

Now  $l \equiv 3 \pmod{4}$ , so  $q_1(i)q_{-1}(i) = 4m_p(i) = 4(1 + i + \dots + i^l) = 4 \cdot ((1 + i - 1 - i) + (1 + i - 1 - i) + \dots + (1 + i - 1 - i)) = 4i$

So  $f(i)^2 - p^*g(i)^2 = f(i)^2 + pg(i)^2 = 4i$ , and so  $y_2^2(1+i^*)^2 + p\xi_2(1-i^*)^2 = 2y_2^2i^* - 2p\xi_2^2i^* = 4i$  or, dividing by  $2i^* = \pm 2i$ ,

$$y_2^2 - p\xi_2^2 = \pm 2$$

$$\Rightarrow (y_2 + \sqrt{p}\xi_2)^2(y_2 - \sqrt{p}\xi_2)^2 = 4$$

Now  $y_2, \xi_2$  are odd, else  $y_2^2 - p\xi_2^2 \equiv y_2^2 + \xi_2^2 \equiv 0 \not\equiv \pm 2 \pmod{4}$ . So the coefficients of  $(y_2 + \sqrt{p}\xi_2)^2 = (y_2^2 + p\xi_2^2) + 2y_2\xi_2\sqrt{p}$  are even. We can thus write  $a = \frac{(y_2^2 + p\xi_2^2)}{2}, b = y_2\xi_2 \in \mathbb{Z}$  and get

$$a^2 - pb^2 = \frac{(y_2 + \sqrt{p}\xi_2)^2(y_2 - \sqrt{p}\xi_2)^2}{2 \cdot 2} = \frac{4}{4} = 1$$

This solves the equation, where

$$(a, b) = \left( \frac{i^*}{4}(pg(i)^2 - f(i)^2), \frac{1}{2}g(i)f(i) \right)$$

where we can directly compute  $f(i)$  and  $g(i)$

To apply this method to the general case of Pell's Equation (where  $d$  is square-free but not necessarily prime), since  $d$  is square-free, it can be written as  $d = \prod_{k=1}^r p_k$  where the  $p_k$ 's are rational primes. So it suffices to study the case where  $d = pq$  for primes  $p$  and  $q$  and deduce the general case by induction. We will not describe said case in depth here since this paper mainly focuses on prime cyclotomic fields, but we remark that taking  $\mathbb{Q}(\zeta_{pq})$ ,  $m_{pq}(x) = m_p(x)m_q(x)\frac{(x^{pq}-1)/(x-1)}{((x^p-1)/(x-1))((x^q-1)/(x-q))} = \frac{(x^{pq}-1)(x-1)}{(x^p-1)(x^q-1)}$  which can be shown to be irreducible by a similar method as the simple proof for showing that  $\sum_{k=0}^{p-1} x^k$  is the minimal polynomial of  $\zeta_p$  in  $\mathbb{Z}[x]$ . Following the same reasoning as in the case where  $d = p$ , we can write  $4m_{pq}(x) = f(x)^2 \pm pqg(x)^2$  where  $f(x), g(x) \in \mathbb{Z}$ . The rest of the problem is solved in a similar fashion as well.

Using some interesting approximation methods and quadratic number fields, Ireland & Rosen [5] show that  $x^2 - dy^2 = 1$  has *infinitely many solutions* for any square-free integer