_2)$ or $(0 : 0)$;

$- P_2)$ or $(0 : 0)$;

$- P_2)$ or $(0 : 0)$;

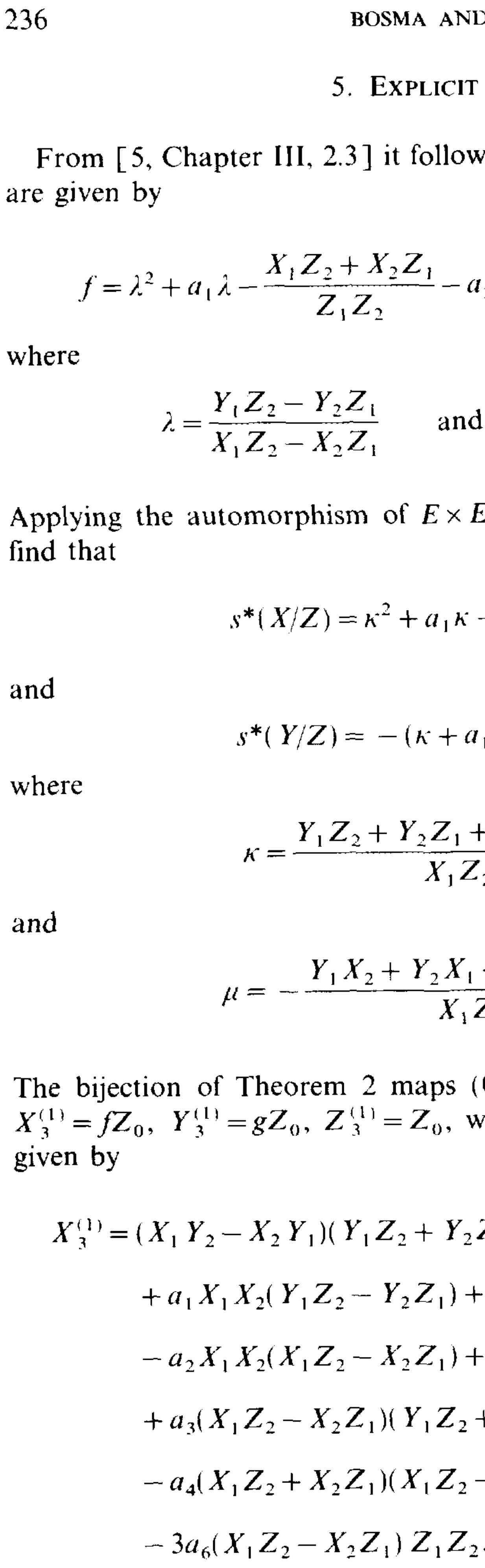
ese is $(0 : 0)$.

$$X_3 = X_1Y_2Z_2T_1 + X_2Y_1Z_1T_2,$$
$$Z_3 = Z_1Z_2T_1T_2 + dX_1X_2Y_1Y_2,$$
$$Y_3 = Y_1Y_2Z_1Z_2 - X_1X_2T_1T_2,$$
$$T_3 = Z_1Z_2T_1T_2 - dX_1X_2Y_1Y_2,$$

$$X_3' = X_1Y_1Z_2T_2 + X_2Y_2Z_1T_1,$$
$$Z_3' = X_1X_2T_1T_2 + Y_1Y_2Z_1Z_2,$$
$$Y_3' = X_1Y_1Z_2T_2 - X_2Y_2Z_1T_1,$$
$$T_3' = X_1Y_2Z_2T_1 - X_2Y_1Z_1T_2.$$

Much, much, much simpler than Lange–Ruppert, Bosma–Lenstra.

Also much easier to prove.



236 BOSMA AND

5. EXPLICIT

From [5, Chapter III, 2.3] it follow
are given by

$$f = \lambda^2 + a_1\lambda - \frac{X_1Z_2 + X_2Z_1}{Z_1Z_2} - a$$

where

$$\lambda = \frac{Y_1Z_2 - Y_2Z_1}{X_1Z_2 - X_2Z_1} \qquad \text{and}$$

Applying the automorphism of $E \times E$
find that

$$s^*(X/Z) = \kappa^2 + a_1\kappa -$$

and

$$s^*(Y/Z) = -(\kappa + a$$

where

$$\kappa = \frac{Y_1Z_2 + Y_2Z_1 +}{X_1Z}$$

and

$$\mu = -\frac{Y_1X_2 + Y_2X_1}{X_1Z}$$

The bijection of Theorem 2 maps (
$X_3^{(1)} = fZ_0$, $Y_3^{(1)} = gZ_0$, $Z_3^{(1)} = Z_0$, w
given by

$$X_3^{(1)} = (X_1Y_2 - X_2Y_1)(Y_1Z_2 + Y_2$$
$$+ a_1X_1X_2(Y_1Z_2 - Y_2Z_1) +$$
$$- a_2X_1X_2(X_1Z_2 - X_2Z_1) +$$
$$+ a_3(X_1Z_2 - X_2Z_1)(Y_1Z_2 +$$
$$- a_4(X_1Z_2 + X_2Z_1)(X_1Z_2 -$$
$$- 3a_6(X_1Z_2 - X_2Z_1)Z_1Z_2$$

E/k :
X^2Y^2,

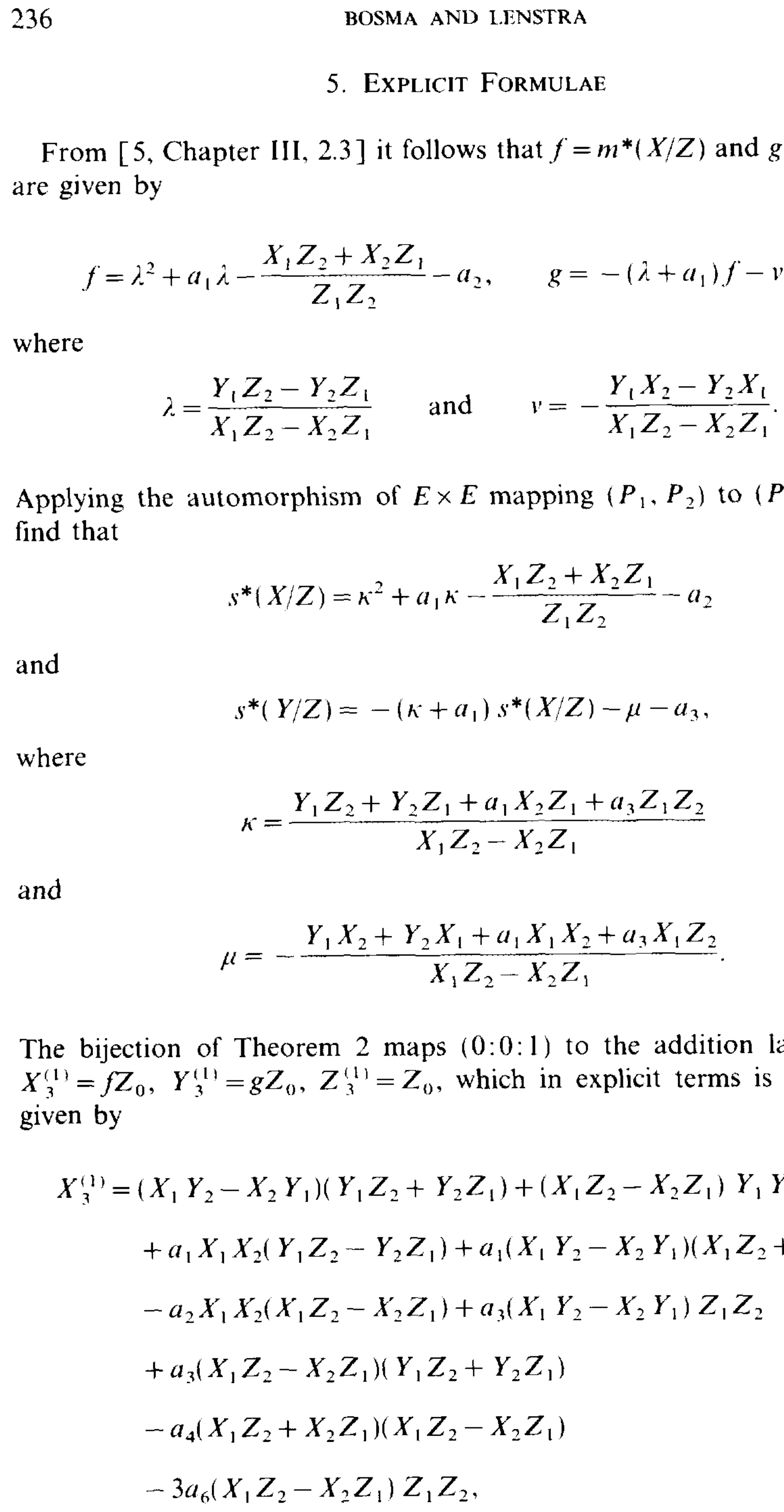
0 : 0);
0 : 0);
: 0);
: 0);
0).

$$X_3 = X_1Y_2Z_2T_1 + X_2Y_1Z_1T_2,$$
$$Z_3 = Z_1Z_2T_1T_2 + dX_1X_2Y_1Y_2,$$
$$Y_3 = Y_1Y_2Z_1Z_2 - X_1X_2T_1T_2,$$
$$T_3 = Z_1Z_2T_1T_2 - dX_1X_2Y_1Y_2,$$

$$X_3' = X_1Y_1Z_2T_2 + X_2Y_2Z_1T_1,$$
$$Z_3' = X_1X_2T_1T_2 + Y_1Y_2Z_1Z_2,$$
$$Y_3' = X_1Y_1Z_2T_2 - X_2Y_2Z_1T_1,$$
$$T_3' = X_1Y_2Z_2T_1 - X_2Y_1Z_1T_2.$$

Much, much, much simpler than Lange–Ruppert, Bosma–Lenstra.

Also much easier to prove.



236 BOSMA AND LENSTRA

5. EXPLICIT FORMULAE

From [5, Chapter III, 2.3] it follows that $f = m^*(X/Z)$ and g are given by

$$f = \lambda^2 + a_1\lambda - \frac{X_1Z_2 + X_2Z_1}{Z_1Z_2} - a_2, \qquad g = -(\lambda + a_1)f - \nu$$

where

$$\lambda = \frac{Y_1Z_2 - Y_2Z_1}{X_1Z_2 - X_2Z_1} \quad \text{and} \quad \nu = -\frac{Y_1X_2 - Y_2X_1}{X_1Z_2 - X_2Z_1}.$$

Applying the automorphism of $E \times E$ mapping (P_1, P_2) to $(P$ find that

$$s^*(X/Z) = \kappa^2 + a_1\kappa - \frac{X_1Z_2 + X_2Z_1}{Z_1Z_2} - a_2$$

and

$$s^*(Y/Z) = -(\kappa + a_1)\, s^*(X/Z) - \mu - a_3,$$

where

$$\kappa = \frac{Y_1Z_2 + Y_2Z_1 + a_1X_2Z_1 + a_3Z_1Z_2}{X_1Z_2 - X_2Z_1}$$

and

$$\mu = -\frac{Y_1X_2 + Y_2X_1 + a_1X_1X_2 + a_3X_1Z_2}{X_1Z_2 - X_2Z_1}.$$

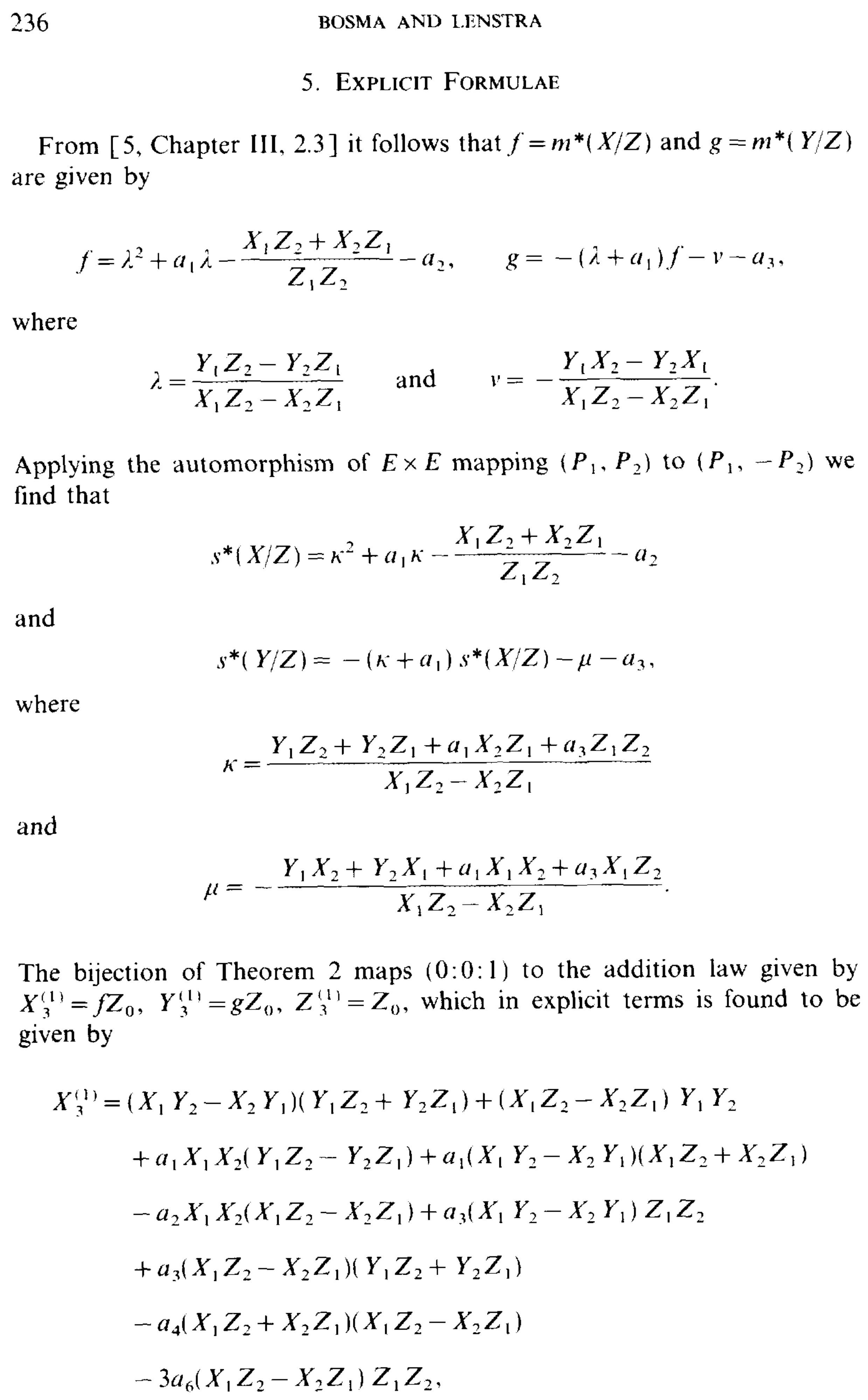
The bijection of Theorem 2 maps $(0{:}0{:}1)$ to the addition la $X_3^{(1)} = fZ_0$, $Y_3^{(1)} = gZ_0$, $Z_3^{(1)} = Z_0$, which in explicit terms is given by

$$\begin{aligned} X_3^{(1)} = {} & (X_1Y_2 - X_2Y_1)(Y_1Z_2 + Y_2Z_1) + (X_1Z_2 - X_2Z_1)\, Y_1 Y \\ & + a_1X_1X_2(Y_1Z_2 - Y_2Z_1) + a_1(X_1Y_2 - X_2Y_1)(X_1Z_2 + \\ & - a_2X_1X_2(X_1Z_2 - X_2Z_1) + a_3(X_1Y_2 - X_2Y_1)\, Z_1Z_2 \\ & + a_3(X_1Z_2 - X_2Z_1)(Y_1Z_2 + Y_2Z_1) \\ & - a_4(X_1Z_2 + X_2Z_1)(X_1Z_2 - X_2Z_1) \\ & - 3a_6(X_1Z_2 - X_2Z_1)\, Z_1Z_2, \end{aligned}$$

$$
\begin{aligned}
X_3 &= X_1Y_2Z_2T_1 + X_2Y_1Z_1T_2,\\
Z_3 &= Z_1Z_2T_1T_2 + dX_1X_2Y_1Y_2,\\
Y_3 &= Y_1Y_2Z_1Z_2 - X_1X_2T_1T_2,\\
T_3 &= Z_1Z_2T_1T_2 - dX_1X_2Y_1Y_2,
\end{aligned}
$$

$$
\begin{aligned}
X_3' &= X_1Y_1Z_2T_2 + X_2Y_2Z_1T_1,\\
Z_3' &= X_1X_2T_1T_2 + Y_1Y_2Z_1Z_2,\\
Y_3' &= X_1Y_1Z_2T_2 - X_2Y_2Z_1T_1,\\
T_3' &= X_1Y_2Z_2T_1 - X_2Y_1Z_1T_2.
\end{aligned}
$$

Much, much, much simpler than Lange–Ruppert, Bosma–Lenstra. Also much easier to prove.



236 BOSMA AND LENSTRA

5. EXPLICIT FORMULAE

From [5, Chapter III, 2.3] it follows that $f = m^*(X/Z)$ and $g = m^*(Y/Z)$ are given by

$$f = \lambda^2 + a_1\lambda - \frac{X_1Z_2 + X_2Z_1}{Z_1Z_2} - a_2, \qquad g = -(\lambda + a_1)f - \nu - a_3,$$

where

$$\lambda = \frac{Y_1Z_2 - Y_2Z_1}{X_1Z_2 - X_2Z_1} \qquad \text{and} \qquad \nu = -\frac{Y_1X_2 - Y_2X_1}{X_1Z_2 - X_2Z_1}.$$

Applying the automorphism of $E \times E$ mapping (P_1, P_2) to $(P_1, -P_2)$ we find that

$$s^*(X/Z) = \kappa^2 + a_1\kappa - \frac{X_1Z_2 + X_2Z_1}{Z_1Z_2} - a_2$$

and

$$s^*(Y/Z) = -(\kappa + a_1)\, s^*(X/Z) - \mu - a_3,$$

where

$$\kappa = \frac{Y_1Z_2 + Y_2Z_1 + a_1X_2Z_1 + a_3Z_1Z_2}{X_1Z_2 - X_2Z_1}$$

and

$$\mu = -\frac{Y_1X_2 + Y_2X_1 + a_1X_1X_2 + a_3X_1Z_2}{X_1Z_2 - X_2Z_1}.$$

The bijection of Theorem 2 maps $(0:0:1)$ to the addition law given by $X_3^{(1)} = fZ_0$, $Y_3^{(1)} = gZ_0$, $Z_3^{(1)} = Z_0$, which in explicit terms is found to be given by

$$
\begin{aligned}
X_3^{(1)} = {} & (X_1Y_2 - X_2Y_1)(Y_1Z_2 + Y_2Z_1) + (X_1Z_2 - X_2Z_1)\,Y_1Y_2\\
& + a_1X_1X_2(Y_1Z_2 - Y_2Z_1) + a_1(X_1Y_2 - X_2Y_1)(X_1Z_2 + X_2Z_1)\\
& - a_2X_1X_2(X_1Z_2 - X_2Z_1) + a_3(X_1Y_2 - X_2Y_1)\,Z_1Z_2\\
& + a_3(X_1Z_2 - X_2Z_1)(Y_1Z_2 + Y_2Z_1)\\
& - a_4(X_1Z_2 + X_2Z_1)(X_1Z_2 - X_2Z_1)\\
& - 3a_6(X_1Z_2 - X_2Z_1)\,Z_1Z_2,
\end{aligned}
$$

$_1Y_2Z_2T_1 + X_2Y_1Z_1T_2$,

$Z_2T_1T_2 + dX_1X_2Y_1Y_2$,

$Y_2Z_1Z_2 - X_1X_2T_1T_2$,

$Z_2T_1T_2 - dX_1X_2Y_1Y_2$,

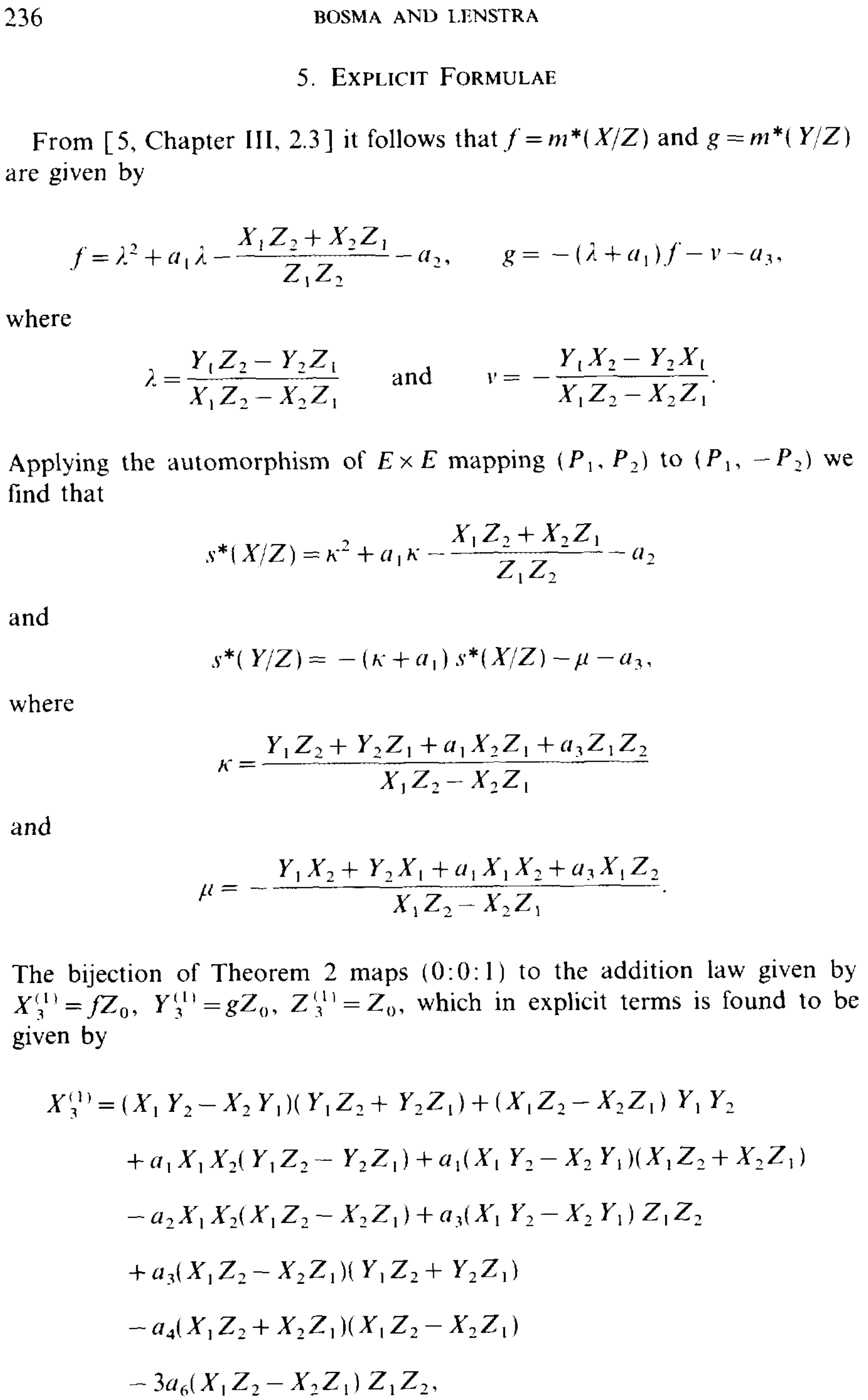
$_1Y_1Z_2T_2 + X_2Y_2Z_1T_1$,

$_1X_2T_1T_2 + Y_1Y_2Z_1Z_2$,

$Y_1Z_2T_2 - X_2Y_2Z_1T_1$,

$Y_2Z_2T_1 - X_2Y_1Z_1T_2$.

nuch, much simpler than
Ruppert, Bosma–Lenstra.
ch easier to prove.



5. EXPLICIT FORMULAE

From [5, Chapter III, 2.3] it follows that $f = m^*(X/Z)$ and $g = m^*(Y/Z)$ are given by

$$f = \lambda^2 + a_1\lambda - \frac{X_1Z_2 + X_2Z_1}{Z_1Z_2} - a_2, \qquad g = -(\lambda + a_1)f - \nu - a_3,$$

where

$$\lambda = \frac{Y_1Z_2 - Y_2Z_1}{X_1Z_2 - X_2Z_1} \quad \text{and} \quad \nu = -\frac{Y_1X_2 - Y_2X_1}{X_1Z_2 - X_2Z_1}.$$

Applying the automorphism of $E \times E$ mapping (P_1, P_2) to $(P_1, -P_2)$ we find that

$$s^*(X/Z) = \kappa^2 + a_1\kappa - \frac{X_1Z_2 + X_2Z_1}{Z_1Z_2} - a_2$$

and

$$s^*(Y/Z) = -(\kappa + a_1)\,s^*(X/Z) - \mu - a_3,$$

where

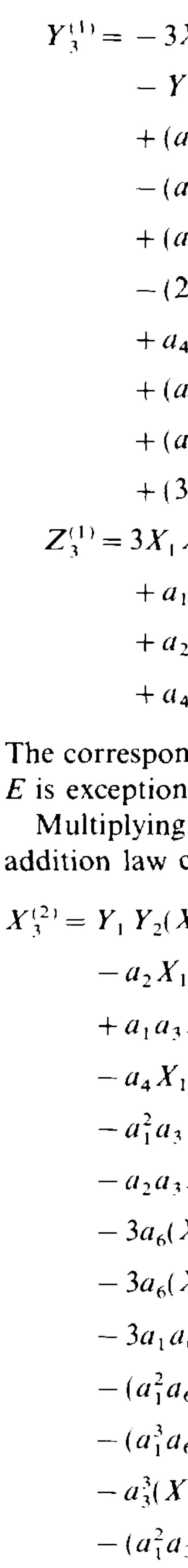
$$\kappa = \frac{Y_1Z_2 + Y_2Z_1 + a_1X_2Z_1 + a_3Z_1Z_2}{X_1Z_2 - X_2Z_1}$$

and

$$\mu = -\frac{Y_1X_2 + Y_2X_1 + a_1X_1X_2 + a_3X_1Z_2}{X_1Z_2 - X_2Z_1}.$$

The bijection of Theorem 2 maps $(0:0:1)$ to the addition law given by $X_3^{(1)} = fZ_0$, $Y_3^{(1)} = gZ_0$, $Z_3^{(1)} = Z_0$, which in explicit terms is found to be given by

$$\begin{aligned}
X_3^{(1)} = {} & (X_1Y_2 - X_2Y_1)(Y_1Z_2 + Y_2Z_1) + (X_1Z_2 - X_2Z_1)\,Y_1Y_2 \\
& + a_1X_1X_2(Y_1Z_2 - Y_2Z_1) + a_1(X_1Y_2 - X_2Y_1)(X_1Z_2 + X_2Z_1) \\
& - a_2X_1X_2(X_1Z_2 - X_2Z_1) + a_3(X_1Y_2 - X_2Y_1)\,Z_1Z_2 \\
& + a_3(X_1Z_2 - X_2Z_1)(Y_1Z_2 + Y_2Z_1) \\
& - a_4(X_1Z_2 + X_2Z_1)(X_1Z_2 - X_2Z_1) \\
& - 3a_6(X_1Z_2 - X_2Z_1)\,Z_1Z_2,
\end{aligned}$$



The correspon
E is exception
Multiplying
addition law c

$- X_2Y_1Z_1T_2,$

$- dX_1X_2Y_1Y_2,$

$X_1X_2T_1T_2,$

$dX_1X_2Y_1Y_2,$

$- X_2Y_2Z_1T_1,$

$- Y_1Y_2Z_1Z_2,$

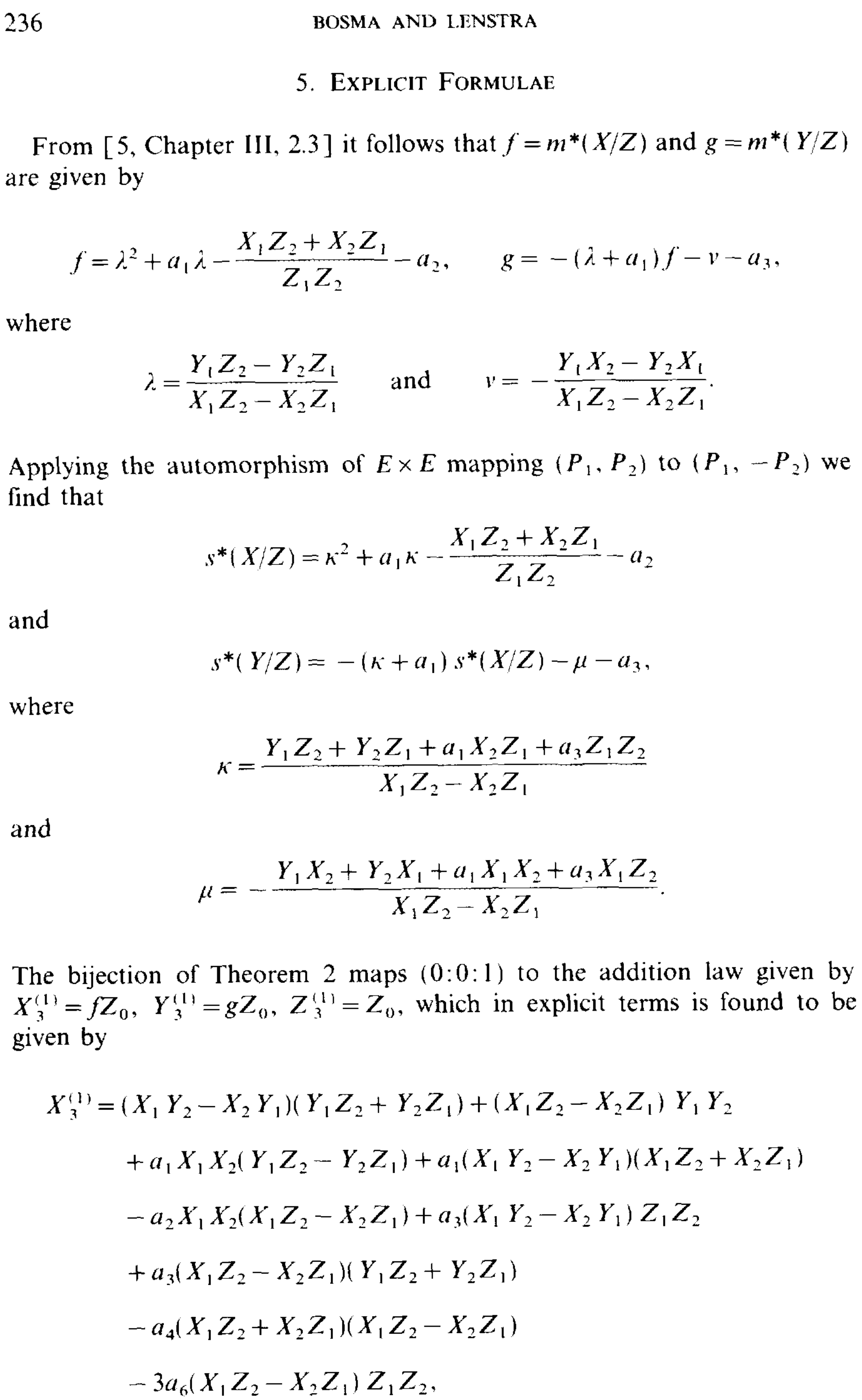
$X_2Y_2Z_1T_1,$

$X_2Y_1Z_1T_2.$

h simpler than

osma–Lenstra.

o prove.



5. Explicit Formulae

From [5, Chapter III, 2.3] it follows that $f = m^*(X/Z)$ and $g = m^*(Y/Z)$ are given by

$$f = \lambda^2 + a_1\lambda - \frac{X_1Z_2 + X_2Z_1}{Z_1Z_2} - a_2, \qquad g = -(\lambda + a_1)f - \nu - a_3,$$

where

$$\lambda = \frac{Y_1Z_2 - Y_2Z_1}{X_1Z_2 - X_2Z_1} \quad \text{and} \quad \nu = -\frac{Y_1X_2 - Y_2X_1}{X_1Z_2 - X_2Z_1}.$$

Applying the automorphism of $E \times E$ mapping (P_1, P_2) to $(P_1, -P_2)$ we find that

$$s^*(X/Z) = \kappa^2 + a_1\kappa - \frac{X_1Z_2 + X_2Z_1}{Z_1Z_2} - a_2$$

and

$$s^*(Y/Z) = -(\kappa + a_1)\, s^*(X/Z) - \mu - a_3,$$

where

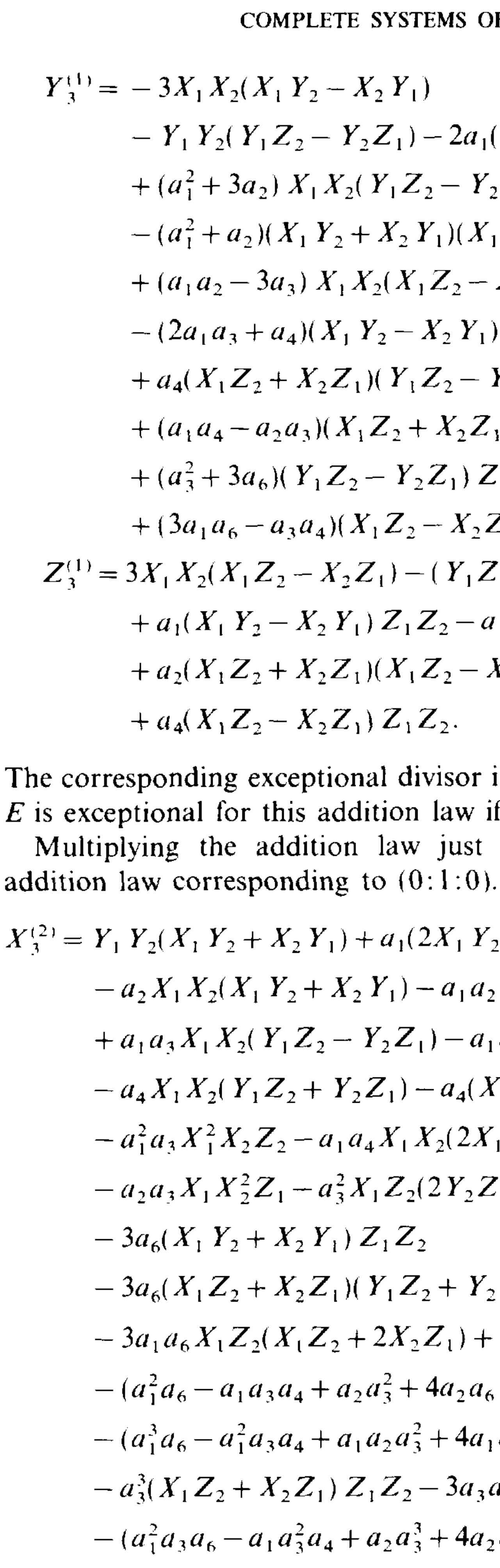
$$\kappa = \frac{Y_1Z_2 + Y_2Z_1 + a_1X_2Z_1 + a_3Z_1Z_2}{X_1Z_2 - X_2Z_1}$$

and

$$\mu = -\frac{Y_1X_2 + Y_2X_1 + a_1X_1X_2 + a_3X_1Z_2}{X_1Z_2 - X_2Z_1}.$$

The bijection of Theorem 2 maps $(0:0:1)$ to the addition law given by $X_3^{(1)} = fZ_0$, $Y_3^{(1)} = gZ_0$, $Z_3^{(1)} = Z_0$, which in explicit terms is found to be given by

$$\begin{aligned} X_3^{(1)} = {} & (X_1Y_2 - X_2Y_1)(Y_1Z_2 + Y_2Z_1) + (X_1Z_2 - X_2Z_1)\,Y_1Y_2 \\ & + a_1X_1X_2(Y_1Z_2 - Y_2Z_1) + a_1(X_1Y_2 - X_2Y_1)(X_1Z_2 + X_2Z_1) \\ & - a_2X_1X_2(X_1Z_2 - X_2Z_1) + a_3(X_1Y_2 - X_2Y_1)\,Z_1Z_2 \\ & + a_3(X_1Z_2 - X_2Z_1)(Y_1Z_2 + Y_2Z_1) \\ & - a_4(X_1Z_2 + X_2Z_1)(X_1Z_2 - X_2Z_1) \\ & - 3a_6(X_1Z_2 - X_2Z_1)\,Z_1Z_2, \end{aligned}$$



$$\begin{aligned} Y_3^{(1)} = {} & -3X_1X_2(X_1Y_2 - X_2Y_1) \\ & - Y_1Y_2(Y_1Z_2 - Y_2Z_1) - 2a_1(\\ & + (a_1^2 + 3a_2)\,X_1X_2(Y_1Z_2 - Y_2 \\ & - (a_1^2 + a_2)(X_1Y_2 + X_2Y_1)(X_1 \\ & + (a_1a_2 - 3a_3)\,X_1X_2(X_1Z_2 - \\ & - (2a_1a_3 + a_4)(X_1Y_2 - X_2Y_1) \\ & + a_4(X_1Z_2 + X_2Z_1)(Y_1Z_2 - \\ & + (a_1a_4 - a_2a_3)(X_1Z_2 + X_2Z_1 \\ & + (a_3^2 + 3a_6)(Y_1Z_2 - Y_2Z_1)\,Z \\ & + (3a_1a_6 - a_3a_4)(X_1Z_2 - X_2Z \end{aligned}$$

$$\begin{aligned} Z_3^{(1)} = {} & 3X_1X_2(X_1Z_2 - X_2Z_1) - (Y_1Z \\ & + a_1(X_1Y_2 - X_2Y_1)\,Z_1Z_2 - a \\ & + a_2(X_1Z_2 + X_2Z_1)(X_1Z_2 - \\ & + a_4(X_1Z_2 - X_2Z_1)\,Z_1Z_2. \end{aligned}$$

The corresponding exceptional divisor i
E is exceptional for this addition law if
Multiplying the addition law just
addition law corresponding to $(0:1:0)$.

$$\begin{aligned} X_3^{(2)} = {} & Y_1Y_2(X_1Y_2 + X_2Y_1) + a_1(2X_1Y_2 \\ & - a_2X_1X_2(X_1Y_2 + X_2Y_1) - a_1a_2 \\ & + a_1a_3X_1X_2(Y_1Z_2 - Y_2Z_1) - a_1 \\ & - a_4X_1X_2(Y_1Z_2 + Y_2Z_1) - a_4(X \\ & - a_1^2a_3X_1^2X_2Z_2 - a_1a_4X_1X_2(2X_1 \\ & - a_2a_3X_1X_2^2Z_1 - a_3^2X_1Z_2(2Y_2Z \\ & - 3a_6(X_1Y_2 + X_2Y_1)\,Z_1Z_2 \\ & - 3a_6(X_1Z_2 + X_2Z_1)(Y_1Z_2 + Y_2 \\ & - 3a_1a_6X_1Z_2(X_1Z_2 + 2X_2Z_1) + \\ & - (a_1^2a_6 - a_1a_3a_4 + a_2a_3^2 + 4a_2a_6 \\ & - (a_1^3a_6 - a_1^2a_3a_4 + a_1a_2a_3^2 + 4a_1 \\ & - a_3^3(X_1Z_2 + X_2Z_1)\,Z_1Z_2 - 3a_3a \\ & - (a_1^2a_3a_6 - a_1a_3^2a_4 + a_2a_3^3 + 4a_2 \end{aligned}$$

$2,$

$Y_2,$

$2,$

$Y_2,$

$1,$

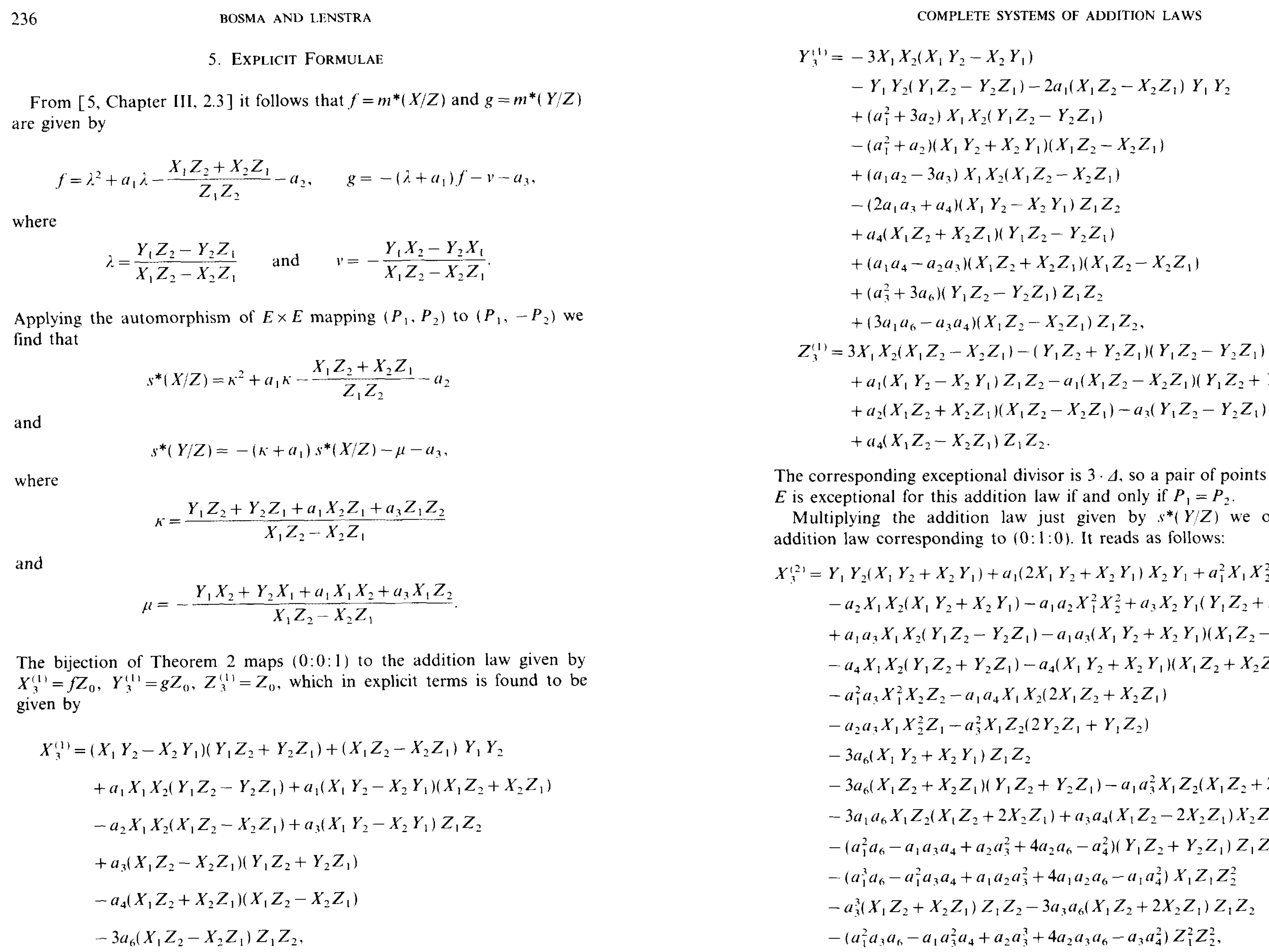
$2,$

$1,$

$2.$

than

stra.



5. EXPLICIT FORMULAE

From [5, Chapter III, 2.3] it follows that $f = m^*(X/Z)$ and $g = m^*(Y/Z)$ are given by

$$f = \lambda^2 + a_1\lambda - \frac{X_1Z_2 + X_2Z_1}{Z_1Z_2} - a_2, \qquad g = -(\lambda + a_1)f - \nu - a_3,$$

where

$$\lambda = \frac{Y_1Z_2 - Y_2Z_1}{X_1Z_2 - X_2Z_1} \qquad \text{and} \qquad \nu = -\frac{Y_1X_2 - Y_2X_1}{X_1Z_2 - X_2Z_1}.$$

Applying the automorphism of $E \times E$ mapping (P_1, P_2) to $(P_1, -P_2)$ we find that

$$s^*(X/Z) = \kappa^2 + a_1\kappa - \frac{X_1Z_2 + X_2Z_1}{Z_1Z_2} - a_2$$

and

$$s^*(Y/Z) = -(\kappa + a_1)\, s^*(X/Z) - \mu - a_3,$$

where

$$\kappa = \frac{Y_1Z_2 + Y_2Z_1 + a_1X_2Z_1 + a_3Z_1Z_2}{X_1Z_2 - X_2Z_1}$$

and

$$\mu = -\frac{Y_1X_2 + Y_2X_1 + a_1X_1X_2 + a_3X_1Z_2}{X_1Z_2 - X_2Z_1}.$$

The bijection of Theorem 2 maps $(0:0:1)$ to the addition law given by $X_3^{(1)} = fZ_0$, $Y_3^{(1)} = gZ_0$, $Z_3^{(1)} = Z_0$, which in explicit terms is found to be given by

$$\begin{aligned} X_3^{(1)} = {} & (X_1Y_2 - X_2Y_1)(Y_1Z_2 + Y_2Z_1) + (X_1Z_2 - X_2Z_1)\, Y_1Y_2 \\ & + a_1X_1X_2(Y_1Z_2 - Y_2Z_1) + a_1(X_1Y_2 - X_2Y_1)(X_1Z_2 + X_2Z_1) \\ & - a_2X_1X_2(X_1Z_2 - X_2Z_1) + a_3(X_1Y_2 - X_2Y_1)\, Z_1Z_2 \\ & + a_3(X_1Z_2 - X_2Z_1)(Y_1Z_2 + Y_2Z_1) \\ & - a_4(X_1Z_2 + X_2Z_1)(X_1Z_2 - X_2Z_1) \\ & - 3a_6(X_1Z_2 - X_2Z_1)\, Z_1Z_2, \end{aligned}$$

$$\begin{aligned} Y_3^{(1)} = {} & -3X_1X_2(X_1Y_2 - X_2Y_1) \\ & - Y_1Y_2(Y_1Z_2 - Y_2Z_1) - 2a_1(X_1Z_2 - X_2Z_1)\, Y_1Y_2 \\ & + (a_1^2 + 3a_2)\, X_1X_2(Y_1Z_2 - Y_2Z_1) \\ & - (a_1^2 + a_2)(X_1Y_2 + X_2Y_1)(X_1Z_2 - X_2Z_1) \\ & + (a_1a_2 - 3a_3)\, X_1X_2(X_1Z_2 - X_2Z_1) \\ & - (2a_1a_3 + a_4)(X_1Y_2 - X_2Y_1)\, Z_1Z_2 \\ & + a_4(X_1Z_2 + X_2Z_1)(Y_1Z_2 - Y_2Z_1) \\ & + (a_1a_4 - a_2a_3)(X_1Z_2 + X_2Z_1)(X_1Z_2 - X_2Z_1) \\ & + (a_3^2 + 3a_6)(Y_1Z_2 - Y_2Z_1)\, Z_1Z_2 \\ & + (3a_1a_6 - a_3a_4)(X_1Z_2 - X_2Z_1)\, Z_1Z_2, \\ Z_3^{(1)} = {} & 3X_1X_2(X_1Z_2 - X_2Z_1) - (Y_1Z_2 + Y_2Z_1)(Y_1Z_2 - Y_2Z_1) \\ & + a_1(X_1Y_2 - X_2Y_1)\, Z_1Z_2 - a_1(X_1Z_2 - X_2Z_1)(Y_1Z_2 + \\ & + a_2(X_1Z_2 + X_2Z_1)(X_1Z_2 - X_2Z_1) - a_3(Y_1Z_2 - Y_2Z_1) \\ & + a_4(X_1Z_2 - X_2Z_1)\, Z_1Z_2. \end{aligned}$$

The corresponding exceptional divisor is $3 \cdot \varDelta$, so a pair of points
E is exceptional for this addition law if and only if $P_1 = P_2$.

Multiplying the addition law just given by $s^*(Y/Z)$ we o
addition law corresponding to $(0:1:0)$. It reads as follows:

$$\begin{aligned} X_3^{(2)} = {} & Y_1Y_2(X_1Y_2 + X_2Y_1) + a_1(2X_1Y_2 + X_2Y_1)\, X_2Y_1 + a_1^2X_1X \\ & - a_2X_1X_2(X_1Y_2 + X_2Y_1) - a_1a_2X_1^2X_2^2 + a_3X_2Y_1(Y_1Z_2 + \\ & + a_1a_3X_1X_2(Y_1Z_2 - Y_2Z_1) - a_1a_3(X_1Y_2 + X_2Y_1)(X_1Z_2 - \\ & - a_4X_1X_2(Y_1Z_2 + Y_2Z_1) - a_4(X_1Y_2 + X_2Y_1)(X_1Z_2 + X_2Z \\ & - a_1^2a_3X_1^2X_2Z_2 - a_1a_4X_1X_2(2X_1Z_2 + X_2Z_1) \\ & - a_2a_3X_1X_2^2Z_1 - a_3^2X_1Z_2(2Y_2Z_1 + Y_1Z_2) \\ & - 3a_6(X_1Y_2 + X_2Y_1)\, Z_1Z_2 \\ & - 3a_6(X_1Z_2 + X_2Z_1)(Y_1Z_2 + Y_2Z_1) - a_1a_3^2X_1Z_2(X_1Z_2 + \\ & - 3a_1a_6X_1Z_2(X_1Z_2 + 2X_2Z_1) + a_3a_4(X_1Z_2 - 2X_2Z_1)\, X_2Z \\ & - (a_1^2a_6 - a_1a_3a_4 + a_2a_3^2 + 4a_2a_6 - a_4^2)(Y_1Z_2 + Y_2Z_1)\, Z_1Z \\ & - (a_1^3a_6 - a_1^2a_3a_4 + a_1a_2a_3^2 + 4a_1a_2a_6 - a_1a_4^2)\, X_1Z_1Z_2^2 \\ & - a_3^3(X_1Z_2 + X_2Z_1)\, Z_1Z_2 - 3a_3a_6(X_1Z_2 + 2X_2Z_1)\, Z_1Z_2 \\ & - (a_1^2a_3a_6 - a_1a_3^2a_4 + a_2a_3^3 + 4a_2a_3a_6 - a_3a_4^2)\, Z_1^2Z_2^2, \end{aligned}$$

5. EXPLICIT FORMULAE

From [5, Chapter III, 2.3] it follows that $f = m^*(X/Z)$ and $g = m^*(Y/Z)$ are given by

$$f = \lambda^2 + a_1\lambda - \frac{X_1Z_2 + X_2Z_1}{Z_1Z_2} - a_2, \qquad g = -(\lambda + a_1)f - \nu - a_3,$$

where

$$\lambda = \frac{Y_1Z_2 - Y_2Z_1}{X_1Z_2 - X_2Z_1} \quad \text{and} \quad \nu = -\frac{Y_1X_2 - Y_2X_1}{X_1Z_2 - X_2Z_1}.$$

Applying the automorphism of $E \times E$ mapping (P_1, P_2) to $(P_1, -P_2)$ we find that

$$s^*(X/Z) = \kappa^2 + a_1\kappa - \frac{X_1Z_2 + X_2Z_1}{Z_1Z_2} - a_2$$

and

$$s^*(Y/Z) = -(\kappa + a_1)\, s^*(X/Z) - \mu - a_3,$$

where

$$\kappa = \frac{Y_1Z_2 + Y_2Z_1 + a_1X_2Z_1 + a_3Z_1Z_2}{X_1Z_2 - X_2Z_1}$$

and

$$\mu = -\frac{Y_1X_2 + Y_2X_1 + a_1X_1X_2 + a_3X_1Z_2}{X_1Z_2 - X_2Z_1}.$$

The bijection of Theorem 2 maps $(0:0:1)$ to the addition law given by $X_3^{(1)} = fZ_0$, $Y_3^{(1)} = gZ_0$, $Z_3^{(1)} = Z_0$, which in explicit terms is found to be given by

$$\begin{aligned}
X_3^{(1)} = {} & (X_1Y_2 - X_2Y_1)(Y_1Z_2 + Y_2Z_1) + (X_1Z_2 - X_2Z_1)\, Y_1Y_2 \\
& + a_1X_1X_2(Y_1Z_2 - Y_2Z_1) + a_1(X_1Y_2 - X_2Y_1)(X_1Z_2 + X_2Z_1) \\
& - a_2X_1X_2(X_1Z_2 - X_2Z_1) + a_3(X_1Y_2 - X_2Y_1)\, Z_1Z_2 \\
& + a_3(X_1Z_2 - X_2Z_1)(Y_1Z_2 + Y_2Z_1) \\
& - a_4(X_1Z_2 + X_2Z_1)(X_1Z_2 - X_2Z_1) \\
& - 3a_6(X_1Z_2 - X_2Z_1)\, Z_1Z_2,
\end{aligned}$$

$$\begin{aligned}
Y_3^{(1)} = {} & -3X_1X_2(X_1Y_2 - X_2Y_1) \\
& - Y_1Y_2(Y_1Z_2 - Y_2Z_1) - 2a_1(X_1Z_2 - X_2Z_1)\, Y_1Y_2 \\
& + (a_1^2 + 3a_2)\, X_1X_2(Y_1Z_2 - Y_2Z_1) \\
& - (a_1^2 + a_2)(X_1Y_2 + X_2Y_1)(X_1Z_2 - X_2Z_1) \\
& + (a_1a_2 - 3a_3)\, X_1X_2(X_1Z_2 - X_2Z_1) \\
& - (2a_1a_3 + a_4)(X_1Y_2 - X_2Y_1)\, Z_1Z_2 \\
& + a_4(X_1Z_2 + X_2Z_1)(Y_1Z_2 - Y_2Z_1) \\
& + (a_1a_4 - a_2a_3)(X_1Z_2 + X_2Z_1)(X_1Z_2 - X_2Z_1) \\
& + (a_3^2 + 3a_6)(Y_1Z_2 - Y_2Z_1)\, Z_1Z_2 \\
& + (3a_1a_6 - a_3a_4)(X_1Z_2 - X_2Z_1)\, Z_1Z_2, \\
Z_3^{(1)} = {} & 3X_1X_2(X_1Z_2 - X_2Z_1) - (Y_1Z_2 + Y_2Z_1)(Y_1Z_2 - Y_2Z_1) \\
& + a_1(X_1Y_2 - X_2Y_1)\, Z_1Z_2 - a_1(X_1Z_2 - X_2Z_1)(Y_1Z_2 + Y_2Z_1) \\
& + a_2(X_1Z_2 + X_2Z_1)(X_1Z_2 - X_2Z_1) - a_3(Y_1Z_2 - Y_2Z_1)\, Z_1Z_2 \\
& + a_4(X_1Z_2 - X_2Z_1)\, Z_1Z_2.
\end{aligned}$$

The corresponding exceptional divisor is $3 \cdot \Delta$, so a pair of points P_1, P_2 on E is exceptional for this addition law if and only if $P_1 = P_2$.

Multiplying the addition law just given by $s^*(Y/Z)$ we obtain the addition law corresponding to $(0:1:0)$. It reads as follows:

$$\begin{aligned}
X_3^{(2)} = {} & Y_1Y_2(X_1Y_2 + X_2Y_1) + a_1(2X_1Y_2 + X_2Y_1)\, X_2Y_1 + a_1^2X_1X_2^2Y_1 \\
& - a_2X_1X_2(X_1Y_2 + X_2Y_1) - a_1a_2X_1^2X_2^2 + a_3X_2Y_1(Y_1Z_2 + 2Y_2Z_1) \\
& + a_1a_3X_1X_2(Y_1Z_2 - Y_2Z_1) - a_1a_3(X_1Y_2 + X_2Y_1)(X_1Z_2 - X_2Z_1) \\
& - a_4X_1X_2(Y_1Z_2 + Y_2Z_1) - a_4(X_1Y_2 + X_2Y_1)(X_1Z_2 + X_2Z_1) \\
& - a_1^2a_3X_1^2X_2Z_2 - a_1a_4X_1X_2(2X_1Z_2 + X_2Z_1) \\
& - a_2a_3X_1X_2^2Z_1 - a_3^2X_1Z_2(2Y_2Z_1 + Y_1Z_2) \\
& - 3a_6(X_1Y_2 + X_2Y_1)\, Z_1Z_2 \\
& - 3a_6(X_1Z_2 + X_2Z_1)(Y_1Z_2 + Y_2Z_1) - a_1a_3^2X_1Z_2(X_1Z_2 + 2X_2Z_1) \\
& - 3a_1a_6X_1Z_2(X_1Z_2 + 2X_2Z_1) + a_3a_4(X_1Z_2 - 2X_2Z_1)\, X_2Z_1 \\
& - (a_1^2a_6 - a_1a_3a_4 + a_2a_3^2 + 4a_2a_6 - a_4^2)(Y_1Z_2 + Y_2Z_1)\, Z_1Z_2 \\
& - (a_1^3a_6 - a_1^2a_3a_4 + a_1a_2a_3^2 + 4a_1a_2a_6 - a_1a_4^2)\, X_1Z_1Z_2^2 \\
& - a_3^3(X_1Z_2 + X_2Z_1)\, Z_1Z_2 - 3a_3a_6(X_1Z_2 + 2X_2Z_1)\, Z_1Z_2 \\
& - (a_1^2a_3a_6 - a_1a_3^2a_4 + a_2a_3^3 + 4a_2a_3a_6 - a_3a_4^2)\, Z_1^2Z_2^2,
\end{aligned}$$

5. Explicit Formulae

Chapter III, 2.3] it follows that $f = m^*(X/Z)$ and $g = m^*(Y/Z)$

$$+ a_1\lambda - \frac{X_1Z_2 + X_2Z_1}{Z_1Z_2} - a_2, \qquad g = -(\lambda + a_1)f - \nu - a_3,$$

$$\lambda = \frac{Y_1Z_2 - Y_2Z_1}{X_1Z_2 - X_2Z_1} \qquad \text{and} \qquad \nu = -\frac{Y_1X_2 - Y_2X_1}{X_1Z_2 - X_2Z_1}.$$

e automorphism of $E \times E$ mapping (P_1, P_2) to $(P_1, -P_2)$ we

$$s^*(X/Z) = \kappa^2 + a_1\kappa - \frac{X_1Z_2 + X_2Z_1}{Z_1Z_2} - a_2$$

$$s^*(Y/Z) = -(\kappa + a_1)\, s^*(X/Z) - \mu - a_3,$$

$$\kappa = \frac{Y_1Z_2 + Y_2Z_1 + a_1X_2Z_1 + a_3Z_1Z_2}{X_1Z_2 - X_2Z_1}$$

$$\mu = -\frac{Y_1X_2 + Y_2X_1 + a_1X_1X_2 + a_3X_1Z_2}{X_1Z_2 - X_2Z_1}.$$

n of Theorem 2 maps (0:0:1) to the addition law given by $Y_3^{(1)} = gZ_0$, $Z_3^{(1)} = Z_0$, which in explicit terms is found to be

$$
\begin{aligned}
&{}_1Y_2 - X_2Y_1)(Y_1Z_2 + Y_2Z_1) + (X_1Z_2 - X_2Z_1)\,Y_1Y_2\\
&a_1X_1X_2(Y_1Z_2 - Y_2Z_1) + a_1(X_1Y_2 - X_2Y_1)(X_1Z_2 + X_2Z_1)\\
&a_2X_1X_2(X_1Z_2 - X_2Z_1) + a_3(X_1Y_2 - X_2Y_1)\,Z_1Z_2\\
&a_3(X_1Z_2 - X_2Z_1)(Y_1Z_2 + Y_2Z_1)\\
&a_4(X_1Z_2 + X_2Z_1)(X_1Z_2 - X_2Z_1)\\
&3a_6(X_1Z_2 - X_2Z_1)\,Z_1Z_2,
\end{aligned}
$$

$$
\begin{aligned}
Y_3^{(1)} = {}& -3X_1X_2(X_1Y_2 - X_2Y_1)\\
&- Y_1Y_2(Y_1Z_2 - Y_2Z_1) - 2a_1(X_1Z_2 - X_2Z_1)\,Y_1Y_2\\
&+ (a_1^2 + 3a_2)\,X_1X_2(Y_1Z_2 - Y_2Z_1)\\
&- (a_1^2 + a_2)(X_1Y_2 + X_2Y_1)(X_1Z_2 - X_2Z_1)\\
&+ (a_1a_2 - 3a_3)\,X_1X_2(X_1Z_2 - X_2Z_1)\\
&- (2a_1a_3 + a_4)(X_1Y_2 - X_2Y_1)\,Z_1Z_2\\
&+ a_4(X_1Z_2 + X_2Z_1)(Y_1Z_2 - Y_2Z_1)\\
&+ (a_1a_4 - a_2a_3)(X_1Z_2 + X_2Z_1)(X_1Z_2 - X_2Z_1)\\
&+ (a_3^2 + 3a_6)(Y_1Z_2 - Y_2Z_1)\,Z_1Z_2\\
&+ (3a_1a_6 - a_3a_4)(X_1Z_2 - X_2Z_1)\,Z_1Z_2,\\
Z_3^{(1)} = {}& 3X_1X_2(X_1Z_2 - X_2Z_1) - (Y_1Z_2 + Y_2Z_1)(Y_1Z_2 - Y_2Z_1)\\
&+ a_1(X_1Y_2 - X_2Y_1)\,Z_1Z_2 - a_1(X_1Z_2 - X_2Z_1)(Y_1Z_2 + Y_2Z_1)\\
&+ a_2(X_1Z_2 + X_2Z_1)(X_1Z_2 - X_2Z_1) - a_3(Y_1Z_2 - Y_2Z_1)\,Z_1Z_2\\
&+ a_4(X_1Z_2 - X_2Z_1)\,Z_1Z_2.
\end{aligned}
$$

The corresponding exceptional divisor is $3 \cdot \Delta$, so a pair of points P_1, P_2 on E is exceptional for this addition law if and only if $P_1 = P_2$.

Multiplying the addition law just given by $s^*(Y/Z)$ we obtain the addition law corresponding to (0:1:0). It reads as follows:

$$
\begin{aligned}
X_3^{(2)} = {}& Y_1Y_2(X_1Y_2 + X_2Y_1) + a_1(2X_1Y_2 + X_2Y_1)\,X_2Y_1 + a_1^2X_1X_2^2Y_1\\
&- a_2X_1X_2(X_1Y_2 + X_2Y_1) - a_1a_2X_1^2X_2^2 + a_3X_2Y_1(Y_1Z_2 + 2Y_2Z_1)\\
&+ a_1a_3X_1X_2(Y_1Z_2 - Y_2Z_1) - a_1a_3(X_1Y_2 + X_2Y_1)(X_1Z_2 - X_2Z_1)\\
&- a_4X_1X_2(Y_1Z_2 + Y_2Z_1) - a_4(X_1Y_2 + X_2Y_1)(X_1Z_2 + X_2Z_1)\\
&- a_1^2a_3X_1^2X_2Z_2 - a_1a_4X_1X_2(2X_1Z_2 + X_2Z_1)\\
&- a_2a_3X_1X_2^2Z_1 - a_3^2X_1Z_2(2Y_2Z_1 + Y_1Z_2)\\
&- 3a_6(X_1Y_2 + X_2Y_1)\,Z_1Z_2\\
&- 3a_6(X_1Z_2 + X_2Z_1)(Y_1Z_2 + Y_2Z_1) - a_1a_3^2X_1Z_2(X_1Z_2 + 2X_2Z_1)\\
&- 3a_1a_6X_1Z_2(X_1Z_2 + 2X_2Z_1) + a_3a_4(X_1Z_2 - 2X_2Z_1)\,X_2Z_1\\
&- (a_1^2a_6 - a_1a_3a_4 + a_2a_3^2 + 4a_2a_6 - a_4^2)(Y_1Z_2 + Y_2Z_1)\,Z_1Z_2\\
&- (a_1^3a_6 - a_1^2a_3a_4 + a_1a_2a_3^2 + 4a_1a_2a_6 - a_1a_4^2)\,X_1Z_1Z_2^2\\
&- a_3^3(X_1Z_2 + X_2Z_1)\,Z_1Z_2 - 3a_3a_6(X_1Z_2 + 2X_2Z_1)\,Z_1Z_2\\
&- (a_1^2a_3a_6 - a_1a_3^2a_4 + a_2a_3^3 + 4a_2a_3a_6 - a_3a_4^2)\,Z_1^2Z_2^2,
\end{aligned}
$$

$$
\begin{aligned}
Y_3^{(2)} = {}& Y_1^2Y\\
&+ a_3\\
&+ (a_1\\
&+ (a\\
&- (a\\
&+ (3\\
&+ (3\\
&- (3\\
&+ (a\\
&+ (a\\
&- a_1^2\\
&+ (a\\
&+ 4a\\
&+ (a\\
&+ 4a\\
&+ 4a\\
Z_3^{(2)} = {}& 3X_1X\\
&+ a_1(\\
&+ a_2\\
&+ a_2(\\
&+ a_1^3\\
&+ 3a\\
&+ 2a\\
&+ 2a\\
&+ a_4(\\
&+ (a\\
&+ a_3^2\\
&+ a_1\\
&+ a_3
\end{aligned}
$$

FORMULAE

s that $f = m^*(X/Z)$ and $g = m^*(Y/Z)$

$${}_2, \qquad g = -(\lambda + a_1) f - \nu - a_3,$$

$$\nu = -\frac{Y_1X_2 - Y_2X_1}{X_1Z_2 - X_2Z_1}.$$

mapping (P_1, P_2) to $(P_1, -P_2)$ we

$$\frac{X_1Z_2 + X_2Z_1}{Z_1Z_2} - a_2$$

$${}_1)\, s^*(X/Z) - \mu - a_3,$$

$$\frac{a_1X_2Z_1 + a_3Z_1Z_2}{{}_2 - X_2Z_1}$$

$$\frac{+ a_1X_1X_2 + a_3X_1Z_2}{Z_2 - X_2Z_1}.$$

0:0:1) to the addition law given by hich in explicit terms is found to be

$$\begin{aligned}
&Z_1) + (X_1Z_2 - X_2Z_1)\, Y_1Y_2 \\
&a_1(X_1Y_2 - X_2Y_1)(X_1Z_2 + X_2Z_1) \\
&a_3(X_1Y_2 - X_2Y_1)\, Z_1Z_2 \\
&- Y_2Z_1) \\
&- X_2Z_1)
\end{aligned}$$

,

$$\begin{aligned}
Y_3^{(1)} = {} & -3X_1X_2(X_1Y_2 - X_2Y_1) \\
& - Y_1Y_2(Y_1Z_2 - Y_2Z_1) - 2a_1(X_1Z_2 - X_2Z_1)\, Y_1Y_2 \\
& + (a_1^2 + 3a_2)\, X_1X_2(Y_1Z_2 - Y_2Z_1) \\
& - (a_1^2 + a_2)(X_1Y_2 + X_2Y_1)(X_1Z_2 - X_2Z_1) \\
& + (a_1a_2 - 3a_3)\, X_1X_2(X_1Z_2 - X_2Z_1) \\
& - (2a_1a_3 + a_4)(X_1Y_2 - X_2Y_1)\, Z_1Z_2 \\
& + a_4(X_1Z_2 + X_2Z_1)(Y_1Z_2 - Y_2Z_1) \\
& + (a_1a_4 - a_2a_3)(X_1Z_2 + X_2Z_1)(X_1Z_2 - X_2Z_1) \\
& + (a_3^2 + 3a_6)(Y_1Z_2 - Y_2Z_1)\, Z_1Z_2 \\
& + (3a_1a_6 - a_3a_4)(X_1Z_2 - X_2Z_1)\, Z_1Z_2, \\
Z_3^{(1)} = {} & 3X_1X_2(X_1Z_2 - X_2Z_1) - (Y_1Z_2 + Y_2Z_1)(Y_1Z_2 - Y_2Z_1) \\
& + a_1(X_1Y_2 - X_2Y_1)\, Z_1Z_2 - a_1(X_1Z_2 - X_2Z_1)(Y_1Z_2 + Y_2Z_1) \\
& + a_2(X_1Z_2 + X_2Z_1)(X_1Z_2 - X_2Z_1) - a_3(Y_1Z_2 - Y_2Z_1)\, Z_1Z_2 \\
& + a_4(X_1Z_2 - X_2Z_1)\, Z_1Z_2.
\end{aligned}$$

The corresponding exceptional divisor is $3 \cdot \Delta$, so a pair of points P_1, P_2 on E is exceptional for this addition law if and only if $P_1 = P_2$.

Multiplying the addition law just given by $s^*(Y/Z)$ we obtain the addition law corresponding to $(0:1:0)$. It reads as follows:

$$\begin{aligned}
X_3^{(2)} = {} & Y_1Y_2(X_1Y_2 + X_2Y_1) + a_1(2X_1Y_2 + X_2Y_1)\, X_2Y_1 + a_1^2X_1X_2^2Y_1 \\
& - a_2X_1X_2(X_1Y_2 + X_2Y_1) - a_1a_2X_1^2X_2^2 + a_3X_2Y_1(Y_1Z_2 + 2Y_2Z_1) \\
& + a_1a_3X_1X_2(Y_1Z_2 - Y_2Z_1) - a_1a_3(X_1Y_2 + X_2Y_1)(X_1Z_2 - X_2Z_1) \\
& - a_4X_1X_2(Y_1Z_2 + Y_2Z_1) - a_4(X_1Y_2 + X_2Y_1)(X_1Z_2 + X_2Z_1) \\
& - a_1^2a_3X_1^2X_2Z_2 - a_1a_4X_1X_2(2X_1Z_2 + X_2Z_1) \\
& - a_2a_3X_1X_2^2Z_1 - a_3^2X_1Z_2(2Y_2Z_1 + Y_1Z_2) \\
& - 3a_6(X_1Y_2 + X_2Y_1)\, Z_1Z_2 \\
& - 3a_6(X_1Z_2 + X_2Z_1)(Y_1Z_2 + Y_2Z_1) - a_1a_3^2X_1Z_2(X_1Z_2 + 2X_2Z_1) \\
& - 3a_1a_6X_1Z_2(X_1Z_2 + 2X_2Z_1) + a_3a_4(X_1Z_2 - 2X_2Z_1)\, X_2Z_1 \\
& - (a_1^2a_6 - a_1a_3a_4 + a_2a_3^2 + 4a_2a_6 - a_4^2)(Y_1Z_2 + Y_2Z_1)\, Z_1Z_2 \\
& - (a_1^3a_6 - a_1^2a_3a_4 + a_1a_2a_3^2 + 4a_1a_2a_6 - a_1a_4^2)\, X_1Z_1Z_2^2 \\
& - a_3^3(X_1Z_2 + X_2Z_1)\, Z_1Z_2 - 3a_3a_6(X_1Z_2 + 2X_2Z_1)\, Z_1Z_2 \\
& - (a_1^2a_3a_6 - a_1a_3^2a_4 + a_2a_3^3 + 4a_2a_3a_6 - a_3a_4^2)\, Z_1^2Z_2^2,
\end{aligned}$$

$$\begin{aligned}
Y_3^{(2)} = {} & Y_1^2Y_2^2 + a_1X_2Y_1^2Y_2 + (a_1a_2 - \\
& + a_3Y_1^2Y_2Z_2 - (a_2^2 - 3a_4)\, X_1^2 \\
& + (a_1a_4 - a_2a_3)(2X_1Z_2 + X_2Z \\
& + (a_1^2a_4 - 2a_1a_2a_3 + 3a_3^2)\, X_1^2X \\
& - (a_2a_4 - 9a_6)\, X_1X_2(X_1Z_2 + \\
& + (3a_1a_6 - a_3a_4)(X_1Z_2 + 2X_2 \\
& + (3a_1^2a_6 - 2a_1a_3a_4 + a_2a_3^2 + 3 \\
& - (3a_2a_6 - a_4^2)(X_1Z_2 + X_2Z_1) \\
& + (a_1^3a_6 - a_1^2a_3a_4 + a_1a_2a_3^2 - a \\
& + (a_1^4a_6 - a_1^3a_3a_4 + 5a_1^2a_2a_6 + \\
& - a_1^2a_4^2 + a_2^2a_3^2 - a_2a_4^2 + 4a_2^2a_6 \\
& + (a_1^2a_2a_6 - a_1a_2a_3a_4 + 3a_1a_3 \\
& + 4a_2^2a_6 - 2a_3^2a_4 - 3a_4a_6)\, X_2Z \\
& + (a_1^3a_3a_6 - a_1^2a_3^2a_4 + a_1^2a_4a_6 \\
& + 4a_1a_2a_3a_6 - 2a_1a_3a_4^2 + a_2a_3^2 \\
& + 4a_2a_4a_6 - a_3^4 - 6a_3^2a_6 - a_4^3 - \\
Z_3^{(2)} = {} & 3X_1X_2(X_1Y_2 + X_2Y_1) + Y_1Y_2(\\
& + a_1(2X_1Y_2 + Y_1X_2)\, Y_1Z_2 + a \\
& + a_2X_1X_2(Y_1Z_2 + Y_2Z_1) \\
& + a_2(X_1Y_2 + X_2Y_1)(X_1Z_2 + X \\
& + a_1^3X_1^2X_2Z_2 + a_1a_2X_1X_2(2X \\
& + 3a_3X_1X_2^2Z_1 + a_3Y_1Z_2(Y_1Z \\
& + 2a_1a_3X_1Z_2(Y_1Z_2 + Y_2Z_1) \\
& + 2a_1a_3X_2Y_1Z_1Z_2 + a_4(X_1Y_2 \\
& + a_4(X_1Z_2 + X_2Z_1)(Y_1Z_2 + Y \\
& + (a_1^2a_3 + a_1a_4)\, X_1Z_2(X_1Z_2 + \\
& + a_3^2Y_1Z_1Z_2^2 + (a_3^2 + 3a_6)(Y_1Z \\
& + a_1a_3^2(2X_1Z_2 + X_2Z_1)\, Z_1Z_2 \\
& + a_3a_4(X_1Z_2 + 2X_2Z_1)\, Z_1Z_2
\end{aligned}$$

$= m^*(Y/Z)$

$- a_3,$

$_1, -P_2)$ we

aw given by
found to be

$_2$

$- X_2Z_1)$

$$\begin{aligned}
Y_3^{(1)} = {} & -3X_1X_2(X_1Y_2 - X_2Y_1) \\
& - Y_1Y_2(Y_1Z_2 - Y_2Z_1) - 2a_1(X_1Z_2 - X_2Z_1)\,Y_1Y_2 \\
& + (a_1^2 + 3a_2)\,X_1X_2(Y_1Z_2 - Y_2Z_1) \\
& - (a_1^2 + a_2)(X_1Y_2 + X_2Y_1)(X_1Z_2 - X_2Z_1) \\
& + (a_1a_2 - 3a_3)\,X_1X_2(X_1Z_2 - X_2Z_1) \\
& - (2a_1a_3 + a_4)(X_1Y_2 - X_2Y_1)\,Z_1Z_2 \\
& + a_4(X_1Z_2 + X_2Z_1)(Y_1Z_2 - Y_2Z_1) \\
& + (a_1a_4 - a_2a_3)(X_1Z_2 + X_2Z_1)(X_1Z_2 - X_2Z_1) \\
& + (a_3^2 + 3a_6)(Y_1Z_2 - Y_2Z_1)\,Z_1Z_2 \\
& + (3a_1a_6 - a_3a_4)(X_1Z_2 - X_2Z_1)\,Z_1Z_2, \\
Z_3^{(1)} = {} & 3X_1X_2(X_1Z_2 - X_2Z_1) - (Y_1Z_2 + Y_2Z_1)(Y_1Z_2 - Y_2Z_1) \\
& + a_1(X_1Y_2 - X_2Y_1)\,Z_1Z_2 - a_1(X_1Z_2 - X_2Z_1)(Y_1Z_2 + Y_2Z_1) \\
& + a_2(X_1Z_2 + X_2Z_1)(X_1Z_2 - X_2Z_1) - a_3(Y_1Z_2 - Y_2Z_1)\,Z_1Z_2 \\
& + a_4(X_1Z_2 - X_2Z_1)\,Z_1Z_2.
\end{aligned}$$

The corresponding exceptional divisor is $3 \cdot \Delta$, so a pair of points P_1, P_2 on E is exceptional for this addition law if and only if $P_1 = P_2$.

Multiplying the addition law just given by $s^*(Y/Z)$ we obtain the addition law corresponding to $(0:1:0)$. It reads as follows:

$$\begin{aligned}
X_3^{(2)} = {} & Y_1Y_2(X_1Y_2 + X_2Y_1) + a_1(2X_1Y_2 + X_2Y_1)\,X_2Y_1 + a_1^2X_1X_2^2Y_1 \\
& - a_2X_1X_2(X_1Y_2 + X_2Y_1) - a_1a_2X_1^2X_2^2 + a_3X_2Y_1(Y_1Z_2 + 2Y_2Z_1) \\
& + a_1a_3X_1X_2(Y_1Z_2 - Y_2Z_1) - a_1a_3(X_1Y_2 + X_2Y_1)(X_1Z_2 - X_2Z_1) \\
& - a_4X_1X_2(Y_1Z_2 + Y_2Z_1) - a_4(X_1Y_2 + X_2Y_1)(X_1Z_2 + X_2Z_1) \\
& - a_1^2a_3X_1^2X_2Z_2 - a_1a_4X_1X_2(2X_1Z_2 + X_2Z_1) \\
& - a_2a_3X_1X_2^2Z_1 - a_3^2X_1Z_2(2Y_2Z_1 + Y_1Z_2) \\
& - 3a_6(X_1Y_2 + X_2Y_1)\,Z_1Z_2 \\
& - 3a_6(X_1Z_2 + X_2Z_1)(Y_1Z_2 + Y_2Z_1) - a_1a_3^2X_1Z_2(X_1Z_2 + 2X_2Z_1) \\
& - 3a_1a_6X_1Z_2(X_1Z_2 + 2X_2Z_1) + a_3a_4(X_1Z_2 - 2X_2Z_1)\,X_2Z_1 \\
& - (a_1^2a_6 - a_1a_3a_4 + a_2a_3^2 + 4a_2a_6 - a_4^2)(Y_1Z_2 + Y_2Z_1)\,Z_1Z_2 \\
& - (a_1^3a_6 - a_1^2a_3a_4 + a_1a_2a_3^2 + 4a_1a_2a_6 - a_1a_4^2)\,X_1Z_1Z_2^2 \\
& - a_3^3(X_1Z_2 + X_2Z_1)\,Z_1Z_2 - 3a_3a_6(X_1Z_2 + 2X_2Z_1)\,Z_1Z_2 \\
& - (a_1^2a_3a_6 - a_1a_3^2a_4 + a_2a_3^3 + 4a_2a_3a_6 - a_3a_4^2)\,Z_1^2Z_2^2,
\end{aligned}$$

$$\begin{aligned}
Y_3^{(2)} = {} & Y_1^2Y_2^2 + a_1X_2Y_1^2Y_2 + (a_1a_2 - 3a_3)\,X_1X_2^2Y_1 \\
& + a_3Y_1^2Y_2Z_2 - (a_2^2 - 3a_4)\,X_1^2X_2^2 \\
& + (a_1a_4 - a_2a_3)(2X_1Z_2 + X_2Z_1)\,X_2Y_1 \\
& + (a_1^2a_4 - 2a_1a_2a_3 + 3a_3^2)\,X_1^2X_2Z_2 \\
& - (a_2a_4 - 9a_6)\,X_1X_2(X_1Z_2 + X_2Z_1) \\
& + (3a_1a_6 - a_3a_4)(X_1Z_2 + 2X_2Z_1)\,Y_1Z_2 \\
& + (3a_1^2a_6 - 2a_1a_3a_4 + a_2a_3^2 + 3a_2a_6 - a_4^2)\,X_1Z_2(X_1Z_2 + \\
& - (3a_2a_6 - a_4^2)(X_1Z_2 + X_2Z_1)(X_1Z_2 - X_2Z_1) \\
& + (a_1^3a_6 - a_1^2a_3a_4 + a_1a_2a_3^2 - a_1a_4^2 + 4a_1a_2a_6 - a_3^3 - 3a_3 \\
& + (a_1^4a_6 - a_1^3a_3a_4 + 5a_1^2a_2a_6 + a_1^2a_2a_3^2 - a_1a_2a_3a_4 - a_1a \\
& - a_1^2a_4^2 + a_2^2a_3^2 - a_2a_4^2 + 4a_2^2a_6 - a_3^2a_4 - 3a_4a_6)\,X_1Z_1Z_2^2 \\
& + (a_1^2a_2a_6 - a_1a_2a_3a_4 + 3a_1a_3a_6 + a_2^2a_3^2 - a_2a_4^2 \\
& + 4a_2^2a_6 - 2a_3^2a_4 - 3a_4a_6)\,X_2Z_1^2Z_2 \\
& + (a_1^3a_3a_6 - a_1^2a_3^2a_4 + a_1^2a_4a_6 + a_1a_2a_3^3 \\
& + 4a_1a_2a_3a_6 - 2a_1a_3a_4^2 + a_2a_3^2a_4 \\
& + 4a_2a_4a_6 - a_3^4 - 6a_3^2a_6 - a_4^3 - 9a_6^2)\,Z_1^2Z_2^2, \\
Z_3^{(2)} = {} & 3X_1X_2(X_1Y_2 + X_2Y_1) + Y_1Y_2(Y_1Z_2 + Y_2Z_1) + 3a_1X_1^2X \\
& + a_1(2X_1Y_2 + Y_1X_2)\,Y_1Z_2 + a_1^2X_1Z_2(2X_2Y_1 + X_1Y_2) \\
& + a_2X_1X_2(Y_1Z_2 + Y_2Z_1) \\
& + a_2(X_1Y_2 + X_2Y_1)(X_1Z_2 + X_2Z_1) \\
& + a_1^3X_1^2X_2Z_2 + a_1a_2X_1X_2(2X_1Z_2 + X_2Z_1) \\
& + 3a_3X_1X_2^2Z_1 + a_3Y_1Z_2(Y_1Z_2 + 2Y_2Z_1) \\
& + 2a_1a_3X_1Z_2(Y_1Z_2 + Y_2Z_1) \\
& + 2a_1a_3X_2Y_1Z_1Z_2 + a_4(X_1Y_2 + X_2Y_1)\,Z_1Z_2 \\
& + a_4(X_1Z_2 + X_2Z_1)(Y_1Z_2 + Y_2Z_1) \\
& + (a_1^2a_3 + a_1a_4)\,X_1Z_2(X_1Z_2 + 2X_2Z_1) + a_2a_3X_2Z_1(2X_1 \\
& + a_3^2Y_1Z_1Z_2^2 + (a_3^2 + 3a_6)(Y_1Z_2 + Y_2Z_1)\,Z_1Z_2 \\
& + a_1a_3^2(2X_1Z_2 + X_2Z_1)\,Z_1Z_2 + 3a_1a_6X_1Z_1Z_2^2 \\
& + a_3a_4(X_1Z_2 + 2X_2Z_1)\,Z_1Z_2 + (a_3^3 + 3a_3a_6)\,Z_1^2Z_2^2.
\end{aligned}$$

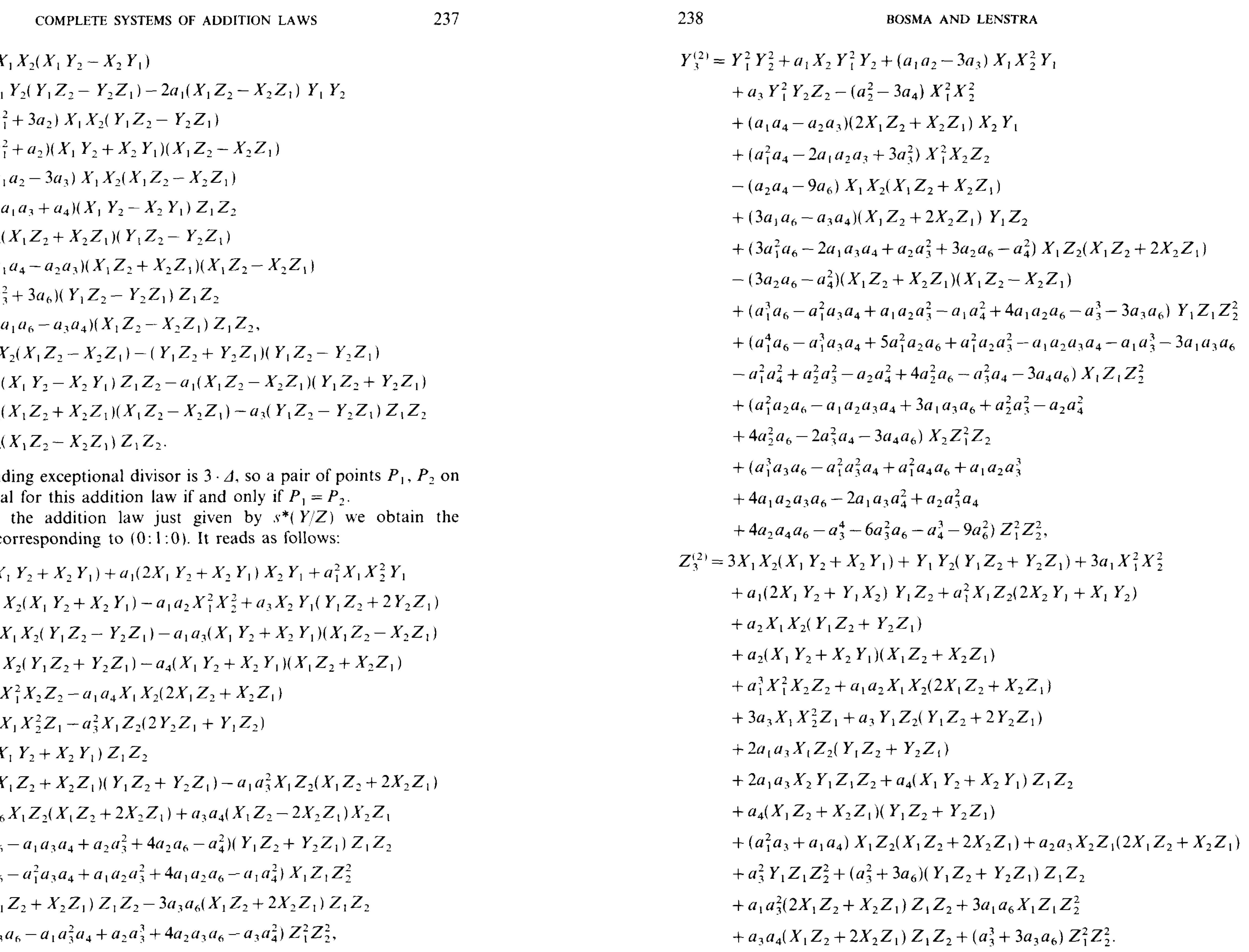
$$\begin{aligned}
Y_3^{(1)} = {} & -3X_1X_2(X_1Y_2-X_2Y_1) \\
& -Y_1Y_2(Y_1Z_2-Y_2Z_1)-2a_1(X_1Z_2-X_2Z_1)\,Y_1Y_2 \\
& +(a_1^2+3a_2)\,X_1X_2(Y_1Z_2-Y_2Z_1) \\
& -(a_1^2+a_2)(X_1Y_2+X_2Y_1)(X_1Z_2-X_2Z_1) \\
& +(a_1a_2-3a_3)\,X_1X_2(X_1Z_2-X_2Z_1) \\
& -(2a_1a_3+a_4)(X_1Y_2-X_2Y_1)\,Z_1Z_2 \\
& +a_4(X_1Z_2+X_2Z_1)(Y_1Z_2-Y_2Z_1) \\
& +(a_1a_4-a_2a_3)(X_1Z_2+X_2Z_1)(X_1Z_2-X_2Z_1) \\
& +(a_3^2+3a_6)(Y_1Z_2-Y_2Z_1)\,Z_1Z_2 \\
& +(3a_1a_6-a_3a_4)(X_1Z_2-X_2Z_1)\,Z_1Z_2, \\
Z_3^{(1)} = {} & 3X_1X_2(X_1Z_2-X_2Z_1)-(Y_1Z_2+Y_2Z_1)(Y_1Z_2-Y_2Z_1) \\
& +a_1(X_1Y_2-X_2Y_1)\,Z_1Z_2-a_1(X_1Z_2-X_2Z_1)(Y_1Z_2+Y_2Z_1) \\
& +a_2(X_1Z_2+X_2Z_1)(X_1Z_2-X_2Z_1)-a_3(Y_1Z_2-Y_2Z_1)\,Z_1Z_2 \\
& +a_4(X_1Z_2-X_2Z_1)\,Z_1Z_2.
\end{aligned}$$

The corresponding exceptional divisor is $3\cdot\Delta$, so a pair of points P_1, P_2 on E is exceptional for this addition law if and only if $P_1=P_2$.

Multiplying the addition law just given by $s^*(Y/Z)$ we obtain the addition law corresponding to $(0:1:0)$. It reads as follows:

$$\begin{aligned}
X_3^{(2)} = {} & Y_1Y_2(X_1Y_2+X_2Y_1)+a_1(2X_1Y_2+X_2Y_1)\,X_2Y_1+a_1^2X_1X_2^2Y_1 \\
& -a_2X_1X_2(X_1Y_2+X_2Y_1)-a_1a_2X_1^2X_2^2+a_3X_2Y_1(Y_1Z_2+2Y_2Z_1) \\
& +a_1a_3X_1X_2(Y_1Z_2-Y_2Z_1)-a_1a_3(X_1Y_2+X_2Y_1)(X_1Z_2-X_2Z_1) \\
& -a_4X_1X_2(Y_1Z_2+Y_2Z_1)-a_4(X_1Y_2+X_2Y_1)(X_1Z_2+X_2Z_1) \\
& -a_1^2a_3X_1^2X_2Z_2-a_1a_4X_1X_2(2X_1Z_2+X_2Z_1) \\
& -a_2a_3X_1X_2^2Z_1-a_3^2X_1Z_2(2Y_2Z_1+Y_1Z_2) \\
& -3a_6(X_1Y_2+X_2Y_1)\,Z_1Z_2 \\
& -3a_6(X_1Z_2+X_2Z_1)(Y_1Z_2+Y_2Z_1)-a_1a_3^2X_1Z_2(X_1Z_2+2X_2Z_1) \\
& -3a_1a_6X_1Z_2(X_1Z_2+2X_2Z_1)+a_3a_4(X_1Z_2-2X_2Z_1)\,X_2Z_1 \\
& -(a_1^2a_6-a_1a_3a_4+a_2a_3^2+4a_2a_6-a_4^2)(Y_1Z_2+Y_2Z_1)\,Z_1Z_2 \\
& -(a_1^3a_6-a_1^2a_3a_4+a_1a_2a_3^2+4a_1a_2a_6-a_1a_4^2)\,X_1Z_1Z_2^2 \\
& -a_3^3(X_1Z_2+X_2Z_1)\,Z_1Z_2-3a_3a_6(X_1Z_2+2X_2Z_1)\,Z_1Z_2 \\
& -(a_1^2a_3a_6-a_1a_3^2a_4+a_2a_3^3+4a_2a_3a_6-a_3a_4^2)\,Z_1^2Z_2^2,
\end{aligned}$$

$$\begin{aligned}
Y_3^{(2)} = {} & Y_1^2Y_2^2+a_1X_2Y_1^2Y_2+(a_1a_2-3a_3)\,X_1X_2^2Y_1 \\
& +a_3Y_1^2Y_2Z_2-(a_2^2-3a_4)\,X_1^2X_2^2 \\
& +(a_1a_4-a_2a_3)(2X_1Z_2+X_2Z_1)\,X_2Y_1 \\
& +(a_1^2a_4-2a_1a_2a_3+3a_3^2)\,X_1^2X_2Z_2 \\
& -(a_2a_4-9a_6)\,X_1X_2(X_1Z_2+X_2Z_1) \\
& +(3a_1a_6-a_3a_4)(X_1Z_2+2X_2Z_1)\,Y_1Z_2 \\
& +(3a_1^2a_6-2a_1a_3a_4+a_2a_3^2+3a_2a_6-a_4^2)\,X_1Z_2(X_1Z_2+2X_2Z_1) \\
& -(3a_2a_6-a_4^2)(X_1Z_2+X_2Z_1)(X_1Z_2-X_2Z_1) \\
& +(a_1^3a_6-a_1^2a_3a_4+a_1a_2a_3^2-a_1a_4^2+4a_1a_2a_6-a_3^3-3a_3a_6)\,Y_1Z_1Z_2^2 \\
& +(a_1^4a_6-a_1^3a_3a_4+5a_1^2a_2a_6+a_1^2a_2a_3^2-a_1a_2a_3a_4-a_1a_3^3-3a_1a_3a_6 \\
& -a_1^2a_4^2+a_2^2a_3^2-a_2a_4^2+4a_2^2a_6-a_3^2a_4-3a_4a_6)\,X_1Z_1Z_2^2 \\
& +(a_1^2a_2a_6-a_1a_2a_3a_4+3a_1a_3a_6+a_2^2a_3^2-a_2a_4^2 \\
& +4a_2^2a_6-2a_3^2a_4-3a_4a_6)\,X_2Z_1^2Z_2 \\
& +(a_1^3a_3a_6-a_1^2a_3^2a_4+a_1^2a_4a_6+a_1a_2a_3^3 \\
& +4a_1a_2a_3a_6-2a_1a_3a_4^2+a_2a_3^2a_4 \\
& +4a_2a_4a_6-a_3^4-6a_3^2a_6-a_4^3-9a_6^2)\,Z_1^2Z_2^2, \\
Z_3^{(2)} = {} & 3X_1X_2(X_1Y_2+X_2Y_1)+Y_1Y_2(Y_1Z_2+Y_2Z_1)+3a_1X_1^2X_2^2 \\
& +a_1(2X_1Y_2+Y_1X_2)\,Y_1Z_2+a_1^2X_1Z_2(2X_2Y_1+X_1Y_2) \\
& +a_2X_1X_2(Y_1Z_2+Y_2Z_1) \\
& +a_2(X_1Y_2+X_2Y_1)(X_1Z_2+X_2Z_1) \\
& +a_1^3X_1^2X_2Z_2+a_1a_2X_1X_2(2X_1Z_2+X_2Z_1) \\
& +3a_3X_1X_2^2Z_1+a_3Y_1Z_2(Y_1Z_2+2Y_2Z_1) \\
& +2a_1a_3X_1Z_2(Y_1Z_2+Y_2Z_1) \\
& +2a_1a_3X_2Y_1Z_1Z_2+a_4(X_1Y_2+X_2Y_1)\,Z_1Z_2 \\
& +a_4(X_1Z_2+X_2Z_1)(Y_1Z_2+Y_2Z_1) \\
& +(a_1^2a_3+a_1a_4)\,X_1Z_2(X_1Z_2+2X_2Z_1)+a_2a_3X_2Z_1(2X_1Z_2+X_2Z_1) \\
& +a_3^2Y_1Z_1Z_2^2+(a_3^2+3a_6)(Y_1Z_2+Y_2Z_1)\,Z_1Z_2 \\
& +a_1a_3^2(2X_1Z_2+X_2Z_1)\,Z_1Z_2+3a_1a_6X_1Z_1Z_2^2 \\
& +a_3a_4(X_1Z_2+2X_2Z_1)\,Z_1Z_2+(a_3^3+3a_3a_6)\,Z_1^2Z_2^2.
\end{aligned}$$



$$X_1 X_2(X_1 Y_2 - X_2 Y_1)$$
$$_1 Y_2(Y_1 Z_2 - Y_2 Z_1) - 2a_1(X_1 Z_2 - X_2 Z_1) Y_1 Y_2$$
$$^2_1 + 3a_2) X_1 X_2(Y_1 Z_2 - Y_2 Z_1)$$
$$^2_1 + a_2)(X_1 Y_2 + X_2 Y_1)(X_1 Z_2 - X_2 Z_1)$$
$$_1 a_2 - 3a_3) X_1 X_2(X_1 Z_2 - X_2 Z_1)$$
$$a_1 a_3 + a_4)(X_1 Y_2 - X_2 Y_1) Z_1 Z_2$$
$$(X_1 Z_2 + X_2 Z_1)(Y_1 Z_2 - Y_2 Z_1)$$
$$_1 a_4 - a_2 a_3)(X_1 Z_2 + X_2 Z_1)(X_1 Z_2 - X_2 Z_1)$$
$$^2_3 + 3a_6)(Y_1 Z_2 - Y_2 Z_1) Z_1 Z_2$$
$$a_1 a_6 - a_3 a_4)(X_1 Z_2 - X_2 Z_1) Z_1 Z_2,$$
$$X_2(X_1 Z_2 - X_2 Z_1) - (Y_1 Z_2 + Y_2 Z_1)(Y_1 Z_2 - Y_2 Z_1)$$
$$(X_1 Y_2 - X_2 Y_1) Z_1 Z_2 - a_1(X_1 Z_2 - X_2 Z_1)(Y_1 Z_2 + Y_2 Z_1)$$
$$(X_1 Z_2 + X_2 Z_1)(X_1 Z_2 - X_2 Z_1) - a_3(Y_1 Z_2 - Y_2 Z_1) Z_1 Z_2$$
$$(X_1 Z_2 - X_2 Z_1) Z_1 Z_2.$$

ding exceptional divisor is $3 \cdot \Delta$, so a pair of points P_1, P_2 on
al for this addition law if and only if $P_1 = P_2$.
the addition law just given by $s^*(Y/Z)$ we obtain the
corresponding to $(0:1:0)$. It reads as follows:

$$_1 Y_2 + X_2 Y_1) + a_1(2X_1 Y_2 + X_2 Y_1) X_2 Y_1 + a_1^2 X_1 X_2^2 Y_1$$
$$X_2(X_1 Y_2 + X_2 Y_1) - a_1 a_2 X_1^2 X_2^2 + a_3 X_2 Y_1(Y_1 Z_2 + 2Y_2 Z_1)$$
$$X_1 X_2(Y_1 Z_2 - Y_2 Z_1) - a_1 a_3(X_1 Y_2 + X_2 Y_1)(X_1 Z_2 - X_2 Z_1)$$
$$X_2(Y_1 Z_2 + Y_2 Z_1) - a_4(X_1 Y_2 + X_2 Y_1)(X_1 Z_2 + X_2 Z_1)$$
$$X_1^2 X_2 Z_2 - a_1 a_4 X_1 X_2(2X_1 Z_2 + X_2 Z_1)$$
$$X_1 X_2^2 Z_1 - a_3^2 X_1 Z_2(2Y_2 Z_1 + Y_1 Z_2)$$
$$X_1 Y_2 + X_2 Y_1) Z_1 Z_2$$
$$X_1 Z_2 + X_2 Z_1)(Y_1 Z_2 + Y_2 Z_1) - a_1 a_3^2 X_1 Z_2(X_1 Z_2 + 2X_2 Z_1)$$
$$_6 X_1 Z_2(X_1 Z_2 + 2X_2 Z_1) + a_3 a_4(X_1 Z_2 - 2X_2 Z_1) X_2 Z_1$$
$$_6 - a_1 a_3 a_4 + a_2 a_3^2 + 4a_2 a_6 - a_4^2)(Y_1 Z_2 + Y_2 Z_1) Z_1 Z_2$$
$$_6 - a_1^2 a_3 a_4 + a_1 a_2 a_3^2 + 4a_1 a_2 a_6 - a_1 a_4^2) X_1 Z_1 Z_2^2$$
$$_1 Z_2 + X_2 Z_1) Z_1 Z_2 - 3a_3 a_6(X_1 Z_2 + 2X_2 Z_1) Z_1 Z_2$$
$$_3 a_6 - a_1 a_3^2 a_4 + a_2 a_3^3 + 4a_2 a_3 a_6 - a_3 a_4^2) Z_1^2 Z_2^2,$$

$$\begin{aligned}
Y_3^{(2)} = {} & Y_1^2 Y_2^2 + a_1 X_2 Y_1^2 Y_2 + (a_1 a_2 - 3a_3) X_1 X_2^2 Y_1 \\
& + a_3 Y_1^2 Y_2 Z_2 - (a_2^2 - 3a_4) X_1^2 X_2^2 \\
& + (a_1 a_4 - a_2 a_3)(2X_1 Z_2 + X_2 Z_1) X_2 Y_1 \\
& + (a_1^2 a_4 - 2a_1 a_2 a_3 + 3a_3^2) X_1^2 X_2 Z_2 \\
& - (a_2 a_4 - 9a_6) X_1 X_2(X_1 Z_2 + X_2 Z_1) \\
& + (3a_1 a_6 - a_3 a_4)(X_1 Z_2 + 2X_2 Z_1) Y_1 Z_2 \\
& + (3a_1^2 a_6 - 2a_1 a_3 a_4 + a_2 a_3^2 + 3a_2 a_6 - a_4^2) X_1 Z_2(X_1 Z_2 + 2X_2 Z_1) \\
& - (3a_2 a_6 - a_4^2)(X_1 Z_2 + X_2 Z_1)(X_1 Z_2 - X_2 Z_1) \\
& + (a_1^3 a_6 - a_1^2 a_3 a_4 + a_1 a_2 a_3^2 - a_1 a_4^2 + 4a_1 a_2 a_6 - a_3^3 - 3a_3 a_6) Y_1 Z_1 Z_2^2 \\
& + (a_1^4 a_6 - a_1^3 a_3 a_4 + 5a_1^2 a_2 a_6 + a_1^2 a_2 a_3^2 - a_1 a_2 a_3 a_4 - a_1 a_3^3 - 3a_1 a_3 a_6 \\
& - a_1^2 a_4^2 + a_2^2 a_3^2 - a_2 a_4^2 + 4a_2^2 a_6 - a_3^2 a_4 - 3a_4 a_6) X_1 Z_1 Z_2^2 \\
& + (a_1^2 a_2 a_6 - a_1 a_2 a_3 a_4 + 3a_1 a_3 a_6 + a_2^2 a_3^2 - a_2 a_4^2 \\
& + 4a_2^2 a_6 - 2a_3^2 a_4 - 3a_4 a_6) X_2 Z_1^2 Z_2 \\
& + (a_1^3 a_3 a_6 - a_1^2 a_3^2 a_4 + a_1^2 a_4 a_6 + a_1 a_2 a_3^3 \\
& + 4a_1 a_2 a_3 a_6 - 2a_1 a_3 a_4^2 + a_2 a_3^2 a_4 \\
& + 4a_2 a_4 a_6 - a_3^4 - 6a_3^2 a_6 - a_4^3 - 9a_6^2) Z_1^2 Z_2^2,
\end{aligned}$$

$$\begin{aligned}
Z_3^{(2)} = {} & 3X_1 X_2(X_1 Y_2 + X_2 Y_1) + Y_1 Y_2(Y_1 Z_2 + Y_2 Z_1) + 3a_1 X_1^2 X_2^2 \\
& + a_1(2X_1 Y_2 + Y_1 X_2) Y_1 Z_2 + a_1^2 X_1 Z_2(2X_2 Y_1 + X_1 Y_2) \\
& + a_2 X_1 X_2(Y_1 Z_2 + Y_2 Z_1) \\
& + a_2(X_1 Y_2 + X_2 Y_1)(X_1 Z_2 + X_2 Z_1) \\
& + a_1^3 X_1^2 X_2 Z_2 + a_1 a_2 X_1 X_2(2X_1 Z_2 + X_2 Z_1) \\
& + 3a_3 X_1 X_2^2 Z_1 + a_3 Y_1 Z_2(Y_1 Z_2 + 2Y_2 Z_1) \\
& + 2a_1 a_3 X_1 Z_2(Y_1 Z_2 + Y_2 Z_1) \\
& + 2a_1 a_3 X_2 Y_1 Z_1 Z_2 + a_4(X_1 Y_2 + X_2 Y_1) Z_1 Z_2 \\
& + a_4(X_1 Z_2 + X_2 Z_1)(Y_1 Z_2 + Y_2 Z_1) \\
& + (a_1^2 a_3 + a_1 a_4) X_1 Z_2(X_1 Z_2 + 2X_2 Z_1) + a_2 a_3 X_2 Z_1(2X_1 Z_2 + X_2 Z_1) \\
& + a_3^2 Y_1 Z_1 Z_2^2 + (a_3^2 + 3a_6)(Y_1 Z_2 + Y_2 Z_1) Z_1 Z_2 \\
& + a_1 a_3^2(2X_1 Z_2 + X_2 Z_1) Z_1 Z_2 + 3a_1 a_6 X_1 Z_1 Z_2^2 \\
& + a_3 a_4(X_1 Z_2 + 2X_2 Z_1) Z_1 Z_2 + (a_3^3 + 3a_3 a_6) Z_1^2 Z_2^2.
\end{aligned}$$

1987 Le

complete

to comp

$E(R)$ fo

rings wit

Define **F**

X, Y, Z

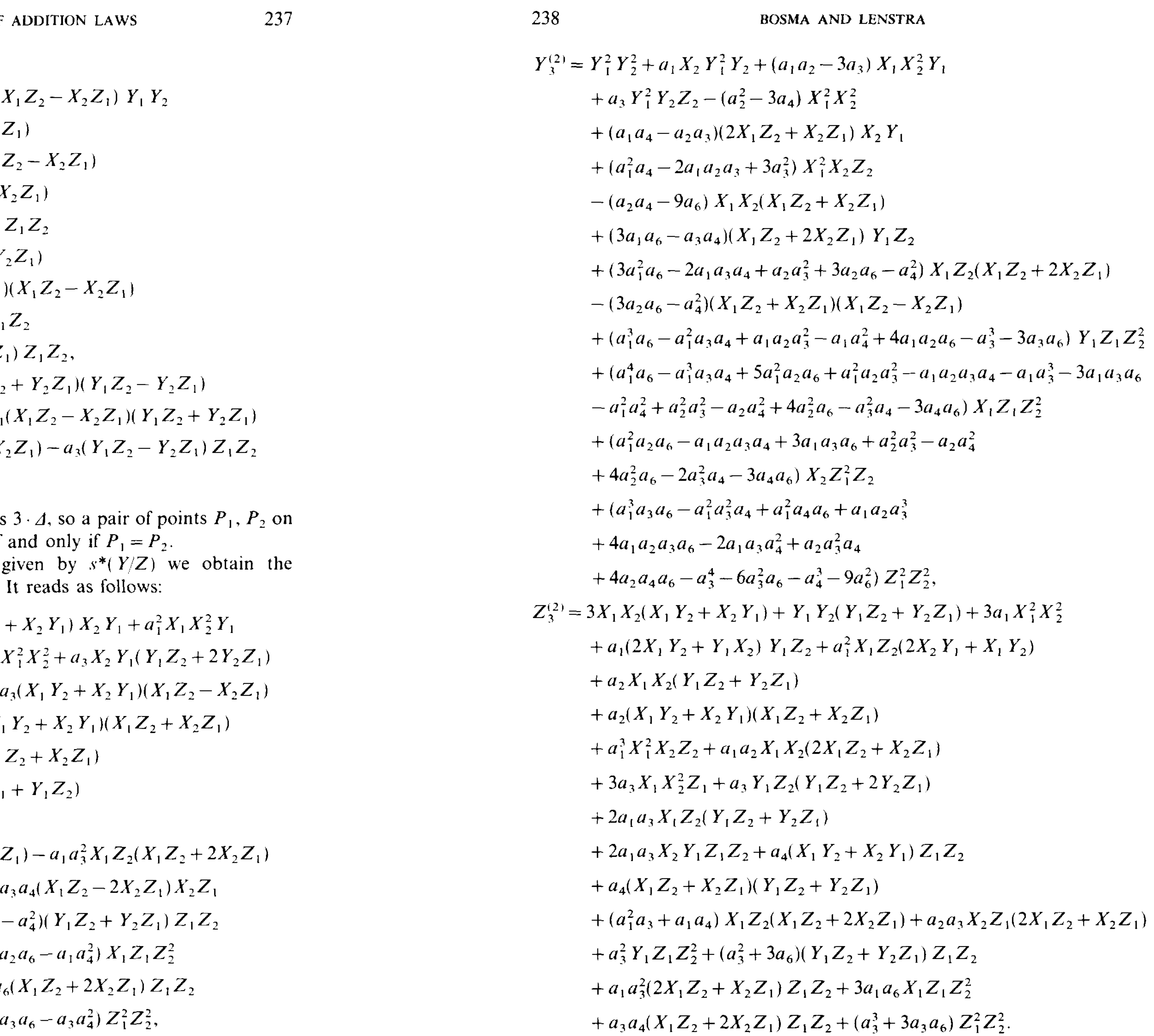
where $($

$\{(\lambda X, \lambda$

Define E

$\{(X : Y$

$Y^2 Z =$



F ADDITION LAWS 237

$X_1Z_2 - X_2Z_1)\ Y_1Y_2$

$Z_1)$

$Z_2 - X_2Z_1)$

$X_2Z_1)$

Z_1Z_2

$Y_2Z_1)$

$)(X_1Z_2 - X_2Z_1)$

${}_1Z_2$

$Z_1)\ Z_1Z_2,$

${}_2 + Y_2Z_1)(Y_1Z_2 - Y_2Z_1)$

${}_1(X_1Z_2 - X_2Z_1)(Y_1Z_2 + Y_2Z_1)$

$Y_2Z_1) - a_3(Y_1Z_2 - Y_2Z_1)\ Z_1Z_2$

s $3 \cdot \Delta$, so a pair of points P_1, P_2 on
f and only if $P_1 = P_2$.
given by $s^*(Y/Z)$ we obtain the
It reads as follows:

$+ X_2Y_1)\ X_2Y_1 + a_1^2X_1X_2^2Y_1$

$X_1^2X_2^2 + a_3X_2Y_1(Y_1Z_2 + 2Y_2Z_1)$

$a_3(X_1Y_2 + X_2Y_1)(X_1Z_2 - X_2Z_1)$

${}_1Y_2 + X_2Y_1)(X_1Z_2 + X_2Z_1)$

$Z_2 + X_2Z_1)$

${}_1 + Y_1Z_2)$

$Z_1) - a_1a_3^2X_1Z_2(X_1Z_2 + 2X_2Z_1)$

$a_3a_4(X_1Z_2 - 2X_2Z_1)X_2Z_1$

$- a_4^2)(Y_1Z_2 + Y_2Z_1)\ Z_1Z_2$

$a_2a_6 - a_1a_4^2)\ X_1Z_1Z_2^2$

${}_6(X_1Z_2 + 2X_2Z_1)\ Z_1Z_2$

$a_3a_6 - a_3a_4^2)\ Z_1^2Z_2^2,$

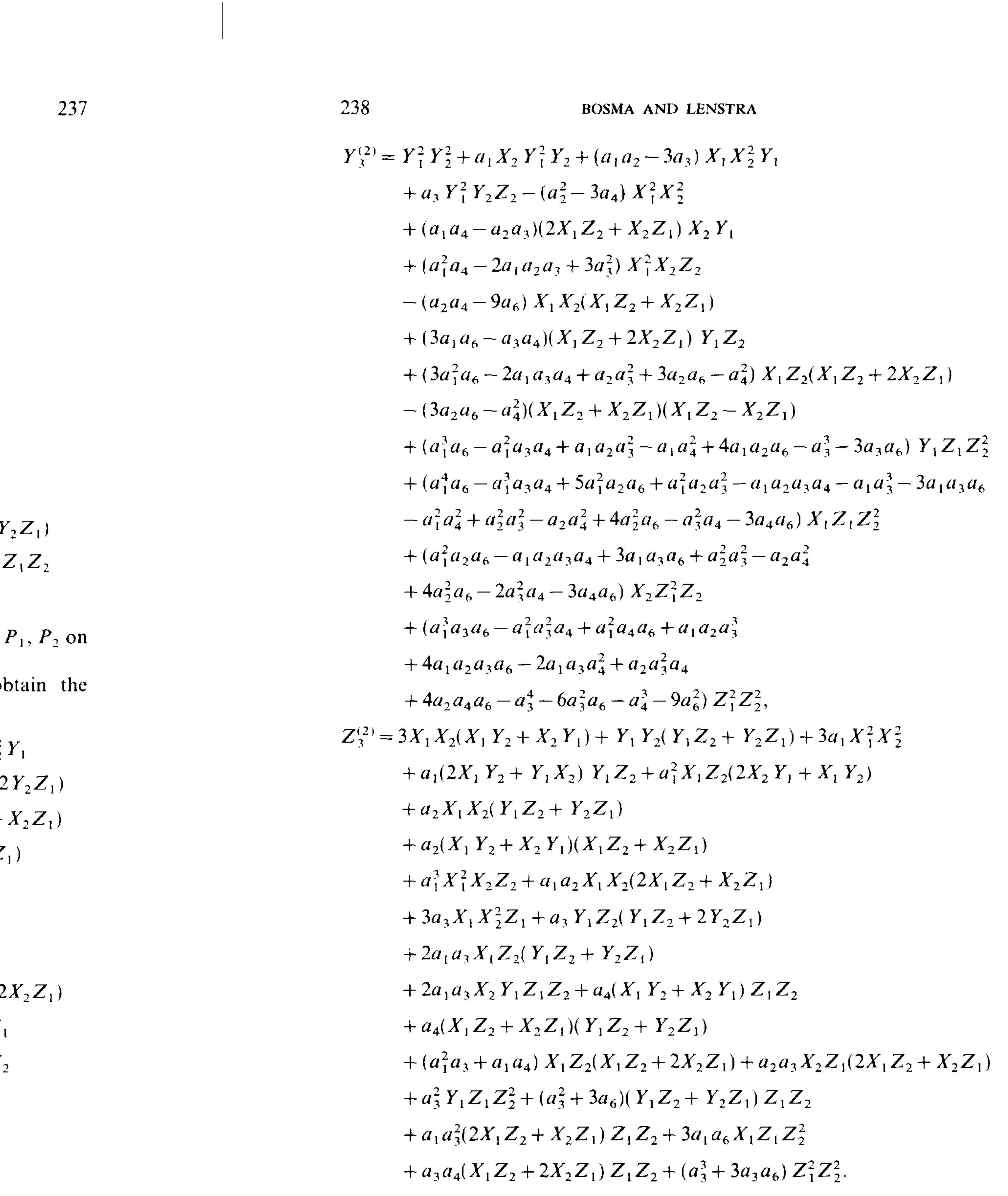
238 BOSMA AND LENSTRA

$$
\begin{aligned}
Y_3^{(2)} = {} & Y_1^2Y_2^2 + a_1X_2Y_1^2Y_2 + (a_1a_2 - 3a_3)\ X_1X_2^2Y_1 \\
& + a_3Y_1^2Y_2Z_2 - (a_2^2 - 3a_4)\ X_1^2X_2^2 \\
& + (a_1a_4 - a_2a_3)(2X_1Z_2 + X_2Z_1)\ X_2Y_1 \\
& + (a_1^2a_4 - 2a_1a_2a_3 + 3a_3^2)\ X_1^2X_2Z_2 \\
& - (a_2a_4 - 9a_6)\ X_1X_2(X_1Z_2 + X_2Z_1) \\
& + (3a_1a_6 - a_3a_4)(X_1Z_2 + 2X_2Z_1)\ Y_1Z_2 \\
& + (3a_1^2a_6 - 2a_1a_3a_4 + a_2a_3^2 + 3a_2a_6 - a_4^2)\ X_1Z_2(X_1Z_2 + 2X_2Z_1) \\
& - (3a_2a_6 - a_4^2)(X_1Z_2 + X_2Z_1)(X_1Z_2 - X_2Z_1) \\
& + (a_1^3a_6 - a_1^2a_3a_4 + a_1a_2a_3^2 - a_1a_4^2 + 4a_1a_2a_6 - a_3^3 - 3a_3a_6)\ Y_1Z_1Z_2^2 \\
& + (a_1^4a_6 - a_1^3a_3a_4 + 5a_1^2a_2a_6 + a_1^2a_2a_3^2 - a_1a_2a_3a_4 - a_1a_3^3 - 3a_1a_3a_6 \\
& - a_1^2a_4^2 + a_2^2a_3^2 - a_2a_4^2 + 4a_2^2a_6 - a_3^2a_4 - 3a_4a_6)\ X_1Z_1Z_2^2 \\
& + (a_1^2a_2a_6 - a_1a_2a_3a_4 + 3a_1a_3a_6 + a_2^2a_3^2 - a_2a_4^2 \\
& + 4a_2^2a_6 - 2a_3^2a_4 - 3a_4a_6)\ X_2Z_1^2Z_2 \\
& + (a_1^3a_3a_6 - a_1^2a_3^2a_4 + a_1^2a_4a_6 + a_1a_2a_3^3 \\
& + 4a_1a_2a_3a_6 - 2a_1a_3a_4^2 + a_2a_3^2a_4 \\
& + 4a_2a_4a_6 - a_3^4 - 6a_3^2a_6 - a_4^3 - 9a_6^2)\ Z_1^2Z_2^2, \\
Z_3^{(2)} = {} & 3X_1X_2(X_1Y_2 + X_2Y_1) + Y_1Y_2(Y_1Z_2 + Y_2Z_1) + 3a_1X_1^2X_2^2 \\
& + a_1(2X_1Y_2 + Y_1X_2)\ Y_1Z_2 + a_1^2X_1Z_2(2X_2Y_1 + X_1Y_2) \\
& + a_2X_1X_2(Y_1Z_2 + Y_2Z_1) \\
& + a_2(X_1Y_2 + X_2Y_1)(X_1Z_2 + X_2Z_1) \\
& + a_1^3X_1^2X_2Z_2 + a_1a_2X_1X_2(2X_1Z_2 + X_2Z_1) \\
& + 3a_3X_1X_2^2Z_1 + a_3Y_1Z_2(Y_1Z_2 + 2Y_2Z_1) \\
& + 2a_1a_3X_1Z_2(Y_1Z_2 + Y_2Z_1) \\
& + 2a_1a_3X_2Y_1Z_1Z_2 + a_4(X_1Y_2 + X_2Y_1)\ Z_1Z_2 \\
& + a_4(X_1Z_2 + X_2Z_1)(Y_1Z_2 + Y_2Z_1) \\
& + (a_1^2a_3 + a_1a_4)\ X_1Z_2(X_1Z_2 + 2X_2Z_1) + a_2a_3X_2Z_1(2X_1Z_2 + X_2Z_1) \\
& + a_3^2Y_1Z_1Z_2^2 + (a_3^2 + 3a_6)(Y_1Z_2 + Y_2Z_1)\ Z_1Z_2 \\
& + a_1a_3^2(2X_1Z_2 + X_2Z_1)\ Z_1Z_2 + 3a_1a_6X_1Z_1Z_2^2 \\
& + a_3a_4(X_1Z_2 + 2X_2Z_1)\ Z_1Z_2 + (a_3^3 + 3a_3a_6)\ Z_1^2Z_2^2.
\end{aligned}
$$

1987 Lenstra: Use
complete system c
to computationally
$E(R)$ for more ge
rings with trivial c

Define $\mathbf{P}^2(R) = \{$
$X, Y, Z \in R$; XR
where $(X : Y : Z)$
$\{(\lambda X, \lambda Y, \lambda Z) : \lambda$

Define $E(R) =$
$\{(X : Y : Z) \in \mathbf{P}^2$
$Y^2Z = X^3 + a_4X$



237

$Y_2Z_1)$

Z_1Z_2

P_1, P_2 on

btain the

Y_1

$2Y_2Z_1)$

$X_2Z_1)$

$Z_1)$

$2X_2Z_1)$

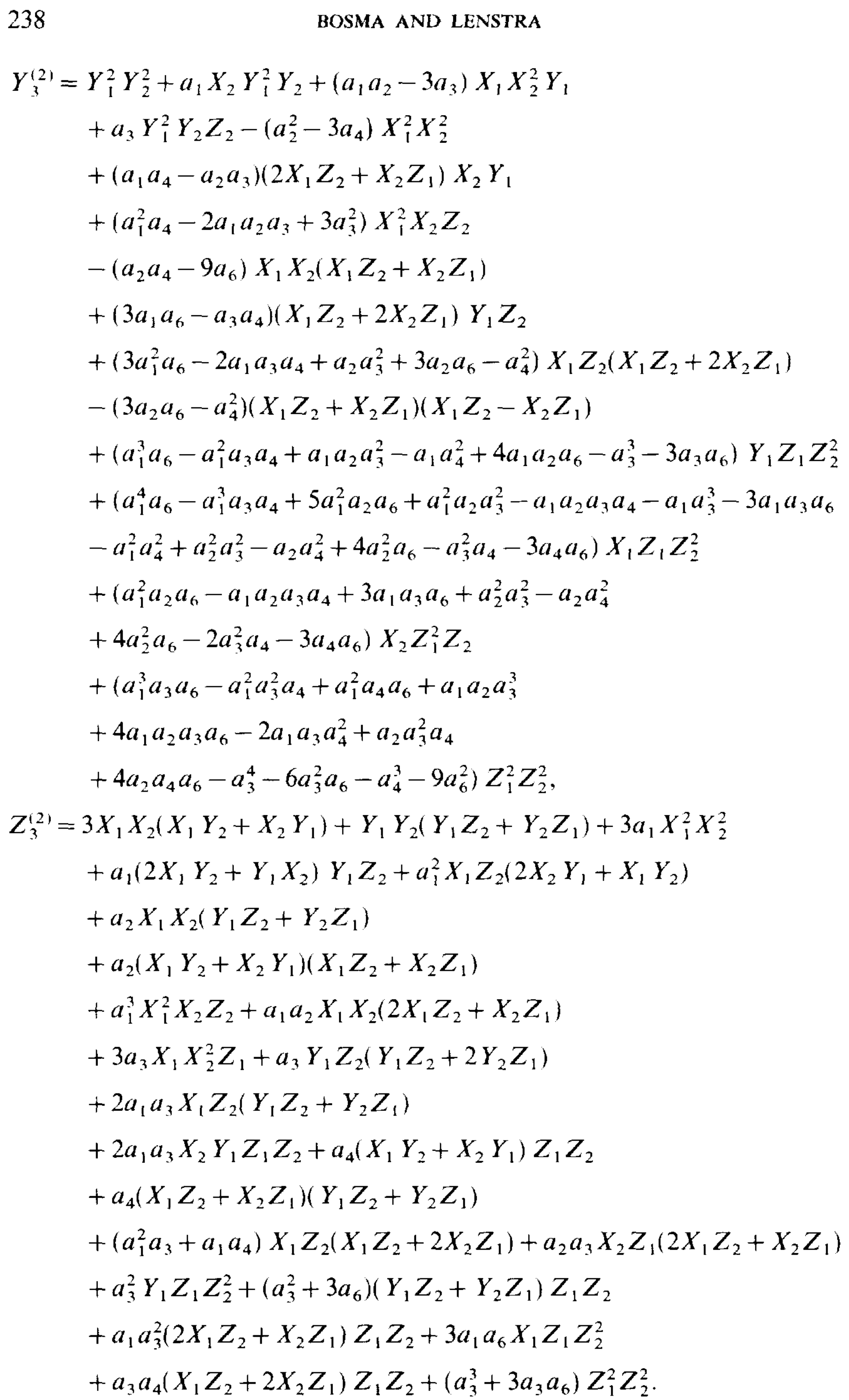
238 BOSMA AND LENSTRA

$$
\begin{aligned}
Y_3^{(2)} = {} & Y_1^2 Y_2^2 + a_1 X_2 Y_1^2 Y_2 + (a_1a_2 - 3a_3)\, X_1 X_2^2 Y_1 \\
& + a_3 Y_1^2 Y_2 Z_2 - (a_2^2 - 3a_4)\, X_1^2 X_2^2 \\
& + (a_1a_4 - a_2a_3)(2X_1Z_2 + X_2Z_1)\, X_2 Y_1 \\
& + (a_1^2a_4 - 2a_1a_2a_3 + 3a_3^2)\, X_1^2 X_2 Z_2 \\
& - (a_2a_4 - 9a_6)\, X_1X_2(X_1Z_2 + X_2Z_1) \\
& + (3a_1a_6 - a_3a_4)(X_1Z_2 + 2X_2Z_1)\, Y_1Z_2 \\
& + (3a_1^2a_6 - 2a_1a_3a_4 + a_2a_3^2 + 3a_2a_6 - a_4^2)\, X_1Z_2(X_1Z_2 + 2X_2Z_1) \\
& - (3a_2a_6 - a_4^2)(X_1Z_2 + X_2Z_1)(X_1Z_2 - X_2Z_1) \\
& + (a_1^3a_6 - a_1^2a_3a_4 + a_1a_2a_3^2 - a_1a_4^2 + 4a_1a_2a_6 - a_3^3 - 3a_3a_6)\, Y_1Z_1Z_2^2 \\
& + (a_1^4a_6 - a_1^3a_3a_4 + 5a_1^2a_2a_6 + a_1^2a_2a_3^2 - a_1a_2a_3a_4 - a_1a_3^3 - 3a_1a_3a_6 \\
& - a_1^2a_4^2 + a_2^2a_3^2 - a_2a_4^2 + 4a_2^2a_6 - a_3^2a_4 - 3a_4a_6)\, X_1Z_1Z_2^2 \\
& + (a_1^2a_2a_6 - a_1a_2a_3a_4 + 3a_1a_3a_6 + a_2^2a_3^2 - a_2a_4^2 \\
& + 4a_2^2a_6 - 2a_3^2a_4 - 3a_4a_6)\, X_2Z_1^2Z_2 \\
& + (a_1^3a_3a_6 - a_1^2a_3^2a_4 + a_1^2a_4a_6 + a_1a_2a_3^3 \\
& + 4a_1a_2a_3a_6 - 2a_1a_3a_4^2 + a_2a_3^2a_4 \\
& + 4a_2a_4a_6 - a_3^4 - 6a_3^2a_6 - a_4^3 - 9a_6^2)\, Z_1^2Z_2^2, \\
Z_3^{(2)} = {} & 3X_1X_2(X_1Y_2 + X_2Y_1) + Y_1Y_2(Y_1Z_2 + Y_2Z_1) + 3a_1X_1^2X_2^2 \\
& + a_1(2X_1Y_2 + Y_1X_2)\, Y_1Z_2 + a_1^2X_1Z_2(2X_2Y_1 + X_1Y_2) \\
& + a_2X_1X_2(Y_1Z_2 + Y_2Z_1) \\
& + a_2(X_1Y_2 + X_2Y_1)(X_1Z_2 + X_2Z_1) \\
& + a_1^3X_1^2X_2Z_2 + a_1a_2X_1X_2(2X_1Z_2 + X_2Z_1) \\
& + 3a_3X_1X_2^2Z_1 + a_3Y_1Z_2(Y_1Z_2 + 2Y_2Z_1) \\
& + 2a_1a_3X_1Z_2(Y_1Z_2 + Y_2Z_1) \\
& + 2a_1a_3X_2Y_1Z_1Z_2 + a_4(X_1Y_2 + X_2Y_1)\, Z_1Z_2 \\
& + a_4(X_1Z_2 + X_2Z_1)(Y_1Z_2 + Y_2Z_1) \\
& + (a_1^2a_3 + a_1a_4)\, X_1Z_2(X_1Z_2 + 2X_2Z_1) + a_2a_3X_2Z_1(2X_1Z_2 + X_2Z_1) \\
& + a_3^2Y_1Z_1Z_2^2 + (a_3^2 + 3a_6)(Y_1Z_2 + Y_2Z_1)\, Z_1Z_2 \\
& + a_1a_3^2(2X_1Z_2 + X_2Z_1)\, Z_1Z_2 + 3a_1a_6X_1Z_1Z_2^2 \\
& + a_3a_4(X_1Z_2 + 2X_2Z_1)\, Z_1Z_2 + (a_3^3 + 3a_3a_6)\, Z_1^2Z_2^2.
\end{aligned}
$$

1987 Lenstra: Use Lange–R
complete system of addition
to computationally define gr
$E(R)$ for more general rings
rings with trivial class group

Define $\mathbf{P}^2(R) = \{(X : Y : Z$
$X, Y, Z \in R;\ XR{+}YR{+}ZR$
where $(X : Y : Z)$ is the mo
$\{(\lambda X, \lambda Y, \lambda Z) : \lambda \in R\}$.

Define $E(R) =$
$\{(X : Y : Z) \in \mathbf{P}^2(R) :$
$Y^2Z = X^3 + a_4XZ^2 + a_6Z$



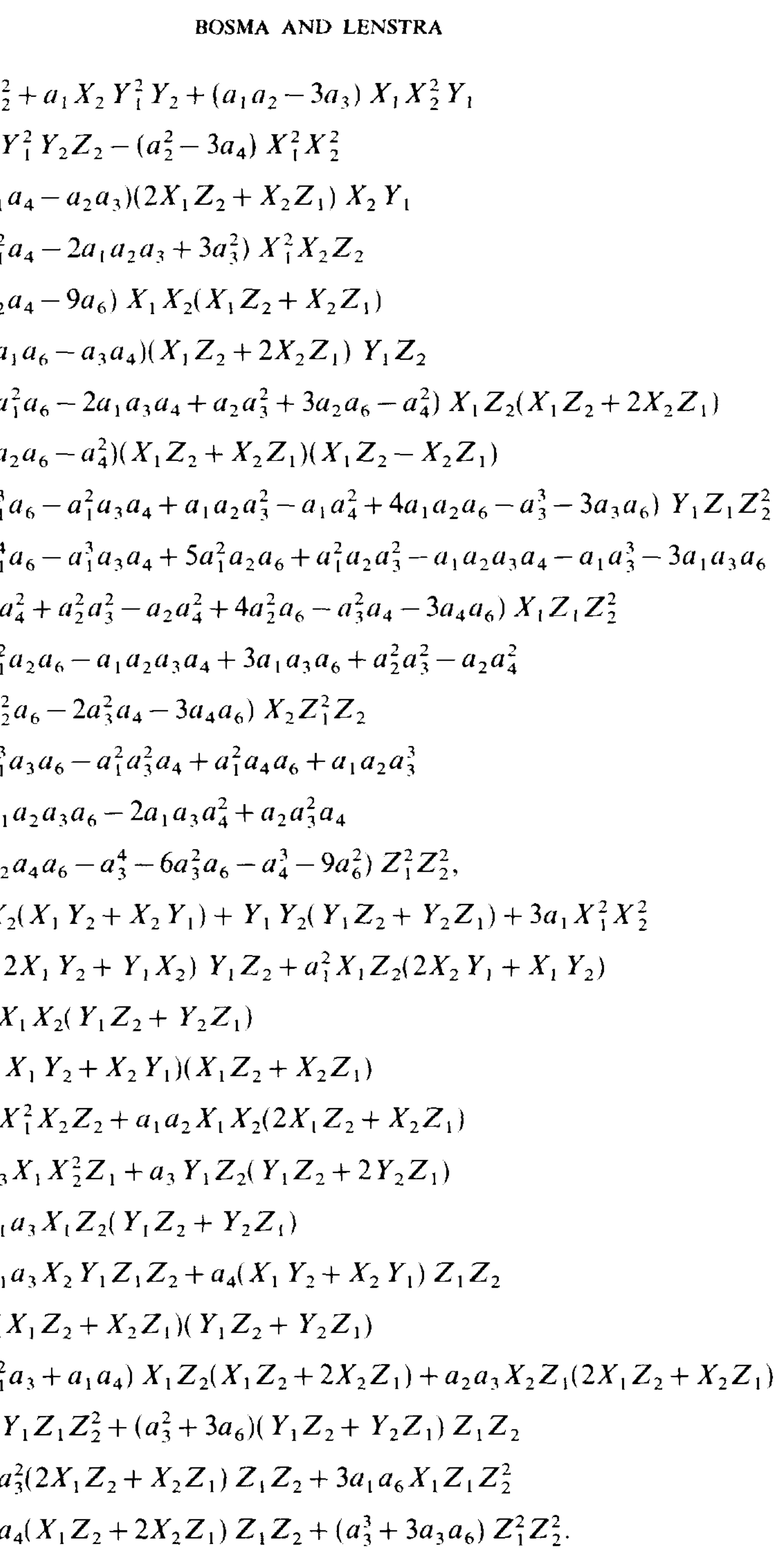
238 BOSMA AND LENSTRA

$$\begin{aligned}
Y_3^{(2)} = {} & Y_1^2 Y_2^2 + a_1 X_2 Y_1^2 Y_2 + (a_1 a_2 - 3a_3)\, X_1 X_2^2 Y_1 \\
& + a_3 Y_1^2 Y_2 Z_2 - (a_2^2 - 3a_4)\, X_1^2 X_2^2 \\
& + (a_1 a_4 - a_2 a_3)(2X_1 Z_2 + X_2 Z_1)\, X_2 Y_1 \\
& + (a_1^2 a_4 - 2a_1 a_2 a_3 + 3a_3^2)\, X_1^2 X_2 Z_2 \\
& - (a_2 a_4 - 9a_6)\, X_1 X_2 (X_1 Z_2 + X_2 Z_1) \\
& + (3a_1 a_6 - a_3 a_4)(X_1 Z_2 + 2X_2 Z_1)\, Y_1 Z_2 \\
& + (3a_1^2 a_6 - 2a_1 a_3 a_4 + a_2 a_3^2 + 3a_2 a_6 - a_4^2)\, X_1 Z_2 (X_1 Z_2 + 2X_2 Z_1) \\
& - (3a_2 a_6 - a_4^2)(X_1 Z_2 + X_2 Z_1)(X_1 Z_2 - X_2 Z_1) \\
& + (a_1^3 a_6 - a_1^2 a_3 a_4 + a_1 a_2 a_3^2 - a_1 a_4^2 + 4a_1 a_2 a_6 - a_3^3 - 3a_3 a_6)\, Y_1 Z_1 Z_2^2 \\
& + (a_1^4 a_6 - a_1^3 a_3 a_4 + 5a_1^2 a_2 a_6 + a_1^2 a_2 a_3^2 - a_1 a_2 a_3 a_4 - a_1 a_3^3 - 3a_1 a_3 a_6 \\
& - a_1^2 a_4^2 + a_2^2 a_3^2 - a_2 a_4^2 + 4a_2^2 a_6 - a_3^2 a_4 - 3a_4 a_6)\, X_1 Z_1 Z_2^2 \\
& + (a_1^2 a_2 a_6 - a_1 a_2 a_3 a_4 + 3a_1 a_3 a_6 + a_2^2 a_3^2 - a_2 a_4^2 \\
& + 4a_2^2 a_6 - 2a_3^2 a_4 - 3a_4 a_6)\, X_2 Z_1^2 Z_2 \\
& + (a_1^3 a_3 a_6 - a_1^2 a_3^2 a_4 + a_1^2 a_4 a_6 + a_1 a_2 a_3^3 \\
& + 4a_1 a_2 a_3 a_6 - 2a_1 a_3 a_4^2 + a_2 a_3^2 a_4 \\
& + 4a_2 a_4 a_6 - a_3^4 - 6a_3^2 a_6 - a_4^3 - 9a_6^2)\, Z_1^2 Z_2^2, \\
Z_3^{(2)} = {} & 3X_1 X_2 (X_1 Y_2 + X_2 Y_1) + Y_1 Y_2 (Y_1 Z_2 + Y_2 Z_1) + 3a_1 X_1^2 X_2^2 \\
& + a_1 (2X_1 Y_2 + Y_1 X_2)\, Y_1 Z_2 + a_1^2 X_1 Z_2 (2X_2 Y_1 + X_1 Y_2) \\
& + a_2 X_1 X_2 (Y_1 Z_2 + Y_2 Z_1) \\
& + a_2 (X_1 Y_2 + X_2 Y_1)(X_1 Z_2 + X_2 Z_1) \\
& + a_1^3 X_1^2 X_2 Z_2 + a_1 a_2 X_1 X_2 (2X_1 Z_2 + X_2 Z_1) \\
& + 3a_3 X_1 X_2^2 Z_1 + a_3 Y_1 Z_2 (Y_1 Z_2 + 2Y_2 Z_1) \\
& + 2a_1 a_3 X_1 Z_2 (Y_1 Z_2 + Y_2 Z_1) \\
& + 2a_1 a_3 X_2 Y_1 Z_1 Z_2 + a_4 (X_1 Y_2 + X_2 Y_1)\, Z_1 Z_2 \\
& + a_4 (X_1 Z_2 + X_2 Z_1)(Y_1 Z_2 + Y_2 Z_1) \\
& + (a_1^2 a_3 + a_1 a_4)\, X_1 Z_2 (X_1 Z_2 + 2X_2 Z_1) + a_2 a_3 X_2 Z_1 (2X_1 Z_2 + X_2 Z_1) \\
& + a_3^2 Y_1 Z_1 Z_2^2 + (a_3^2 + 3a_6)(Y_1 Z_2 + Y_2 Z_1)\, Z_1 Z_2 \\
& + a_1 a_3^2 (2X_1 Z_2 + X_2 Z_1)\, Z_1 Z_2 + 3a_1 a_6 X_1 Z_1 Z_2^2 \\
& + a_3 a_4 (X_1 Z_2 + 2X_2 Z_1)\, Z_1 Z_2 + (a_3^3 + 3a_3 a_6)\, Z_1^2 Z_2^2.
\end{aligned}$$

1987 Lenstra: Use Lange–Ruppert complete system of addition laws to computationally define group $E(R)$ for more general rings R—rings with trivial class group.

Define $\mathbf{P}^2(R) = \{(X : Y : Z) : X, Y, Z \in R;\ XR + YR + ZR = R\}$ where $(X : Y : Z)$ is the module $\{(\lambda X, \lambda Y, \lambda Z) : \lambda \in R\}$.

Define $E(R) = \{(X : Y : Z) \in \mathbf{P}^2(R) : Y^2 Z = X^3 + a_4 X Z^2 + a_6 Z^3\}$.



BOSMA AND LENSTRA

$${}^2_2 + a_1 X_2 Y_1^2 Y_2 + (a_1 a_2 - 3a_3) X_1 X_2^2 Y_1$$
$$Y_1^2 Y_2 Z_2 - (a_2^2 - 3a_4) X_1^2 X_2^2$$
$${}_1 a_4 - a_2 a_3)(2X_1 Z_2 + X_2 Z_1) X_2 Y_1$$
$${}^2_1 a_4 - 2a_1 a_2 a_3 + 3a_3^2) X_1^2 X_2 Z_2$$
$${}_2 a_4 - 9a_6) X_1 X_2 (X_1 Z_2 + X_2 Z_1)$$
$$a_1 a_6 - a_3 a_4)(X_1 Z_2 + 2X_2 Z_1) Y_1 Z_2$$
$$a_1^2 a_6 - 2a_1 a_3 a_4 + a_2 a_3^2 + 3a_2 a_6 - a_4^2) X_1 Z_2 (X_1 Z_2 + 2X_2 Z_1)$$
$$a_2 a_6 - a_4^2)(X_1 Z_2 + X_2 Z_1)(X_1 Z_2 - X_2 Z_1)$$
$${}^3_1 a_6 - a_1^2 a_3 a_4 + a_1 a_2 a_3^2 - a_1 a_4^2 + 4a_1 a_2 a_6 - a_3^3 - 3a_3 a_6) Y_1 Z_1 Z_2^2$$
$${}^4_1 a_6 - a_1^3 a_3 a_4 + 5a_1^2 a_2 a_6 + a_1^2 a_2 a_3^2 - a_1 a_2 a_3 a_4 - a_1 a_3^3 - 3a_1 a_3 a_6$$
$$a_4^2 + a_2^2 a_3^2 - a_2 a_4^2 + 4a_2^2 a_6 - a_3^2 a_4 - 3a_4 a_6) X_1 Z_1 Z_2^2$$
$${}^2_1 a_2 a_6 - a_1 a_2 a_3 a_4 + 3a_1 a_3 a_6 + a_2^2 a_3^2 - a_2 a_4^2$$
$${}^2_2 a_6 - 2a_3^2 a_4 - 3a_4 a_6) X_2 Z_1^2 Z_2$$
$${}^3_1 a_3 a_6 - a_1^2 a_3^2 a_4 + a_1^2 a_4 a_6 + a_1 a_2 a_3^3$$
$${}_1 a_2 a_3 a_6 - 2a_1 a_3 a_4^2 + a_2 a_3^2 a_4$$
$${}_2 a_4 a_6 - a_3^4 - 6a_3^2 a_6 - a_4^3 - 9a_6^2) Z_1^2 Z_2^2,$$
$${}_2(X_1 Y_2 + X_2 Y_1) + Y_1 Y_2 (Y_1 Z_2 + Y_2 Z_1) + 3a_1 X_1^2 X_2^2$$
$$2X_1 Y_2 + Y_1 X_2) Y_1 Z_2 + a_1^2 X_1 Z_2 (2X_2 Y_1 + X_1 Y_2)$$
$$X_1 X_2 (Y_1 Z_2 + Y_2 Z_1)$$
$$X_1 Y_2 + X_2 Y_1)(X_1 Z_2 + X_2 Z_1)$$
$$X_1^2 X_2 Z_2 + a_1 a_2 X_1 X_2 (2X_1 Z_2 + X_2 Z_1)$$
$${}_3 X_1 X_2^2 Z_1 + a_3 Y_1 Z_2 (Y_1 Z_2 + 2Y_2 Z_1)$$
$${}_1 a_3 X_1 Z_2 (Y_1 Z_2 + Y_2 Z_1)$$
$${}_1 a_3 X_2 Y_1 Z_1 Z_2 + a_4 (X_1 Y_2 + X_2 Y_1) Z_1 Z_2$$
$$(X_1 Z_2 + X_2 Z_1)(Y_1 Z_2 + Y_2 Z_1)$$
$${}^2_1 a_3 + a_1 a_4) X_1 Z_2 (X_1 Z_2 + 2X_2 Z_1) + a_2 a_3 X_2 Z_1 (2X_1 Z_2 + X_2 Z_1)$$
$$Y_1 Z_1 Z_2^2 + (a_3^2 + 3a_6)(Y_1 Z_2 + Y_2 Z_1) Z_1 Z_2$$
$$a_3^2 (2X_1 Z_2 + X_2 Z_1) Z_1 Z_2 + 3a_1 a_6 X_1 Z_1 Z_2^2$$
$$a_4 (X_1 Z_2 + 2X_2 Z_1) Z_1 Z_2 + (a_3^3 + 3a_3 a_6) Z_1^2 Z_2^2.$$

1987 Lenstra: Use Lange–Ruppert complete system of addition laws to computationally define group $E(R)$ for more general rings R—rings with trivial class group.

Define $\mathbf{P}^2(R) = \{(X : Y : Z) : X, Y, Z \in R;\ XR + YR + ZR = R\}$ where $(X : Y : Z)$ is the module $\{(\lambda X, \lambda Y, \lambda Z) : \lambda \in R\}$.

Define $E(R) = \{(X : Y : Z) \in \mathbf{P}^2(R) : Y^2 Z = X^3 + a_4 X Z^2 + a_6 Z^3\}$.

To defin

$(X_1 : Y_1$

Consider

Lange–R

$(X'_3 : Y'_3$

Add thes

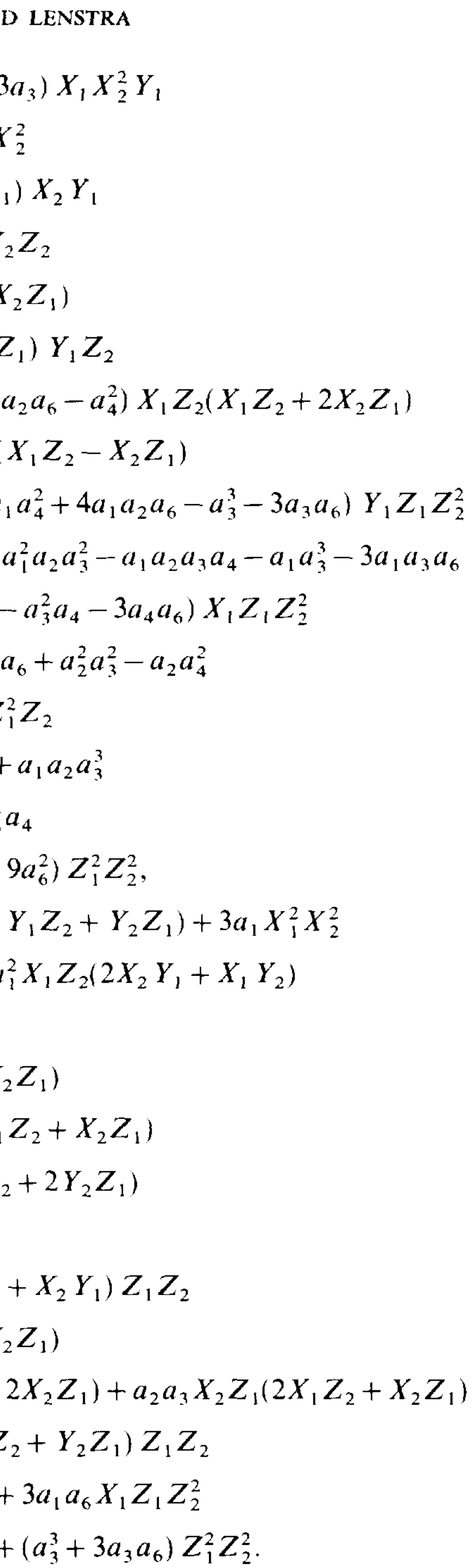
$\{\quad (\lambda X_3$

$+ (\lambda' X$

$+ (\lambda'' X$

Express

using tri



$3a_3)\ X_1 X_2^2 Y_1$

Y_2^2

$_1)\ X_2 Y_1$

$_2 Z_2$

$X_2 Z_1)$

$Z_1)\ Y_1 Z_2$

$a_2 a_6 - a_4^2)\ X_1 Z_2 (X_1 Z_2 + 2X_2 Z_1)$

$(X_1 Z_2 - X_2 Z_1)$

$_1 a_4^2 + 4a_1 a_2 a_6 - a_3^3 - 3a_3 a_6)\ Y_1 Z_1 Z_2^2$

$a_1^2 a_2 a_3^2 - a_1 a_2 a_3 a_4 - a_1 a_3^3 - 3a_1 a_3 a_6$

$- a_3^2 a_4 - 3a_4 a_6)\ X_1 Z_1 Z_2^2$

$a_6 + a_2^2 a_3^2 - a_2 a_4^2$

$_1^2 Z_2$

$+ a_1 a_2 a_3^3$

a_4

$9a_6^2)\ Z_1^2 Z_2^2,$

$Y_1 Z_2 + Y_2 Z_1) + 3a_1 X_1^2 X_2^2$

$_1^2 X_1 Z_2 (2X_2 Y_1 + X_1 Y_2)$

$_2 Z_1)$

$Z_2 + X_2 Z_1)$

$_2 + 2Y_2 Z_1)$

$+ X_2 Y_1)\ Z_1 Z_2$

$_2 Z_1)$

$2X_2 Z_1) + a_2 a_3 X_2 Z_1 (2X_1 Z_2 + X_2 Z_1)$

$Z_2 + Y_2 Z_1)\ Z_1 Z_2$

$+ 3a_1 a_6 X_1 Z_1 Z_2^2$

$+ (a_3^3 + 3a_3 a_6)\ Z_1^2 Z_2^2.$

1987 Lenstra: Use Lange–Ruppert complete system of addition laws to computationally define group $E(R)$ for more general rings R—rings with trivial class group.

Define $\mathbf{P}^2(R) = \{(X : Y : Z) : X, Y, Z \in R;\ XR + YR + ZR = R\}$ where $(X : Y : Z)$ is the module $\{(\lambda X, \lambda Y, \lambda Z) : \lambda \in R\}$.

Define $E(R) = \{(X : Y : Z) \in \mathbf{P}^2(R) : Y^2 Z = X^3 + a_4 X Z^2 + a_6 Z^3\}$.

To define (and co

$(X_1 : Y_1 : Z_1) + ($

Consider (and com

Lange–Ruppert $(X$

$(X'_3 : Y'_3 : Z'_3)$, $(X$

Add these R-modu

$\{ \quad (\lambda X_3, \lambda Y_3, \lambda Z_3$

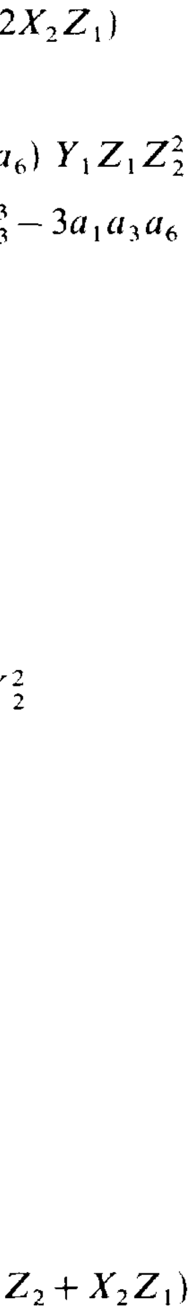
$+ (\lambda' X'_3, \lambda' Y'_3, \lambda'$

$+ (\lambda'' X''_3, \lambda'' Y''_3,$

λ, λ

Express as $(X : Y$

using trivial class



$2X_2Z_1)$

$a_6)\ Y_1Z_1Z_2^2$

$^3_3 - 3a_1a_3a_6$

$^2_2$

$Z_2 + X_2Z_1)$

1987 Lenstra: Use Lange–Ruppert complete system of addition laws to computationally define group $E(R)$ for more general rings R—rings with trivial class group.

Define $\mathbf{P}^2(R) = \{(X : Y : Z) :$ $X, Y, Z \in R;\ XR + YR + ZR = R\}$ where $(X : Y : Z)$ is the module $\{(\lambda X, \lambda Y, \lambda Z) : \lambda \in R\}$.

Define $E(R) =$ $\{(X : Y : Z) \in \mathbf{P}^2(R) :$ $Y^2Z = X^3 + a_4XZ^2 + a_6Z^3\}$.

To define (and compute) su

$(X_1 : Y_1 : Z_1) + (X_2 : Y_2 : Z$

Consider (and compute)

Lange–Ruppert $(X_3 : Y_3 : Z$

$(X_3' : Y_3' : Z_3')$, $(X_3'' : Y_3'' : Z$

Add these R-modules:

$\{\ \ (\lambda X_3, \lambda Y_3, \lambda Z_3)$

$+ (\lambda' X_3', \lambda' Y_3', \lambda' Z_3')$

$+ (\lambda'' X_3'', \lambda'' Y_3'', \lambda'' Z_3'') :$

$\lambda, \lambda', \lambda'' \in R$

Express as $(X : Y : Z)$,

using trivial class group of R

1987 Lenstra: Use Lange–Ruppert complete system of addition laws to computationally define group $E(R)$ for more general rings R— rings with trivial class group.

Define $\mathbf{P}^2(R) = \{(X : Y : Z) : X, Y, Z \in R;\ XR+YR+ZR = R\}$ where $(X : Y : Z)$ is the module $\{(\lambda X, \lambda Y, \lambda Z) : \lambda \in R\}$.

Define $E(R) = \{(X : Y : Z) \in \mathbf{P}^2(R) : Y^2Z = X^3 + a_4XZ^2 + a_6Z^3\}$.

To define (and compute) sum $(X_1 : Y_1 : Z_1) + (X_2 : Y_2 : Z_2)$:

Consider (and compute) Lange–Ruppert $(X_3 : Y_3 : Z_3)$, $(X_3' : Y_3' : Z_3')$, $(X_3'' : Y_3'' : Z_3'')$.

Add these R-modules:

$$\begin{aligned}\{\quad &(\lambda X_3, \lambda Y_3, \lambda Z_3)\\ &+ (\lambda' X_3', \lambda' Y_3', \lambda' Z_3')\\ &+ (\lambda'' X_3'', \lambda'' Y_3'', \lambda'' Z_3'') :\\ &\qquad\qquad \lambda, \lambda', \lambda'' \in R\}.\end{aligned}$$

Express as $(X : Y : Z)$, using trivial class group of R.