ISSN 1000-9825, CODEN RUXUEW
Journal of Software, Vol.18, No.7, July 2007, pp.1774−1777
DOI: 10.1360/jos181774

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel/Fax: +86-10-62562563

构造有限域上具有给定阶点的椭圆曲线*

王鲲鹏+, 李 宝

(中国科学院 研究生院 信息安全国家重点实验室,北京 100049)

Construction of Elliptic Curves over Finite Fields with a Point of Given Order

WANG Kun-Peng+, LI Bao

(State Key Laboratory of Information Security, Graduate University, The Chinese Academy of Sciences, Beijing 100049, China)

+ Corresponding author: Phn: +86-10-88256069, Fax: +86-10-88258713, E-mail: kunpengwang@263.net, http://home.is.ac.cn

Wang KP, Li B. Construction of elliptic curves over finite fields with a point of given order. *Journal of Software*, 2007,18(7):1774−1777. http://www.jos.org.cn/1000-9825/18/1774.htm

Abstract: The elliptic curves over a finite field with q elements are constructed. Let l be a prime, it is proved in this paper that if the equation $U^2-D(x)V^2=\varepsilon(x-a)^l$ defined over $GF(q)[x]$ has a primitive solution over $GF(q)[x]$, where $D(x)\in GF(q)[x]$ is a monic squarefree degree three polynomial, then the elliptic curve $y^2=D(x)$ has a point (a,b) with order l. This result provides an algorithm on constructing elliptic curves with a point of the prescribed order.
Key words: elliptic curve; quadratic function field; public cryptography; Diophantian equation

摘 要: 考虑有限域上椭圆曲线的构造.设 q 是一个奇素数的方幂,l 是一个素数.证明了,如果 $GF(q)[x]$上的方程 $U^2-D(x)V^2=\varepsilon(x-a)^l$ 有本原解,其中,$D(x)\in GF(q)[x]$是一个首 1 三次无平方因子的多项式,则椭圆曲线 $y^2=D(x)$上的点(a,b)的阶是 l.由此,给出了一种构造具有给定阶点的椭圆曲线的算法.
关键词: 椭圆曲线;二次函数域;公钥密码;不定方程
中图法分类号: TP309 文献标识码: A

椭圆曲线密码体制是基于椭圆曲线离散对数问题的公钥密码体制.椭圆曲线密码体制最早于 1985 年由 Miller 和 Koblitz 分别提出.由于这种公钥密码体制在速度和密钥长度上具有明显的优越性,所以,近年来受到人们广泛的关注.人们对这种密码体制做了大量的研究,其中,关于它的实现研究是一个重点内容.

为了实现椭圆曲线密码体制,人们首先要找到一条椭圆曲线 E,使得它上面的点的个数足够多,然后再在上面找到一个阶数足够大的点 $P\in E$ 作为生成元,构造一个 Diffi-Hellman 密码体系.本文将从一个关于多项式变量的不定方程出发,给出构造具有给定素数阶点的椭圆曲线的算法.

1 主要结果叙述

设 q 是一个奇素数的方幂,$GF(q)$是具有 q 个元素的有限域,$R=GF(q)[x]$是 $GF(q)$上未定元 x 的多项式环.

* Supported by the National Natural Science Foundation of China under Grant No.60673073 (国家自然科学基金); the National High-Tech Research and Development Plan of China under Grant No.2006AA01Z427 (国家高技术研究发展计划(863)); the Presidential Foundation of Graduate University of the Chinese Academy of Sciences under Grant No.Y1039 (中国科学院研究生院院长基金)

Received 2005-06-13; Accepted 2006-04-26

$GF(q)$上的椭圆曲线 E 是符合方程 $y^2=D(x)$的 $GF(q)^2$ 上的点全体再添加上一个无穷远点 O 构成的射影曲线,其中,$D(x)$是一个 $GF(q)$上的首 1 三次无平方因子多项式.椭圆曲线上的点对于用弦切律定义的加法构成一个 Abel 群,叫作 Mordell-Weil 群,这个群的单位元就是无穷远点 O.

多项式环 $R=GF(q)[x]$的分式域 $k=GF(q)(x)$称为有理函数域.如果 $D(x)$是一个如前所述的多项式,则 k 的二次扩域 $K=k(\alpha)$是一个虚二次代数函数域,其中$\alpha^2=D(x)$.易见 K 是椭圆曲线 E 的函数域,其 1 次素除子与 E 的 $GF(q)$有理点一一对应.R 在 K 中的整闭包称为 K 的整函数环,记为 O_K.O_K 中全体分式理想构成一个群 $I(D(x))$,叫做 K 的分式理想群;O_K 中全体主分式理想构成一个群 $P(D(x))$,叫做 K 的主分式理想子群.商群 $H(D(x))=I(D(x))/P(D(x))$称为 K 的理想类群.K 的理想类群的阶是一个正整数,称为 K 的理想类数,记为 $h(D(x))$.

我们知道:K 的理想类群同构于 K 的除子类群的一个商群,而 K 又是椭圆曲线 E 的函数域,因此,它的除子类群同构于 E 的 Mordell-Weil 群[1].这就告诉我们:如果我们有了一个理想类群中含有给定阶元的虚二次代数函数域 $K=k(\alpha)$,其中,$D(x)$是一个无平方因子的三次多项式,且$\alpha^2=D(x)$,则我们就可以找到一条椭圆曲线,使得它的一个点具有给定的阶.文献[2]给出了二次代数函数域的理想类群含有给定阶元的一个充分必要条件.借助这个条件,我们给出以下定理:

定理 **1**. 设 $D(x)$是 $GF(q)[x]$中的一个三次首 1 无平方因子多项式,$a\in GF(q)^{\times}$,l 是一个素数.如果关于未知量 U,V 的不定方程

$$U^2-D(x)V^2=(x-a)^l$$

在 $GF(q)[x]$上有本原解,即有多项式 $U(x),V(x)\in GF(q)[x]$,符合$(U(x),V(x))=1$,使得

$$U(x)^2-D(x)V(x)^2=(x-a)^l,$$

则 $GF(q)$上椭圆曲线 $E:y^2=D(x)$上有一个 l 阶点 $P=(a,b)$,其中,b 是 $GF(q)$中一个符合方程 $b^2=D(a)$的数.

从这个定理出发,我们就可以给出一个构造 $GF(q)$上具有 l 阶点的椭圆曲线的以下算法,而且,此算法还可以具体给出这个 l 阶点.算法描述中的符合 $A\leftarrow_R B$ 表示由集合 B 中随机取一个元素赋值于变量 A;$A\leftarrow b$ 表示把表达式 b 的值赋给变量 A.

算法 **1**. 第 1 步:$a\leftarrow_R GF(q)^{\times}$;

第 2 步:$U(x)\leftarrow_R GF(q)[x]$;

第 3 步:$V_m(x)\leftarrow U(x)^2-(x-a)^l$;

第 4 步:作分解 $V_m(x)=V(x)^2D(x)$;

第 5 步:(1) 如果 $D(x)$是一个三次无平方因子的多项式,则返回曲线$y^2=D(x)$以及曲线上的点(a,b)(其中,$b^2=D(a)$)并停止;

(2) 不然,从第 1 步再重新开始.

2 定理 1 的证明

由定理的条件,$D(x)$是一个首 1 三次无平方因子的多项式,则在 k 上添加 $D(x)$的平方根α得到的域 $K=k(\alpha)$是一个虚二次代数函数域.由于 k 的无穷除子$\infty=(1/T)$在 K 中完全分歧,故而 K 又称为是分歧虚二次代数函数域,易见 k 的常数域 $GF(q)$在 K 中的扩张还是 $GF(q)$.由于 $a\in GF(q)^{\times}$,因此,$x-a$ 是 $GF(q)[x]$中的一个一次不可约多项式,即 $p=\langle x-a\rangle$是 O_K 中的一个一次素理想,而 p 所决定的 k 的素除子是一个一次素除子.设 l 是一个素数,如果方程

$$U^2-V^2D(x)=(x-a)^l$$

在 $GF(q)[x]$中有解,即有多项式 $U(x),V(x)\in GF(q)[x]$,使得

$$U(x)^2-V(x)^2D(x)=(x-a)^l \tag{1}$$

首先一点我们知道,存在 $GF(q)^{\times}$中的一个元素 b,使得

$$D(x)\equiv b^2(\mathrm{mod}\ x-a) \tag{2}$$

于是,K 的极小多项式 $f(X)=X^2-D(x)$满足

$$f(X)=X^2-D(x)\equiv X^2-b^2\equiv(X-b)(X+b)(\mathrm{mod}\ x-a).$$

又因为 q 是奇数,故而

$$(X-b)\neq(X+b)(\mathrm{mod}\ x-a).$$

由 Kummer 定理[3]可知,p 在 K 中分裂成两个互素的素理想的积:

$$p=P\cdot P^*;$$

其中:$P=\langle x-a,b+\alpha\rangle$,$P^*=\langle x-a,b-\alpha\rangle$.把式(1)写成理想等式就有,

$$(U(x)+\alpha V(x))(U(x)-\alpha V(x))=P^l\cdot P^{*l}.$$

由于 $U(x)+\alpha V(x)$和 $U(x)-\alpha V(x)$互素,故而 $P^l=\langle U(x)+V(x)\alpha\rangle$或者 $P^l=\langle U(x)+V(x)\alpha\rangle$.不妨设,

$$P^l=\langle U(x)+V(x)\alpha\rangle \tag{3}$$

则 $P^{*l}=\langle U(x)-V(x)\alpha\rangle$.把式(3)写成理想类的等式(其中,$A$ 所在的理想类记为$[A]$),就有

$$[P^l]=[\langle U(x)+V(x)\alpha\rangle]=[1].$$

如果我们能证明 P 不是一个主理想,则我们就知道了$[P]$是一个阶为 l 的理想类.下面我们就来证明这一点.

我们断言 P 不是一个主理想,否则就有 $A(x),B(x)\in GF(q)[x]$,使得 $P=\langle A(x)+B(x)\alpha\rangle$,两边取范就有 k 中理想的等式:$\langle x-a\rangle=\langle A(x)^2-B(x)^2\alpha\rangle$.写成 k 中元素的等式就有 $c(x-a)=A(x)^2-B(x)^2\alpha$,其中,$c$ 是 k 中单位,即 $c\in GF(q)^\times$.这个等式显然不能成立,因此矛盾.也就是说,P 不是主理想,即$[P]$是一个阶为 l 的理想类.在证明的过程中可见,P 是一个一次素理想.以上内容可参见文献[2].

下面我们来看一下 K 的理想类群和除子类群的关系.令 D 是 K 的所有素除子为基作成的自由 Abel 群,也即 K 的除子群.其每个元素可以表示为

$$A=\Sigma_P P^{n(P)}(\text{其中},n(P)\text{是整数}),$$

称为 K 的一个除子.而除子的次数定义为 $degA=\Sigma_P n(P)$.

用 $D^0(K)$表示 K 的全体 0 次除子构成的子群,$D_\infty(K)$表示 K 的全体无穷除子构成的子群.进而对于每个元素 $f\in K^\times$可以定义一个除子:

$$div(f)=\Pi_P P^{v(P,f)},$$

称为由 f 定义的主除子,其中,$v(P,f)$表示 f 在 P 处的赋值.

设有集合 $A\subset K$,用 $div(A)$表示集合$\{div(f)|f\in A\}$.令 $D_\infty^0(K)=D_\infty(K)\cap D^0(K)$,$U_K$ 是 K 的单位群.

$C^0(K)=D^0(K)/div(K)$是 K 的 0 次除子类群,$H(D(x))$是 K 的理想类群,作用在 0 次除子类群上的映射 ψ的作用是去掉无穷部分,则有正合列[4]:

$$0\to D^0(K)/div(U_K)\to C^0(K)\to_\psi H(D(x))\to 0.$$

在虚二次代数函数域中有 $D_\infty^0(K)=\{0\}$,$div(U_K)=\{div(f)|f\in GF(q)^\times\}=\{0\}$.因此,$C^0(K)\cong H(D(x))$.即在 ψ的作用之下,有 $\psi^{-1}([p])=(p)-\infty$.于是我们知道:除子$(p)-\infty$所在的除子类的阶是 l,而且$(p)$是一个一次除子.

下面再看一下 K 的除子类与曲线 $E:y^2=D(x)$的除子类之间的关系[5],构造映射,

$$\psi:D(K)\to D(E),$$

$$\infty\mapsto(O),$$

$$P\mapsto(a_1,b_1)+(a_2,b_2)+\ldots+(a_n,b_n),$$

其中:$n=degP$;$PO_K=P_1\ldots P_n$;$P_i=(x-a_i,b_i+\alpha)$,则 ψ诱导了一个群同构,

$$\psi^+:D^0(K)\to Pic^0(E).$$

于是,$\psi([p]-\infty)=(a,b)-(O)$是一个 l 阶元.

最后,我们看一下 E 的除子类群和 E 的 Mordell-Weil 群之间的关系.椭圆曲线的群结构是由

$$\sigma:Pic^0(E)\to E,$$

$$(P)-(O)\mapsto P$$

诱导的[2],因此,$P=(a,b)$是一个 l 阶点.

3 结 论

本文给出的算法把构造具有特定性质的椭圆曲线归结为寻找符合特定性质的不定方程,转化了问题的难度.但是,这种算法目前只是在理论上给出了构造椭圆曲线的一个途径,其效率等内容还有待于进一步研究.尤其是算法的第 4 步,涉及到有限域上多项式的分解,计算量必然很大.如何改进这一算法,是我们今后工作的方向.

近年来,构造椭圆曲线的方法是用椭圆曲线的复乘理论,把曲线提升到有理数域上,然后经过浮点运算计算出有理数域上的 j-不变量,再由有理数域上的 j-不变量构造有限域上的 j-不变量,从而构造出有限域上的椭圆曲线(见文献[6]及其后所附参考文献).这种方法计算比较有效,但缺点是我们无法事先确定有限域的特征,而且在算法中没有具体给出一个曲线上符合要求的点.而本文给出的算法却在这两点上都可以做到.

致谢 本文作者感谢审稿人提供的宝贵意见和建议.

References:

[1] Silverman JH. The Arithmetic of Elliptic Curves. Springer-Verlag, 1986.

[2] Wang KP. The arithmetic structure of quadratic algebraic function fields [Ph.D. Thesis]. Beijing: Tsinghua University, 2000 (in Chinese with English abstract).

[3] Zhang XK. Introduction to Algebraic Number Theory. Changsha: Hu'nan Education Press Hall, 1999 (in Chinese).

[4] Feng KQ. Cyclotomic Function Fields. Shanghai: Shanghai Science Technology Publishers, 1997 (in Chinese).

[5] Zhu YF, Ye DF, Pei DY. Public key cryptography based on imaginary quadratic function fields. Progress Nature Science, 1995,5(5):601−608 (in Chinese with English abstract).

[6] Freeman D. Constructing pairing-friendly elliptic curves with embedding degree 10. 2006. http://eprint.iacr.org/2006/026.pdf

附中文参考文献:

[2] 王鲲鹏.二次代数函数域的数论结构[博士学位论文].北京:清华大学,2000.

[3] 张贤科.代数数论导引.长沙:湖南教育出版社,1999.

[4] 冯克勤.分圆函数域.上海:上海科学技术出版社,1997.

[5] 祝跃飞,叶顶锋,裴定一.基于虚二次函数域的公钥密码.自然科学进展,1995,5(5):601−608.

王鲲鹏(1971－),男,河北尚义人,博士,副教授,主要研究领域为密码学.

李宝(1962－),男,博士,研究员,博士生导师,主要研究领域为密码学.