

University of Groningen

Weil pairing and the Drinfeld modular curve

van der Heiden, Gerrit

IMPORTANT NOTE: You are advised to consult the publisher's version (publisher's PDF) if you wish to cite from it. Please check the document version below.

Document Version

Publisher's PDF, also known as Version of record

Publication date:

2003

[Link to publication in University of Groningen/UMCG research database](#)

Citation for published version (APA):

van der Heiden, G. (2003). Weil pairing and the Drinfeld modular curve Groningen: s.n.

Copyright

Other than for strictly personal use, it is not permitted to download or to forward/distribute the text or part of it without the consent of the author(s) and/or copyright holder(s), unless the work is under an open content license (like Creative Commons).

Take-down policy

If you believe that this document breaches copyright please contact us providing details, and we will remove access to the work immediately and investigate your claim.

Downloaded from the University of Groningen/UMCG research database (Pure): <http://www.rug.nl/research/portal>. For technical reasons the number of authors shown on this cover page is limited to 10 maximum.

WEIL PAIRING AND THE DRINFELD MODULAR CURVE

GERT-JAN VAN DER HEIDEN

RIJKSUNIVERSITEIT GRONINGEN

WEIL PAIRING AND THE
DRINFELD MODULAR CURVE

PROEFSCHRIFT

ter verkrijging van het doctoraat in de
Wiskunde en Natuurwetenschappen
aan de Rijksuniversiteit Groningen
op gezag van de
Rector Magnificus, dr. F. Zwarts,
in het openbaar te verdedigen op
vrijdag 31 oktober 2003
om 16.00 uur

door

GERRIT JAN VAN DER HEIDEN

geboren op 6 mei 1976
te Elburg

Promotor: Prof. dr. M. van der Put

Co-promotor: Dr. J. Top

Beoordelingscommissie: Prof. dr. G. Böckle
Prof. dr. S.J. Edixhoven
Prof. dr. J. Van Geel

Contents

1	Introduction	1
1.1	Elliptic curves	4
1.1.1	The Weil pairing	4
1.1.2	The moduli problem for elliptic curves	8
1.1.3	Cusps and the Tate elliptic curve	11
1.2	Drinfeld modules	14
1.2.1	Definition of a Drinfeld module over a field	14
1.2.2	The analytic construction	16
1.2.3	Kronecker's Jugendtraum	16
1.2.4	The Weil pairing	18
1.2.5	The analytic moduli problem	19
1.2.6	The Weil pairing and the Drinfeld modular curve	21
1.2.7	The Tate-Drinfeld module and the cusps	22
1.3	Outline of this thesis	23
2	Factoring Polynomials using Drinfeld Modules	27
2.1	Introduction	27
2.2	Drinfeld modules	27
2.2.1	Drinfeld modules acting on A/NA	28
2.3	The algorithm	30
2.4	Complexity analysis	32
3	Local-Global Problem for Drinfeld Modules	35
3.1	Introduction	35
3.2	The Drinfeld module case	35
3.2.1	The group $S(a, K)$	36
3.2.2	The group $H^1(G, E[a](K_0))$	39
3.2.3	The rank 2 case.	39
3.3	Examples of non-trivial $S(a, K)$	46
3.4	The elliptic curve case	49
4	Weil Pairing for Drinfeld Modules	53
4.1	Introduction	53
4.2	Abelian A -modules and A -motives	55
4.3	Pure A -motives	60
4.3.1	Newton polygons	61

4.3.2	Purity with Newton polygons	66
4.3.3	Purity with lattices	66
4.4	The \mathfrak{a} -torsion of an abelian A -module	73
4.5	Construction of the Weil pairing.	75
4.5.1	Properties of the Weil pairing	77
4.6	Extension to inverse and direct limits	78
4.7	The case $A = \mathbb{F}_q[t]$	80
4.7.1	An explicit example for $r = 2$	80
5	Weil Pairing and the Drinfeld Modular Curve	83
5.1	Introduction	83
5.2	Drinfeld modules over schemes	84
5.2.1	Line bundles and morphisms	85
5.2.2	Drinfeld modules over a scheme	85
5.2.3	Level structures	86
5.3	The moduli problem	87
5.3.1	Actions on $M^r(\mathfrak{n})$	88
5.3.2	Assumptions in this chapter	90
5.4	The Weil pairing on the modular schemes.	91
5.5	Drinfeld modules of rank 2 with stable reduction of rank 1	94
5.5.1	Drinfeld's bijection without level structure	95
5.5.2	The bijection with level f -structure	96
5.6	Tate-Drinfeld modules	100
5.6.1	The construction of the lattice	100
5.7	The universal Tate-Drinfeld module	105
5.7.1	The universal property of \mathcal{Z}	109
5.8	The compactification of $M^2(f)$	111
5.8.1	The morphism j_a	111
5.8.2	The compactification	112
5.8.3	The scheme of cusps	113
5.9	The cusps and the Tate-Drinfeld module	114
5.9.1	The proof of Proposition 5.9.1	115
5.10	Components of $M^2(f)$	118
5.10.1	The analogue of $X_0(N)$	119
6	Drinfeld Data on the Compactified Modular Scheme	121
6.1	Introduction	121
6.1.1	Notations and results from the previous chapter	122
6.1.2	The choice of a representative of $(\varphi^{\text{td}}, \lambda^{\text{td}})$	123
6.2	Extending the universal Drinfeld module	123
6.3	Minimal models and Néron models	125
6.3.1	Definition of a model	125
6.3.2	Mumford's paper	127
6.3.3	Construction of a minimal model	129
6.3.4	The Néron model	132
6.4	Group structure and A -action on M^*	133

6.5 Drinfeld data on the compactification	134
Bibliography	137
Samenvatting	141
Dankwoord	145

