Euclid's Extended Algorithm

Ex 1: Find gcd(a ,b), where a = 47831429 and b = 19847553.
Also find integers x and y with $xa + yb$ = gcd(a ,b).

i	$q[i]$	$r[i]$	$x[i]$	$y[i]$
-1	-	47831429	1	0
0	-	19847553	0	1
1	2	8136323	1	-2
2	2	3574907	-2	5
3	2	986509	5	-12
4	3	615380	-17	41
5	1	371129	22	-53
6	1	244251	-39	94
7	1	126878	61	-147
8	1	117373	-100	241
9	1	9505	161	-388
10	12	3313	-2032	4897
11	2	2879	4225	-10182
12	1	434	-6257	15079
13	6	275	41767	-100656
14	1	159	-48024	115735
15	1	116	89791	-216391
16	1	43	-137815	332126
17	2	30	365421	-880643
18	1	13	-503236	1212769
19	2	4	1371893	-3306181
20	3	**1**	**-4618915**	**11131312**
21	4	0		

The rows with i = –1 and i = 0 are filled in, as illustrated. The top two entries in the ***r* [*i*]** column are a and b .

The remaining rows are calculated using:

($q[i]$, $r[i]$) = quotient and remainder obtained by dividing $r[i-2]$ by $r[i-1]$.

($x[i]$, $y[i]$) = ($x[i-2]$, $y[i-2]$) – $q[i]$ * ($x[i-1]$, $y[i-1]$).

The calculation stops with the row in which $r[i]$ = 0. The $x[i]$ and $y[i]$ entries of this row are omitted. The last three entries in the previous row are gcd(a ,b), x , and y .

Thus $gcd(a,b) = 1$, and
$-4618915\,a + 11131312\,b = 1$.
In the integers modulo a , $b^{-1} = 11131312$.

Ex 2: Find gcd(a ,b), where a = 109395 and b = 34104.
Also find integers x and y with $xa + yb$ = gcd(a ,b).

i	$q[i]$	$r[i]$	$x[i]$	$y[i]$
-1	-	109395	1	0
0	-	34104	0	1
1	3	7083	1	-3
2	4	5772	-4	13
3	1	1311	5	-16
4	4	528	-24	77
5	2	255	53	-170
6	2	18	-130	417
7	14	**3**	**-1873**	**6008**
8	6	0		

Thus gcd(a ,b) = 3, and $-1873\ a + 6008\ b = 3$.