

MA330 Lecture Notes

Date: Oct 3rd

Group 1:

Lane Murphy

Jack Gilbert

Dan King

D

$(a, b, 4)$ i.e. $a^2 - Db^2 = 4$

$\langle a, b, 4 \rangle * \langle a, b, 4 \rangle = a^2 + Db^2, 2ab, 16$

---- reduce, divide by 2

$\langle Db^2 + 2, ab, 4 \rangle$

$a^2 = Db^2 + 4$

$a^2 + Db^2 = 2Db^2 + 4$

If a or b is even

Then ab is even

$Db^2 + 2$ if b is odd and a is even then there is no further reduction

Case 1: $b = 2r$

$\langle 4Dr^2 + 2, 2ar, 4 \rangle \rightarrow \langle 2Dr^2 + 1, ar, 1 \rangle$

Case 2: b is odd

Calculate $\langle a, b, 4 \rangle * \langle Db^2 + 2, ab, 4 \rangle = \langle a(Db^2 + 2) + Dab^2, a^2b + Db^3 + 2b, 16 \rangle$

Remember $a^2 = Db^2 + 4$

$\langle 2Dab^2 + 2a, 2Db^3 + 4b, 16 \rangle$

----- reduce divide by 2

$\langle Dab^2 + a, Db^3 + 3b, 4 \rangle$ $b = 2r + 1$

$B(Db^2 + 3)$

$B(D + 1) \pmod 2$

Case 3: a is odd b is odd

Consider $a^2 = Db^2 + 4$

Look mod 4

$x = 0, 1, 2, 3$

$x^2 = 0, 1, 0, 1$

$a^2 = Db^2 \pmod 4$

Case 4: $b^2 = 0 \pmod 4$

$$A^2 = 0 \pmod{4}$$

So a, b are both even

If $b^2 = 1$ then $a^2 = 1$ is possible but then $D = 1 \pmod{4}$ on $a^2 = 0 \pmod{4}$ and $D = 0 \pmod{4}$