椭圆曲线点乘加速方法

1.坐标系转换避免求逆运算

2.三种点乘运算：二进制表示、NAF算法、wNAF算法

3.蒙哥马利算法对模乘进行优化，将取模运算中大量的试除操作转换为位移操作

手动增加求逆运算的时间来对比说明求逆运算的影响

三种标量乘的运算时间对比

蒙哥马利模乘的优化，对三种坐标下进行对比，标准射影坐标和Jacobian加重射影坐标的结果明显，而仿射坐标下甚至可能造成运算时间增加，原因是，在仿射坐标下进行点加运算会进行模逆运算而模逆运算的结果会改变参数蒙哥马利形式，会进行蒙哥马利表示，增加了取模运算。反射坐标下的模乘计算量相对较小，多次的位移运算反而会增加开销。

分析三种方法的优缺点和硬件实现难度

对运算量最小的仿射坐标进行verilog语言实现，并进行仿真测试

实际应用中Jacobian加重射影坐标对标准射影坐标更常用，雅可比坐标系在数学邻域有着更为重要的研究

A4AEC4C6C5BFC1C31B8588D2295156C4D0B73F5BF191B018A961762A9023EE67

二进制表示（仿射坐标）：

仿射坐标表示：

X坐标： 3D6A77AB4EFAC4D12994BE8CBB1557839DDBB86BAEBB55A1BB83CF7C6B6BD2E0

Y坐标： BD6386F2034E80DF78EB014768392F5CB06ED72DDC001CF2FD61A62B0C3B8E54

1

执行时间：15563

二进制表示（仿射坐标）(蒙哥马利优化）：

仿射坐标表示：

X坐标： -C2958853B1053B2ED66B417344EAA87C622447935144AA5F447C308394942D1F

Y坐标： -429C790CFCB17F208714FEB897C6D0A34F9128D123FFE30E029E59D4F3C471AB

1

执行时间：17500

二进制表示（标准射影坐标）：

标准射影坐标表示:

X坐标： 44EF578128C4BD366E3F2FCBB6C3894B9C66435B3D54A365C0F7E3BC4B654436

Y坐标： C233B766255F40F9DDA26A62BE3B92C7C7B95BDF8232139BD279E5A3FE37D9C3

Z坐标： 9F02BA0B5C88AB647B84A3C117DFE464932FC176A51CE7FC4C894EC5A01F5DAF

1

执行时间：15625

二进制表示（标准射影坐标）(蒙哥马利优化）：

标准射影坐标表示:

X坐标： -BB10A87DD73B42C991C0D034493C76B46399BCA3C2AB5C9B3F081C43B49ABBC9

Y坐标： -3DCC4898DAA0BF06225D959D41C46D383846A41F7DCDEC652D861A5C01C8263C

Z坐标： -60FD45F3A377549B847B5C3EE8201B9B6CD03E885AE31804B376B13A5FE0A250

1

执行时间：10766

二进制表示（Jacobian加重射影坐标）：

雅可比坐标表示:

X坐标： A3E5425A40983D9FA2E89BBB51A9D8EBF2995729A384BCEA0D9999855437EBCD

Y坐标： DF9890C151CF6D6C96D91F7A92E18F2AEAB6C36534C1D0DDE4A8489C2FDB36C

Z坐标： 6516991B0451DD281141DD1E03E4F2A076B757E67190FFFC0F651B51CEECB170

1

执行时间：18328

二进制表示（Jacobian加重射影坐标）(蒙哥马利优化）：

雅可比坐标表示:

X坐标： -E78B4A2B9157CA772668588E05B7C98385C5969BAB877B3A1D45ECD5FEA96B3E

Y坐标： -AF7FDDBFC2D32A224BFDC6884AE074C38E4E534E8CFD1D57EE22BEB37ADE2733

Z坐标： -68C199D8F88C4F51141BF1A78AD7A5F32A3D9E6B606DAF54A45A41EAD124A9A0

0

执行时间：13922

NAF表示（仿射坐标）：

仿射坐标表示：

X坐标： 3D6A77AB4EFAC4D12994BE8CBB1557839DDBB86BAEBB55A1BB83CF7C6B6BD2E0

Y坐标： BD6386F2034E80DF78EB014768392F5CB06ED72DDC001CF2FD61A62B0C3B8E54

1

执行时间：13875

NAF表示（仿射坐标）(蒙哥马利优化）：

仿射坐标表示：

X坐标： -C2958853B1053B2ED66B417344EAA87C622447935144AA5F447C308394942D1F

Y坐标： -429C790CFCB17F208714FEB897C6D0A34F9128D123FFE30E029E59D4F3C471AB

1

执行时间：16593

NAF表示（标准射影坐标）：

标准射影坐标表示:

X坐标： 779B9B90C5352308628FA65CCF57BDD5EEBCA00F259173AA229F4F5B8E71801D

Y坐标： 62CE74B4A0D832033ECB72FBF46CE865452326F33DA121B45F0A10B821D9BCA7

Z坐标： 37ECAB83786B11B29360497A1C14C2227EA07B0A484DEE9A13EC56A6E2D85E8C

1

执行时间：13563

NAF表示（标准射影坐标）(蒙哥马利优化）：

标准射影坐标表示:

X坐标： -49A33B5D001461FA5C82B182A3CA0866DFCF442E3BC3ED35C80B2FF2518B320A

Y坐标： -7FDDF3BE1E8B51C98628CDAEA9E25E18CEDDF8EAA8FD16AA6EF3B3D300129BE9

Z坐标： -51D009092583608FDBF4F87130C746DCDF20A9DEB3AC8BB553FE81FC93BCE26C

1

执行时间：9765

NAF表示（Jacobian加重射影坐标）：

雅可比坐标表示:

X坐标： BCCAFD5BF18D68C974C264EAE18D898937CF33031F275AD0C71BBF5E7D349FEE

Y坐标： A54F0752EB2EB44B78415500B54E66F7CEB0D32E5CEE22B2E581D52DCE0B6143

Z坐标： 3F66287569E5397BA4D8C876471D5BEF1494B4AE19C1A7E9FF760ED466970E3A

1

执行时间：14375

NAF表示（Jacobian加重射影坐标）（蒙哥马利优化）：

雅可比坐标表示:

X坐标： -9CD7C1209FC36D2CCCDB6B4081A8B375CB90445BE5ED7037A02000E1AA14EBE1

Y坐标： -EED75B50644EB065A4120FC327FC5BBFAA5FBE5EBB05AF7B6A58EBE4E611C772

Z坐标： -C69DA48B1EF141D67904925087D7017584F84869678C81C0C1425C84B45A8A55

1

执行时间：11079

wNAF表示（仿射坐标）：

计算预计算表的执行时间：4421

仿射坐标表示：

X坐标： 3D6A77AB4EFAC4D12994BE8CBB1557839DDBB86BAEBB55A1BB83CF7C6B6BD2E0

Y坐标： BD6386F2034E80DF78EB014768392F5CB06ED72DDC001CF2FD61A62B0C3B8E54

1

执行时间：15828

wNAF表示（仿射坐标）(蒙哥马利优化）：

计算预计算表的执行时间：5656

仿射坐标表示：

X坐标： -2D1D6B8F4DD0527D023ECAC1BC98E0EC5019D3AD44F37724378B3D92ED5D8CE

Y坐标： -71F444012A988569817C40540616B4BC9111B45ED06B7C8B2420614CEBE97075

1

执行时间：18859

wNAF表示（标准射影坐标）：

计算预计算表的执行时间：5453

标准射影坐标表示:

X坐标： ECDEA96EF05933F053F97CA1AB4B4924812676A73AE696F62BCAB9F4AA46A97B

Y坐标： 4754EC37ED686A43ED6B037C64D7E34B8E07EDD17B049270818F964B7560A845

Z坐标： E85DBB6468DF3099714FE0D119BB5C30DA84A83CD0C07118CD5896D46523E8F8

1

执行时间：17016

wNAF表示（标准射影坐标）(蒙哥马利优化）：

计算预计算表的执行时间：3422

标准射影坐标表示:

X坐标： -E3A5E48B4B4182B336CC67544165A4628076C8AD269F07C4EB318801C7CD6166

Y坐标： -249C233CABE05E7F3C40F760AAC1AE3561B5AA0CEAD186912E356D941576887C

Z坐标： -1368EA5891164B32FBAE6FC4943B720E17C51FDF3358F7FA8A37700B904B4843

1

执行时间：11672

wNAF表示（Jacobian加重射影坐标）：

计算预计算表的执行时间：8031

1

雅可比坐标表示:

X坐标： 95FFDB1B4E93FD6AB623B6DD79D0F474859766086F7258494EC79AE7DB6DC853

Y坐标： 50B5983DF35908B6BF38675B8DDE7FB2845D88BFE3CB2D0F69F3B1D98653CB2B

Z坐标： 7FECF4D1E1CA78EFE82F71199CC55575E3E4AFD17352533CA6DFE7D43E20F253

执行时间：20187

wNAF表示（Jacobian加重射影坐标）：

计算预计算表的执行时间：5578

1

雅可比坐标表示:

X坐标： -9B051A53931EFEA13B53446C646F354F7F9E90A2E40277473E6C2F501CD24BAE

Y坐标： -57BCDD9BE63511F19DA8EFC7E361136AF615E8C76B2ED8E8B0FDCDB66A908F93

Z坐标： -35580695F3CA1A0FC9D4B7BB7DFD7C72594945A4CB96CD466CB6C646491F5662

执行时间：14250

以上为测试内容。

C:\Users\86185\source\repos\wxw\_2\Project1\x64\Debug\Project1.exe (进程 27800)已退出，代码为 0。

要在调试停止时自动关闭控制台，请启用“工具”->“选项”->“调试”->“调试停止时自动关闭控制台”。

按任意键关闭此窗口. . .