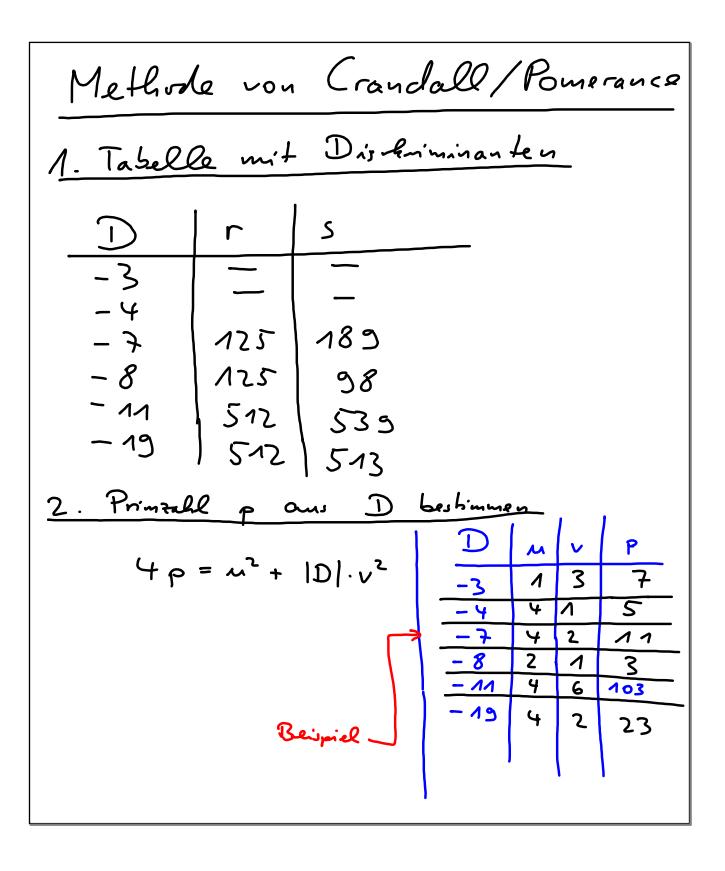
Prinktezahl für spezielle E Kurven mit CM = complex mult. man wählt eine Diskriminante \mathbb{D} ---> Pnuzahl p -> 2, 4 oder 6 Kurven E und 2, 4 oder 6 Punitzahlen/El Beispiel: (a1, b) (a, b,) |E,| |E^| bekannt { [E_1], [E]} -> Zuordnungsproblem dieses lösen mit der Eigenschaft $|E| \cdot P = O$



3. Quadrahischen Nichtnest g mod p finden
Bedenhug: es darf hein y geben mit
G² = g mod p
Kriterium: p-1
g² = -1 mod p
Fortfilmug der Beispeiels:
P=M,
$$\Lambda = 4, V = 2, D = -7$$

Quadmhischer Nichtvert, probiere $g = 2$
 $g^2 = 2^5 = 10 = -1 \mod 11$
 $\Rightarrow g = 2$ auswählen
Ergährung:
falls $D = -3$ darf g auch kein
kubischer Rest sein, d.h. g muss
 $g^2 = 1 \mod p$
erfüllen

4. mögliche Work für 1E1 in Beispiel P+1 + M P = M, M = 4p+1+m = 16p+1-m = 8p+1 - 1 5. Fallunterscheidung nach D $\frac{D=-3:}{y^2=x^3-g^k} \mod p, \frac{D\leq k\leq 5}{6 \ 4u - u = n}$ =) 4 weitere |E|-Werte $p+1 \pm (m \pm 3v)/2$ $\underline{\mathbf{D}} = -\mathbf{C} \mathbf{C} \mathbf{C}$ $y^2 \equiv x^3 - g \cdot x \mod p$, $O \leq k \leq 3$ 4 kurnon =) 2 weitere |E|-Werke P+1 ± 2v D & { -3, -4} benutie r, s and Tabelle (Schritt 1) y² = x³ - 3 - s³g² X + 2 - s⁵g² mod p für k € { 0, 1 }